Phrack RU issue 026

Русская версия Phrack, выпуск 026. Полный текст статей с кодом и таблицами.

Темы выпуска: Unix/Linux, BSD, Windows NT и администрирование систем; сети, маршрутизация, TCP/IP, Cisco, телефония и телеком-инфраструктура; культура Phrack, новости сцены, loopback, prophile и хакерские манифесты.

Материалы выпуска: Содержание:; Компьютерные системы в операциях Bell System; Поимка с поличным — Правовые процедуры; NSFnet: Национальная сеть Фонда науки; COSMOS — Компьютерная система для работы с мэйнфреймами. Часть первая; Основные концепции трансляции; Прослушка телефонов: подпольная индустрия телекоммуникаций; Future Transcendent Saga, Приложение III: «От Лимба до бесконечности» — Домены интернета; Phrack World News; «Протяни руку и прослушай кого-нибудь» — April 3, 1989; Galactic Hacker Party (вечеринка галактических хакеров) — 30 марта 1989.

Содержание:

Автор: Taran King и Knight Lightning

25 апреля 1989 года

Приветствуем и добро пожаловать в 26-й выпуск Phrack Inc. Страсти накаляются по мере того, как стремительно приближается SummerCon '89. Обязательно загляните в Phrack World News за подробной информацией об этом замечательном событии. Пропустить его никак нельзя.

В этом выпуске Disk Jockey представляет собственное изложение событий, которые могут произойти в ходе уголовного судопроизводства (в конце концов, ему это известно не понаслышке). Некоторые термины и ситуации могут различаться от штата к штату в силу незначительных различий в законодательстве отдельных штатов.

Мы также представляем вам файл о COSMOS, написанный скорее с точки зрения безопасности, нежели с точки зрения советов по хакерскому проникновению. В этом выпуске продолжается «Future Transcendent Saga» — файл о сети NSFnet и третье приложение к бесконечной серии. Данное конкретное приложение предназначено для использования в качестве общего справочника к третьей главе FTSaga — «Limbo To Infinity». Поскольку этот файл представляет собой скорее каталог-справочник, нежели практическое руководство, мы рассматриваем его просто как релиз Phrack Inc.

Как всегда, мы просим всех, у кого есть доступ к сети, написать нам на наши адреса в Bitnet или Internet...


```
          Taran King                      Knight Lightning
     C488869@UMCVMB.BITNET           C483307@UMCVMB.BITNET
  C488869@UMCVMB.MISSOURI.EDU     C483307@UMCVMB.MISSOURI.EDU
```

Компьютерные системы в операциях Bell System

Автор: Taran King

Данный файл содержит описание различных операционных систем, применявшихся в Bell System. Некоторые из них хорошо знакомы большинству специалистов, другие практически неизвестны. Каждый подраздел даёт краткое описание функций соответствующей компьютерной системы.

Оглавление

TIRKS (Trunks Integrated Records Keeping System — Интегрированная система учёта магистральных линий)

TIRKS является главной системой учёта записей для сети. Она поддерживает сетевые операции, связанные с развитием и изменением сети, обеспечивая точный учёт каналов и компонентов, находящихся в эксплуатации и доступных для использования. Система была разработана для механизации процесса предоставления каналов связи. Применяются два аспекта этого процесса: ежедневное предоставление каналов и текущее планирование.

Ежедневное предоставление каналов — это обработка заявок для удовлетворения потребностей клиентов в специализированных каналах, а также обработка заявок на магистральные линии и системы носителей для PSTN. Процесс начинается в различных операционных центрах и завершается в CPC (Circuit Provision Centers — Центрах предоставления каналов), которые отслеживают заявки, проектируют каналы и назначают компоненты с помощью TIRKS. Система также подготавливает рабочие пакеты и распределяет их среди техников, работающих в поле.

Текущее планирование определяет требования к оборудованию и средствам для будущих новых каналов. Оно распределяет прогнозы по каналам среди проектов, запланированных для новых соединений.

TIRKS состоит из пяти основных взаимодействующих компонентных систем: COC (Circuit Order Control — система управления заявками на каналы), E1 (Equipment system — система оборудования), F1 (Facility system — система средств связи), C1 (Circuit system — система каналов) и FEPS (Facility and Equipment Planning System — система планирования средств и оборудования).

• **COC** управляет заявками на магистральные линии, заявками на специальные услуги и заявками на системы носителей, отслеживая критические даты на протяжении всего жизненного цикла заявки — от источника до CPC и далее до полевых подразделений. Система предоставляет руководству актуальный статус всех заявок на каналы и передаёт данные в другие компонентные системы TIRKS для обновления статуса назначенного оборудования, средств связи и каналов по мере обработки заявок.

• **C1** является ядром TIRKS. Она автоматически определяет типы оборудования, необходимого для данного канала, назначает необходимое оборудование и средства связи, определяет уровни в различных точках уровня передачи на канале, задаёт требования к тестированию и формирует записи о каналах. Все записи об уже установленных каналах хранятся в C1 для последующих дополнений или изменений.

• **E1** — одна из двух основных компонентных систем инвентаризации в TIRKS. Содержит записи об инвентаре оборудования, записи о назначениях и ожидающие заявки на оборудование. В записях указывается количество свободного оборудования и его идентификатор канала.

• **F1** — вторая из основных компонентных систем инвентаризации. Содержит инвентарь кабелей и носителей, а также записи о назначениях.

• **FEPS** поддерживает процесс текущего планирования, определяющего средства передачи и оборудование, которые потребуются для новых услуг. Система использует данные из E1, F1 и C1, а также другие прогнозы для эффективного распределения существующих запасов, определения будущих потребностей в средствах и оборудовании, а также обновления проектных решений.

TIRKS использует аппаратное обеспечение, совместимое с IBM-370, и устройства прямого доступа к данным. Система приносит пользу BOC за счёт улучшения обслуживания клиентов, экономии капитала и расходов, а также улучшения управленческого контроля.

PICS (Plug-in Inventory Control System — Система управления инвентарём подключаемых модулей)

PICS — механизированная операционная система, разработанная для эффективного управления большими объёмами инвентаря оборудования. Она помогает как в управлении инвентарём, так и в управлении материалами. Менеджеры по инвентарю формируют корпоративную политику в отношении типов оборудования и его использования, помогают инженерным организациям внедрять новые типы оборудования при выводе из эксплуатации устаревших, а также устанавливают цели использования, которые уравновешивают задачи обслуживания и расходы на хранение запасного оборудования. Менеджеры по материалам работают над достижением целей использования, приобретая запасное оборудование для нужд роста и технического обслуживания. Они также администрируют иерархию мест хранения запасного оборудования.

PICS/DCPR (PICS с подробными текущими имущественными записями) администрирует все типы оборудования CO. Часть DCPR в PICS/DCPR служит подробной инвестиционной базой данных,

поддерживающей бухгалтерские записи для всех типов подключаемого и «жёстко подключённого» оборудования CO. PICS/DCPR достигает своих целей по увеличению использования, сокращению ручного труда и ведению подробных учётных записей инвестиций телефонной компании посредством программного обеспечения, баз данных, административных процедур и рабочих процессов.

В BOC создаются два новых функциональных подразделения: PIA (Plug-In Administration — Администрация подключаемых модулей) и центральный склад. PIA является менеджером по материалам и отвечает за приобретение оборудования, его распределение по полевым точкам по мере необходимости, ремонт и учёт. Центральный склад — это хранилище, где запасное оборудование консолидируется и управляется.

В PICS/DCPR существует пять подсистем:

• **Подсистема инвентаря подключаемых модулей** — ведёт записи о заявках, ремонте и инвентаре для всех типов подключаемого оборудования.

• **Подсистема управления инвентарём** — предоставляет PIA механизированные процессы для помощи в различных задачах.

• **Подсистема DCPR для подключаемых модулей** — предоставляет процессы, необходимые для ведения инвестиционных записей для подключаемых модулей.

• **Подсистема DCPR для жёстко подключённого оборудования** — ведёт подробные бухгалтерские записи для жёстко подключённого оборудования CO.

• **Подсистема справочных файлов** — предоставляет и поддерживает справочные данные, используемые всеми остальными подсистемами.

PICS/DCPR работает на IBM-совместимом оборудовании с менеджером баз данных IBM Information Management System. Система взаимодействует с TIRKS, а также с несколькими другими системами предоставления каналов.

PREMIS (PREMises Information System — Информационная система объектов)

PREMIS обеспечивает быстрый и удобный доступ к информации, необходимой для ответа на запросы об услугах. Она была разработана в ответ на потребность в стандартизации адресов. Система имеет три механизированные базы данных: данные адресов, кредитный файл и список доступных телефонных номеров. Она также выполняет функцию для LAC (Loop Assignment Center — Центра назначения шлейфов), называемую PREMIS/LAC. PREMIS/LAC является расширением адресной базы данных и обеспечивает хранение данных о средствах внешней сети для каждой адресной записи.

PREMIS поддерживает следующие задачи представителей по обслуживанию:

• **Определение правильного адреса клиента.** Информация, связанная с адресом и вводимая по адресу, является основной функцией PREMIS. Если входящий запрос не содержит точного или полного адреса, PREMIS отображает информацию, которую можно использовать для уточнения у клиента. Адресная база данных позволяет PREMIS выдавать полный адрес и информацию о географическом районе, включая WC (Wire Center — Узловой центр), зону обмена, налоговую зону, группу справочника и доступные в этом районе функции обслуживания. Также отображаются имя и номер телефона существующего или предыдущего клиента, модульная схема разъёмов по адресу и указание на то, остался ли проложенный от адреса до CO внешний шлейф сети. Если обслуживание по данному адресу было прекращено, отображаются причина и дата отключения.

• **Обсуждение функций обслуживания.** PREMIS указывает на функции обслуживания, которые можно предложить по данному адресу, предоставляя полезную информацию для обсуждения с клиентом.

• **Согласование даты обслуживания.** Если система указывает на то, что внешний шлейф до CO был оставлен на месте, PREMIS допускает более раннюю установку, поскольку техник не нуждается в посещении объекта.

• **Проверка кредитного статуса клиента.** PREMIS ведёт файл клиентов с непогашенными долгами перед телефонной компанией, доступный по имени. При совпадении в базе данных отображается файл клиента.

• **Выбор телефонного номера.** В PREMIS имеется файл с перечнем всех доступных телефонных номеров, из которого представители по обслуживанию запрашивают номера для конкретного адреса. Доступные телефонные номера считываются с магнитной ленты COSMOS (COmputer System for Mainframe OperationS).

В PREMIS/LAC имеется функция DPAC (Dedicated Plant Assignment Card — Карточка назначения выделенной сети). Записи об адресах, где средства внешней сети выделены, организуются и доступны по адресу через DPAC в LAC.

PREMIS является интерактивной системой реального времени, основными пользователями которой являются представители по обслуживанию, взаимодействующие с клиентами. В качестве основного компьютера используется UNIVAC 1100. Система также имеет сетевые связи с различными другими компьютерными системами для получения различных сведений, необходимых или полезных для эффективного выполнения функций обслуживания.

TNDS (Total Network Data System — Полная система сетевых данных)

TNDS фактически представляет собой большой и сложный набор скоординированных систем, поддерживающих широкий спектр видов деятельности, которые зависят от точных данных о трафике. Это скорее концепция, включающая различные подсистемы, чем единая компьютерная система. Она состоит как из ручных процедур, так и из компьютерных систем, которые предоставляют менеджерам операционных компаний всестороннюю, своевременную и точную информацию о сети, помогающую в её анализе. TNDS поддерживает операционные центры, ответственные за администрирование транкинговой сети, сбор сетевых данных, ежедневный контроль нагрузки на коммутационную сеть, использование оборудования коммутационной сетью и проектирование локального и CO коммутационного оборудования для удовлетворения будущих потребностей в обслуживании.

Модули TNDS, собирающие и форматирующие данные о трафике, обычно имеют выделенные мини-компьютеры, находящиеся в MMOC/MMC (Minicomputer Maintenance Operations Center / Minicomputer Maintenance Center) операционной компании. Другие модули генерируют инженерные и административные отчёты о коммутационных системах и о транкинговой сети магистральных линий сообщений, их связывающей. Они в основном работают на универсальных компьютерах. Ещё часть систем расположена в центрах AT&T и доступна различным операционным компаниям для получения данных.

Функции TNDS выполняются различными компьютерными системами, поскольку TNDS сама по себе является лишь концепцией. Эти подсистемы включают EADAS, EADAS/NM, TDAS, CU/EQ, LBS, 5XB COER, SPCS COER, ICAN, SONDS, TSS, CU/TK, TFS и CSAR. Следующие разделы кратко описывают эти системы.

EADAS (Engineering and Administrative Data Acquisition System — Система сбора инженерных и административных данных)

EADAS является основной системой сбора данных TNDS и работает на выделенном мини-компьютере в NDCC (Network Data Collection Center — Центре сбора сетевых данных). Каждая EADAS обслуживает до пятидесяти коммутационных узлов. Системы 4ESS и No. 4 XBAR имеют собственные встроенные системы сбора данных и передают свои данные непосредственно в другие компонентные системы TNDS, расположенные ниже по потоку от EADAS, тем самым устраняя необходимость в EADAS для этих коммутаторов. EADAS в режиме реального времени обобщает собранные данные для обработки нижестоящими системами TNDS. Сетевые администраторы используют EADAS для определения качества обслуживания и выявления проблем коммутации. Система также предоставляет этим администраторам дополнительную информацию реального времени в виде истории данных о трафике за последние 48 часов. Эта история данных гибко настраивается через модуль NORGEN (Network Operations Report GENerator — Генератор отчётов о сетевых операциях), чтобы администраторы могли адаптировать запросы информации для определения конкретных показателей. Информация из EADAS передаётся в другие нижестоящие системы TNDS через каналы данных или магнитные ленты.

EADAS/NM (EADAS/Network Management — EADAS/Управление сетью)

EADAS/NM — одна из трёх систем TNDS, в которые EADAS передаёт данные о трафике нижестоящим системам по каналам данных или магнитным лентам. EADAS/NM использует данные непосредственно из EADAS, а также получает данные от тех коммутационных систем, которые не взаимодействуют с EADAS (упоминавшихся ранее). Система отслеживает коммутационные системы и транковые группы, назначенные сетевыми менеджерами, и сообщает о существующих или ожидаемых перегрузках на панели отображения в местных и региональных NMC (Network Management Centers — Центрах управления сетью). Она используется для анализа проблем в режиме, близком к реальному времени, для определения их местонахождения и причин. EADAS/NM предоставляет информацию, требующую национальной координации, в NOC (Network Operations Center — Центр сетевых операций) AT&T Long Lines в Бедминстере, Нью-Джерси, который использует свою систему NOCS (NOC System) для выполнения функций, аналогичных EADAS/NM, в национальном масштабе. Как и EADAS, EADAS/NM использует выделенные мини-компьютеры для обеспечения интерактивного взаимодействия и управления в режиме реального времени.

TDAS (Traffic Data Administration System — Система администрирования данных о трафике)

Второй из трёх систем TNDS, расположенных ниже по потоку от EADAS, является TDAS, которая форматирует данные о трафике для использования большинством других нижестоящих систем. Она принимает данные от EADAS, местных вендорских систем и крупных транзитных коммутационных систем на еженедельной основе в виде магнитных лент. Система функционирует

в основном как склад и распределительный пункт для данных о трафике и работает в пакетном режиме в вычислительном центре. Правильное соответствие между зафиксированными данными о трафике и коммутирующими или транкинговыми элементами достигается благодаря совместному использованию информации между TDAS и CU/EQ. Данные, обработанные через TDAS, сопоставляются с данными, хранящимися в CU/EQ. Еженедельно данные обобщаются на магнитной ленте или в распечатке и направляются для подготовки инженерного или административного отчёта.

CU/EQ (Common Update/EQuipment — Общее обновление/Оборудование)

CU/EQ — главная база данных, хранящая измерения трафика, снятые TDAS, и обменивающаяся информацией с TDAS, ICAN и LBS. Как уже говорилось, правильное соответствие между зафиксированными данными о трафике и коммутирующими или транкинговыми элементами обеспечивается благодаря совместному использованию информации между CU/EQ и TDAS. Система работает в пакетном режиме на том же компьютере, что и TDAS, и регулярно обновляется пакетными транзакциями для поддержания актуальности с учётом изменений в физическом расположении коммутационных машин CO — это обеспечивает единообразную обработку зафиксированных измерений в каждой из систем отчётности, использующих записи CU/EQ.

ICAN (Individual Circuit ANalysis — Анализ отдельных каналов)

Последней из трёх систем, расположенных ниже по потоку от EADAS, является ICAN, которая также использует данные непосредственно из EADAS, но обращается к CU/EQ за справочной информацией. Это система отчётности CO, которая обнаруживает неисправности электромеханических коммутационных систем путём выявления аномальных паттернов нагрузки на отдельные каналы в группе каналов. ICAN формирует серию отчётов, используемых NAC (Network Administration Center — Центром администрирования сети) для анализа отдельных каналов и проверки правильности их соотнесения с соответствующими группами.

LBS (Load Balance System — Система балансировки нагрузки)

LBS — система пакетного исполнения, помогающая сетевому администратору обеспечить равномерное распределение трафиковых нагрузок в каждой коммутационной системе. Она анализирует данные о трафике для установления трафиковых нагрузок на каждую линейную группу коммутационной системы. NAC использует полученные отчёты для определения слабонагруженных линейных групп, к которым можно подключить новые абонентские линии. LBS также вычисляет индексы балансировки нагрузки для каждой системы и агрегирует результаты по всей BOC.

5XB COER (No. 5 Crossbar Central Office Equipment Reports — Отчёты об оборудовании АТС No. 5 Crossbar)

5XB COER предоставляет информацию о работе оборудования с общим управлением для различных типов коммутационных систем. Это система пакетного исполнения, работающая на мейнфрейме BOC, которая анализирует данные о трафике для определения степени загрузки различных компонентов коммутационной системы и измерения определённых параметров обслуживания. Система рассчитывает производительность коммутатора No. 5 Crossbar. Сетевые администраторы используют отчёты 5XB COER для ежедневного мониторинга производительности коммутации, диагностики потенциальных неисправностей коммутации и прогнозирования будущих потребностей в обслуживании. Инженеры по трафику опираются на отчёты для оценки производительности коммутационного узла и прогнозирования потребностей в оборудовании. Система формирует отчёты по часу наибольшей нагрузки и сезону наибольшей нагрузки, чтобы измерения качества обслуживания и трафиковой нагрузки были наиболее полезны для прогнозирования.

SPCS COER (Stored-Program Control Systems Central Office Equipment Reports — Отчёты об оборудовании АТС систем с хранимой программой управления)

SPCS COER в основном аналогична 5XB COER, поскольку также контролирует качество обслуживания коммутационной системы и измеряет её использование теми же способами, что описаны выше. Существенные различия между 5XB COER и SPCS COER состоят в том, что последняя рассчитывает производительность коммутационных узлов 1ESS, 2ESS и 3ESS в отличие от коммутатора No. 5 Crossbar, а также в том, что SPCS COER является интерактивной системой, работающей на централизованном мейнфрейме AT&T.

SONDS (Small Office Network Data System — Система сетевых данных малых офисов)

SONDS собирает собственные данные из небольших пошаговых офисов независимо от EADAS и TDAS. Система выполняет полный спектр функций обработки данных и экономично предоставляет ряд функций TNDS для небольших электромеханических пошаговых офисов. Собираемые данные поступают непосредственно из измеряемых офисов. Система обрабатывает данные и автоматически распространяет еженедельные, ежемесячные, исключительные и созданные по запросу отчёты менеджерам NAC через коммутируемые терминалы. SONDS работает в интерактивном режиме на централизованном мейнфрейме AT&T.

CU/TK (Common Update/TrunKing — Общее обновление/Транкинг)

CU/TK — база данных, содержащая информацию о транкинговой сети, а также другую информацию, необходимую для TSS (Trunk Servicing System — Системы обслуживания транков) и TFS (Trunk Forecasting System — Системы прогнозирования транков). CU/TK регулярно обновляется персоналом CAC (Circuit Administration Center — Центра администрирования каналов) для поддержания актуальности с учётом изменений в физическом расположении транков и коммутационных машин в CO. Для обеспечения правильной конфигурации транкинга и коммутации при обработке в TSS и TFS этот процесс обновления — включающий поддержание информации о

росте офиса и идентификации каналов в стандартном «общем языке» для всех отдельных коммутационных машин — гарантирует, что данные о трафике, предоставляемые TDAS, будут правильно соотнесены.

TSS (Trunk Servicing System — Система обслуживания транков)

TSS помогает администраторам транков разрабатывать краткосрочные планы и определять количество каналов, необходимых в транковой группе. Данные из TDAS обрабатываются в TSS, и вычисляется предлагаемая нагрузка для каждой транковой группы. На основе расчёта предлагаемой нагрузки на уровне каждой транковой группы TSS вычисляет теоретически необходимое количество транков для обработки данной трафиковой нагрузки при заданном классе обслуживания. TSS формирует еженедельные отчёты, показывающие, какие транковые группы имеют слишком много транков, а какие — слишком мало и не достигают целевого класса обслуживания. CAC принимает решения о добавлении или отключении транков на основе информации, предоставляемой TSS.

