Global Information Assurance Certification Paper

The Evolution of Security in Today's Networks

Abstract:

This paper discusses the evolution of security in networks. It begins by explaining the development of the predominately mechanical devices that did not require network security because they were not linked together. The paper then moves to the development of the personal computers and the problems that were introduced. The paper discusses the different security measures that were introduced to combat these problems. Next this paper focuses on the development of hacking and what security measures were developed to prevent it. This paper also discusses the fact that the network defenses currently in place will not be enough for the future networks. It concludes with the development and furtherance of biometrics.

The Evolution of Security in Today's Networks

Computers have been a part of human lives for about 5,000 years. Of course, computers have drastically changed in their designs, functions, operations, and popularity within their evolution. Through the evolutionary period, the need for security has also drastically changed. Many implementations of securing computers and the networks they are attached to have been developed.

For example, the abacus, a system of beads arranged on racks, used by merchants in keeping trade transactions did not warrant the need for security.[1] The next major improvement in computers, occurring 12 centuries later, when Blaise Pascal developed the numerical wheel calculator known as the Pascaline, mainly a mechanical device consisting of a brass rectangular box with eight rotary dials used to add sums up to eight digits long.[2] The Pascaline received its modernization in 1634 when German mathematician and philosopher Gottfried Wilhem von Leibniz enabled multiplication. However, the major breakthrough in computing occurred in 1820 when Charles Xavier Thomas de Colmar developed a device that could add, subtract, multiply, and divide—a device more commonly known as the calculator.

Computers that were developed by Charles Babbage in 1822 were the concepts of computing used in computers as we know them today. Charles had a thorough understanding and passion to marry the concepts of mathematics and mechanics. His goal was to develop machines that would not make mistakes. One of his visions was the Difference Engine. "He produced a prototype of this "difference engine" by 1822 and with the help of the British government started work on the full machine in 1823. It was intended to be steam-powered; fully automatic, even to the printing of the resulting

[1] LaMorte, Christopher and Lilly, John. "Computers: History and Development." Jones Telecommunications & Multimedia Encyclopedia. 1999. URL: http://www.digitalcentury.com/encyclo/update/comp_hd.html (16 Nov 02).
[2] LaMorte and Lilly.

tables; and commanded by a fixed instruction program."[3] This system, however, never came to fruition. Charles Babbage's and his assistant, Augusta Ada King, revised his plans for the prototype, obtained funding from the British government, and advertised the goal to develop a general purpose computer. With these plans, Charles Babbage uncovered the fundamental concepts in computers: 1. input devices; 2. stored memory, 3. processors; and 4. output devices.

Inventor Herman Hollerith borrowed Charles Babbage's idea with using cards to instruct the machine. Only, Herman Hollerith used the cards "to store data used cards to store data information which he fed into a machine that compiled the results mechanically."[4] On these cards, one punch referred to a number while two punches masked a letter. These "punch cards" were used extensively in tabulating machines in the business world, what would be known in 1924 as International Business Machines (IBM) computers. These computers that were developed in 1896 still had no networking capability. Because these computers were not connected to one another, the only line of defense needed was, possibly, physical defense; such as physically securing the romm or building these systems resided in. At this point, "hacking" referred to acts of people trying to discover how things worked. For example, "a group of teenage boys hired to run the switchboards were kicked off of a telephone system in New York…The boys were more interested in knowing how the phone system worked than in making proper connections and directing calls to the correct place. In essence, they were trying to "hack" the system to see how it worked."[5]

Vannevar Bush (1890-1974) invented a calculator for solving complex differential equations. The machine consisted of hundreds of gears and shafts required to represent numbers and their various relationships to each other. To eliminate this bulkiness, John V. Atanasoff and his graduate student, Clifford Berry**,** envisioned an all-electronic computer that applied Boolean algebra to computer circuitry. They extended this concept to electronic circuits in the form of on or off and developed the first all-electronic computer by 1940. "Their project, however, lost its funding and their work was overshadowed by similar developments by other scientists."[6]

Computer development then progressed through five generations, which shaped the electronic devices to the modern design. The first generation computers were developed from 1945 to 1956, during the Second World War. These computers generally had operating instructions written for a particular job. "Each computer had a different binary-coded program called a machine language that told it how to operate. This made the computer difficult to program and limited its versatility and speed."[7] Other developments of first generation computers included using vacuum tubes and

---

[3] Hoyle, Michelle A. Computers: From the Past to the Present. "The Difference Engine." 1994 – 2002. URL: http://www.eingang.org/Lecture/difference.html. (25 Nov 02).
[4] LaMorte and Lilly.
[5] Devitt, Michael. Online Technology. "A Brief History of Computer Hacking." 2002. URL: http://www.chiroweb.com/columnist/devitt/. 21 Aug 2002
[6] LaMorte and Lilly.
[7] LaMorte and Lilly.

magnetic drums for data storage. The first generation computers were not designed to work with each other and therefore needed no network defense.

