**The History of Information Security**

The history of information security begins with computer security. The need for computer security—that is, the need to secure physical locations, hardware, and software from threats—arose during World War II when the first mainframes, developed to aid computations for communication code breaking (see Figure 1-1), were put to use. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data. Access to sensitive military locations, for example, was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards.

During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage. One of the first documented security problems that fell outside these categories occurred in the early 1960s, when a systems administrator was working on an MOTD (message of the day) file, and another administrator was editing the password file. A software glitch mixed

**История информационной безопасности**

История информационной безопасности берет свое начало с области компьютерной безопасности. Необходимость в защите физических мест, аппаратных и программных ресурсов от угроз возникла в период Второй мировой войны, когда первые основные компьютеры, созданные для содействия в вычислениях при расшифровке коммуникационных кодов (см. Рисунок 1-1), были введены в эксплуатацию. Для обеспечения защиты этих основных компьютеров и сохранения целостности их данных были внедрены различные уровни безопасности. Например, доступ к секретным военным объектам контролировался при помощи значков, ключей и идентификации лиц уполномоченного персонала силами охраны. Растущая потребность в обеспечении национальной безопасности в конечном итоге привела к внедрению более сложных и технологически продвинутых мер по обеспечению компьютерной безопасности.

В эти ранние годы информационная безопасность была простым процессом, состоящим в основном из физической безопасности и простых схем классификации документов. Основные угрозы безопасности

he two files, and the entire password file was printed on every output file.

включали физическую кражу оборудования, шпионаж в отношении системных продуктов и саботаж. Одним из первых документированных инцидентов безопасности, не укладывающихся в упомянутые категории, произошло в начале 1960-х годов. В тот момент администратор системы занимался редактированием файла MOTD (Message of the Day - сообщение дня), в то время как другой администратор редактировал файл с паролями. Из-за сбоя в программном обеспечении произошла перепутка двух файлов, и в результате весь файл с паролями был внесен в каждый выходной файл.

**The 1960s**

During the Cold War, many more mainframes were brought online to accomplish more complex and sophisticated tasks. It became necessary to enable these mainframes to communicate via a less cumbersome process than mailing magnetic tapes between computer centers. In response to this need, the Department of Defense’s Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military’s exchange of information. Larry Roberts, known as the founder of the Internet, developed the project—which was called ARPANET—from its inception. ARPANET is the predecessor to the Internet (see Figure 1-2 for an excerpt from the ARPANET Program Plan).

**1960-е годы**

Во времена Холодной войны было подключено значительно больше главных рабочих машин для выполнения более сложных и утонченных задач. Стало необходимым обеспечить возможность взаимодействия этих главных рабочих машин менее громоздким способом, чем отправка магнитных лент по почте между центрами обработки данных. В ответ на эту потребность Агентство перспективных исследовательских проектов (ARPA) Министерства обороны начало изучение возможности создания резервируемой сетевой системы связи для поддержки обмена информацией в военных целях. Ларри Робертс, известный как основатель интернета, разработал проект, который был назван ARPANET. ARPANET является предшественником интернета (см. рисунок 1-2 за выдержкой из плана программы ARPANET).

**The 1970s and 80s**

During the next decade, ARPANET became popular and more widely used, and the potential for its misuse grew. In December of 1973, Robert M. “Bob” Metcalfe, who is credited with the development of Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security. Individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded: vulnerability of password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorization to the system. Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET. Because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET, network security was referred to as network insecurity. In 1978, a famous study entitled “Protection Analysis: Final Report” was published. It focused on a project undertaken by ARPA to discover the vulnerabilities of operating system security. For a timeline that includes this and other seminal studies of computer security, see Table 1-1.

The movement toward security that went beyond protecting physical locations began with a single paper sponsored by the Department of Defense, the Rand

**1970-е и 80-е**

В течение следующего десятилетия ARPANET стал популярным и широко используемым, и возрос потенциал его злоупотребления. В декабре 1973 года Роберт М. "Боб" Меткалф, которому приписывается создание Ethernet, одного из наиболее популярных сетевых протоколов, выявил фундаментальные проблемы безопасности ARPANET. У отдельных удаленных сайтов не было достаточных средств управления и защиты для защиты данных от несанкционированных удаленных пользователей. Другие проблемы также существовали: уязвимость структуры и формата паролей; отсутствие процедур безопасности для модемных подключений; отсутствие идентификации пользователя и авторизации в системе. Номера телефонов широко распространялись и открыто публиковались на стенах телефонных будок, что предоставляло хакерам легкий доступ к ARPANET. Из-за масштаба и частоты нарушений безопасности компьютера и взрывного роста числа хостов и пользователей на ARPANET сетевая безопасность получила название сетевой небезопасности. В 1978 году было опубликовано знаменитое исследование под названием "Protection Analysis: Final Report". Он фокусировался на проекте, проведенном ARPA, чтобы выявить уязвимости безопасности

Report R-609, which attempted to define the multiple controls and mechanisms necessary for the protection of a multilevel computer system. The document was classified for almost ten years, and is now considered to be the paper that started the study of computer security.