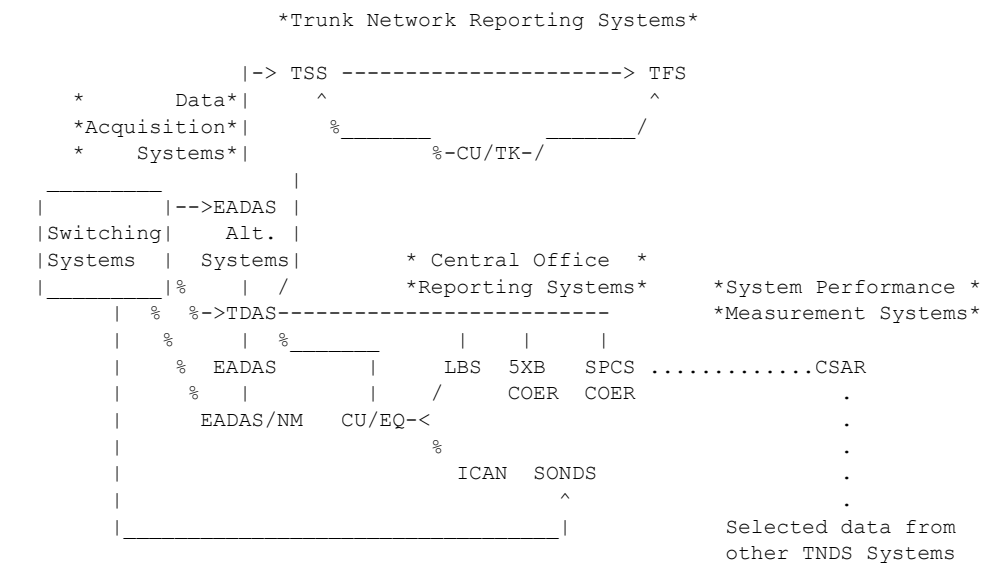
TFS (Trunk Forecasting System — Система прогнозирования транков)

TFS использует данные о трафиковой нагрузке, рассчитанные TSS, а также информацию о конфигурации сети и параметры прогнозирования, хранящиеся в базе данных CU/TK, для долгосрочного строительного планирования новых транков. TFS прогнозирует потребности в магистральных транках на следующие пять лет в качестве основного входного сигнала для процесса планирования, ведущего к предоставлению дополнительных средств связи.

CSAR (Centralized System for Analysis and Reporting — Централизованная система анализа и отчётности)

CSAR разработана для мониторинга и измерения качества обработки данных через TNDS. Система собирает и анализирует данные из других систем TNDS и предоставляет персоналу операционных компаний в NDCC, NAC и CAC количественные показатели точности, своевременности и полноты потока данных TNDS, а также согласованности баз записей TNDS. CSAR также представляет достаточно информации для обнаружения и идентификации проблем сбора данных. Система обобщает результаты мониторинга TNDS для компании в качестве входных данных для TPMP (TNDS Performance Measurement Plan — Плана измерения производительности TNDS), который ежемесячно публикуется AT&T. CSAR работает как централизованная интерактивная система в вычислительном центре AT&T. Её данные помещаются в специальные файлы, которые по окончании работы CSAR объединяются и передаются в вычислительный центр AT&T. CSAR выполняет необходимые соответствия и анализирует результаты каждой системы. Эти результаты получают менеджеры компаний через коммутируемые соединения; результаты можно представить в ряде форматов с подробными сведениями об общей производительности TNDS или эффективности отдельных систем. С помощью этих отчётов также можно выявить конкретные проблемы.

Схема потоков данных между системами TNDS



SCCS (Switching Control Center System — Система центра управления коммутацией)

Центр управления коммутацией (SCC) был создан для централизации администрирования, технического обслуживания и управления коммутационной системой 1ESS. Используя удалённое взаимодействие через MCC (Master Control Center — Главный центр управления) — стойку оборудования в системе 1ESS, отображающую текущее состояние офисного оборудования, — SCC функционирует как централизованный центр технического обслуживания коммутатора.

В SCC добавляется мини-компьютерная система CSS (Computer Sub-System), которая вместе с оборудованием, обеспечивающим удалённый доступ к MCC, образует SCCS. CSS может поддерживать несколько SCC. Как правило, CSS располагается в MMOC. Фактически каждый SCC обслуживает несколько коммутаторов, а различные SCC обслуживаются CSS.

SCCS содержит данные технического обслуживания и административные данные, поступающие непосредственно от коммутаторов. Через SCCS техник может удалённо управлять клавишами MCC на подключённых к ней коммутаторах, а также выполнять любую доступную команду или задачу, поддерживаемую коммутатором. SCCS может обслуживать 30 и более офисов, хотя обычно на один SCC приходится около 15. Это число также зависит от размеров офисов и объёма передаваемых данных.

Крупные аварийные сигналы, звучащие в коммутационном офисе, в течение нескольких секунд активируют сигналы тревоги в SCC, а также вызывают обновление статуса офиса на панели критических индикаторов и отображение конкретного описания аварийного состояния на CRT-мониторе аварийных сигналов на рабочей станции. Программные усовершенствования SCCS подразделяются на четыре широких класса:

• **Расширенное оповещение** — помимо звуковых сигналов тревоги, поступающие данные могут генерировать описания неисправностей для удобной интерпретации и применения методов анализа в реальном времени.

• **Взаимодействие с историей сообщений** — используя прошлую информацию о неисправностях коммутатора, SCCS позволяет предоставлять соответствующую информацию о конкретном коммутаторе в случае аварийного сигнала.

• **Механизация функций обслуживания** — в ряде случаев больше нет необходимости в непосредственном осмотре. Если срабатывает сигнал тревоги, SCCS может выполнить стандартные тесты и устранить проблему наилучшим образом, а если это не удастся — создаётся заявка на устранение неисправности.

• **Поддержка администрирования коммутаторов** — через SCCS данные могут автоматически направляться в различные операционные центры и другие операционные системы, которым требуются данные от коммутаторов.

С момента ввода в эксплуатацию исходной SCCS произошло множество изменений. Текущая SCCS поддерживает все коммутаторы семейства ESS, а также оборудование сетевой передачи, может обслуживать несколько вспомогательных процессорных систем — таких как TSPS (Traffic Service Position System — Система позиций обслуживания трафика) и AIS (Automatic Intercept System — Система автоматического перехвата) — и поддерживает оборудование сетевой передачи.

COEES (Central Office Equipment Engineering System — Система инженерии оборудования центрального офиса)

COEES — система разделения времени, работающая на DEC PDP-10. Это стандартная система для планирования и инженерии локального коммутационного оборудования. COEES содержит компонентные системы для коммутационных систем Step-By-Step, Crossbar, 1/1AESS и 2/2BESS, каждая из которых имеет различные возможности.

База данных COEES хранит информацию, полученную из прогнозов для каждого локального коммутационного офиса: количество линий всех типов, количество транков всех типов, среднюю интенсивность вызовов на линию и транк, среднее использование на линию и транк, а также все функции, типы сигнализации и т.д., которые требуются. COEES определяет количество каждого типа оборудования в офисе, необходимого для обеспечения прогнозируемой нагрузки при целевых уровнях обслуживания, определяет ориентировочную стоимость инженерии, закупки и установки необходимого дополнительного оборудования и затем суммирует затраты восемью различными способами для ознакомления сетевого проектировщика. Система также учитывает варьируемые параметры, такие как интенсивность вызовов или доля линий с определёнными функциями, — это называется анализом чувствительности.

На основе информации, предоставленной прогнозом COEES, проектировщик может сформулировать рекомендацию. После принятия решения по рекомендации COEES распечатывает заказ, чтобы дополнительное оборудование можно было получить быстрее и проще.

COEES также формирует отчёт о памяти хранилища вызовов (call store) для 1ESS, в котором указывается инженеру и поставщику оборудования, сколько памяти выделить под различные функции коммутатора в зависимости от входных данных, предоставляемых инженером системе.

MATFAP (Metropolitan Area Transmission Facility Analysis Program — Программа анализа средств передачи в городской сети)

MATFAP — компьютерная программа, помогающая в планировании средств связи. Она анализирует альтернативы, доступные операционной компании для её будущего оборудования и средств передачи, используя приведённую стоимость будущих расходов и другие показатели.

Объединяя прогнозы по транкам и специализированным каналам с планами коммутации, конфигурацией сети, данными о стоимости и инженерными нормами, MATFAP может определить, какие средства передачи потребуются в различных местах и когда. Система также определяет экономические последствия конкретного выбора средств и/или оборудования, а также вариантов маршрутизации, и обеспечивает наиболее экономичное назначение каналов каждому средству как ориентир для процесса предоставления каналов. Система ориентирована на городские сети и средства/оборудование, характерные для таких сетей.

MATFAP предоставляет два преимущества: помогает автоматизировать процесс планирования передачи и учитывает экономию, которую невозможно выявить при ограниченном анализе. Система также балансирует нагрузку каналов на высокоёмких цифровых линиях с дополнительным мультиплексным оборудованием. Данные из MATFAP редактируются через RDES (Remote Data Entry System — Систему удалённого ввода данных).

Различные операционные системы

Ниже приведён перечень других операционных систем, используемых в Bell System, с краткими описаниями:

ATRS (Automated Trouble Reporting System — Автоматизированная система отчётности об авариях) — помогает в анализе отчётов об авариях путём их сортировки, форматирования, пересылки и проверки по всей стране на предмет стандартных ошибок.

BOSS (Billing and Order Support System — Система поддержки биллинга и заявок) — обеспечивает доступ к записям клиентов, CN/A, корректировкам счетов и маршрутизации информации.

CAROT (Centralized Automatic Reporting On Trunks — Централизованная автоматическая отчётность по транкам) — операционная система, тестирующая транк в электромеханических и электронных коммутационных системах и передающая результаты на удалённый компьютерный терминал.

CATLAS (Centralized Automatic Trouble Locating and Analysis System — Централизованная автоматическая система обнаружения и анализа неисправностей) — операционная система, автоматизирующая процедуры обнаружения неисправностей, которые выявляют дефектные платы в коммутаторе при обнаружении и диагностике неисправности.

CMDS (Centralized Message Data System — Централизованная система данных сообщений) — анализирует ленты AMA для определения паттернов трафика.

COSMOS (COmputer System for Mainframe OperationS) — хранит полный инвентарь телефонных номеров.

CRIS (Customer Records Information System — Информационная система записей клиентов) — содержит базу данных биллинга клиентов.

CRS (Centralized Results System — Централизованная система результатов) — управленческая информационная система, автоматизирующая сбор, анализ и публикацию многих результатов измерений.

CUCRIT (Capital Utilization CRITeria — Критерии использования капитала) — применяется главным образом для экономической оценки проектов, составления капитального бюджета и планирования.

DACS (Digital Access Cross-connect System — Система цифрового доступа с перекрёстным соединением) — удалённый цифровой доступ для тестирования специализированных каналов в аналоговой или цифровой форме.

EFRAP (Exchange Feeder Route Analysis Program — Программа анализа фидерных маршрутов коммутации) — применяется при планировании абонентской сети.

IFRPS (Intercity Facility Relief Planning System — Система планирования замены межгородских средств связи) — аналогична MATFAP, но работает с радио и коаксиальным кабелем в отличие от средств голосовой частоты.

IPLAN (Integrated PLanning And Analysis system — Интегрированная система планирования и анализа) — применяется главным образом для экономической оценки проектов.

LMOS (Loop Maintenance Operations System — Система операций технического обслуживания шлейфов) — обслуживает прерывания обслуживания на шлейфах удалённо силами сотрудника сервисной службы.

LRAP (Long Route Analysis Program — Программа анализа длинных маршрутов) — аналогична EFRAP, применяется при планировании абонентской сети.

LSRP (Local Switching Replacement Planning system — Система планирования замены локальной коммутации) — система, применяемая при планировании узловых центров.

NOTIS (Network Operations Trouble Information System — Информационная система отчётности о неисправностях сетевых операций) — помогает в анализе отчётов об авариях.

NSCS (Network Service Center System — Система центра сетевого обслуживания) — в NSC помогает в анализе отчётов об авариях.

OFNPS (Outstate Facility Network Planning System — Система планирования сети средств связи в отдалённых районах) — аналогична MATFAP, но содержит инструмент поддержки принятия решений, определяющий стратегии внедрения цифровых средств в преимущественно аналоговую сеть; планирование сети средств передачи в сельской местности.

RDES (Remote Data Entry System — Система удалённого ввода данных) — обеспечивает удалённое редактирование данных в онлайн-компьютере.

RMAS (Remote Memory Administration System — Система удалённого администрирования памяти) — изменяет трансляции в коммутационных системах.

SARTS (Switched Access Remote Test System — Система удалённого тестирования с коммутируемым доступом) — используется для выполнения сложных тестов большинства типов специализированных каналов.

SMAS (Switched Maintenance Access System — Система коммутируемого доступа для технического обслуживания) — посредством реле обеспечивает сосредоточенный металлический доступ к отдельным каналам для удалённого доступа и тестирования через SARTS.

TASC (Telecommunications Alarm Surveillance and Control System — Система наблюдения и управления телекоммуникационными аварийными сигналами) — программа сигнализации, идентифицирующая станцию и передающая информацию в центральный пункт технического

обслуживания.

TCAS (T-Carrier Administration System — Система администрирования Т-носителей) — операционная система, ответственная за сигналы тревоги Т-носителей.

TCSP (Tandem Cross Section Program — Программа поперечного сечения транзита) — программа для анализа планирования транспортной сети.

TFLAP (T-carrier Fault-Locating Application Program — Прикладная программа обнаружения неисправностей Т-носителей) — подпрограмма Универсальной программы анализа кабельных цепей, анализирующая сети с ответвлениями, множественными окончаниями и мостовыми отводами.

Глоссарий аббревиатур

AIS	Automatic Intercept System
AMA	Automatic Message Accounting
ATRS	Automated Trouble Reporting System
BOSS	Billing and Order Support System
C1	Circuit system
CAC	Circuit Administration Center
CAROT	Centralized Automatic Reporting On Trunks
CATLAS	Centralized Automatic Trouble Locating and Analysis System
CMDS	Centralized Message Data System
CPC	Circuit Provision Center
CO	Central Office
COC	Circuit Order Control
COEES	Central Office Equipment Engineering System
COSMOS	COmputer System for Mainframe OperationS
CRIS	Customer Records Information System
CRS	Centralized Results System
CRT	Cathode-Ray Tube
CSAR	Centralized System for Analysis and Reporting
CSS	Computer SubSystem
CUCRIT	Capital Utilization CRITeria
CU/EQ	Common Update/EQuipment system
CU/TK	Common Update/TrunKing system
DACS	Digital Access and Cross-connect System
DPAC	Dedicated Plant Assignment Card
E1	Equipment system
EADAS	Engineering and Administrative Data Acquisition System
EADAS/NM	EADAS/Network Management
EFRAP	Exchange Feeder Route Analysis Program
ESS	Electronic Switching System
F1	Facility system
FEPS	Facility and Equipment Planning System
5XB COER	No. 5 Crossbar Central Office Equipment Report system
ICAN	Individual Circuit ANalysis
IFRPS	Intercity Facility Relief Planning System
IPLAN	Integrated PLanning and ANalysis
LAC	Loop Assignment Center
LBS	Load Balance System
LMOS	Loop Maintenance Operations System
LRAP	Long Route Analysis Program
LSRP	Local Switching Replacement Planning system
MATFAP	Metropolitan Area Transmission Facility Analysis Program
MCC	Master Control Center
MMC	Minicomputer Maintenance Center
MMOC	Minicomputer Maintenance Operations Center
NAC	Network Administration Center
NDCC	Network Data Collection Center
NMC	Network Management Center
NOC	Network Operations Center
NOCS	Network Operations Center System

```
NORGEN     Network Operations Report GENerator
NOTIS      Network Operations Trouble Information System
NSCS       Network Service Center System
OFNPS      Outstate Facility Network Planning System
PIA        Plug-In Administrator
PICS       Plug-in Inventory Control System
PICS/DCPR  PICS/Detailed Continuing Property Records
PREMIS     PREMises Information System
PSTN       Public Switched Telephone Network
RDES       Remote Data Entry System
RMAS       Remote Memory Administration Center
SARTS      Switched Access Remote Test System
SCC        Switching Control Center
SCCS       Switching Control Center System
SMAS       Switched Maintenance Access System
SONDS      Small Office Network Data System
SPCS COER  Stored-Program Control System/Central Office Equipment Report
TASC       Telecommunications Alarm Surveillance and Control system
TCAS       T-Carrier Administration System
TCSP       Tandem Cross Section Program
TDAS       Traffic Data Administration System
TFLAP      T-Carrier Fault-Locating Applications Program
TFS        Trunk Forecasting System
TIRKS      Trunks Integrated Records Keeping System
TNDS       Total Network Data System
TPMP       TNDS Performance Measurement Plan
TSPS       Traffic Service Position System
TSS        Trunk Servicing System
WC         Wire Center
```

Рекомендуемые источники:

• Bell System Technical Journals
• Engineering and Operations in the Bell System
• Phrack IX, файл о LMOS, автор Phantom Phreaker
• Phrack XII, файл о TNDS, автор Doom Prophet
• Различные файлы о COSMOS авторства LOD/H, KOTRT и др.

Завершено 17.03.1989

Поимка с поличным — Правовые процедуры

Автор: The Disk Jockey

24 марта 1989 года

Непредвзятый взгляд на механизм уголовного судопроизводства

Предисловие

В этом материале я постараюсь разъяснить, какие правовые действия предпринимаются в ходе расследования телефонного мошенничества. Вся изложенная здесь информация основана на реальных фактах; несмотря на некоторые различия от штата к штату, большая её часть применима повсеместно. Вокруг реального хода событий во время и после расследования накопилось немало заблуждений, поэтому я надеюсь ответить на вопросы, которые слишком часто остаются незаданными.

Возбуждение дела

В нашей истории расследование начинается с телефонного звонка в службу безопасности U.S. Sprint. Поразительно, как много «хакеров» звонят туда с доносами на других «хакеров». Когда один пользователь злится на другого и ищет «мести», он звонит в отдел безопасности и сообщает, что знает человека, незаконно пользующегося услугами дальней связи данной компании. Как правило, такой человек говорит либо с рядовым представителем службы поддержки, либо с сотрудником отдела безопасности. Обычно разговор сводится примерно к следующему: «Эй, один парень по имени "Джо" пользуется вашими кодами, которые он взломал, его домашний номер — 312-xxx-xxxx».

Получив информацию, сотрудник безопасности должен решить, насколько достоверен звонок. Если всё выглядит правдоподобно, он инициирует собственное внутреннее расследование. Оно может начаться с простой проверки CN/A (Customer Name and Address — имя и адрес абонента) по указанному номеру телефона, чтобы установить, на кого он зарегистрирован, и убедиться, является ли данное лицо законным подписчиком системы.

Затем следует звонок в местную телефонную компанию, обслуживающую подозреваемого. Обычно устанавливается контакт с сотрудником отдела безопасности или лицом, выполняющим аналогичные функции. Совместно они договариваются об установке на телефонную линию абонента устройства DNR (Dialed Number Recorder — регистратор набранных номеров), которое на узкой бумажной ленте (наподобие ленты кассового аппарата) фиксирует все данные: набранные номера, режим набора (DTMF или импульсный), любые факты появления тона 2600 Гц, набранные коды и прочие цифры, входящие звонки — в том числе количество гудков до снятия трубки, время подъёма и опускания трубки и т. д.

DNR может находиться на телефонной линии абонента от нескольких недель до нескольких месяцев.

В какой-то момент представитель службы безопасности U.S. Sprint или сотрудник безопасности телефонной компании решают, что собранных данных достаточно, и приступают к анализу записей

DNR. Представитель Sprint может лично приехать в офис телефонной компании и изучить записи там, либо те будут переправлены в офис Sprint.

Изучив записи и обнаружив номера дозвона и коды, которые, по всей видимости, использовались незаконно, Sprint разыскивает законных владельцев этих кодов и удостоверяется в том, что коды действительно применялись без их ведома и разрешения. Параллельно составляется оценка «ущерба», куда могут входить стоимость доступа к порту дозвона, расходы на расследование, а также фактические суммы тарифицированных переговоров.

После этого представитель службы безопасности Sprint и сотрудник безопасности местной телефонной компании обращаются в местную полицию — как правило, в штатную или в ту структуру, которая обладает реальными полномочиями в данном районе. Они представляют детективу или иному следователю результаты расследования и, если выводы выглядят достаточно убедительно, составляют ходатайство об обыске. После полного оформления ордера (иногда это просто короткий бланк с пропусками для заполнения) трое участников расследования — детектив полиции, представитель безопасности местной телефонной компании и следователь безопасности Sprint — предстают перед судьёй и под присягой излагают доказательства и результаты расследования, содержащиеся в документе под названием «дискавери» (раскрытие доказательств), что служит основанием для выдачи ордера на обыск. Если выводы признаются убедительными, судья подписывает ордер, после чего тот вступает в силу на указанный в нём срок. Как правило, ордер действителен круглосуточно, поскольку звонки, по всей видимости, совершались в любое время суток.

В согласованный день все вышеперечисленные лица являются к дому подозреваемого, исполняют ордер на обыск и, скорее всего, изымают всё телефонное и компьютерное оборудование, доставляя его в отделение штатной полиции для дальнейшей экспертизы.

Затем вся информация, улики и отчёты передаются в прокуратуру, которая определяет, какие обвинения, если таковые вообще будут предъявлены, целесообразно поддерживать.

После того как прокуратура окончательно формулирует обвинения, составляется новый документ «дискавери» с перечнем всех обвинений и обоснованием каждого из них. Документ снова передаётся судье, и в случае одобрения выдаются ордера на арест указанных в нём лиц.

Ордера исполняются, как правило, следующим образом: местный офицер полиции приходит к дому подозреваемого, стучит в дверь, представляется, просит нужного человека, предъявляет ему ордер и доставляет его в участок.

Задержанного оформляют: как правило, его фотографируют и снимают отпечатки пальцев дважды — один комплект для ФБР, второй для государственного архива, — после чего помещают в камеру предварительного заключения или обычную тюремную камеру.

Иногда залог устанавливается ещё до ареста, но бывает и иначе. В последнем случае залог назначается на слушании по предъявлению обвинений.

В течение 72 часов подозреваемому должно быть предъявлено официальное обвинение. Слушание по предъявлению обвинений — это момент, когда перед судьёй официально зачитываются обвинения, назначается залог (если он ещё не установлен), и подозреваемый выбирает форму суда: суд присяжных или суд судьи. Разумеется, это предполагает, что подозреваемый намерен заявить о своей невиновности, что в большинстве серьёзных дел является наилучшей тактикой. В это же время назначаются последующие заседания суда. Если обвиняемый не может позволить себе нанять адвоката, суд в этот момент назначает ему государственного защитника.