During this first generation, computers were developed by Konrad Zuse to aid in designing aircraft and missiles and by the British to decrypt German secret messages.[8] The latter system, called the Colossus, was kept secret due to its function, hence creating the first need for defense. The type of defense required for the Colossus was basically physical in nature, due to the fact that the Colossus was not networked with any other system.

The next system developed in the WW II generation was the all-electronic calculator, called the Harvard-IBM Automatic Sequence Controlled Calculator, or Mark I Howard H. Aiken produced this system to aid in creating ballistics charts used by the Navy in the war. The system was created with an electronic relay concept, in which electromagnetic signals move mechanical parts and was therefore extremely slow, but effective in solving complex mathematical problems.[9]

After the Mark I was developed, work from a partnership of the U.S. government and the University of Pennsylvania began working on a computer "consisting of 18,000 vacuum tubes, 70,000 resistors, and 5 million soldered joints."[10] This computer, developed by John Presper Eckert and John W. Mauchly was called the Electronic Numerical Integrator and Computer (ENIAC) and considered a general-purpose computer that could process computations up to 1000 times faster than the Mark I.

The era between 1956 and 1963 marked the second-generation computers. Essentially, the development of the transistor that replaced the vacuum tube provided for rapid modernization of computers during this generation. This age of computers also introduced advances in magnetic-core memory. Advances in memory coupled with the development of the transistor paved the way for smaller, faster, and more energy-efficient computers. "Second generation computers replaced machine language with assembly language, allowing abbreviated programming codes to replace long, difficult binary codes."[11] This development produced a boom in the software industry and created a wide variety of technical career fields ranging from programmers to computer systems experts.

IBM's Stretch and Sperry-Rand's LARC marked the first "supercomputers" to take advantage of the transistor. Both systems were "developed for atomic energy laboratories [and] could handle an enormous amount of data; a capability much in demand by atomic scientists."[12] However, these two machines were enormous in size, too expensive, and therefore did not attract the commercial business sector.

[8] LaMorte and Lilly.
[9] LaMorte and Lilly.
[10] LaMorte and Lilly.
[11] LaMorte and Lilly.
[12] LaMorte and Lilly.

The second generation computers did not infiltrate businesses, universities, and government until Burroughs, Control Data, Honeywell, IBM, Sperry-Rand, and others, entered the market and included printers, tape storage, disk storage, memory, operating systems, and stored programs with the computer systems they developed. The IBM 1401 was one of the examples of the systems developed that was "universally accepted throughout industry, and is considered by many to be the Model T of the computer industry."[13] By 1965, most business used these second generation computers to process financial data.

Even though the second generation computers were increasing in popularity and were storing financial data, "hacking" into these systems was still not considered a negative act. "Hacking" in the 1960's was defined as "…shortcuts that would modify and improve the performance of a computer's operating system or applications and allow more tasks to be completed in a shorter time."[14] Obviously, businesses at this point determined that the best line of defense with their systems was physical in nature.

This same mentality of defending the early computers remained even through the development of the third generation computers from 1964 to 1971. This generation introduced the quartz rock which solved the earlier problems of large systems overheating during their processing periods. Jack Kilby, an engineer with Texas Instruments, used the quartz rock in developing the integrated circuit (IC) in 1958. "The IC combined three electronic components onto a small silicon disc." [15] This development provided the thrust for scientists to fit more components on a single chip called a semiconductor. Computer, thus, became smaller, faster, and more reliable. The third generation computers also introduced the use of an operating system that could run many different programs at once as well as monitor and mange the computer's memory.

During the third generation computer era, hacking was essentially limited to the phone system. Computer hobbyist John Draper discovered that a toy whistle could mimic an audio tone that could open a telephone line. He used this discovery to make free long-distance calls. John dubbed the hack as "Captain Crunch," and was arrested several times for tampering with the phone system.[16]

1971 to the present marks the fourth generation computers. During this generation the integrated circuits were being down-sized and more than 100 components were being placed onto these chips known as large scale integration, thus driving up the speed and processing power, exponentially. By the early 1980's, computer manufacturers were compacting hundreds of thousands of components onto one chip known as very large scale integration. "The Intel 4004 chip, developed in 1971, took the integrated circuit one step further by locating all the components of a computer (central processing unit, memory, and input and output controls) on a

[13] LaMorte and Lilly.
[14] Devitt.
[15] LaMorte and Lilly.
[16] Devitt.

minuscule chip. Whereas previously the integrated circuit had had to be manufactured to fit a special purpose, now one microprocessor could be manufactured and then programmed to meet any number of demands."[17] These integration techniques drove down the size and cost of computers, making them more available to the public market. Integrated chips appeared in many household appliances as well as desktop computers.