The security—or lack thereof—of the systems sharing resources inside the Department of Defense was brought to the attention of researchers in the spring and summer of 1967. At that time, systems were being acquired at a rapid rate and securing them was a pressing concern for both the military and defense contractors.

In June of 1967, the Advanced Research Projects Agency formed a task force to study the process of securing classified information systems. The Task Force was assembled in October of 1967 and met regularly to formulate recommendations, which ultimately became the contents of the Rand Report R-609.9

The Rand Report R-609 was the first widely recognized published document to identify the role of management and policy issues in computer security. It noted that the wide utilization of networking components in information systems in the military introduced security risks that could not be mitigated by the routine practices then used to secure these systems. This paper

операционных систем. Для временной линии, включающей это и другие ключевые исследования по компьютерной безопасности, см. Таблицу 1-1.

Движение в сторону обеспечения безопасности, выходящее за пределы защиты физических мест, началось с опубликованной статьи, поддержанной Министерством обороны, известной как отчет Rand R-609. В данном отчете предпринималась попытка определить множество контрольных мер и механизмов, необходимых для защиты многоуровневой компьютерной системы. Документ был секретным почти десять лет и сегодня считается важным шагом в направлении исследования компьютерной безопасности.

Безопасность - или ее отсутствие - систем, использующих общие ресурсы внутри Министерства обороны, привлекла внимание исследователей весной и летом 1967 года. В это время системы приобретались с высокой скоростью, и обеспечение их безопасности было насущной задачей как для военных, так и для оборонных подрядчиков.

В июне 1967 года Управление перспективных исследовательских проектов создало рабочую группу для изучения процесса обеспечения безопасности классифицированных информационных систем.

signaled a pivotal moment in computer security history—when the scope of computer security expanded significantly from the safety of physical locations and hardware to include the following:

• Securing the data

• Limiting random and unauthorized access to that data

• Involving personnel from multiple levels of the organization in matters pertaining to information security.

Рабочая группа была сформирована в октябре 1967 года и регулярно встречалась для разработки рекомендаций, которые в конечном итоге стали содержанием отчета Rand R-609.9.

Доклад Rand R-609 стал первым публично признанным известным опубликованным документом, который выделил роль управления и политических аспектов в контексте компьютерной безопасности. В этом отчете отмечалось, что распространенное использование сетевых компонентов в информационных системах военного назначения создает угрозы безопасности, которые нельзя было решить с использованием существующих на тот момент обыденных методов обеспечения безопасности этих систем.

Этот доклад был ключевым моментом в истории компьютерной безопасности, когда область этой дисциплины значительно расширилась, включив в себя следующие аспекты:

* Обеспечение безопасности данных
* Ограничение случайного и несанкционированного доступа к этим данным
* Вовлечение персонала с разных уровней организации в вопросы информационной безопасности.

**MULTICS**

Much of the early research on computer security centered on a system called Multiplexed Information and Computing Service (MULTICS). Although it is now obsolete, MULTICS is noteworthy because it was the first operating system to integrate security into its core functions. It was a mainframe, time-sharing operating system developed in the mid1960s by a consortium of General Electric (GE), Bell Labs, and the Massachusetts Institute of Technology (MIT).

In mid-1969, not long after the restructuring of the MULTICS project, several of its developers (Ken Thompson, Dennis Ritchie, Rudd Canaday, and Doug McIlro) created a new operating system called UNIX. While the MULTICS system implemented multiple security levels and passwords, the UNIX system did not. Its primary function, text processing, did not require the same level of security as that of its predecessor. In fact, it was not until the early 1970s that even the simplest component of security, the password function, became a component of UNIX.

In the late 1970s, the microprocessor brought the personal computer and a new age of computing. The PC became the workhorse of modern computing, thereby moving it out of the data center.

**МУЛЬТИКС**

MULTICS (Multiplexed Information and Computing Service) - операционная система для мейнфреймов, разработанная в середине 1960-х годов при участии консорциума General Electric (GE), Bell Labs и Массачусетского технологического института (MIT). Хотя MULTICS устарел, он привлекает внимание как первая операционная система, в которой безопасность была встроена в ее основные функции.