После слушания по предъявлению обвинений подозреваемого либо отпускают под залог, либо возвращают в камеру ожидать следующего заседания. Следующее заседание — «омнибус» — обычно назначается примерно через месяц.

Если установленный залог кажется неоправданно высоким, ваш адвокат может подать ходатайство о снижении залога. Вы предстанете перед судьёй: ваш адвокат будет доказывать, почему залог следует снизить, и приводить аргументы в пользу вашей социальной стабильности и ответственности, исключающих бегство. Прокурор, в свою очередь, будет возражать против снижения.

На слушании «омнибус», известном также как слушание по установлению фактических обстоятельств дела (в некоторых штатах оно называется «предварительным слушанием» — *примеч. ред.*), подозреваемый снова предстаёт перед судьёй вместе со своим адвокатом и прокурором. Государство в лице прокурора представляет доказательства против подозреваемого, а судья решает, достаточно ли их для содержания обвиняемого под стражей или же для продолжения дела до судебного разбирательства. Почти всегда доказательств оказывается достаточно: ордера на арест не выдаются при их отсутствии, поскольку в противном случае государство рискует стать ответчиком по иску о незаконном задержании. После этого назначается дата «предварительного суда» — опять же, как правило, примерно через месяц.

Предварительный суд — последний шанс для обвиняемого передумать и признать себя виновным, либо продолжить добиваться оправдательного приговора. Это также последний момент, когда прокурор может предложить сделку о признании вины: обвиняемый признаёт себя виновным в обмен на согласованное смягчение обвинений или приговора. Если обвиняемый по-прежнему настаивает на своей невиновности, назначается дата отбора присяжных.

В ходе отбора присяжных вы, ваш адвокат и прокурор имеете право поочерёдно встречаться с любым количеством кандидатов в присяжные, задавать им вопросы и принимать или отклонять их — исходя из того, считаете ли вы данного кандидата объективным. Это позволяет максимально исключить из состава присяжных тех, кто предубеждён ещё до начала рассмотрения дела. После того как прокурор и ваш адвокат приходят к согласию относительно состава коллегии, назначается дата судебного заседания — как правило, примерно через неделю.

На суде прокурор представляет дело коллегии присяжных: сначала допрашиваются детективы и следователи о том, как изначально было обнаружено дело и каким образом следствие вышло на вас. На каждом этапе ваш адвокат вправе проводить «перекрёстный допрос» каждого свидетеля, задавая собственные вопросы и тем самым стараясь зародить у присяжных сомнения в достоверности показаний. Затем вашему адвокату предоставляется право вызывать собственных свидетелей, которых в свою очередь вправе допрашивать прокурор. По закону вы не обязаны давать показания, если не хотите, поскольку имеете право не свидетельствовать против себя. По завершении всего прокурор выступает с «заключительной речью» — кратким изложением всего представленного и обоснованием того, почему вас следует признать виновным; затем ваш адвокат обращается к присяжным с аргументами в пользу вашей невиновности.

Присяжные удаляются на совещание, которое может занять как несколько минут, так и несколько дней. Они должны единогласно проголосовать за признание вас виновным или невиновным. По окончании совещания суд возобновляется и присяжные объявляют вердикт.

Если вас признают виновным, у вас, как правило, есть около 10 дней для подачи апелляции, которая передаст ваше дело в вышестоящую инстанцию. В противном случае назначается дата вынесения приговора — снова обычно примерно через месяц.

На слушании по вынесению приговора ваш адвокат будет добиваться мягкого наказания, а прокурор — строгого. Судья принимает решение с учётом аргументов обеих сторон и назначает наказание. После этого вас передают под надзор соответствующего ведомства — будь то служба пробации, система исполнения наказаний или окружная тюрьма.

Я надеюсь, что этот материал дал вам более чёткое представление о том, как работает правовая система. В следующих материалах я намерен обсудить конкретные рекомендации «что делать и чего не делать» в рамках правовой системы, а также рассказать о тактических приёмах, которыми пользуются юридические органы власти.

Вопросы, комментарии и угрозы можно направлять мне по адресу:

Lunatic Labs 415.278.7421

— The Disk Jockey

Написано специально для Phrack Newsletter, 1989. Данный материал может использоваться полностью или частично при условии полного указания авторства.

NSFnet: Национальная сеть Фонда науки

Автор: Knight Lightning

16 апреля 1989 года

Продолжение саги «Будущее за горизонтом»...

Сеть NSF связывает научное сообщество и центры суперкомпьютеров

Когда в 1985 году Национальный научный фонд (NSF) создал свои национальные центры суперкомпьютеров, он также планировал построить коммуникационную сеть, которая обеспечила бы удалённым площадкам доступ к этим передовым вычислительным мощностям. Специалисты NSF задумали систему, получившую название «NSFNET». Основанная на «магистрали», связывающей центры суперкомпьютеров, NSFNET должна была объединить существующие и вновь создаваемые сети в единую InterNet — сеть сетей — для обслуживания самих центров и их пользователей. Помимо доступа к вычислительным ресурсам центров, исследователи из географически разрозненных точек становились бы участниками общенациональной исследовательской сети, по которой могли обмениваться научной информацией. Хотя главной задачей NSFNET по-прежнему остаётся доступ к суперкомпьютерам, финансируемым NSF, и другим уникальным научным ресурсам, её роль как универсальной сети, позволяющей учёным делиться результатами исследований, становится всё более значимой.

Компоненты NSFnet

NSFNET организована по трёхуровневой иерархии: магистраль; широкозонные сети с автономным управлением, обслуживающие научные сообщества; и кампусные сети. Магистраль функционирует с июля 1986 года и находится в полностью рабочем состоянии. Она обеспечивает резервные маршруты между суперкомпьютерными центрами NSF. К магистрали NSFNET уже подключён ряд широкозонных сетей; другие строятся при частичном финансировании NSF и будут подключены по мере завершения строительства (см. раздел о компонентных сетях NSFnet).

Центры суперкомпьютеров

NSF создал суперкомпьютерные центры в ответ на растущую обеспокоенность тем, что нехватка доступа к мощным вычислительным ресурсам серьёзно сдерживала академические исследования. Конкурс на создание проектов, объявленный в июне 1984 года, завершился открытием следующих центров: Национальный суперкомпьютерный центр имени Джона фон Неймана в Принстоне (штат Нью-Джерси); Суперкомпьютерный центр Сан-Диего на базе Калифорнийского университета в Сан-Диего; Национальный центр суперкомпьютерных приложений при Университете Иллинойса; Национальный суперкомпьютерный центр Корнелла при Корнеллском университете; Питтсбургский

суперкомпьютерный центр под совместным руководством Westinghouse Electric Corporation, Университета Карнеги — Меллона и Питтсбургского университета. Все центры носят мультидисциплинарный характер и открыты для любого исследователя, имеющего право на поддержку NSF. Они предоставляют доступ к компьютерам производства Cray Research Inc., Control Data Corporation, ETA и IBM. Шестым центром, входящим в NSFNET, является Отдел научных вычислений Национального центра атмосферных исследований (SCD). Отдел оказывает передовые вычислительные услуги научному сообществу в области атмосферных наук с конца 1960-х годов.

Протоколы

NSFNET использует протоколы TCP/IP из набора DARPA InterNet в качестве начального стандарта. Система нацелена на постепенное принятие международных стандартов по мере их формирования. Протоколы связывают сети, основанные на разных технологиях и протоколах соединения, и предоставляют унифицированный набор транспортных и прикладных протоколов. По мере развития NSFNET рядовой пользователь, работающий за терминалом или рабочей станцией, сможет подключаться к различным вычислительным ресурсам — в том числе к суперкомпьютерным центрам — и запускать интерактивные и пакетные задания, получать результаты, передавать файлы и общаться с коллегами по всей стране посредством электронной почты. Большинство исследователей будут подключены либо через терминал, связанный с локальным суперминикомпьютером, либо через графическую рабочую станцию. Эти устройства подключаются к локальной вычислительной сети, которая в свою очередь подключена к кампусной сети, а через шлюзовую систему — к широкозонной сети.

Управление

Временное управление NSFNET разделено между четырьмя организациями: Университет Иллинойса (общее руководство проектом и сетевая инженерия), Корнеллский университет (эксплуатация сети и первоначальная техническая поддержка), Институт информационных наук Университета Южной Калифорнии (совершенствование протоколов и техническая поддержка высшего уровня) и Университетская корпорация атмосферных исследований (управление Сетевым сервисным центром NSF по контракту с BBN Laboratories, Inc.).

Сетевой сервисный центр NSF

Сетевой сервисный центр NSF (NNSC) предоставляет общую информацию о NSFNET, включая сведения о состоянии компонентных сетей, поддерживаемых NSF, и суперкомпьютерных центрах. NNSC расположен в BBN Laboratories Inc. в Кембридже (штат Массачусетс) и является спонсируемым NSF проектом Университетской корпорации атмосферных исследований.

NNSC располагает информацией и документами как в онлайн-формате, так и в печатном виде; в его планах — распространение новостей через сетевые списки рассылки, бюллетени, информационные письма и онлайн-отчёты. NNSC также ведёт базу данных контактных лиц и источников дополнительной информации о компонентных сетях NSFNET и суперкомпьютерных

центрах.

Если потенциальные или действующие пользователи не знают, к кому обратиться по вопросам использования NSFNET, им следует связаться с NNSC. NNSC отвечает на общие вопросы, а по детальным вопросам, касающимся конкретных компонентов NSFNET, помогает найти подходящий контакт для получения дальнейшей помощи.

Кроме того, NNSC будет содействовать развитию и выявлению локальной технической поддержки кампусных сетей в интересах будущих пользователей NSFNET.

Подключение к NSFnet

NSFNET входит в совокупность взаимосвязанных IP-сетей, именуемых InterNet. IP (Internet Protocol) — это сетевой протокол, позволяющий объединять разнородные сети в единую виртуальную сеть. TCP (Transmission Control Protocol) — транспортный протокол, реализующий механизмы обнаружения потери пакетов и ошибок, необходимые для поддержания надёжного соединения между двумя точками сети. Таким образом, TCP/IP обеспечивает надёжную передачу данных между разнородными компьютерами в различных сетях. Примером приложения, использующего TCP/IP, является TELNET, который предоставляет сервис виртуального терминала через сеть.

К Интернету могут подключаться только IP-сети; поэтому организация, планирующая использовать NSFnet, должна либо иметь собственную IP-сеть, либо иметь доступ к таковой. Многие крупные университеты и технические компании уже имеют каналы в InterNet. Наиболее вероятными источниками сведений об IP-подключении или о существующих локальных каналах являются факультет информатики университета или отдел инженерной поддержки компании. Потенциальные пользователи могут обратиться в NNSC с просьбой выяснить, подключена ли та или иная организация к Интернету.

Если у организации нет IP-канала, его можно получить несколькими способами:

• NSF реализует программу финансирования подключения организаций к региональным/государственным/общественным сетям NSF, входящим в NSFNET. Подробнее об этой программе можно узнать в NNSC.

• Компьютерная научная сеть (CSNET) предоставляет шлюзовые услуги для нескольких IP-сетей, включая NSFNET. Для получения услуг CSNET организация должна стать её членом.

• Пользователи могут получить доступ к NSFNET через аккаунты с разделением времени на машинах других организаций — например, местных университетов или компаний.

Некоторые суперкомпьютерные центры поддерживают системы доступа, отличные от NSFNET, — такие как Bitnet, коммерческие сети X.25 и коммутируемые линии, не использующие IP-протоколы. Пользовательские службы суперкомпьютерных центров могут предоставить дополнительную информацию об этих альтернативах (см. список).

Компонентные сети NSF

Государственные и региональные сети

• BARRNET (Bay Area Regional Research Network — Региональная исследовательская сеть района залива, Калифорния)

• MERIT (Michigan Educational Research Network — Мичиганская образовательно-исследовательская сеть)
• MIDNET (Midwest Network — Сеть Среднего Запада)
• NORTHWESTNET (Северо-западные штаты)
• NYSERNET (New York State Educational and Research Network — Образовательно-исследовательская сеть штата Нью-Йорк)
• SESQUINET (Texas Sesquicentennial Network — Техасская Полуторасотлетняя сеть)
• SURANET (Southeastern Universities Research Association Network — Сеть Ассоциации исследовательских университетов Юго-Востока)
• WESTNET (Юго-западные штаты)

Консорциумные сети

• JVNCNET связывает Национальный суперкомпьютерный центр имени Джона фон Неймана в Принстоне (штат Нью-Джерси) с рядом университетов.
• PSCAANET — сеть группы академических партнёров Питтсбургского суперкомпьютерного центра.
• SDSCNET базируется в Суперкомпьютерном центре Сан-Диего.

COSMOS — Компьютерная система для работы с мэйнфреймами. Часть первая

Автор: King Arthur

Введение

На протяжении последнего десятилетия компьютеры играют всё возрастающую роль в хранении и поиске информации. В большинстве компаний компьютеризированные базы данных вытеснили значительную часть бумажных архивов. Если раньше на поиск нужных данных в стопках бумаг уходило до десяти минут, то теперь ту же информацию можно извлечь из компьютера за долю секунды.

Прежде конфиденциальные сведения вполне можно было считать «защищёнными» в картотечном шкафу — единственным способом добраться до них был физический доступ к папкам. Сегодня человек с компьютерным терминалом и модемом способен сделать один телефонный звонок и получить доступ к частным записям. Печально, что существуют «хакеры», пытающиеся получить несанкционированный доступ к компьютерам. Но не менее печально то, что большинства зафиксированных взломов можно было бы избежать, уделяя защите компьютеров чуть больше внимания и здравого смысла.

Хакеры

Телефонные компании Bell (BOC) зафиксировали немало случаев компьютерных преступлений, однако трудно судить о реальном числе взломов. Следует помнить: в официальную статистику попадают лишь те инциденты, которые были обнаружены. В беседе с анонимным хакером мне рассказали об одном взломе, который, возможно, так и не был никуда сообщён. «Мой друг получил номер, когда ошибся при наборе делового офиса — именно так мы поняли, что это телефонная компания. Судя по всему, тот Unix был частью какой-то крупной компьютерной сети Bellcore», — рассказывает хакер.

По его словам, эта система была одной из многих, которые различные BOC использовали для того, чтобы крупные клиенты Centrex могли самостоятельно перекомпоновывать свои группы Centrex. На системе обнаружился текстовый файл с телефонными номерами и паролями от нескольких разработческих систем Bellcore. «На системе Bellcore в Нью-Джерси, которая называлась CCRS, мы нашли список из примерно двадцати систем COSMOS… Номера, пароли и коды Wire Center со всей страны!» — добавляет он. — «Если точнее — из пяти штатов».

Хакеру удалось получить доступ к исходной Unix-системе, потому что, по его словам, «те ребята оставили все дефолтные пароли рабочими». Войти в систему удалось с именем пользователя `games` и паролем `games`. «Оказавшись внутри, мы обнаружили, что у большого количества учётных записей паролей нет вовсе. Mary, John, test, banana, system — вот лишь несколько примеров». Оттуда удалось в конечном счёте добраться до нескольких баз данных COSMOS — с доступом ко ВСЕМ файлам и ресурсам системы.

COSMOS

COSMOS — аббревиатура от COmputer System for Mainframe OperationS («Компьютерная система для работы с мэйнфреймами») — это пакет баз данных, поддержку которого в настоящее время осуществляет Bellcore. COSMOS используется каждой BOC, а также компаниями Cincinnati Bell и Rochester Telephone. COSMOS заменяет бумажное делопроизводство и другие механизированные системы учёта в сфере управления инфраструктурой. Изначально COSMOS создавался для того, чтобы снизить нагрузку на Главный распределительный фрейм (MDF) за счёт поддержания кратчайших перемычек.

Сегодня система умеет поддерживать балансировку нагрузки на коммутаторе, распределять офисное оборудование, коммутационные пары, мостовые выключатели и тому подобное. Дополнительные приложения позволяют COSMOS участвовать в «переключении» на новый коммутатор или даже генерировать сообщения о последних изменениях для ввода в электронные коммутаторы. Чаще всего COSMOS используется для подключения новых абонентов и обслуживания существующих следующими подразделениями: кросс (MDF), Центр присвоения номеров абонентских линий (LAC), Центр обработки памяти о последних изменениях (RCMAC), центр управления сетью и служба ремонта.

В следующем году COSMOS отметит своё 15-летие — весьма значительный срок для компьютерной программы. Первая версия, или «generic», COSMOS была выпущена Bell Laboratories в 1974 году. В марте того же года New Jersey Bell стала первой компанией, запустившей COSMOS, — в Пасейике, штат Нью-Джерси. Вскоре к системе присоединились Pacific Telesis, NYNEX, Southern Bell и многие другие BOC. Southwestern Bell выжидала до 1977 года, однако Wire Center в Пасейике, штат Нью-Джерси, работает под управлением COSMOS и по сей день.

Изначально COSMOS функционировал на миникомпьютере DEC PDP 11/45. Пакет был написан на Fortran и работал под управлением операционной системы COSNIX. Впоследствии его адаптировали для работы на DEC PDP 11/70 — машине большей мощности. Беверли Крус, сотрудник технического персонала отдела проектирования систем COSMOS в Bellcore, поясняет: «COSNIX — это производная от Unix 1.0; она выросла из оригинального Unix, но была адаптирована для проекта COSMOS. Она во многом схожа с Unix, однако больше напоминает ранние версии, нежели нынешние… Приложение COSMOS теперь работает на другом оборудовании под управлением стандартного Unix».

«Новейшая версия COSMOS работает под управлением стандартной операционной системы Unix System V. Мы будем сертифицировать её для использования на конкретных процессорах, исходя из потребностей наших клиентов», — говорит Эд Пиннес, районный менеджер отдела проектирования систем COSMOS в Bellcore. Эта версия COSMOS под Unix написана на языке C. В настоящее время COSMOS доступна для суперминикомпьютера AT&T 3B20, работающего под управлением Unix System V. «Всего существует более 700 систем COSMOS, подавляющее большинство которых — DEC PDP 11/70. Число постоянно меняется: компании начинают заменять 11/70 другими машинами», — отмечает Крус.

В 1981 году Bell Laboratories представила для телефонных компаний интегрированный системный пакет под названием Facility Assignment Control System (FACS). FACS — это сеть систем, регулярно обменивающихся информацией. В её состав входят: COSMOS, Loop Facilities Assignment and Control System (LFACS), Service Order Analysis and Control (SOAC) и Work Manager (WM). Заявка на обслуживание из делового офиса вводится в SOAC. SOAC анализирует заявку и через WM направляет запрос на распределение в LFACS. WM выступает в роли коммутатора пакетов, передавая сообщения между остальными компонентами FACS. LFACS назначает объекты распределительной сети (кабели, терминалы и т. д.) и возвращает заявку в SOAC. Получив информацию от LFACS, SOAC направляет запрос на распределение в COSMOS. COSMOS отвечает данными о распределении оборудования центрального узла: коммутационного оборудования, оборудования передачи, мостовых выключателей и тому подобного. SOAC собирает

всю информацию от LFACS и COSMOS, добавляет её к заявке и отправляет её дальше по назначению.

Компьютерная безопасность

Телефонные компании, судя по всему, несут основной удар попыток несанкционированного доступа. Огромное число сотрудников и размеры большинства телефонных компаний крайне затрудняют контроль над каждым человеком и каждым процессом. В ходе изучения вопросов компьютерной безопасности стало очевидно, что COSMOS является привлекательной целью для хакеров. «Количество систем COSMOS, на большинстве из которых есть коммутируемый доступ… создаёт почву для огромного числа возможных взломов», — говорит Крус. Именно поэтому компаниям особенно важно научиться защищать себя.

«COSMOS — это власть, вся эта штука — сплошной трип власти, чувак. Это как Большой Брат: видишь в компьютере номер какого-то типа, который тебе не нравится, — создаёшь заявку на отключение; COSMOS недостаточно умён, чтобы отличить тебя от настоящего сотрудника телефонной компании», — говорит один хакер. «Я думаю, они получают то, что заслуживают: там реально катастрофа с безопасностью. Если такие ребята, как мы, могут так легко получить доступ, представьте настоящего врага — русских», — шутит другой.

Большинство попыток несанкционированного доступа объясняется ошибками системных операторов, и столь же многие — виной пользователей этих систем. Если вы будете на шаг впереди хакеров, заблаговременно распознаете эти проблемы и будете следить за появлением аналогичных уязвимостей, вы сбережёте своей компании немало хлопот.

«В Калифорнии мой знакомый умел находить пароли в мусоре. Компьютер должен был распечатать поверх пароля несколько случайных символов. Вместо этого пароль печатался ПОСЛЕ них», — рассказывает один хакер. У некоторых пользователей COSMOS есть печатающие терминалы с полудуплексным режимом. При запросе пароля COSMOS должен вывести на печать ряд символов, а затем отправить символы забоя. После этого пользователь вводит свой пароль. Когда пароль печатается поверх других символов, его не видно. Если же пароль выводится после них, значит, терминал не принимает символы забоя должным образом.

Другая серьёзная проблема — отсутствие защиты паролей. Как уже упоминалось применительно к CCRS, на некоторых системах у многих учётных записей паролей нет вовсе. «В COSMOS есть стандартизированные имена учётных записей. Это облегчает системным операторам отслеживание, кто пользуется системой. Например: все учётные записи, принадлежащие кросс-комнате, содержат MF. Скажем, MF01 — сразу понятно, что она относится к кросс-комнате. (MF расшифровывается как Main Frame, главный фрейм.) Большинство таких имён, судя по всему, одинаковы на большинстве систем COSMOS повсюду. В одном городе ни у одной из этих пользовательских учётных записей нет паролей. Достаточно знать имя учётной записи — и ты внутри. В другом городе, который останется безымянным, пароли СОВПАДАЮТ С ЧЁРТОВЫМИ ИМЕНАМИ! Например, у MF01 пароль MF01. Эти ребята, похоже, вовсе не заботятся о безопасности».