In 1981, IBM developed a personal computer (PC) for use in the home, office, and schools. IBM's PC became the springboard for several computer manufactures to clone and market, flooding the industry with affordable and practical computers. "The number of personal computers in use more than doubled from 2 million in 1981 to 5.5 million in 1982. Ten years later, 65 million PCs were being used."[18] Manufacturers continued to decrease the size of their computers, thus creating laptop computers and palmtop. Software developers were also included in making the computers more available to the public sector because they were developing operating systems and programs that were easy to operate. They replaced the command-line driven software with graphical user integration; allowing the common person to point and click on pictures to perform many functions.

With computers becoming more popular in business and more powerful, the need was sparked to link them together. This linking together or networking enables computers to share memory space, software, information and communicate with each other. Unlike a mainframe computer, one computer that shared time with many terminals for many applications, networked computers enable individual computers to form electronic co-ops. These co-ops grew by expanding the cabling linking them together into what are called Local Area Networks (LAN), by use of telephone lines and fiber optic lines. LAN's developed into Wide Area Networks (WAN) and Metropolitan Area Networks (MAN) via satellite links, microwave links, etc. As the LAN's, WAN's, and MAN's gained in popularity, the Internet was born. The Internet developed to provide a plethora of information available at the common household user's fingertips. As the Internet exploded in size and popularity, it became an area of concern in the White House. "During the 1992 U.S. presidential election, vice-presidential candidate Al Gore promised to make the development of this so-called 'information superhighway' an administrative priority."[19]

With the Internet providing the means to easily link computers within an office as well as across the world, file/information sharing became rampant. Such information related to individual identity; i.e. an individual's social security number, personal financial data, personal addresses and phone numbers that would be available to anyone in the world, military information; i.e. battle plans, sensitive aircraft/weaponry information, and research and development information, and financial institution information; i.e. personal account numbers. With such information available to anyone, "hacking," as we know it today, was born. For example in the late 1980s, "veteran

[17] LaMorte and Lilly.
[18] LaMorte and Lilly.
[19] LaMorte and Lilly.

hacker Kevin Mitnick secretly monitors the e-mail of MCI and Digital Equipment security officials. He is convicted of damaging computers and stealing software and is sentenced to one year in prison."[20] Also, in the late 1980s, "First National Bank of Chicago is the victim of a $70-million computer heist."[21] In the early 1990s, "a 17-month search ends in the capture of hacker Kevin Lee Poulsen ('Dark Dante'), who is indicted for stealing military documents. Hackers break into Griffith Air Force Base, then pewwwte computers at NASA and the Korean Atomic Research Institute. Scotland Yard nabs 'Data Stream,' a 16-year-old British teenager."[22] In 1998, "hackers claim to have broken into a Pentagon network and stolen software for a military satellite system. They threaten to sell the software to terrorists."[23]

Given these examples and many others, the computer industry, the federal government, and financial institutions determined that security in computers needed to be developed and enforced. As early as 1970, the federal government was the first of these entities to develop computer security measures that paved the way for others to follow. The report drafted by the United Stated Defense Science Board "contained recommendations on minimizing the risk of classified information that was processed on remote-access computer systems. This work led to the founding of the Department of Defense's first computer security standard called the TCSEC; better know as the Trusted Computer System Evaluation Criteria,"[24] which became the standard in computer network security.

The basic fundamentals developed by the Department of Defense in securing their computers was, "secure systems will control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information."[25] From these basic fundamentals, the DoD derived six requirements into their computer security policy. The first requirement, called security policy, mandated a "well-defined security policy enforced by the system."[26] Next, DoD stated that "access control labels must be associated with objects."[27] This requirement was entitled marking. Marking meant that the sensitivity of files as well as the classification of systems had to be labeled accordingly. The third requirement referred to identification. Essentially, this meant that any access to information had to be identified by stating who accessed the data and "what classes of information they are authorized to deal with. This identification and authorization information must be securely maintained by the

---

[20] Trigaux, Robert. St. Petersburg Times Online. "A History of Hacking." 2000. URL: http://www.sptimes.com/Hackers/history.hacking.html. 1 Jan 2003.
[21] Trigaux, Robert.
[22] Trigaux, Robert.
[23] Trigaux, Robert.
[24] Angermiller, Daniel, Bauer, Casey, Patel, Paula, and Turner, Mike. Security and Hacking Group Project. URL: http://webpages.acs.ttu.edu/dangermi/FriendsofClyde-SecurityandHacking.doc. 1 Jan 2003.
[25] Department of Defense, *Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, Dec. 1985. URL: http://csrc.nist.gov/publications/history/dod85.pdf. pp. 9.
[26] DoD. pp. 9.
[27] DoD. pp. 9.