В середине 1969 года, сразу после пересмотра проекта MULTICS, группа разработчиков, включая Кена Томпсона, Денниса Ритчи, Руда Кенади и Дуга Макилроя, создала новую операционную систему под названием UNIX. В отличие от MULTICS, в которой были реализованы множественные уровни безопасности и системы паролей, в UNIX эти меры безопасности изначально отсутствовали. Поскольку основной задачей UNIX была обработка текста, ей не требовался такой же высокий уровень безопасности, как у её предшественника. Фактически, даже простейший механизм безопасности - система паролей - был внедрен в UNIX только в начале 1970-х годов.

В конце 1970-х годов микропроцессор принёс персональный компьютер и новую эру вычислительной техники. ПК стал основным инструментом

This decentralization of data processing systems in the 1980s gave rise to networking—that is, the interconnecting of personal computers and mainframe computers, which enabled the entire computing community to make all their resources work together.

**The 1990s**

At the close of the twentieth century, networks of computers became more common, as did the need to connect these networks to each other. This gave rise to the Internet, the first global network of networks. The Internet was made available to the general public in the 1990s, having previously been the domain of government, academia, and dedicated industry professionals. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network (LAN). After the Internet was commercialized, the technology became pervasive, reaching almost every corner of the globe with an expanding array of uses.

Since its inception as a tool for sharing Defense Department information, the Internet has become an interconnection of millions of networks.

современных вычислений, переместив их из центров обработки данных.

Децентрализация систем обработки данных в 1980-х годах привела к возникновению сетей - то есть взаимосвязи персональных компьютеров и мейнфреймов, что позволило всему сообществу вычислительной техники объединить свои ресурсы для совместной работы.

**1990-е годы**

В конце XX века сети компьютеров стали более широко распространенными, и возросла потребность в их взаимосвязи. Это привело к созданию Интернета - первой всемирной сети, объединяющей различные сети. В 1990-х годах Интернет стал доступен широкой общественности, ранее он принадлежал государственным учреждениям, академическому сообществу и профессионалам. Интернет обеспечил подключение практически всех компьютеров, способных подключаться к телефонным линиям или локальным сетям с доступом в Интернет. После коммерциализации технологии Интернета стали всеобъемлющими, охватывая почти каждый уголок земного шара и предоставляя разнообразные возможности использования.

At first, these connections were based on de facto standards, because industry standards for interconnection of networks did not exist at that time. These de facto standards did little to ensure the security of information though as these precursor technologies were widely adopted and became industry standards, some degree of security was introduced. However, early Internet deployment treated security as a low priority. In fact, many of the problems that plague e-mail on the Internet today are the result of this early lack of security. At that time, when all Internet and e-mail users were (presumably trustworthy) computer scientists, mail server authentication and e-mail encryption did not seem necessary. Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats.

С момента своего создания как инструмента для обмена информацией в ведомственной сети обороны, Интернет превратился в объединение миллионов сетей.

Вначале эти соединения основывались на фактических стандартах, поскольку стандартов промышленной связи сетей тогда не существовало. Эти фактические стандарты мало что гарантировали в области безопасности информации, однако по мере того, как эти предварительные технологии были широко приняты и стали промышленными стандартами, внесённая некоторая степень безопасности. Тем не менее, на раннем этапе развертывания Интернета безопасность рассматривалась как низкоприоритетная. Фактически, многие проблемы, с которыми сталкиваются сегодня электронная почта в Интернете, являются результатом этого раннего отсутствия безопасности. В то время, когда все пользователи Интернета и электронной почты были (предположительно надёжными) компьютерными учёными, аутентификация почтового сервера и шифрование электронной почты не казались необходимыми. Ранние подходы к вычислениям полагались на безопасность, встроенную в физическую среду центра обработки данных, где находились компьютеры. По мере того, как сетевые компьютеры стали доминирующим стилем вычислений,

**2000 to Present**

Today, the Internet brings millions of unsecured computer networks into continuous communication with each other. The security of each computer’s stored information is now contingent on the level of security of every other computer to which it is connected. Recent years have seen a growing awareness of the need to improve information security, as well as a realization that information security is important to national defense. The growing threat of cyber-attacks has made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure. There is also growing concern about nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.

возможность физически обезопасить сетевой компьютер была потеряна, и хранимая информация стала более уязвимой для угроз безопасности.

**2000 по настоящее временя**

В настоящее время Интернет обеспечивает непрерывное взаимодействие множества незащищенных компьютерных сетей. Безопасность хранящейся информации в каждом компьютере зависит от уровня безопасности каждого другого компьютера, с которым он соединен. В последние годы возрастает осознание необходимости улучшения информационной безопасности и понимание того, что информационная безопасность играет важную роль в национальной обороне. Растущая угроза кибератак заставляет правительства и компании уделять больше внимания защите компьютерных систем управления коммунальными службами и другой критической инфраструктурой. Также возрастает беспокойство относительно возможности государств вести информационную войну, а также о том, что бизнес- и личные информационные системы могут стать жертвами, если не обеспечены защитой.