Одна из самых серьёзных, и, на мой взгляд, пугающих проблем — то, что хакеры называют «социальной инженерией». Социальная инженерия — это, по существу, искусство выдавать себя за другого человека ради получения конфиденциальной информации. «Я знаю одного парня. Он может провести кого угодно, лучший болтун из всех, кого я видел. Он звонит в какой-нибудь офис телефонной компании — например, в бюро ремонтного обслуживания, которое использует COSMOS. Мы выяснили, что большинство операторов в службе ремонта не особенно сообразительны». По словам хакера, разговор, как правило, шёл по следующей схеме:

Хакер: Привет, это Фрэнк из компьютерного центра COSMOS. У нас возникла проблема с записями, и мне интересно, не могли бы вы помочь?

Сотрудник телефонной компании: О, что случилось?

Х: Похоже, мы потеряли часть пользовательских данных. Надеюсь, если я смогу устранить проблему, вы сегодня не потеряете время доступа. Не могли бы вы назвать своё системное имя входа?

С: Ну, я использую RS01.

Х: Хм, это может создать проблему. Вы не могли бы сообщить мне пароль и Wire Center, которые вы используете с ним?

С: Ну, я просто ввожу s-u-c-k-e-r как пароль, а мои Wire Center'ы: TK, KL, GL и PK.

Х: Вы звоните в систему или у вас только терминалы с прямым подключением?

С: Ну, когда я включаю машину, у меня прямое соединение. Она просто просит войти в систему. Но я знаю, что в задней комнате им приходится что-то набирать. Подождите, дайте проверю. (Три минуты спустя…) Она говорит, что просто звонит по 555-1212.

Х: Хорошо, думаю, я всё уладил. Спасибо, удачного дня.

С: Отлично, значит, у меня не будет никаких проблем?

Х: Нет, но если возникнут — просто позвоните в компьютерный центр, мы разберёмся.

С: О, спасибо, дорогой. Удачного дня!

«Работает не всегда, но нередко срабатывает. Думаю, они просто не ожидают звонка от человека, который на самом деле не является сотрудником их компании», — говорит хакер. «Однажды я применил социальную инженерию к центру управления COSMOS. Они дали мне номера коммутируемого доступа для нескольких систем и даже сообщили один пароль. Я сказал, что звоню из RCMAC и не могу войти в COSMOS», — добавляет другой.

Последний пример — наглядная иллюстрация того, что я имею в виду, говоря о предотвратимости этих проблем при должной осторожности и здравом смысле в вопросах компьютерной безопасности. «Иногда, когда мы хотим попасть в COSMOS, но у нас нет пароля, мы звоним на коммутируемый номер COSMOS примерно в пять часов вечера. Чтобы выйти из COSMOS, нужно нажать CONTROL-Y. Если этого не сделать, следующий позвонивший продолжит сеанс с того места, где его прервали. Очень часто люди забывают выйти из системы. В спешке, торопясь домой, они просто выключают терминалы».

Приведённые примеры не исчерпывают всех способов, которыми хакеры проникают в системы, однако большинство описанных проблем может существовать вне зависимости от того, какие именно системы использует ваша компания. Во второй статье рассматриваются решения этих проблем.

Основные концепции трансляции

Автор: The Dead Lord и The Chief Executive Officers

17 февраля 1989 года

Этот материал предназначен для хардкорных хакеров, вошедших в мир коммутаторов ESS. Информация здесь полезна и ценна, хотя и не бесценна. Вы можете с лёгкостью пользоваться преимуществами доступа к коммутатору, даже зная только RC:LINE, но чтобы по-настоящему изучить систему изнутри и снаружи, нужно освоить концепции трансляции.

В электромеханических коммутаторах переключение напрямую управлялось тем, что набирал абонент. Если набиралась цифра 5, селектор перемещался на 5 позиций, и так далее. Не было никаких устройств хранения цифр — ни регистров, ни сендеров. По мере роста сети такой подход становился неэффективным, и в эксплуатацию были введены коммутирующие системы с накоплением и декодированием цифр. В такой схеме абонент набирает номер, который записывается в регистр, или сендер. Затем сендер использует декодер и подаёт содержимое регистра на вход. Декодер преобразует входные данные в формат, пригодный для установления соединения, и возвращает результат трансляции обратно в устройство хранения цифр. Это упрощённый пример трансляции: на входе — набранные цифры, на выходе — маршрутизируемая информация. Но он показывает суть трансляции: преобразование информации из одной формы в другую.

Когда коммутатор 1 ESS был впервые испытан в Моррисе, штат Иллинойс, в 1960 году, он ввёл метод коммутации под названием «Управление с хранимой программой» (Stored Program Control). Вместо того чтобы функции коммутации и логики выполнялись аппаратно, они были реализованы через компьютерные программы. Это значительно расширило функцию трансляции. Поскольку вызовы обрабатываются множеством программ, каждой из них необходимо предоставлять информацию. Например, когда абонент снимает трубку, коммутатору нужно знать: запрещён ли исходящий сервис, ведётся ли наблюдение за линией, класс линии, специальные возможности оборудования и т. д. Номер линейного оборудования (LEN) подаётся на вход программы трансляции. Транслятор преобразует LEN и выдаёт ответы на эти и другие важные вопросы в закодированной форме, пригодной для использования центральным процессором коммутатора.

Если звонок является межстанционным, первые три набранные цифры подаются транслятору на вход и преобразуются в индекс маршрута и, возможно, другую информацию. Индекс маршрута, в свою очередь, подаётся на вход другому транслятору, который выдаёт: какой транк использовать (идентификатор транка), идентификатор передатчика, альтернативный маршрут и т. д. Таким образом, в ранних системах трансляция была однократной операцией, тогда как в системах с хранимой программой (SPCS) функция трансляции используется многократно.

В коммутаторе 1 ESS данные трансляции хранятся на магнитных картах памяти в хранилище программ (program store). Однако, поскольку данные трансляции постоянно изменяются, предусмотрена возможность хранить изменения в области памяти хранилища вызовов (call store), которая называется областью последних изменений (recent change area, RC). Со временем изменения переписываются из хранилища вызовов в хранилище программ с помощью устройства записи на магнитные карты.

В коммутаторе 1A ESS данные трансляции хранятся в неудвоенном хранилище вызовов, с резервным копированием в виде дискового хранилища, называемого файловым хранилищем (file store). Кроме того, с области трансляции хранилища вызовов создаются магнитные ленты. При внесении изменения в трансляцию оно сначала записывается в дублированную копию хранилища

вызовов. После проверки корректности изменения (формата и всего остального) оно помещается в неудвоенную копию хранилища вызовов. Затем изменение также записывается в набор дисковых файлов файлового хранилища. Перед записью новых данных старые данные записываются в часть дискового файла, называемую «rollback» (откат).

DATA	1 ESS	1A ESS
Transient Information	Duplicated Call Store	Duplicated Call Store
Generic Program	Duplicated Program Store	Program Store
Parameter Table	Duplicated Program Store	Unduplicated Call Store
Translation Information	Duplicated Call Store + Program Store	Unduplicated Call Store

Временная информация (Transient Information): Телефонные звонки или передача данных в процессе; текущее состояние всех линий, соединительных устройств (junctors) и транков в офисе.

Базовая программа (Generic Program): Операционный интеллект системы. Управляет такими действиями, как сканирование линий и транков, установление и разрыв соединений и т. д.

Таблица параметров (Parameter Table): Информирует базовую программу о размере и составе офиса. Включает элементы оборудования (стойки и блоки), распределение хранилища вызовов (регистры вызовов, буферы, очереди и т. д.) и параметры офиса (дни переключения лент AMA и т. д.).

Информация трансляции (Translation Information): Ежедневно изменяемые данные, к которым обращаются программы-трансляторы. Включает также таблицы форм и списки, называемые «трансляторами», связанные в иерархическую структуру.

Это цитата из книги «Engineering and Operations in the Bell System», страницы 415–416:

> *«1 ESS включает полностью дублированный блок центрального процессора No. 1 (Central Control включает базовую программу), шину хранилища программ, шину хранилища вызовов, хранилища программ и хранилища вызовов. 1 ESS использует модули хранилища программ с постоянными магнитными твистерами в качестве основных элементов памяти. Они обеспечивают память, принципиально доступную только для чтения, с циклом работы 5,5 микросекунды. Хранилище вызовов обеспечивает "черновую", то есть временную дублированную, память.*
> *Как и в 1 ESS, центральный процессор 1A имеет ЦПУ, шину хранилища программ и шину хранилища вызовов, которые полностью дублированы. Однако процессор 1A использует читаемую и записываемую память как для хранилища программ, так и для хранилища вызовов, а цикл составляет 700 наносекунд. При этом хранилища программ не полностью дублированы, но для надёжности предусмотрены 2 резервных хранилища. Часть хранилища вызовов дублирована, однако определённые программы распознавания ошибок, параметрическая информация и данные трансляции предоставляются только в одном экземпляре. Дополнительная копия недублированного хранилища программ и хранилища вызовов хранится в файловом хранилище.»*

Область трансляции хранилища программ в 1 ESS и область трансляции недублированного хранилища вызовов в 1A ESS содержат всю информацию, которая может изменяться день ото дня для данного офиса. Вот перечень того, что хранится в области трансляции:

• Номер линейного оборудования (LEN), абонентский номер (DN), назначения транков (объяснение далее).
• Коды офиса.
• Информация о тарификации и маршрутизации.
• Информация об измерении трафика.
• Сопутствующая прочая информация для обработки вызовов и тарификации.

Хранилище вызовов можно представить как ОЗУ: оно заполнено, пока ESS находится под питанием.

Хранилище программ подобно ПЗУ: оно физически записывается на магнитные карты. Файловое хранилище — это просто информация на магнитных лентах (или дисковых накопителях). Все изменяемые данные (тарификация и маршрутизация, функции абонентов, выбор транков, альтернативные пути и т. д.) называются данными трансляции и хранятся в области трансляции.

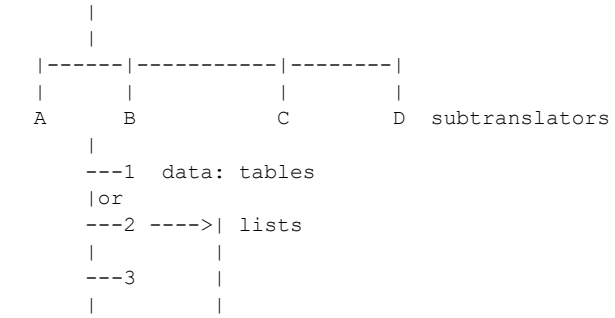
Изменения в трансляции называются последними изменениями (recent changes) и хранятся в области последних изменений (recent change area).

Ещё раз подчеркну: эта статья является своего рода «мастер-файлом» для хакеров, интересующихся ESS. Если концепции кажутся слишком сложными — не паникуйте. Знания приходят со временем. Не расстраивайтесь, если что-то не усваивается сразу.

Данные трансляции хранятся в виде таблиц или списков. Каждая таблица связана в иерархическую структуру. Таблицы верхнего уровня иерархии содержат указатели (адреса) на таблицы нижнего уровня. Таблицы нижнего уровня содержат фактические данные.

Большинство трансляторов разбиты на субтрансляторы, которые связаны головной таблицей (Head Table, HT). HT указывает на различные ST'шки, хранящиеся в памяти, — так же, как оглавление книги указывает на страницы каждой главы. Таким образом, при добавлении новой функции достаточно добавить новую запись в HT и указать этой записью на новый ST.

Входные данные трансляции делятся на 2 части: селектор и индекс. Селектор определяет, к какому ST обратиться, а индекс — к какому элементу (номеру слова) в этом ST. В некоторых случаях информация трансляции не умещается в отведённое для ST место, поэтому могут потребоваться указатели на вспомогательные блоки и/или таблицы расширения. Можно провести аналогию с программой на BASIC, где GOSUB указывает на подпрограмму по адресу 4000. Если подпрограмма занимает 100 байт, а места есть только 75, нужно выдать ещё один GOSUB, чтобы указать на остаток подпрограммы. Таким образом, полный транслятор является довольно большой единицей — он может иметь головную таблицу, субтрансляторы, вспомогательные блоки, сокращённые коды, списки, субвспомогательные блоки и таблицы расширения. Пример ниже показывает нестандартную функцию вызова, существующую в 5 ESS: Dog Control Frequency, «DCF». На диаграмме DCF представляет головную таблицу и содержит список указателей, определяющих расположение субтрансляторов «A» — «D». Поле данных «2» в субтрансляторе «D» слишком мало для хранения всей подпрограммы, поэтому была создана таблица расширения «2A» для размещения полной программы.



```
  etc       % /  expansion
2-Atable
```

Программы ESS обращаются к трансляторам, находя их восьмеричный адрес в главной головной таблице (Master Head Table, MHT), которую также называют базовым транслятором (Base Translator).

MHT коммутатора 1 ESS

В коммутаторе 1 ESS имеется 2 копии MHT: одна в хранилище программ и одна в хранилище вызовов. Копия в хранилище вызовов используется в обычном режиме, так как память хранилища вызовов имеет более короткий цикл. Копия в хранилище программ служит резервной. Длина MHT составляет 338 байт (23-битных байта), и, как упоминалось, она используется в качестве своеобразного справочника для поиска трансляторов. MHT может указывать на начальные адреса головных таблиц (которые указывают на трансляторы) или на таблицы и списки. Головные таблицы указывают на субтрансляторы. Субтрансляторы могут указывать на вспомогательные блоки и блоки расширения, списки или таблицы.

Существует ещё одна главная головная таблица, называемая вспомогательной главной головной таблицей (Auxiliary Master Head Table, AMHT), которая указывает на другие трансляторы. Имеется 2 копии AMHT: одна в хранилище программ и одна в хранилище вызовов. AMHT находится через MHT, и для интересующихся: адрес AMHT расположен в 28-м байте MHT. MHT фиксирована: первый байт ВСЕГДА является адресом транслятора DN. Последний байт ВСЕГДА является адресом головной таблицы JNNL в JNNT/JCN (объяснение далее). ESS нужна таблица, чтобы читать эту таблицу. Иначе как она знала бы, куда ведёт каждый байт? В параметрической области хранилища программ по (восьмеричному адресу) 1105615 находится «восьмеричная Т-программа чтения», используемая для чтения главной головной таблицы. Этот адрес хранится в базовой программе.

1A ESS

Байт хранилища вызовов коммутатора 1A ESS содержит 26 бит, пронумерованных от 0 до 25, — это куда больше, чем может предложить какой-нибудь Apple. Биты 24 и 25 используются для чётности и не задействуются для данных. Это приводит к тому, что известно как K-код. Нет, K-код используется не жалкими программными пиратами категории K-rad, а нами — хакерами ESS. Каждый K-код хранилища вызовов содержит 65 536 байт и может рассматриваться как «страница» памяти.

Итак, данные трансляции хранятся в недублированном хранилище вызовов. Напомню, мы по-прежнему говорим о 1A ESS. В базовом программном обеспечении 1AE6 и более ранних версиях недублированное хранилище вызовов начинается с K-кода 17, и по мере заполнения данными трансляции расширяется вниз: K-код 16, 15, 14 и т. д. В базовом ПО версии 7 и выше хранилище вызовов значительно увеличилось благодаря огромному блоку расширения памяти. В ранних версиях ПО всё хранилище вызовов и хранилище программ должно было уместиться в 38 K-кодах. В более поздних версиях для хранилища вызовов выделено 38 K-кодов (разделённых между дублированным и недублированным), и ещё 38 K-кодов — для хранилища программ.

Не все K-коды могут быть задействованы, так что это не обязательно полные 38 K-кодов — нельзя же иметь всю память и при этом её использовать целиком. Тем не менее, поскольку в базовом ПО 1A E7 и выше хранилище вызовов очень велико, удобно разделить его на 3 части: «дублированное хранилище вызовов» (DCS), расположенное в самом верху карты памяти; «низкое

недублированное хранилище вызовов» (LUCS), расположенное в средней части; и «высокое недублированное хранилище вызовов» (HUCS). Область LUCS начинается с K-кода 17 и расширяется вниз по мере заполнения (тщательно следя за тем, чтобы не попасть в область DCS). Область HUCS начинается с K-кода 37 и расширяется вниз до K-кода 20, не задевая LUCS. Трансляторы классифицируются как трансляторы HUCS или LUCS (но не оба сразу).

Трансляторы LUCS не фиксированы: они могут находиться в любом месте области, при условии идентификации через MHT. Трансляторы HUCS могут быть как фиксированными, так и нет. Заметим, что в базовом ПО 1AE6 и более ранних версиях такого разграничения нет, так как памяти недостаточно для его практического применения. Что касается расположения MHT: в базовом ПО 1AE6 и более ранних версиях она находится в K-коде 17 по восьмеричному адресу 3724000 и имеет длину 1376 байт. В более поздних версиях MHT была перемещена в K-код 37 по восьмеричному адресу 7720000 и имеет длину 3424 байта.

Типы трансляторов

Как было сказано, трансляторы принимают данные на вход и преобразуют их в другую форму для вывода. Все трансляторы существуют в виде иерархических списков и таблиц. На коммутаторах 1A они располагаются в хранилище вызовов, на коммутаторах 1 — в хранилище программ. Данные верхнего уровня транслятора указывают на расположение данных нижнего уровня. Данные нижнего уровня содержат фактическую информацию. Различные трансляторы находятся через главную головную таблицу, содержащую указатели на все трансляторы в системе. Переводимые данные являются изменяемыми данными.

Например:

• номер линейного оборудования
• абонентский номер
• 3/6-значные коды
• номер транковой сети → номер группы транков
• номер транковой сети → номер периферийного оборудования

Существует два типа трансляторов: многоуровневые и расширяемые. Многоуровневые трансляторы содержат максимум шесть уровней информации в виде связанных иерархических таблиц:

1. Головная таблица (Head Table)
2. Субтранслятор (Subtranslator)
3. Первичное слово трансляции (Primary Translation Word)
4. Вспомогательный блок или таблица расширения (Auxiliary Block / Expansion Table)
5. Список (List)
6. Субвспомогательный блок (Subauxiliary Block)

(1) Головная таблица (HT): HT — это «справочник» транслятора. Она содержит адреса или указатели на каждый субтранслятор.

(2) Субтранслятор: ST'шки являются основными подразделениями: по мере роста офиса или добавления новых функций число ST'шек увеличивается. Например, существует один транслятор на каждые 1000 абонентских номеров, поэтому при росте офиса с 3000 до 8000 линий необходимо добавить 5 дополнительных субтрансляторов. Входные данные для трансляции должны содержать 2 элемента: селектор и индекс. Селектор содержит информацию о том, какой субтранслятор использовать (в случае DCF это A, B, C или D). Индекс показывает, к какому элементу или слову в данном субтрансляторе обращаться. В примере с DCF, если селектор — «D», индекс может быть 1, 2, 3 и т. д.

(3) Первичное слово трансляции (PTW): Каждый индекс указывает на PTW — байт информации. Нередко достаточно 1 байта информации (помните, что каждый байт состоит из 23 бит!). Если данные не хранятся в PTW, там будет адрес, указывающий на вспомогательный блок или таблицу расширения, где и находятся данные. ESS определяет, содержит ли байт данные или адрес, по следующему признаку:

• 1 ESS: 3 наиболее значимых бита равны 0.
• 1A ESS: 4 наиболее значимых бита равны 0.

Таким образом, если все 3 (или 4 для 1A) наиболее значимых бита содержат нули, слово интерпретируется как адрес. (Кто-нибудь хочет загнать коммутатор ESS в бесконечный цикл????)

(4) Вспомогательный блок: Первый байт в AB содержит длину блока. Этот байт называется номером слова (WRDN) и используется ESS, чтобы знать, где заканчивается вспомогательный блок. Помните, что когда ESS читает данные, она видит лишь:

```
11000101100010101010010010111001001010100010101010010010111
```

Поэтому, чтобы остановиться в конце блока, необходимо наличие числа WRDN.

(5) Список: Список используется, когда нужна дополнительная информация сверх стандартной, хранящейся во вспомогательном блоке. Список, как и ST, имеет связанный индекс. Адрес списка находится в AB, а индекс указывает, какой элемент данных в списке следует рассмотреть. Хорошим примером информации, хранящейся в списке, является список ускоренного набора (speed calling list).

(6) Субвспомогательный блок: Список достаточен лишь для хранения 7-значного номера телефона, и если необходимо хранить больше информации (например, 10-значный номер или идентификатор транка), в списке хранится адрес, указывающий на SB, который функционирует аналогично AB.

Транслятор расширения

Транслятор расширения имеет одну таблицу (называемую таблицей расширения). Этот тип транслятора получает на вход только индекс, поскольку представляет собой просто набор слов. У него могут быть вспомогательные блоки, если места, отведённого слову, недостаточно.

Область последних изменений хранилища вызовов (1 ESS)

Область последних изменений состоит из:

• первичной области последних изменений
• вспомогательной области последних изменений
• последних изменений, инициированных абонентом (CORC)

Начальные и конечные адреса этих областей RC хранятся в MHT. Первичная область последних изменений используется для хранения изменений, затрагивающих первичные слова трансляции. Каждое изменение хранится в первичном RC-регистре, состоящем из двух 23-битных байтов. Эти два байта содержат биты состояния, адрес первичной трансляции в хранилище программ и адрес первичного слова трансляции (PTW) в хранилище вызовов. Первый байт регистра является «адресным словом» (AW), второй — новым первичным словом трансляции. При просмотре AW биты 22 и 21 указывают, какой тип последнего изменения реализуется:

```
11: временное (не переносится в хранилище программ)
10: постоянное (переносится в хранилище программ)
```

```
01: отложенное (ещё не активно)
00: удалённое (это место свободно)
```

PTW (сокращения делают всё НАМНОГО проще) содержит данные трансляции или адрес вспомогательного RC (TAG). Определить, являются ли данные RC или адресом, можно, рассмотрев биты с 22 по 18: если они равны 0, байт содержит адрес, хранящийся в битах с 17 по 0.

Прослушка телефонов: подпольная индустрия телекоммуникаций

Автор: Split Decision

На фоне сегодняшней повсеместной инсайдерской торговли, выкупов за счёт заёмных средств и слияний неудивительно, что внутри телекоммуникационной отрасли возникла новая подпольная индустрия — слежка и прослушивание.

Жучки стоят дёшево (от 30 долларов) и могут быть установлены буквально за 10 секунд. И можно не сомневаться, что эти расходы ничтожны по сравнению с выгодой от того, чтобы узнать планы поглощения, маркетинговые стратегии и разработки новых продуктов конкурентов.

По словам Фрица Ланга из компании Tactical Research Devices (Брюстер, штат Нью-Йорк), на американском рынке сложилась настоящая эпидемия прослушки. Агентства контрнаблюдения вроде TRD расплодились повсюду. Они ищут подслушивающую аппаратуру и уведомляют клиента, если его телефон прослушивается. Дальнейшие меры — уже дело клиента.

Каждый сотрудник TRD — бывший оперативник ЦРУ или ФБР. В своё время они устанавливали жучки по заданию дяди Сэма. Поскольку устанавливать их для кого-либо ещё незаконно, эти люди теперь занимаются контрнаблюдением: выявляют подслушивающие устройства — а порой и тех, кто их поставил, — в интересах корпоративных клиентов TRD.

Куда ставят жучки?

Ваш **ТЕЛЕФОН**, разумеется, — удобнейшее место для установки подслушивающего устройства. Но это не означает, что незаконная прослушка ограничится только телефонными разговорами.

Электронные телефоны имеют микрофоны, которые остаются «живыми» даже когда трубка лежит на рычаге. Прикрепите к микрофону усилитель и передатчик — и получите постоянное наблюдение за всеми разговорами в комнате, независимо от того, снята ли трубка в данный момент.

Стремительно набирает популярность среди нынешних телефонных «жучковщиков» замена телефонной мембраны на внешне неотличимый аналог, содержащий крошечный передатчик и выглядящий в точности как стандартная мембрана аппарата серии 2500. Пока жертва отходит к кулеру или в туалет, достаточно одной минуты, чтобы незаметно произвести подмену.

ГРОМКОГОВОРИТЕЛИ — ещё одно излюбленное место для прослушки, поскольку они способны улавливать разговоры, даже когда не используются. Системы оповещения, трансляция музыки и телефонные системы — все они содержат тот или иной усилитель, которым злоумышленник может воспользоваться в своих целях.

ЛИНЕЙНЫЕ ПЕРЕХВАТЧИКИ дают слушателям более широкий охват: из одного поста прослушивания можно контролировать не только онлайн-коммуникации.

Впрочем, число мест, где можно обнаружить жучок, ограничено лишь фантазией установщика. Выключатели света, розетки, часы, калькуляторы, ножки деревянных стульев, степлеры, пепельницы, нижняя поверхность унитаза — всё это уже было признано благодатной почвой для маленьких «паразитов».

Инструменты для поиска жучков

Специалисты TRD используют запатентованный приёмник поиска устройств наблюдения для обнаружения жучков. Приёмник работает в широком диапазоне радиочастот — от 25 кГц до 7 ГГц.

Если на объекте обнаруживается неучтённое радиочастотное излучение, приёмник отображает его на небольшом анализаторе спектра. Затем сигнал прослеживается до своего неизбежного источника — жучка.

Для поиска комнатных жучков также применяется детектор нелинейных переходов, способный точно локализовать любые электронные полупроводники и резисторы в конструкции здания.

Детектор посылает в стены, мебель и прочие объекты мощный микроволновый сигнал, заставляя скрытые схемы генерировать паразитные гармоники. Как только они начинают осциллировать, их можно обнаружить.

Г-н Ланг развеивает распространённое заблуждение относительно советского жучкования американского посольства в Москве. «Они не нашпиговали здание настоящими жучками — вместо этого они замуровали в бетон миллионы крошечных резисторов».

В результате посольство превратилось в рассадник ложных срабатываний. Всякий раз, когда американские специалисты по контрмерам приходили со своими детекторами на поиск жучков, приборы фиксировали паразитные сигналы от бесчисленных резисторов и конденсаторов, вмурованных в стены. Найти настоящие жучки на этом фоне было значительно сложнее, чем искать иголку в стоге сена.

Для поиска прослушки на телефонных линиях TRD использует компьютеризированный электронный анализатор телефонных линий. Он выполняет 18 различных тестов участка линии между блоком клиентского оборудования (CPE) и АТС (CO). Сопротивление, напряжение и баланс линии — лишь некоторые из них. Обнаружив прослушиваемую линию, специалисты посылают по ней импульс с помощью рефлектометра временно́го домена, который позволяет точно установить место подключения жучка.

Следует иметь в виду, что телефонная прослушка — дело крайне трудоёмкое. Каждый рабочий день необходимо прослушивать до 20 часов переговоров. Именно поэтому, как правило, на прослушку ставятся только телефоны ключевых руководителей.

Поимка виновника

Найти прослушку проще, чем установить личность шпиона, оборудовавшего ею ваш офис. Прямые проводные подключения можно проследить до удалённого места, где соглядатай хранит свой автоматический кассетный магнитофон. Обнаружив пост прослушивания, остаётся лишь дежурить поблизости, пока кто-нибудь не явится забрать старые кассеты и поставить новые.

Что касается комнатных жучков, лучшая тактика — вывести устройство из строя, не извлекая его, и ждать, пока слушатель не придёт его починить или заменить.

Одного раза никогда не бывает достаточно

Одни клиенты TRD проверяют свои офисы ежемесячно, другие — раз в квартал. После первоначального обследования можно установить на телефонных линиях оборудование, которое постоянно мониторит любую подозрительную активность.

TRD предлагает гарантию возврата денег, если не обнаружит установленный на объекте жучок. Г-н Ланг заверяет, что каждая компания из списка Fortune 500 в той или иной мере подвергалась прослушке. Таков реальный масштаб проблемы.

Ближе к концу нашего разговора г-н Ланг делает паузу. «Значит, вы действительно собираетесь это опубликовать? Вы действительно честный человек?» — и после этого выдаёт всё как есть.

Выясняется, что г-н Фриц Ланг — на самом деле г-н Фрэнк Джонс (по его словам), лицензированный частный детектив с широкой репутацией в отрасли. Он использовал псевдоним, поскольку подозревал, что я из конкурирующего агентства контрмер или, что ещё хуже, телефонный прослушщик, пытающийся внедриться в его операции.

Что вполне возможно соответствует действительности. В шпионском деле нельзя доверять никому.

Future Transcendent Saga, Приложение III: «От Лимба до бесконечности» — Домены интернета

Автор: Henry Nussbacher (составитель)

Апрель 1989

Особая благодарность Генри Нуссбахеру, который фактически составил этот список. Те из вас, кто находится в сети Bitnet, возможно, уже видели его в виде BITNET GATES.

Для читателей, которые не вполне понимают, что демонстрирует этот файл, я попробую немного объяснить. Как вы уже знаете из серии Future Transcendent Saga, по всему миру существует множество различных сетей. Большинство из них так или иначе связаны друг с другом и обычно все вместе именуются интернетом.

Как вам должно быть известно, Taran King и Knight Lightning оба имеют адреса в Bitnet на узле UMCVMB.BITNET. Однако этот же узел существует в интернете в другой форме: UMCVMB.MISSOURI.EDU.

EDU — это домен интернета для академических узлов. Не каждый узел в Bitnet имеет соответствие в интернете. С другой стороны, лишь небольшая часть узлов интернета имеет эквиваленты в Bitnet.

Таким образом, этот файл по существу показывает, в какую сеть вы отправляете почту, когда в адресе содержится имя узла или маршрутный идентификатор, выглядящий немного непривычно. Для пользователей Bitnet он также показывает, какой адрес Bitnet служит шлюзом между Bitnet и той сетью интернета, куда они отправляют сообщение.

Ниже приведена таблица шлюзов между Bitnet и другими сетями. Формат следующий:

Domain (Домен): Имя верхнего уровня, распознаваемое почтовой системой VM Колумбийского университета.

Name (Название): Описательное название сети.

Gateway (Шлюз): Куда отправляется почта в Bitnet. Если не указано иное, шлюз ожидает получить конверт BSMTP (Batch Simple Mail Transfer Protocol). Рядовым пользователям, как правило, не нужно беспокоиться о содержимом этого поля. Это не почтовый ящик для общих вопросов, а серверная машина (демон), выступающая транспортировщиком почты из одной сети в другую. Почтовые администраторы программного обеспечения должны настроить свои системы так, чтобы они отправляли почту на ближайший шлюз, а не на шлюз по умолчанию.

Translation (Трансляция): В отдельных случаях некоторые адреса будут транслироваться внутри системы с указанием на косвенный шлюз. В таком случае указывается полный адрес.

Коммерческие клиенты интернета (COM)

[Таблица из 4 записей — опущена]

Академические клиенты интернета (EDU)

[Таблица из 65 записей — опущена]

Правительственные домены США (GOV)

[Таблица из 4 записей — опущена]

Итальянская национальная сеть (IT)

[Таблица из 3 записей — опущена]

Прочие стандартные домены

[Таблица из 32 записей — опущена]

Отдельные замечания по специфическим доменам:

• **SUNET** (шведская университетская сеть X.400): шлюзы на CERNVAX и UWOCC1 более не поддерживаются в связи с высокой стоимостью передачи данных через сети X.25 — используйте домен SE.
• **UK** (сеть университетов и исследовательских организаций Великобритании, Janet): имя NRS — по существу, реверс адреса домена. Пример: `user@GK.RL.AC.UK` преобразуется в `user%UK.AC.RL.GK@AC.UK`
• **UUCP** (сеть Unix): альтернативная адресация:
• `user%node.UUCP@HARVARD.HARVARD.EDU`
• `user%node.UUCP@RUTGERS.EDU`
• Шлюзы: 1) MAILER@PSUVAX1 (США), 2) MAILER@UWOCC1 (Канада), 3) BSMTP@UNIDO (Германия), 4) MAILER@MCVAX (Нидерланды)
• Примечания: отправлять на UNIDO разрешено только пользователям из Германии. Всем европейским пользователям рекомендуется использовать MCVAX.
• **CDN** (канадская университетская исследовательская сеть X.400): шлюз на CERNVAX более не поддерживается из-за высокой стоимости передачи данных через публичные сети X.25.

Региональные шлюзы Bitnet — интернет

Ниже приведён список сайтов, которые обрабатывают региональный трафик между Bitnet и интернетом:

```
SMTP@CUNYVM
SMT@CORNELLC
MAILER@MITVMA
MAILER@ICNUCEVM - доступен только для итальянских узлов
```

Вы должны **ВСЕГДА** использовать универсальный адрес `SMTP@INTERBIT` и никогда не использовать ни один из адресов, перечисленных выше. Указанные выше адреса предназначены

исключительно для информационных целей и отладки. Несоблюдение этого правила приведёт к тому, что владельцы шлюза закроют свой сервис для всех пользователей Bitnet и EARN.

Косвенные домены

Домены, недостижимые напрямую, но транслируемые через интернет-выход Mailer:

Домен: DEC
Название: Внутренняя сеть Digital Equipment (Easynet)
Шлюз: SMTP@INTERBIT
Пример: `user@domain.DEC`
Транслируется в: `user%node.DEC@DECWRL.DEC.COM`

Домен: OZ (в скором времени станет OZ.AU)
Название: Австралийская университетская сеть
Шлюз: SMTP@INTERBIT
Пример: `user@node.OZ`
Транслируется в: `user%node.OZ@UUNET.UU.NET`

Домены, недостижимые напрямую, но доступные при явном указании адреса:

Название: Внутренняя сеть Xerox (Grapevine)
Пример: `user.Registry@Xerox.Com`

Название: Внутренняя сеть IBM (VNET)
Пример: `user@Vnet`

Примечания:
1. Почта должна отправляться непосредственно пользователю, а не через сторонний почтовый сервер (например, VM Mailer server).
2. Пользователь внутри VNET должен сначала получить разрешение внутри IBM на установление соединения, а затем инициировать виртуальный контур. Пользователь Bitnet не может установить связь с пользователем VNET без выполнения вышеуказанного требования.
3. Этот шлюз открыт только для избранных узлов внутри IBM, имеющих связи с академическими структурами (например, ACIS).

Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        %%%%%%%%%%%   %%%%%%%%%   %%%%%%%    PWN
PWN                Issue XXVI/Part 1            PWN
PWN                                             PWN
PWN                 April 25, 1989              PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

Добро пожаловать в выпуск XXVI Phrack World News. В этом номере — материалы о Роберте Тэппэне Моррисе, ITT, Telenet, PC Pursuit, хакерском съезде в Голландии, государственной прослушке, вирусах, номерах социального страхования, соперничестве между двумя фракциями журнала TAP и многом другом.

По мере того как SummerCon '89 приближается, всё важнее понимать, кого ждать и с кем нужно связаться для передачи дополнительной информации.

Поскольку в настоящее время мы поддерживаем прямой контакт лишь с ограниченным кругом людей, рекомендуем обращаться к Red Knight, Aristotle или Violence (либо к другим участникам группы VOID hackers). Они, в свою очередь, свяжутся с нами, и мы ответим вам. Помните: точное место проведения SummerCon '89 будет сообщено только тем, кто сможет выйти на связь с нами напрямую.

Пожалуйста, не откладывайте всё на последний момент — важная информация и изменения могут появиться в любое время.

:Knight Lightning

Комиссия Корнелла признала Морриса ответственным за компьютерного червя — 6 апреля 1989

По материалам Денниса Мередита (Cornell Chronicle)

Аспирант Роберт Тэппэн Моррис-младший, действуя в одиночку, создал и запустил программу-«червь», заразившую компьютеры по всей стране в ноябре прошлого года. К такому выводу пришла внутренняя следственная комиссия, назначенная проректором Робертом Баркером.

Комиссия установила, что программа технически не является «вирусом» — программой, которая внедряется в программу-хозяина для размножения, — несмотря на то что именно этот термин фигурировал в популярных публикациях. Комиссия квалифицировала программу как «червя» — самостоятельную программу, которая самовоспроизводится по компьютерной сети.

В своём докладе «The Computer Worm» комиссия охарактеризовала действия Морриса как «ребяческий поступок, в котором были проигнорированы очевидные возможные последствия». Это поведение, по заключению комиссии, свидетельствует о «безрассудном пренебрежении вероятными последствиями».

Баркер, откладывавший публикацию доклада на шесть недель по просьбе федеральных прокуроров и адвоката защиты Морриса, заявил: «Мы чувствуем первостепенную обязанность перед коллегами и общественностью — сообщить всё, что нам известно об этом глубоко тревожащем инциденте».

Комиссия стремилась установить причастность Морриса и других членов корнеллского сообщества к атаке червя, а также изучила мотивацию и этические вопросы, связанные с его запуском.

Доказательства собирались путём опросов преподавателей, сотрудников и аспирантов Корнелла, а также персонала и бывших студентов Гарвардского университета, где Моррис получал степень бакалавра.

Моррис отказался давать показания по совету адвоката. Он запросил и получил академический отпуск в Корнелле; федеральный закон запрещает университету делать какие-либо дальнейшие комментарии относительно его статуса студента.

Комиссии также не удалось связаться с Полом Грэмом, аспирантом Гарварда, хорошо знавшим Морриса. По имеющимся сведениям, 2 ноября 1988 года — в день запуска червя — Моррис связывался с Грэмом, а также несколько раз до и после этой даты.

Опираясь на файлы из учётной записи Морриса, документы факультета информатики Корнелла, записи телефонных переговоров, публикации в СМИ и технические отчёты других университетов, комиссия установила следующее:

• Моррис нарушил прямо выраженные правила факультета информатики о недопустимости злоупотреблений в сфере компьютеров. Хотя, по всей видимости, он предпочёл не посещать вводные занятия, где эти правила разъяснялись, копия правил ему была вручена. Кроме того, политика Корнелла аналогична гарвардской, с которой он должен был быть знаком.

• Ни один член корнеллского сообщества не знал, что Моррис работал над червём. Хотя он обсуждал вопросы компьютерной безопасности с коллегами-аспирантами, своих планов им не раскрывал. Корнелл впервые узнал о причастности Морриса из телефонного звонка Washington Post в редакцию новостей университета.

• Моррис предпринял лишь минимальные усилия, чтобы остановить червя после его распространения, и не сообщил ни одному ответственному лицу о существовании или содержании программы.

• Моррис, по всей видимости, не намеревался уничтожать данные или файлы, однако, вероятно, рассчитывал на широкое распространение червя. Данных о том, что он намеренно стремился к неконтролируемому размножению программы, нет.

• Сообщения СМИ о том, что было заражено 6 000 компьютеров, основывались на первоначальной приблизительной оценке, которую подтвердить не удалось. «Общее число поражённых компьютеров, безусловно, исчислялось тысячами», — заключила комиссия.

• Оценка одной из отраслевых ассоциаций в сфере компьютерной безопасности, согласно которой ущерб от червя составил около 96 миллионов долларов, является «грубым преувеличением» и «продиктована корыстными интересами».

• Несмотря на техническую изощрённость, «червь мог бы быть создан многими студентами — аспирантами или бакалаврами, — особенно если бы они заранее знали об используемых уязвимостях или аналогичных недостатках системы».

Комиссию возглавлял вице-президент Корнелла по информационным технологиям М. Стюарт Линн. В её состав вошли: профессор права Теодор Айзенберг, профессор информатики Дэвид Грис, профессор инженерных наук и информатики Юрис Хартманис, профессор физики Дональд Холкомб и помощник университетского советника Томас Сантаро.

Запуск червя не был «героическим поступком, обнажившим слабые места операционных систем», говорится в докладе. «То, что UNIX ... имеет множество уязвимостей в системе безопасности, было широко известно — равно как и потенциальная опасность вирусов и червей».

Червь атаковал лишь те компьютеры, которые были подключены к Internet — национальной исследовательской компьютерной сети — и работали под управлением определённых версий операционной системы UNIX.

«Эксплуатация подобных уязвимостей — не проявление гениальности или героизма», — констатировала комиссия.

Комиссия также отвергла аргументы о том, что одним из предполагаемых результатов запуска червя должно было стать повышение общественного внимания к компьютерной безопасности.

«Это стало случайным побочным продуктом произошедшего и последовавшего медийного интереса», — говорится в докладе. «Общество не оправдывает кражу со взломом на том основании, что она повышает обеспокоенность вопросами безопасности».

Характеризуя произошедшее, комиссия отметила: «Возможно, это было просто бесцельным интеллектуальным блужданием хакера, целиком поглощённого своим творением и не сдерживаемого соображениями о конкретных целях или возможных последствиях».

Поскольку связаться с Грэмом не удалось, комиссия не смогла установить, обсуждал ли он червя с Моррисом во время визита последнего в Гарвард примерно за две недели до запуска программы. «Было бы интересно узнать, например, к чему именно Грэм обращался в электронном письме Моррису от 26 октября, спрашивая, есть ли 'какие-нибудь новости о блестящем проекте?'» — говорится в докладе.

По сведениям комиссии, многие в сообществе компьютерных учёных склоняются к применению дисциплинарных мер в отношении Морриса.

«Вместе с тем, по всей видимости, преобладает мнение, что такие меры должны оставлять возможность для исправления и потому не быть настолько суровыми, чтобы нанести непоправимый урон карьере виновного», — говорится в докладе.

Комиссия подчеркнула, что этот вывод — лишь впечатление от проведённых исследований, а не результат систематического опроса учёных-компьютерщиков.

«Хотя поступок был безрассудным и импульсивным, он представляется нетипичным для Морриса» — с учётом его прежних усилий в Гарварде и других местах по укреплению компьютерной безопасности, говорится в докладе.

О необходимости усиления безопасности исследовательских компьютеров комиссия написала: «Сообщество учёных не должно возводить стены до неба, чтобы защитить разумные ожидания неприкосновенности частной жизни, — тем более что такие стены в равной мере будут препятствовать свободному обмену информацией».

Доверие между учёными принесло плоды для информатики и для мира в целом, отмечается в докладе.

«Нарушения этого доверия нельзя оправдать. Даже если существуют непредвиденные побочные выгоды — что спорно, — для сообщества в целом потери оказываются бóльшими».

Комиссия не предложила конкретных изменений в политике факультета информатики Корнелла и отметила, что запреты на злоупотребления в компьютерной сфере уже действуют для централизованных вычислительных ресурсов. Вместе с тем комиссия призвала создать комитет для выработки единой общеуниверситетской политики в этой области с учётом широкого распространения компьютеров по всему кампусу.

Комиссия также обратила внимание на «амбивалентное отношение к раскрытию уязвимостей UNIX» в университетской и коммерческой среде. Одни пользователи выступают за публичное сообщение об уязвимостях, другие опасаются, что подобная информация лишь обнажит слабые места системы.

«Моррис изучал безопасность UNIX в этой атмосфере неопределённости, где не было чётких правил игры и где ни коллеги, ни наставники не давали ясных ориентиров», — говорится в докладе.

«Трудно упрекнуть его за то, что он не сообщал об обнаруженных уязвимостях. С его точки зрения, это могло быть наиболее ответственным образом действий — и таким, который поддерживали его коллеги».

В докладе комиссии также содержится краткое описание пути червя по Internet. После своего запуска незадолго до 19:26 2 ноября 1988 года червь распространился на компьютеры Массачусетского технологического института, корпорации RAND, Калифорнийского университета в Беркли и ряда других учреждений.

Червь состоял из двух частей — короткого «зонда» и значительно большего «корпуса». Зонд пытался проникнуть в компьютер и в случае успеха запрашивал корпус.

Программа располагала четырьмя основными методами атаки и несколькими защитными механизмами для уклонения от обнаружения и нейтрализации. Методы атаки эксплуатировали различные уязвимости и особенности операционных систем UNIX на целевых компьютерах. Червь также пытался получить доступ, «угадывая» пароли — в частности, пользуясь склонностью пользователей выбирать в качестве паролей обычные слова.

Авторы исследования выразили благодарность учёным-компьютерщикам Калифорнийского университета в Беркли за предоставление «декомпилированной» версии червя и иной технической информации. Корнеллская комиссия также опиралась на анализ червя, выполненный Юджином Х. Спэффордом из Университета Пердью и Донном Сили из Университета Юты.

Дело против ITT Communications Services, Inc. — 29 марта 1989

УВЕДОМЛЕНИЕ О КОЛЛЕКТИВНОМ ИСКЕ И ПРЕДЛАГАЕМОМ УРЕГУЛИРОВАНИИ ДЛЯ ОТДЕЛЬНЫХ НЫНЕШНИХ И БЫВШИХ КЛИЕНТОВ UNITED STATES TRANSMISSION SYSTEMS, INC. (НЫНЕ ИЗВЕСТНОЙ КАК ITT COMMUNICATIONS SERVICES, INC.)

По решению Окружного суда США для Восточного округа Мичигана, НАСТОЯЩИМ УВЕДОМЛЯЕМ:

Коллективный иск подан от имени ряда бывших и нынешних клиентов против United States Transmission Systems, Inc., ныне известной как ITT Communications Services, Inc., далее именуемой «USTS». Суд предварительно одобрил урегулирование данного иска.

ВАМ НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТСЯ ВНИМАТЕЛЬНО ПРОЧИТАТЬ ЭТО УВЕДОМЛЕНИЕ, ПОСКОЛЬКУ ОНО ЗАТРАГИВАЕТ ВАШИ ПРАВА И БУДЕТ ОБЯЗАТЕЛЬНЫМ ДЛЯ ВАС В БУДУЩЕМ.

I. УВЕДОМЛЕНИЕ О РАССМАТРИВАЕМОМ КОЛЛЕКТИВНОМ ИСКЕ

A. Описание иска

Истцы предъявили иск к USTS, утверждая, что компания взимала с клиентов плату за определённые безответные телефонные звонки, время удержания линии, сигналы «занято» и сообщения автоответчиков телефонных узлов (далее — «безответные звонки»), не раскрывая

должным образом суть таких начислений клиентам или общественности. Истцы добиваются защиты как своих требований о возврате платы за безответные звонки, так и аналогичных требований других нынешних и бывших клиентов USTS.

USTS отрицает нарушения, вменяемые истцами, и утверждает, что во все времена выставляла счета абонентам справедливо и надлежащим образом, а также в полной мере и честно раскрывала основания для своих тарифов на дальнюю связь. USTS согласилась на урегулирование иска исключительно во избежание расходов, неудобств и потрясений, связанных с продолжением судебного разбирательства.

Настоящее уведомление не выражает мнения суда о существе данного дела или о Соглашении об урегулировании. Жалоба, Соглашение об урегулировании и другие материалы дела можно ознакомиться в рабочее время в канцелярии Окружного суда США для Восточного округа Мичигана по адресу: 231 West Lafayette Boulevard, Detroit, MI 48226.

B. Класс истцов в рамках урегулирования

Истцы и USTS заключили Соглашение об урегулировании, которое предварительно одобрено судом. Согласно условиям Соглашения, стороны договорились — исключительно в целях урегулирования — считать настоящий иск поданным от имени следующего класса лиц, находящихся в аналогичном положении с истцами (далее — «Класс»):

Все физические лица и организации, которые в любое время в период с 1 января 1979 года по 31 декабря 1985 года являлись абонентами и пользовались услугами дальней связи USTS или её предшественника — ITT Corporate Communication Services, Inc., именуемых в совокупности «USTS».

C. Как остаться участником Класса

Если вы являлись абонентом и пользовались услугами дальней связи USTS в любое время в указанный период, вы являетесь участником Класса. Для участия в урегулировании от вас не требуется никаких действий. Оставаясь участником Класса, вы будете связаны результатами урегулирования и/или решением суда по данному иску.

D. Как выйти из Класса

Вступать в Класс необязательно. Если вы не желаете быть участником Класса, вы должны направить Уведомление об исключении с указанием вашего имени, текущего адреса и намерения выйти из Класса в канцелярию Окружного суда США для Восточного округа Мичигана по адресу, указанному в конце настоящего Уведомления, с датой почтового штемпеля не позднее 20 апреля 1989 года. Если вы исключаете себя из Класса, вы не можете участвовать в урегулировании. Вместе с тем вы не будете связаны судебным решением об отклонении данного иска и сохраняете право самостоятельно отстаивать свои законные интересы.

II. УСЛОВИЯ УРЕГУЛИРОВАНИЯ

Соглашение об урегулировании обязывает USTS предоставить участникам Класса до 750 000 минут кредита на дальнюю связь максимальной стоимостью 225 000 долларов (по 30 центов за минуту), далее именуемых «Кредиты по урегулированию», а также денежные возвраты на общую сумму до 50 000 долларов. Эти льготы доступны участникам Класса, подавшим заявление о возмещении в установленный срок (см. раздел III ниже). Участники Класса вправе выбрать одну из следующих форм компенсации:

A. *Стандартный кредит* на дальнюю связь USTS в размере 1,50 доллара за каждый год с 1979 по 1985 год, в котором участник Класса (i) являлся клиентом USTS и (ii) заявляет, что USTS взимала с него плату за безответные звонки; либо

B. *Стандартный денежный возврат* в размере 90 центов за каждый год с 1979 по 1985 год, в котором участник Класса (i) являлся клиентом USTS и (ii) заявляет, что USTS взимала с него плату за безответные звонки; либо

C. *Детализированный кредит* на дальнюю связь USTS в размере 30 центов за каждую минуту безответных звонков, за которые участнику Класса был выставлен счёт в период действия Класса (с 1 января 1979 года по 31 декабря 1985 года) и которые не были ранее возмещены или зачтены; либо

D. *Детализированный денежный возврат* в размере 30 центов за каждую минуту безответных звонков, за которые участнику Класса был выставлен счёт в период действия Класса (с 1 января 1979 года по 31 декабря 1985 года) и которые не были ранее возмещены или зачтены.

Для получения *детализированного* кредита или денежного возврата участник Класса обязан перечислить и подтвердить каждый безответный звонок, по которому истребуется возмещение. Если совокупный объём истребуемых кредитов превысит 750 000 кредитных минут, каждый участник Класса, претендующий на Кредиты по урегулированию, получит пропорциональную долю от общего доступного объёма.

Участникам Класса не обязательно быть действующими клиентами USTS для получения стандартных и детализированных кредитов. USTS автоматически откроет счёт любому участнику Класса, который запросит кредиты и подпишет соответствующее разрешение. Если участнику Класса местная телефонная компания выставит счёт за открытие счёта USTS, USTS зачтёт полную сумму этого сбора на счёт участника Класса при получении соответствующего счёта от местной телефонной компании. USTS не несёт ответственности за иные сборы, которые местная телефонная компания может взимать за заказ, использование или прекращение услуг USTS.

Соглашение об урегулировании обязывает USTS нести расходы по рассылке настоящего Уведомления (не более 120 000 долларов) и по администрированию описанного выше урегулирования.

Соглашение об урегулировании также предусматривает, что после окончательного утверждения урегулирования суд вынесет решение об отклонении с предубеждением всех требований истцов и участников Класса, которые были или могли быть заявлены в рамках данного дела и связаны с практикой выставления счетов USTS и раскрытия информации о безответных звонках.

Адвокаты Класса изучили факты и обстоятельства, связанные с требованиями к USTS и её возражениями. С учётом этих обстоятельств адвокаты Класса пришли к выводу, что настоящее Соглашение об урегулировании является справедливым и разумным и отвечает интересам Класса.

III. КАК ПОДАТЬ ЗАЯВЛЕНИЕ

Для получения Кредитов по урегулированию или денежного возврата необходимо сначала получить бланк Заявления о возмещении, заполнить все требуемые сведения и направить его в канцелярию суда с датой почтового штемпеля не позднее 30 июня 1989 года.

Для получения бланков заявлений:	Для подачи заполненного заявления:
USTS Class Action Claim Administrator	Clerk of the United States Court
ITT Communication Services, Inc.	ATTN: USTS Settlement
100 Plaza Drive	231 W. Lafayette Blvd. Room 740
Secaucus, NJ 07096	Detroit, MI 48226

По всем вопросам, связанным с настоящим Уведомлением или подачей Заявления о возмещении, *пишите* Администратору USTS Class Action по указанному выше адресу. По вопросам, касающимся данного иска или вашего участия в нём в качестве участника Класса, *пишите* ведущему адвокату истцов —

```
Sachnoff Weaver & Rubenstein, Ltd.
ATTN: USTS Settlement
30 South Wacker Drive, Suite 2900
Chicago, IL 60606
```

По всем юридическим вопросам, затрагивающим ваши права в любом коллективном иске, обращайтесь к собственному адвокату.

НЕ ЗВОНИТЕ в суд.

НЕ ЗВОНИТЕ адвокатам истцов.

НЕ ЗВОНИТЕ Администратору по претензиям, в какой-либо офис USTS или кому-либо из её сотрудников.

НЕ ЗВОНИТЕ ни в какую телефонную компанию с вопросами по данному делу. Судом будет рассматриваться только *письменная корреспонденция, поданная в установленный срок*.

Telenet объявляет новые условия PC Pursuit — 9 апреля 1989

В начале этого года Telenet объявила новые условия программы PC Pursuit, предусматривающие лимиты на использование сервиса и новые тарифы.

******* Большая часть нововведений ОТМЕНЕНА *******

В письме от 29 марта 1989 года Флойд Х. Трогдон, вице-президент и генеральный директор по сетевым сервисам, объявил о нескольких изменениях в ранее озвученных планах. Данное письмо отменяет все предыдущие меморандумы и соглашения об использовании и вступает в силу с 1 июля 1989 года.

Предусмотрены ТРИ тарифных плана:

• **ОБЫЧНЫЙ** план — 30 долларов в месяц за до 30 часов использования в нерабочее время (вечера и выходные). Доступен только подписчику. Другим лицам пользоваться запрещено.

• **СЕМЕЙНЫЙ** план — 50 долларов в месяц за до 60 часов использования в нерабочее время (вечера и выходные). Доступен подписчику и непосредственным членам семьи, проживающим с ним в одном домохозяйстве. Если одному человеку требуется более 30 часов в месяц, ему следует выбрать «семейный» план, даже если вся «семья» состоит из него одного.

• **ЛЬГОТНЫЙ (для людей с ограниченными возможностями)** план — 30 долларов в месяц за до 90 часов использования в нерабочее время (вечера и выходные). Для оформления необходимо подтверждение физической инвалидности. За точными условиями обращайтесь в Telenet.

СВЕРХЛИМИТНЫЕ ЧАСЫ свыше 30 (или 60/90) в месяц в нерабочее время оплачиваются по тарифу 3,00 доллара в час. Это меньше ранее предложенной ставки в 4,50 доллара в час.

ИСПОЛЬЗОВАНИЕ В РАБОЧЕЕ ВРЕМЯ оплачивается по тарифу 10,50 доллара в час вне зависимости от оставшегося времени в рамках тарифного плана PCP.

Счета выставляются в следующем месяце за предыдущий: то есть за июльское использование счёт выставляется в августе и т.д. Детализация звонков автоматически предоставляется подписчикам, превысившим тридцать часов в месяц.

ЛЬГОТНЫЙ ПЕРИОД: все звонки получают одну минуту льготного времени для установления соединения. Плата за звонки продолжительностью не более одной минуты не взимается никогда. Если вы разрываете соединение сразу, убедившись, что звонок по какой-либо причине не завершился, плата не взимается.

После истечения первой минуты минимальная продолжительность соединения составляет две минуты. В остальных случаях время округляется до *ближайшей* минуты для целей выставления счёта.

НОВЫЕ ПАРОЛИ И ИДЕНТИФИКАТОРЫ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ВСЕХ: в апреле 1989 года всем действующим подписчикам PC Pursuit будут выданы новые пароли и идентификаторы пользователей. С 1 мая 1989 года все существующие пароли и идентификаторы будут аннулированы.

Новые пользователи, подключающиеся после 1 июля 1989 года, заплатят 30 долларов за открытие счёта. Замена пароля стоит 5,00 доллара. *Действующие* пользователи никогда не будут платить за изменение тарифного плана в сторону увеличения или уменьшения (обычный семейный). В июне 1989 года пользователям с более чем 30 часами использования будет предоставлена детализация звонков для помощи в выборе тарифного плана; при этом оплата сверхлимитных часов до июля не предусматривается.

В связи с путаницей и неудовлетворительным информированием пользователей за последние несколько месяцев официальный переход с безлимитного на повременной учёт перенесён с первоначально запланированного июня на 1 июля.

Выше приведены лишь выдержки из письма подписчикам, опубликованного на BBS Net Exchange. Если вы являетесь подписчиком PC Pursuit, рекомендую войти в систему и прочитать полный текст меморандума вместе с прилагаемыми Условиями использования и тарифными расписаниями.

Помните: любые изменения, внесённые вами в феврале/марте в ожидании смены условий, которая первоначально планировалась на май/июнь, теперь аннулированы. Telenet объявила, что с 1 июля все пользователи по умолчанию переводятся на ОБЫЧНЫЙ план, если только они специально не изменят его в течение мая или июня.

```
Telenet Customer Service:  1-800-336-0437
Telenet Telemarketing:     1-800-TELENET
```

Регистрация через модем с номером кредитной карты под рукой: 1-800-835-3001.

Чтобы прочитать полные бюллетени, войдите в Net Exchange, позвонив на местный узел Telenet и подключившись к `@pursuit`.

«Протяни руку и прослушай кого-нибудь» — April 3, 1989

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                 PWN
PWN        P h r a c k   W o r l d   N e w s        PWN
PWN        %%%%%%%%%%   %%%%%%%%   %%%%%%         PWN
PWN                Issue XXVI/Part 2                PWN
PWN                                                 PWN
PWN                 April 25, 1989                  PWN
PWN                                                 PWN
PWN          Created, Written, and Edited           PWN
PWN               by Knight Lightning               PWN
PWN                                                 PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

Двое бывших сотрудников Cincinnati Bell, уволенных компанией «по веской причине» — по словам председателя совета директоров Dwight Hibbard — заявляют, что в период с 1972 по 1984 год установили более 1200 незаконных прослушек по указанию своих руководителей в телефонной компании и местной полиции.

Среди предполагаемых объектов слежки — действующие и бывшие члены Конгресса, федеральные судьи, видные политики, бизнесмены, адвокаты и медийные личности города.

Leonard Gates и Robert Draise утверждают, что прослушивали даже гостиничный номер, где останавливался президент Gerald Ford во время двух его визитов в Цинциннати; эта часть их рассказа по меньшей мере подтверждена ныне ушедшим на пенсию начальником службы безопасности гостиницы.

По мере того как каждый день всплывают новые подробности, жители Цинциннати получают редкую возможность взглянуть на полицейское управление, которое, судя по всему, само за собой шпионило, — и на расследование большого жюри, которое побудило одного бывшего сотрудника ФБР высказать предположение, что Министерство юстиции больше заинтересовано в дискредитации обвинителей, нежели в поиске истины.

Руководители Cincinnati Bell заявляют, что Gates и Draise просто хотят «свести счёты» с компанией за увольнение. Однако то, что уже стало известно, позволяет предположить: в словах обоих мужчин о компании, где они работали, есть хотя бы доля правды.

По словам Gates и Draise, они были всего лишь сотрудниками, выполнявшими приказы своих начальников в Cincinnati Bell. Но Dwight Hibbard, председатель совета директоров Cincinnati Bell, назвал их обоих лжецами и заявил, что их единственный мотив — нанести ущерб компании.

Cincinnati Bell отреагировала на обвинения в непосредственном участии в незаконном прослушивании, подав иск о клевете против Gates и Draise. Те в ответ подали встречный иск против телефонной компании. Помимо этого, четверо из людей, за которыми якобы велась слежка, подали коллективный иск против компании.

В самом последнем развитии событий Cincinnati Bell предала огласке — по их словам, лишь недавно обнаруженные — компрометирующие подробности о внебрачной связи Gates. Федеральное большое жюри в Цинциннати пытается распутать клубок взаимных обвинений, однако пока никаких обвинительных заключений вынесено не было.

Почти ежедневно Gates и Draise сообщают всё новые подробности своей деятельности, в том числе о прослушках, которые они, по их словам, устанавливали на Cincinnati Stock Exchange и на заводе авиационных двигателей General Electric в пригороде Evendale.

По словам Draise, он начал выполнять эти «особые задания» в 1972 году, когда к нему обратился сотрудник полиции Цинциннати из засекреченного разведывательного подразделения. Полицейский попросил его прослушать линии «чёрных националистов» и подозреваемых наркоторговцев, рассказал Draise.

Полицейский заверил его, что прослушивание будет законным и что его одобрило руководство телефонной компании. Draise согласился и предложил привлечь Gates, своего коллегу. Вскоре оба они устанавливали по несколько прослушек в неделю по заданию разведывательного управления полиции Цинциннати.

Однако примерно к 1975 году направление и масштаб операции изменились, говорят мужчины. Запросы на прослушивание поступали уже не от полиции, а от James West и Peter Gabor, руководителей отдела безопасности Cincinnati Bell, которые утверждали, что *получают приказы от своего начальства*.

И объектами слежки были уже не уголовные элементы: Draise и Gates говорят, что им велели прослушивать телефоны политиков, бизнесменов и даже самого начальника полиции, а также личные линии некоторых сотрудников телефонной компании.

Draise рассказал, что «начал сомневаться во всём этом деле в 1979 году», когда ему было приказано прослушивать личный телефон городского журналиста-обозревателя. «Я сказал им, что больше этим заниматься не буду», — заявил он в интервью на неделе 2 апреля 1989 года.

Gates продолжал этим заниматься вплоть до 1984 года, и, по его словам, он струсил в конце того же года, когда «через виноградную лозу пришла новость» о том, что ему нужно прослушать телефонные линии, подключённые к компьютерам на заводе General Electric в Evendale. Тогда он отказался и попросил его больше в это не впутывать, а также утверждает, что в тот момент ему намекали на возможные репрессии — угрозы «рассказать, что мы о тебе знаем...»

Когда Dwight Hibbard был застигнут в своём офисе в Cincinnati Bell и попрошен прокомментировать обвинения бывших сотрудников, он ответил, что оба они лжецы. «Телефонная компания не стала бы делать ничего подобного, — заявил Hibbard. — И на обоих подан иск именно за то, что они говорят, будто мы это делаем». Hibbard отказался отвечать на более конкретные вопросы местной прессы и государственных следователей.

Фактически Draise был уволен в 1979 году, вскоре после того, как, по его словам, сообщил руководству, что больше не будет устанавливать прослушки на линии. Вскоре после того, как он перестал выполнять «особые задания», его арестовали и предъявили ему обвинение в проступке в связи с одной прослушкой, которую Draise, по его словам, установил для друга, желавшего следить за своей бывшей подругой. Cincinnati Bell заявляет, что не имеет никакого отношения к его аресту и обвинительному приговору по этому делу, однако «была вынуждена уволить его» после того, как он признал свою вину.

Gates был уволен в 1986 году за нарушение дисциплины. Он утверждает, что Cincinnati Bell мстила ему за поддержку двух сотрудников, подавших на компанию в суд за сексуальные домогательства; однако суд признал его увольнение законным.

История начала всплывать, когда Gates и Draise обратились к репортёру [Mount Washington Press], небольшой еженедельной газеты в пригороде Цинциннати. Газета опубликовала их обвинения, и сердитые отклики посыпались почти сразу.

Поначалу полиция отрицала само существование разведывательного управления — а тем более то, что подобная организация могла использовать агентов в Cincinnati Bell для слежки за людьми.

Позднее, когда их вызвали перед федеральным большим жюри и предупредили о недопустимости лжи, пятеро ушедших в отставку полицейских, в том числе бывший начальник, воспользовались Пятой поправкой. В конце прошлого месяца эти пятеро через своего адвоката опубликовали заявление, в котором признали 12 незаконных прослушек в 1972–1974 годах и назвали неустановленных агентов Cincinnati Bell своими контактами для установки прослушек.

После того как лёд был сломлен и официальные формальности были соблюдены, другие начали выходить вперёд со схожими историями. Howard Lucas, бывший директор службы безопасности отеля Stouffer's в Цинциннати, вспомнил инцидент 1975 года: он не пустил Gates, West и нескольких сотрудников в штатском в телефонную комнату гостиницы — примерно за месяц до приезда президента Ford.

Телефонная комната была закрыта на замок, и сотрудников впускали через систему внутренней связи те, кто уже находился внутри, вспоминает Lucas. Помимо коммутаторов, в комнате находились распределительные рамы, от которых пары проводов расходились по всей гостинице. Lucas отказался пускать полицейских без ордера на обыск — и они больше с ним не возвращались.

Однако через два дня, по словам Lucas, один из операторов по секрету посоветовал ему заглянуть в один из тамошних шкафов. Lucas рассказал, что нашёл там диктофон с голосовой активацией и «пару катушек, которые используются для создания прослушки». По его словам, он сообщил о находке полиции и Cincinnati Bell, однако «никто не захотел её признавать, так что я просто вытащил всё это и выбросил в мусорный бак».

Недавно руководители General Electric встретились с Draise и Gates, чтобы выяснить масштаб прослушки, осуществлявшейся на заводе. По словам Draise, адвокат GE David Kindleberger был потрясён, узнав о масштабах слежки, и связал её с очевидной утечкой закрытой информации к Pratt & Whitney — конкурирующему производителю авиационных двигателей.

Теперь Kindleberger вдруг замолчал. Интересно, кто его обработал? Он признаёт факт встречи с Draise, но заявляет, что никогда не обсуждал с ним Pratt & Whitney или какую-либо конкурентную ситуацию. Однако адвокат, присутствовавший на встрече, подтверждает версию Draise.

После первоначального шквала пресс-релизов с опровержением всех обвинений в незаконном прослушивании Cincinnati Bell погрузилась в молчание и теперь отказывается обсуждать это дело вообще — разве что отвечает всем желающим, что «Draise и Gates — пара лжецов, желающих свести с нами счёты...» И вот теперь компания вдруг обнаружила сведения о личной жизни Gates.

Сеть прослушки ФБР/Bell? — April 3, 1989

[Отредактировано для настоящей публикации]

Bob Draise/WB8QCF был сотрудником Cincinnati Bell Telephone с 1966 по 1979 год. Он и другие причастны к скандалу с прослушкой колоссального масштаба. По их словам, ими было установлено более 1000 прослушек на телефонах судей, сотрудников правоохранительных органов, адвокатов, телеведущих, газетных обозревателей, профсоюзов, подрядчиков Министерства обороны, крупных корпораций (таких как Proctor & Gamble и General Electric), политиков (в том числе экс-президента Gerald Ford) — по запросу полиции Цинциннати и руководителей службы безопасности Cincinnati Bell, которые утверждали, что прослушки нужны для полиции. Им говорили, что многие из прослушек устанавливались по заданию ФБР.

Другой радиолюбитель, Vincent Clark/KB4MIT, техник South-Central Bell с 1972 по 1981 год, сообщил, что устанавливал незаконные прослушки, аналогичные тем, что делал Bob Draise, по приказу своих руководителей — и по просьбе местных полицейских в Луисвилле, штат Кентукки.

На вопрос о том, как он оказался вовлечён в незаконное прослушивание, Bob рассказал, что приятель позвонил ему и попросил спуститься, чтобы встретиться с полицией Цинциннати. Оперативный сержант разведки спросил Bob'a о прослушке линий «Чёрных мусульман». Он также сообщил Bob'у, что служба безопасности Cincinnati Bell одобрила прослушку — и что это нужно для ФБР. Сержант указал на своё масонское кольцо, точно такое же, что носил Bob, — иначе говоря, давал понять, что говорит правду под масонской клятвой, которую Bob воспринимал очень серьёзно.

Большинство объектов первых прослушек были связаны с наркотиками или преступным миром. Однако впоследствии ситуация вышла из-под контроля — ФБР потребовало прослушивать видных граждан. «Мы начали заниматься людьми, у которых были деньги. Как использовалась эта информация, я вам не скажу».

В «Newsday» от 29 января Draise сообщил следователям, что среди прослушек, которые он устанавливал с 1972 по 1979 год, было несколько на линиях, использовавшихся Wren Business Communications — конкурентом Bell. По всей видимости, когда Wren договаривалась о встрече с потенциальным клиентом, оказывалось, что Bell уже побывала там без приглашения. Президент Wren — радиолюбитель David Stoner/K8LMB.

В разговоре Dave Stoner сказал следующее:

> *«На мой взгляд, исходный источник всего этого — ФБР. ФБР, по всей видимости, выстроило структуру по всей Соединённым Штатам, используя, судя по всему, начальников служб безопасности различных компаний Bell. Говорят, что в Соединённых Штатах были и другие подобные случаи, как у нас в Цинциннати, однако они носили локальный характер — без осознания общей схемы, которая за ними стоит».*
>
> *«Связующее звено всего этого — если уйти далеко в прошлое, во времена Гувера в ФБР — состоит в том, что он, по всей видимости, договорился с людьми из службы безопасности AT&T. Существует организация, которая, полагаю, действует и по сей день, проводящая регулярные встречи сотрудников безопасности различных компаний Bell. Это означало, что ФБР могло работать с группой из 20–30 человек, представлявших ключевые точки безопасности всех подразделений Bell и AT&T в Соединённых Штатах. Думаю, ключ ко всему этому восходит к Гуверу. ФБР действовало через эту группу, которая затем организовала деятельность на местах в результате централизованного планирования».*
>
> *«Несмотря на то что многие указывают на начало 70-х как на период существования этой проблемы, я убеждён, что никакого прекращения этой работы до сих пор нет. Я практически уверен, что она продолжается. Всё это выглядит как масштабная операция слежки, частью которой был Цинциннати».*
>
> *«Федеральный прокурор Kathleen Brinkman оказалась в безвыходном положении. Если она успешно доведёт это дело до конца, она навлечёт неприятности на собственное Министерство юстиции. Она не может успешно завершить это дело».*

Против Cincinnati Bell и полицейского управления уже поданы иски на общую сумму около 200 миллионов долларов. Несколько сотрудников полицейского управления воспользовались Пятой поправкой перед большим жюри, отказавшись отвечать на вопросы о своей роли в схеме прослушивания.

Bob Draise/WB8QCF подал иск против Cincinnati Bell на 78 долларов — за злоумышленное преследование и клевету — в ответ на иск Cincinnati Bell против Bob'a за диффамацию. Сразу после того как они подали иск, несколько полицейских вышли вперёд и признали, что вместе с ними устанавливали незаконные прослушки. Полиция Цинциннати заявила, что прекратила это в 1974 году, — хотя другой полицейский, по имеющимся сведениям, сообщил, что прослушивание

фактически прекратилось в 1986 году.

Сейчас телевизионная программа «60 Minutes» на CBS заинтересовалась происходящим в Цинциннати и направила туда бригаду журналистов-расследователей. Ed Bradley из «60 Minutes» уже взял интервью у Bob Draise/WB8QCF, и ожидается, что в этом месяце (апрель) выйдет репортаж «60 Minutes» о шпионаже ФБР. Кроме того, по имеющимся сведениям, CNN — кабельный новостной канал Ted Turner'a — также готовит материал под рабочим названием «Прослушка Америки».

Призывы ужесточить борьбу с хакерами — April 9, 1989

Из Chicago Tribune (раздел 7, стр. 12b)

«Сделайте наказание соразмерным преступлению», — требуют лидеры компьютерной индустрии

ДАЛЛАС (AP) — Правовая система не смогла в полной мере отреагировать на угрозу, которую хакеры представляют для компьютерных сетей, жизненно важных для корпоративной Америки, — считает один из компьютерных экспертов.

Многие компьютерные хакеры «отделываются лёгким испугом», — заявил Mark Leary, старший аналитик International Data Corp., на заседании круглого стола на прошлой неделе.

«Судебная система должна признать... что эти люди злонамеренны, что они преступники и что они грабят банки — ничуть не меньше, чем если бы пришли с дробовиком», — сказал он.

Другие участники дискуссии выразили недовольство тем, что хакерам, благодаря их умению взламывать компьютерные системы, порой даже дают работу — в том числе в качестве консультантов по безопасности.

Эксперты выступили на круглом столе, организованном журналом Network World — изданием для пользователей и администраторов компьютерных сетей.

Компьютерные сети стали незаменимы для бизнеса — от передачи и обработки информации до контроля за производственными процессами и управления ими.

Широкая публика также всё больше сталкивается с сетями через такие устройства, как банкоматы, системы бронирования авиабилетов и компьютеры, хранящие информацию о счетах.

Компании стали охотнее тратить деньги на компьютерную безопасность после нашумевшего в прошлом году вторжения в общенациональную сеть вируса, предположительно выпущенного аспирантом [Robert Tappen Morris], отметили эксперты.

«Этот инцидент заставил нас пересмотреть приоритеты, с которыми мы оцениваем те или иные угрозы», — сказал Dennis Steinaur, руководитель группы по управлению компьютерной безопасностью Национального института стандартов и технологий.

Однако компьютерная безопасность — это не только вопрос защиты от несанкционированного доступа, отметил Max Hopper, старший вице-президент по информационным системам в American Airlines.

Hopper рассказал, что American создала для своих компьютерных систем объект, напоминающий «Шайеннскую гору», призванный защититься от самых разных угроз, включая перебои с электричеством и стихийные бедствия. Проводя аналогию с подземным командным центром Министерства обороны в горах Колорадо, он упомянул, что меры безопасности в American включают даже трёхдневный запас продовольствия.

«Мы, как нам кажется, сделали всё возможное для защиты общей инфраструктуры», — заявил Hopper.

Hopper и Steinaur отметили, что, несмотря на высокотехнологичный образ компьютерного терроризма, это остаётся административной проблемой, к которой следует подходить как к рутинному управленческому вопросу.

Вместе с тем эксперты согласились, что наибольшую опасность для компьютерных сетей представляют вовсе не внешние хакеры. Самая серьёзная угроза, по их словам, исходит от недовольных сотрудников или других лиц, изначально имевших законный доступ к системам.

Хотя проверка сотрудников полезна, отметил Steinaur, важнее встроить в компьютерные системы механизмы отслеживания несанкционированного использования и пропагандировать то, что взлом поддаётся отслеживанию.

Steinaur отметил, что растущая компьютерная грамотность, а также деятельность некоторых незлонамеренных хакеров в каких-то отношениях помогают менеджерам по безопасности.

Расширение знаний «вынуждает нас как менеджеров по безопасности не полагаться на невежество», — сказал Steinaur.

«Безопасность должна быть частью системы, а не "докучливым дополнением", — заявил Steinaur, — и, вероятно, мы не слишком хорошо справились с тем, чтобы донести до руководства мысль: безопасность — неотъемлемая часть системы».

Leary из IDC сообщил, что опросы организации среди компаний Fortune 1000 неожиданно выявили значительное число компаний, почти не принимающих мер для защиты своих систем.

Дискуссия — первая из трёх, запланированных Network World, — состоялась, потому что компьютерный саботаж «является реальной проблемой, о которой люди не подозревают», — сообщил редактор John Gallant.

Напечатано для PWN: Hatchet Molly

Бывший сотрудник обвинён в создании вируса — базы данных были предполагаемой целью — April 12, 1989

by Jane M. Von Bergen (Philadelphia Inquirer)

Вчера бывшему сотруднику было предъявлено обвинение в заражении компьютерной базы данных его компании — в том, что считается первым арестом по делу о компьютерном вирусе в районе Филадельфии.

«Мы полагаем, что он сделал это из мести», — заявил вчера помощник прокурора округа Камден Norman Muhlbaier, комментируя мотивы сотрудника, который якобы установил программу для уничтожения баз данных своей бывшей компании — Datacomp Corp. в Воорхисе, штат Нью-Джерси.

Chris Young, 21 год, проживающий в квартале 2000 по Liberty Street в Трентоне, обвинён в округе Камден по одному пункту — компьютерное хищение путём изменения базы данных. Судья Высшего суда E. Stevenson Fluharty отпустил Young'а под обязательство уплатить 10 000 долларов в случае неявки в суд. В случае обвинительного приговора Young грозит 10 лет лишения свободы и штраф в 100 000 долларов. Получить комментарий от Young не удалось.

«Ущерб нанесён не был», — заявил Muhlbaier, поскольку компания обнаружила вирус прежде, чем он успел причинить вред. Если бы вирус сработал, он мог бы повредить базы данных стоимостью в несколько сотен тысяч долларов, сообщил Muhlbaier.

Datacomp Corp., расположенная в торговом центре Echelon Mall, занимается телефонным маркетингом. Компания с 30–35 сотрудниками имела договор с крупной телефонной компанией на проверку содержимого её телефонных справочников и попытки продать выделенные жирным шрифтом или иные специальные строки в справочниках, сообщила пресс-секретарь Datacomp. По её словам, база данных, которую Young обвиняется в попытке уничтожить, — это список имён от телефонной компании.

Muhlbaier рассказал, что в день, когда Young уволился из компании — 7 октября 1988 года, — он использовал вымышленные пароли, чтобы войти в компьютер компании, и запрограммировал вирус начать уничтожение 7 декабря 1988 года — в день Пёрл-Харбора. Young, проработавший в компании с перерывами два года, последнее время занимавший должность руководителя, был недоволен рядом неблагоприятных оценок своей работы, сообщил прокурор.

В итоге операторы компании заметили сбои в компьютерной системе. Приглашённый программист, разбираясь в проблеме, обнаружил, что программа была изменена, и выявил вирус, уничтожавший данные, — рассказал Muhlbaier. «Чего Mr. Young не знал, так это того, что компьютерная система имеет множество функций безопасности, позволяющих отследить действия вплоть до конкретной даты, времени и терминала, — сказал Muhlbaier. — Нам удалось... доказать, что он работал за этим терминалом». Вирус Young'a, по словам Muhlbaier, относится к типу, известному как «логическая бомба», поскольку запрограммирован на срабатывание в определённое время. В данном случае база данных была бы поражена при первом включении компьютера 7 декабря, пояснил он.

Norma Kraus, вице-президент материнской компании Datacomp — Volt Information Sciences Inc, — заявила вчера, что потенциальные потери компании включали не только базы данных, но и время, потраченное на поиск и устранение вируса. «Всю работу пришлось остановить», — что привело к задержкам поставок по контрактам, сказала она. «Нам просто повезло, что у нас есть сотрудники, которые умеют определить, в чём проблема, и проявляют желание что-то предпринять. В данном случае сотрудник не остановился на устранении неисправности, а продолжал разбираться, в чём была причина». Компания Volt, со штаб-квартирой в Нью-Йорке, ведёт бизнес на 500 миллионов долларов в год — в области телефонного маркетинга, обработки данных и технической поддержки. Она также организует временную занятость, в особенности в сфере обработки данных, и устанавливает телекоммуникационные системы, рассказала Kraus.

Телефонная система Мексики уходит в частные руки? — April 17, 1989

By Oryan QUEST (Специальный испаноязычный корреспондент)

Мексиканская телефонная компания, она же Telefonos de Mexico, она же Telmex, по всей видимости, перейдёт в частные руки в течение ближайшего года-двух. Мексиканское правительство всерьёз рассматривает возможность продажи своей контрольной доли в национальной системе связи, невзирая на очень жёсткое сопротивление местных профсоюзов, предпочитающих сохранить существующую бюрократическую машину.

Предполагаемая продажа — часть шагов по модернизации телефонной системы (а она *действительно* нуждается в модернизации) за счёт привлечения большего частного инвестирования — входит в растущую тенденцию к приватизации ранее национализированных отраслей в Мексике.

Мексиканская телефонная компания более года разрабатывала план реструктуризации на 14 миллиардов долларов сроком пять лет, в котором AT&T и региональным холдинговым компаниям Bell, вероятно, отведена роль в проведении улучшений.

Один из планов, обсуждаемых мексиканским правительством, — полный раздел Telmex, аналогичный принудительному разделению AT&T, осуществлённому несколько лет назад по решению суда. По этому плану в Мексике появилась бы одна центральная компания дальней связи под государственным контролем, тогда как местные и вспомогательные услуги оказывали бы частные региональные компании.

Представители мексиканского правительства неоднократно беседовали с руководством Southwestern Bell о подготовке официального предложения. Точно так же Pacific Bell зондировала почву на переговорах с мексиканской стороной. Посмотрим, что из этого выйдет.

Около двух лет назад журнал Teleconnect в юмористической статье о разделении AT&T опубликовал вымышленную карту территорий, закреплённых за каждой BOC, — с Техасом, Нью-Мексико и Аризоной, объединёнными под наименованием «Taco Bell».

Любая телефонная компания, которая возьмётся за мексиканскую систему, окажется лучше нынешнего оператора, который медленно деградирует на протяжении нескольких лет.

PS: *Я Требую* Вернуть Меня На MSP!

Galactic Hacker Party (вечеринка галактических хакеров) — 30 марта 1989

Автор: Knight Lightning

25 апреля 1989 года

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                 PWN
PWN        P h r a c k   W o r l d   N e w s        PWN
PWN        %%%%%%%%%%%   %%%%%%%%%   %%%%%%%        PWN
PWN                Issue XXVI/Part 3                PWN
PWN                                                 PWN
PWN                 April 25, 1989                  PWN
PWN                                                 PWN
PWN          Created, Written, and Edited           PWN
PWN               by Knight Lightning               PWN
PWN                                                 PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

```
                    GALACTIC HACKER PARTY
                      August 2-4, 1989
                PARADISO, AMSTERDAM, HOLLAND
```

Летом 1989 года мир, каким мы его знаем, окажется на грани перегрузки. Межзвёздный поток хакеров, телефонных фрикеров, радиоактивистов и всевозможных технологических подрывников сольёт свои энергии в медийный взрыв — глобальная деревня на три захватывающих дня подключится к Амстердаму ради обмена информацией и электронных приключений.

Вооружённые передовыми коммуникационными технологиями, к которым они привыкли, хакерские силы будут обсуждать стратегии, играть в игры и просто хорошо проводить время. Свободный доступ к постоянно открытым онлайн-ресурсам позволит им поддерживать связь с домашней базой — где бы та ни находилась.

Всех, кто по праву опасается угрозы информационной тирании и хочет узнать, что с этим можно сделать, настоятельно приглашают встретиться в Амстердаме в августе. Будет чему поучиться у людей, которые разбираются в деле. Известные гости с важными словами будут присутствовать — физически или в электронном обличье.

Силу необходимо поддерживать. Если вас не пропустили в транспорт, потому что ваш ноутбук похож на бомбу, если вы отрезаны на вражеской территории или по иным причинам не можете приехать — присоединяйтесь к нам по сетям. Другие хакерские группы призываются организовать аналогичные встречи, совпадающие по времени с нашей. В ходе конференции мы сможем обеспечить недорогие международные каналы связи.

```
[  Despite the wishes of those planning the "Galactic Hacker   ]
[  Party," there will be NO change in plans for SummerCon '89! ]
```

Для получения дополнительной информации обращайтесь как можно скорее:

```
          HACK-TIC                          PARADISO
          P.O. box 22953                    Weteringschans 6-8
          1100 DL  Amsterdam                1017 SG  Amsterdam
          The Netherlands                   The Netherlands

      tel: +31 20 6001480               tel: +31 20 264521 / +31 20 237348
```

Подрывные электронные доски объявлений — 26 марта 1989

В газете из Великобритании появилась статья о компьютерной доске объявлений, которую вёл 14-летний мальчик из Уилмслоу, Чешир, Англия. На ней содержалась информация о таких вещах, как изготовление пластиковых взрывчатых веществ.

Сообщается, что антитеррористические детективы ведут расследование о возможном нарушении Закона о непристойных публикациях. По всей видимости, журналистам удалось без труда получить доступ к этой доске объявлений и ознакомиться со статьями на такие темы, как мошенничество с кредитными картами, изготовление различных видов взрывчатых веществ, уличные боевые приёмы и уклонение от радаров дорожной полиции.

Одна из статей была явно адресована детям и описывала, как сделать бомбу для использования против «машины учителя, который вам не нравится», — она должна была уничтожить шину автомобиля при запуске.

Родители мальчика, судя по всему, не считали, что их сын делает что-то плохое: им было предпочтительнее видеть его за компьютером, а не шатающимся по улицам.

Лондонский компьютерный консультант Ноэл Брэдфорд, по его словам, ознакомился с доской объявлений и обнаружил там сообщения с обсуждением «способов взлома British Telecom, способов выкачивания денег из людей и мошенничества с компаниями, выпускающими кредитные карты. Там приводились номера кредитных карт, а также PIN-коды, имена, адреса и прочие данные».

История двух журналов TAP! — 24 апреля 1989

Казалось неизбежным, что рано или поздно разгорится борьба за права на TAP, хотя многие недоумевают, почему это заняло так много времени.

The Renegade Chemist, давний член Phortune 500 и один из его «членов совета директоров», не менее двух лет говорил о возобновлении выпуска TAP Magazine... ничего конкретного до сих пор не происходило. TRC утверждает, что команда TAP Magazine в Кентукки — сплошное мошенничество, а сам он выпускает «настоящий» журнал.

Чтобы получить бесплатный экземпляр TAP Magazine от The Renegade Chemist, пришлите конверт с обратным адресом и маркой по адресу:

```
Data Security Consultants, Inc.
TAP Magazine
P.O. Box 271
South Windam, CT  06266-0271
```

С другой стороны, Aristotle из кентуккийского TAP Magazine демонстрирует практически равнодушное отношение к заявлениям The Renegade Chemist. По его словам, он «не особо возражает, если эти люди выпустят журнал. Честно говоря, я просто хочу помочь сообществу, а чем больше журналов и информации — тем лучше».

По-настоящему громкая новость о кентуккийском TAP Magazine появилась в субботу, 22 апреля 1989 года. По всей видимости, из-за проблем с местными банками и Налоговой службой (IRS) TAP Magazine теперь БЕСПЛАТНЫЙ!

Единственный нюанс: чтобы его получить, нужно присылать конверт с обратным адресом и маркой на каждый номер, либо «можно прислать наличными, но только столько, сколько нужно на почтовые расходы — 25 центов хватит». Никаких чеков и/или денежных переводов. Все уже

отправленные чеки будут возвращены или как минимум не будут обналичены. Редакция TAP Magazine берёт расходы на печать на себя.

Для получения БЕСПЛАТНОГО TAP Magazine пришлите конверт с обратным адресом и маркой по адресу:

```
P.O. Box 20264
Louisville, KY  40220
```

93-й номер должен выйти в конце апреля 1989 года, но Aristotle также просил передать всем, что он будет присутствовать на SummerCon '89 и привезёт с собой немало экземпляров всех выпусков TAP, которые они с Olorin The White и Predat0r успели издать.

Поскольку TAP от TRC я лично не видел — воздержусь от суждений. Вместо этого предлагаю получить оба журнала БЕСПЛАТНО и сравнить самостоятельно. Рынок сам решит, который из TAP продолжит существование.

Информация предоставлена Aristotle и The Renegade Chemist

Компьютерная организация предостерегает от влияния спецслужб — 11 апреля 1989

Из San Francisco Chronicle

Группа защиты общественных интересов заявила, что Агентство национальной безопасности — крупнейшая разведывательная структура страны — может получить чрезмерный контроль над программой по усилению защиты компьютерных систем всего федерального правительства.

Группа Computer Professionals for Social Responsibility (Компьютерные специалисты за социальную ответственность), базирующаяся в Пало-Альто, призвала ключевых членов Конгресса уделить «особо пристальное внимание» роли агентства в реализации законодательства, направленного на защиту конфиденциальных, но несекретных данных в федеральных компьютерных системах.

«Постоянно существует риск того, что федеральные ведомства под видом усиления компьютерной безопасности обнаружат, что их программы — в той мере, в какой они опираются на компьютерные системы, — всё больше оказываются под надзором крупнейшей и наиболее засекреченной разведывательной организации страны», — говорится в заявлении группы.

Верификация номеров социального страхования — 11 апреля 1989

Из The New York Times

Dorkas P. Харди, комиссар Администрации социального обеспечения, сообщила парламентскому комитету, что ведомство проверило миллионы номеров SSN (Social Security Numbers) для частных кредитных компаний.

TRW, крупнейшая в стране компания по кредитным рейтингам, недавно предложила выплатить Администрации социального обеспечения 1 000 000 долларов за верификацию 140 миллионов номеров.

Пресс-секретарь ведомства Фил Гамбино в прошлом месяце сообщил, что агентство проверяло номера социального страхования исключительно по запросу самих застрахованных или их работодателей и никогда не верифицировало более 25 номеров за один раз. По его словам, такие

сведения предоставлялись в соответствии с Законом о свободе информации.

На вчерашних слушаниях Доркас Р. Харди поначалу отрицала какие-либо иные случаи верификации. Однако впоследствии она признала, что в начале 1980-х годов для CitiCorp было проверено 3 000 000 номеров социального страхования, а в прошлом году для TRW — 151 000 номеров. Г-жа Харди назвала верификацию 151 000 номеров лишь «пробным запуском».

Сенатор Дэвид Прайор, демократ от Арканзаса и председатель Специального комитета по проблемам пожилых людей, заявил, что предыдущие комиссары, Служба парламентских исследований Библиотеки Конгресса и Дональд А. Гонья, главный советник по социальному обеспечению, — все они пришли к выводу, что подобная верификация является незаконной.

PWN: Краткие заметки

1. Ложное предупреждение о вирусе (28 марта 1989). Некий человек разместил в государственной сервисной системе в районе залива Сан-Франциско сообщение с «бомбой замедленного действия»: «ВНИМАНИЕ! Компьютерный вирус заразил систему!» Теперь этот человек осознаёт, что подобная шутка воспринимается примерно так же, как заявление о бомбе в ручной клади при посадке на самолёт.
— Брюс Бейкер, Программа информационной безопасности, SRI International

•- -

2. Словарь хакера по-японски? (30 марта 1989). Что это такое, спросите вы? Этот забавный сборник был составлен десяток лет назад аспирантами по искусственному интеллекту (ИИ) из Стэнфорда, MIT и Карнеги-Меллона — они зафиксировали тогдашний жаргон своих общих субкультур. Делали они это ради развлечения, но сборник каким-то образом всё же был опубликован.

«Словарь хакера» содержит немало каламбуров, шуток и прочего, что трудно поддаётся переводу: например, «moby» — как в «moby memory», или «fubar» с его региональными вариантами «foo bar» и «foo baz».

•- -

3. Воздушные силы AT&T. У AT&T есть авиация, патрулирующая трассы её кабелей, — на некоторых маршрутах круглосуточно, 365 дней в году. В распоряжении «воздушных сил AT&T» — вертолёты и самолёты с неподвижным крылом. В ряде районов AT&T использует пехоту и бронеавтомобили. Сью Флеминг из AT&T говорит: «Мы надеемся НЕ обнаруживать никакой активности. Мы не хотим никого "ловить". Но если мы замечаем землекопов, обычная процедура такова: пилот по радио передаёт координаты наземной команде, которая выезжает на проверку. Иногда сбрасывают записки или даже приземляются — это зависит от того, где находится объект. В некоторых районах — например, в Нью-Джерси — несанкционированная посадка влечёт серьёзные санкции».

•- -

4. Террористическая угроза? Научные советники правительства сообщили сенатской комиссии, что телекоммуникационные сети являются соблазнительными мишенями для террористической деятельности. По словам экспертов, риск возрастает из-за развития технологий — в частности, волоконной оптики, концентрирующей оборудование и данные, — а также вследствие фрагментации телекоммуникационной отрасли после разукрупнения AT&T. Пожар на узле связи в Хинсдейле, Иллинойс, и недавнее обрывание волоконной магистрали в Нью-Джерси наглядно показали, насколько уязвима телекоммуникационная сеть нашей страны.

•----------

5. FCC выносит решение по AOS. FCC вынесла решение по жалобе, поданной этим летом двумя потребительскими организациями против пяти компаний альтернативных операторских услуг (Alternative Operator Services, AOS). FCC признала жалобу обоснованной и обязала компании AOS незамедлительно прекратить ряд практик.

Согласно решению, абоненты должны получать уведомление о том, что их звонок обрабатывается оператором AOS; операторы обязаны сообщать о тарифах; владельцы гостиниц или таксофонов не вправе блокировать звонки другим операторам дальней связи. (Абоненты, не предпринявшие никаких специальных действий при звонке, по-прежнему будут направляться к заранее подключённому оператору.)

FCC также обязала компании отказаться от практики «сплэшинга» (splashing) везде, где это технически осуществимо. Сплэшинг — это перенаправление звонка на удалённую точку присутствия оператора с выставлением абоненту счёта за звонок именно с этой точки.

•----------

6. Отличный новый сервис. Пользователи CompuServe (крупнейшей в мире компьютерной доски объявлений) теперь могут подключаться и искать статьи из множества различных технических отраслевых журналов. База данных составлена компанией Information Access Company. На данный момент она содержит полные тексты статей из 50 изданий и краткие аннотации ещё 75. Большинство материалов охватывают период начиная с января 1987 года.

Можно искать по названию журнала, автору, ключевому слову, ключевой фразе и т. д., затем открывать аннотации интересующей статьи и при необходимости и наличии — её полный текст. Пользоваться системой легко.

Стоимость услуги: $24 в час, $1 за каждую аннотацию и $1,50 за каждый полный текст. CompuServe берёт $12,50 в час за время подключения. Оба почасовых тарифа пересчитываются пропорционально фактически затраченному времени, и поскольку базами данных очень удобно пользоваться, вы вряд ли будете сидеть в системе более 10–15 минут, так что реальные расходы окажутся ниже.

```
CompuServe              800-848-8199
Information Access      800-227-8431
```

•----------

7. Служба идентификации вызывающего номера ISDN (7 апреля 1989). Технический справочник Bellcore TR-TSY-000860, «ISDN Calling Number Identification Services», можно приобрести за $46 по адресу:

```
Bellcore
Customer Service
60 New England Ave
Piscataway, NJ 08854-4196
(201) 699-5800
```

Данный технический справочник содержит позицию Bellcore относительно общих требований к поддержке идентификации вызывающего номера ISDN (I-CNIS). Функция I-CNIS распространяет концепции доставки вызывающего номера и блокировки его доставки на линии ISDN. I-CNIS также позволяет абоненту указывать, какой номер телефонного справочника (Directory Number, DN) следует использовать для каждого исходящего вызова, и обеспечивает сетевую проверку корректности указанного DN. I-CNIS обрабатывает вызывающий номер как для коммутируемых, так и для пакетных вызовов ISDN и предусматривает четыре компонентные функции: предоставление номера, проверка номера, конфиденциальность номера и доставка номера. Также включены материалы об изменении настроек конфиденциальности вызывающей стороной и о

переопределении конфиденциальности вызываемой стороной.

• -

8. Основатель TAP Magazine Эбби Хоффман, родившийся в 1936 году, скончался 12 апреля 1989 года. Его нашли мёртвым в квартире в Нью-Хоупе, Пенсильвания. Он был полностью одет и лежал под одеялом. Вскрытие не дало окончательного ответа. Статья о нём опубликована в номере Time Magazine от 24 апреля 1989 года: «A Flower in a Clenched Fist» («Цветок в сжатом кулаке»), стр. 23.

• -

9. Билл Ландрет, он же The Cracker, автор книги «Out Of The Inner Circle», объявился вновь. По имеющимся сведениям, сейчас он работает переплётчиком в округе Оринджа, Калифорния, и живёт с сисопом доски объявлений под названием «Pig Sty».
— Dark Sorcerer (19 апреля 1989)

• -

10. Хакер/фрикер получил «жёсткое» наказание (Грин-Бей, Висконсин). Дэвид Келси, он же Stagehand, признал себя виновным по двум статьям уголовного преступления класса «E» и был приговорён к 90 дням заключения. По окончании срока ему предстоит трёхлетний испытательный срок и неопределённое количество часов общественных работ.

Помимо этого, Stagehand обязан выплатить компенсацию в размере $511,00 компании Schneider Communications из Грин-Бея, Висконсин. В рамках досудебного соглашения ему вернули всё компьютерное оборудование — за исключением материалов, признанных «незаконно нажитым» имуществом.

Незаконные прослушки Bell — история продолжается

(Примечание: следующий материал является продолжением статьи из предыдущей части выпуска.)

Другой радиолюбитель, Винсент Кларк / KB4MIT, техник South-Central Bell с 1972 по 1981 год, заявил, что устанавливал незаконные прослушки, аналогичные тем, что делал Боб Дрейз, — по приказу своих руководителей и по просьбе местных полицейских в Луисвилле, Кентукки.

На вопрос о том, как он начал заниматься незаконными прослушками, Боб рассказал, что друг позвонил ему и попросил встретиться с сотрудниками полиции Цинциннати. Следственный сержант спросил Боба о возможности прослушки членов организации «Чёрные мусульмане». Он также сказал, что служба безопасности Cincinnati Bell одобрила прослушку и что она проводится для ФБР. Сержант указал на свой масонский перстень — такой же носил и Боб, — иначе говоря, он давал понять, что говорит правду под масонской клятвой, а это для Боба значило очень много.

Поначалу прослушивались преимущественно люди, связанные с наркотиками или криминалом. Однако впоследствии всё вышло из-под контроля — ФБР стало требовать прослушки известных граждан. «Мы начали заниматься людьми с деньгами. Как использовалась эта информация — я вам сказать не могу».

В «Newsday» от 29 января сообщалось, что Дрейз рассказал следователям: среди прослушек, установленных им с 1972 по 1979 год, было несколько на линиях компании Wren Business Communications — конкурента Bell. По всей видимости, когда Wren договаривалась о встрече с потенциальным клиентом, оказывалось, что Bell уже побывала там без вызова. Президент Wren — радиолюбитель Дэвид Стонер / K8LMB.

В разговоре с журналистами Дэйв Стонер сказал следующее:

> *«На мой взгляд, изначальным источником всего этого было ФБР. По всей видимости, ФБР создало структуру по всей территории США, используя начальников служб безопасности различных компаний Bell. Говорят, что в других городах США были аналогичные случаи, как у нас в Цинциннати, но они носили локальный характер — и никто не осознавал общей закономерности».*
>
> *«Связующим звеном всего этого является то, что если углубиться в историю — в эпоху Гувера в ФБР — он, по всей видимости, наладил контакт со службами безопасности AT&T. Существует организация, которая, полагаю, действует по сей день и проводит регулярные встречи сотрудников служб безопасности различных компаний Bell. Это означало, что ФБР могло взаимодействовать с группой из 20–30 человек, представлявших ключевые звенья безопасности всей системы Bell и AT&T в США. Думаю, ключ ко всему этому — в эпохе Гувера. ФБР действовало через эту группу, которая затем создавала нужную активность на местах в результате централизованного планирования».*
>
> *«Я убеждён, что, несмотря на то что многие называют это проблемой начала 1970-х, никакого прекращения этой деятельности по сей день нет. Я практически уверен, что она продолжается. Всё это выглядит как масштабная слежка, частью которой был Цинциннати».*
>
> *«Федеральный прокурор Кэтлин Бринкман находится в положении, в котором не выиграть в любом случае. Если она успешно доведёт это дело до конца — она навлечёт беду на собственное Министерство юстиции. Она не может успешно провести этот процесс».*

Против Cincinnati Bell и полицейского управления уже поданы иски на общую сумму около 200 миллионов долларов. Ряд сотрудников полиции воспользовался Пятой поправкой перед большим жюри, отказавшись отвечать на вопросы о своей роли в схеме прослушек.

Боб Дрейз / WB8QCF подал иск против Cincinnati Bell на $78 за злонамеренное уголовное преследование и клевету в ответ на иск Cincinnati Bell против Боба о диффамации. Сразу после того как Bell подала иск, несколько полицейских вышли вперёд и признались в проведении незаконных прослушек совместно с ними. Полиция Цинциннати заявила, что прекратила это в 1974 году, — хотя, по имеющимся сведениям, другой полицейский утверждает, что прослушки на самом деле прекратились лишь в 1986-м.

Теперь программа CBS «60 Minutes» проявила интерес к цинциннатским событиям и направила туда группу журналистов-расследователей. Эд Брэдли из «60 Minutes» уже взял интервью у Боба Дрейза / WB8QCF, и ожидается, что в течение этого месяца (апрель) мы увидим репортаж «60 Minutes» о слежке ФБР. Также стало известно, что CNN, кабельный новостной канал Теда Тёрнера, готовит разоблачительный материал «Прослушка в Америке».

Призывы усилить борьбу с хакерами — 9 апреля 1989

Из Chicago Tribune (раздел 7, стр. 12b)

«Пусть наказание соответствует преступлению», — требуют руководители компьютерной отрасли.

ДАЛЛАС (AP) — Правовая система не справляется с угрозой, которую хакеры представляют для компьютерных сетей, жизненно важных для корпоративной Америки, — считает один из экспертов.

«Многим компьютерным хакерам дают лишь лёгкий нагоняй», — заявил Марк Лири, старший аналитик International Data Corp., на заседании круглого стола на прошлой неделе.

«Система правосудия должна признать... что эти люди злонамеренны, что они преступники и что они грабят банки ничуть не меньше, чем если бы пришли с дробовиком», — сказал он.

Другие участники дискуссии жаловались на то, что хакерам — благодаря их способности взламывать компьютерные системы — порой даже предлагают работу, в том числе в качестве консультантов по безопасности.

Эксперты выступили на круглом столе, организованном журналом Network World — изданием для пользователей и менеджеров компьютерных сетей.

Компьютерные сети стали жизненно важны для бизнеса: они используются для передачи и обработки информации, а также для управления производственными процессами.

Общество всё шире соприкасается с сетями через такие устройства, как банкоматы, системы бронирования авиабилетов и компьютеры, хранящие информацию о выставленных счетах.

По словам экспертов, компании стали более охотно тратить деньги на компьютерную безопасность после нашумевшего в прошлом году проникновения вируса в общенациональную сеть — его предположительно запустил аспирант [Роберт Таппен Моррис].

«Этот инцидент заставил нас пересмотреть приоритеты в оценке определённых угроз», — сказал Деннис Штайнауэр, руководитель группы управления компьютерной безопасностью Национального института стандартов и технологий.

Однако компьютерная безопасность — это не только защита от несанкционированного доступа, подчеркнул Макс Хоппер, старший вице-президент по информационным системам American Airlines.

Хоппер рассказал, что American Airlines создала для своих компьютерных систем установку «типа Шайенн-Маунтин» как защиту от различных угроз — включая отключение электроэнергии и стихийные бедствия. Проводя аналогию с подземным нервным центром Министерства обороны в горах Колорадо, он отметил, что среди принятых мер предосторожности есть даже трёхдневный запас продовольствия.

«Мы сделали всё возможное, на наш взгляд, для защиты всей среды», — заявил Хоппер.

Хоппер и Штайнауэр указали, что, несмотря на высокотехнологичный образ компьютерного терроризма, это по сути административная проблема, которую следует решать в рамках стандартного менеджмента.

Тем не менее эксперты сошлись во мнении: главная опасность для компьютерных сетей исходит не от внешних хакеров. По их словам, наибольшую угрозу представляют недовольные сотрудники или иные лица, изначально имевшие законный доступ к системам.

Хотя проверка персонала полезна, отметил Штайнауэр, важнее встраивать в компьютерные системы механизмы отслеживания несанкционированного использования и распространять информацию о том, что хакерские действия поддаются отслеживанию.

По словам Штайнауэра, рост компьютерной грамотности населения, а также деятельность некоторых добросовестных хакеров в ряде аспектов помогают специалистам по безопасности.

Расширение знаний «заставляет нас как менеджеров по безопасности не полагаться на невежество [пользователей]», — сказал Штайнауэр.

«Безопасность должна быть частью системы, а не "навязанным дополнением", — заявил Штайнауэр. — И мы, пожалуй, не очень хорошо справились с задачей убедить руководство в том, что безопасность — неотъемлемая часть системы».

Лири из IDC сообщил, что опросы, проводимые организацией среди компаний из списка Fortune 1000, неожиданно показали: значительное число компаний практически не предпринимает усилий для защиты своих систем.

Дискуссия, первая из трёх запланированных Network World, была организована потому, что компьютерный саботаж — «это реальная проблема, о которой люди не знают», — сказал редактор Джон Гэллант.

По его словам, это также проблема, к которой многие отраслевые поставщики не хотят привлекать внимание, поскольку это ставит под сомнение надёжность компании.

Набрал для PWN: Hatchet Molly

Бывший сотрудник обвиняется по делу о вирусе — базы данных стали предполагаемой целью — 12 апреля 1989

Автор: Джейн М. Фон Берген (Philadelphia Inquirer)

Бывший сотрудник был вчера обвинён в заражении компьютерной базы данных своей компании — предположительно в первом случае ареста, связанного с компьютерным вирусом, в районе Филадельфии.

«Мы считаем, что он совершил это из мести», — заявил помощник прокурора округа Камден Норман Мульбайер, комментируя предполагаемый мотив сотрудника, якобы установившего программу для уничтожения баз данных в бывшей компании — Datacomp Corp. в Воорхиз, Нью-Джерси.

Крис Янг, 21 год, проживающий на квартале 2000 улицы Либерти в Трентоне, был обвинён в округе Камден по одному эпизоду компьютерной кражи путём изменения базы данных. Судья Верховного суда Э. Стивенсон Флюхарти освободил Янга под письменное обязательство явиться в суд с залогом в $10 000. В случае обвинительного приговора Янгу грозит 10 лет тюремного заключения и штраф в $100 000. Связаться с Янгом для получения комментариев не удалось.

«Ущерб причинён не был», — сказал Мульбайер, поскольку компания обнаружила вирус до того, как он успел нанести вред. Если бы вирус активировался, он мог бы повредить базы данных стоимостью в несколько сотен тысяч долларов, отметил Мульбайер.

Компания Datacomp Corp., расположенная в торговом центре Echelon Mall, занимается телефонным маркетингом. В компании работает от 30 до 35 сотрудников; она заключила контракт с крупной телефонной компанией на проверку содержимого белых страниц телефонного справочника и продажу выделенных или иных специальных видов объявлений в белых страницах, сообщила представитель Datacomp. База данных, которую Янг якобы пытался уничтожить, — это список имён из телефонной компании, пояснила она.

По словам Мульбайера, в день своего увольнения — 7 октября 1988 года — Янг использовал поддельные пароли для получения доступа к компьютеру компании и запрограммировал вирус на начало разрушения 7 декабря 1988 года — в День Пёрл-Харбора. Янг, работавший в компании с перерывами в течение двух лет — в последнее время в должности супервайзера, — был недоволен полученными неблагоприятными оценками своей работы, сказал прокурор.

В какой-то момент операторы компании заметили сбои в компьютерной системе. Приглашённый для устранения неполадок программист обнаружил, что программа была изменена, и выявил вирус, уничтожающий данные, рассказал Мульбайер. «Чего господин Янг не знал — так это того, что в компьютерной системе имеется множество функций безопасности, позволяющих отследить

конкретную дату, время и терминал, — сказал Мульбайер. — Мы смогли... доказать, что он работал с этим терминалом». Вирус Янга, по словам Мульбайера, относится к типу «логическая бомба» (time bomb), поскольку запрограммирован на срабатывание в определённое время. В данном случае база данных была бы поражена при первом включении компьютера 7 декабря, пояснил он.

Норма Краус, вице-президент материнской компании Datacomp — Volt Information Sciences Inc, — сообщила, что потенциальные потери компании включают не только базы данных, но и время, затраченное на обнаружение и устранение вируса. «Вся работа остановилась», что повлекло задержки выполнения контрактов, сказала она. «Нам просто повезло, что у нас есть сотрудники, способные определить, что пошло не так, и при этом заинтересованные в том, чтобы что-то с этим сделать. В данном случае сотрудник не остановился на починке системы, а продолжил выяснять, в чём была причина». Компания Volt, базирующаяся в Нью-Йорке, ежегодно ведёт бизнес на сумму $500 миллионов, предоставляя такие услуги, как телефонный маркетинг, обработка данных и техническая поддержка. Кроме того, она занимается временным персоналом — в особенности в сфере обработки данных — и монтажом телекоммуникационных систем, рассказала Краус.

Мексиканская телефонная сеть уходит в частные руки? — 17 апреля 1989

Автор: Oryan QUEST (специальный корреспондент по Латинской Америке)

Мексиканская телефонная компания, известная как Telefonos de Mexico, или Telmex, по всей видимости, перейдёт в частную собственность в течение ближайшего года-двух. Мексиканское правительство всерьёз рассматривает возможность продажи контрольного пакета акций в национальной коммуникационной сети, невзирая на серьёзное противодействие со стороны местных профсоюзов, предпочитающих сохранить существующую бюрократическую структуру.

Предполагаемая продажа, представляющая собой часть усилий по модернизации телефонной сети страны — а она *действительно* нуждается в модернизации, — за счёт привлечения большего объёма частных инвестиций вписывается в общую тенденцию к приватизации ранее национализированных отраслей в Мексике.

Мексиканская телефонная компания более года работала над планом реструктуризации стоимостью $14 миллиардов, рассчитанным на пять лет, который, по всей видимости, отведёт роль в преобразованиях AT&T и региональным холдинговым компаниям Bell.

Один из обсуждаемых правительством вариантов — полное разделение Telmex по образцу судебного разукрупнения AT&T несколько лет назад. По этому плану в Мексике появится единая компания дальней связи, которую контролирует государство, тогда как региональные местные и вспомогательные услуги будут предоставлять частные региональные компании.

Представители мексиканского правительства не раз встречались с руководством Southwestern Bell, обсуждая возможность официального предложения. Аналогичные зондирующие контакты с мексиканской стороной предпринимала Pacific Bell. Интересно будет посмотреть, чем это обернётся.

Около двух лет назад журнал Teleconnect Magazine в юмористической статье о разукрупнении опубликовал выдуманную карту территорий, отведённых каждой компании BOC, где Техас, Нью-Мексико и Аризона были объединены в некую структуру под названием «Taco Bell».

Любая телефонная компания, которая возьмёт под управление мексиканскую систему, будет лучше нынешней, которая несколько лет подряд медленно деградирует.

P.S.: Я Требую*, чтобы меня пустили обратно на MSP!*

==Phrack Inc.==

Том 3, выпуск 26, файл 11 из 11