computer system and be associated with every active element that performs some security-relevant action in the system."[28] The fourth requirement in the computer security policy related to accountability, which stated, "A trusted system must be able to record the occurrences of security-relevant events in an audit log."[29] In other words, any action taken on a trusted system required auditing with enough detail, that the action could be traced back to the perpetrator. Not only did the system need to audit all actions, but it also had to store the logs in such away that they could not be manipulated in any way. DoD stated that the computer security policy had to include assurance, the fifth requirement. "In order to assure that the four requirements of Security Policy, Marking, Identification, and Accountability are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions."[30] The last requirement that DoD included in their policy was continuous protection. "The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes."[31]

Corporations have expounded upon the DoD's initiative of implementing security on their networks. According to Donna Howell, in her white paper, "Smart Cards, Firewalls and Biometric Sensors Keep Bad Guys at Bay," major investment organizations have stated, "One of the most basic (in facilitating safe and secure trading) is encrypting customers' financial information as it's sent over the Internet."[32] Investment companies have strongly advised their customers to procure devices that can encrypt and lock personal financial data residing on their local hard drives. This is a layer subsequent to existing personal firewalls, intrusion detection devices, and antivirus software. Such a device is called an A-key, which plugs in to the Universal Serial Bus (USB) port on a personal computer. Currently, Automatic Teller Machines use the same technology incorporated in the A-key; financial data being decrypted after a validated user enters the proper password, or Personal Identification Number.

"Another kind of two-factor security method could rely on a password and one or another biometric (physical measure), such as a fingerprint scan. Laptop computers are available with biometric finger pads to recognize, and grant access to, the owner alone. Desktop PC users can set up their systems in a similar way with a special mouse equipped with a biometric finger pad."[33] What is biometric authentication? According to Maggie Biggs, in her article, "Fraud, negative ROI to lead businesses to embrace emerging biometric techniques," "Biometrics use unique physical or behavioral characteristics to verify identity. Physical biometrics validate things such as faces, hands, fingerprints, and the retina in your eyes. Behavioral biometrics has to do with

[28] DoD. pp. 10.
[29] DoD. pp. 10.
[30] DoD. pp. 10.
[31] DoD. pp. 10.
[32] Howell, Donna. Investor's Business Daily. "Smart Cards, Firewalls and Biometric Sensors Keep Bad Guys at Bay." 25 Nov 2002. URL: http://www.authenex.com/pdf/11252002Investors_Business_Daily.pdf. 17 Feb 2003.
[33] Howell, Donna.

things such as voice or handwriting."[34] Even though biometrics provides much added security, there are major hurdles to overcome before it becomes a common practice. The first obstacle to eliminate is the expense. Biometrics is still in the development stages and is therefore very expensive to procure and implement. Another blockage to its full-scale implementation relates to the error rates involved. For example, the technology incorporated in face recognition, does not compensate for physical changes as a person ages. Biometrics not being widely understood or accepted by the general population presents another hurdle for its full scale implementation. The public cannot discard the "Big Brother" syndrome that biometrics appears to pose. As a matter of fact, "The more intrusive the biometric, the less acceptance you will find."[35]

To address the misconception held by the general public and to further biometrics' popularity, a non-profit organization, known as the International Biometric Industry Association (IBIA) has been formed. As stated in their charter, the "IBIA will serve as the industry's voice, carrying out a program of public education as well as direct advocacy to convince opinion leaders, the public, and government officials that biometric technologies can be trusted to protect privacy, will produce major gains in productivity, can reduce risks, and are user friendly. IBIA will also serve the industry by keeping it informed about key biometric developments worldwide, monitoring the development of standards on behalf of its members, and mobilizing resources to combat legislation and regulation which would inhibit the use of biometric applications."[36] Since this organization's formation, biometrics has cropped some acceptance from the public. The public, along with the business sector and the DoD, have determined that firewalls, intrusion detection devices, passwords and antivirus software are not enough to protect their most sensitive data. With the development of biometrics exceeding expectations, the ease of use being introduced into biometrics, and the cost of implementing biometrics being driven down, facial scanning, retina scanning, fingerprint scanning, etc. will be incorporated into defending the networks in the near future.

In summary, the need for network defense wasn't even thought of in the first developments of computers. However, as the computer system' development progressed from basic mechanical operations to the processing power available today, the general public, business sector, and the DoD have determined the need for network defense paramount. The uses of computers, beginning with experimental and mathematical and moving to being a part of everyone's lifestyle, also drove the increased awareness of network defense. It is evident that computers will be more of a major necessity in every business, military, and personal life. With computer technology being integrated into products such as small and common household appliances, it will be the responsibility of the Information Technology personnel to maintain the highest standards of network defense. As more personal data is stored on the various storage

[34] Biggs, Maggie. InfoWorld. "Fraud, negative ROI to lead businesses to embrace emerging biometric techniques." URL: http://archive.infoworld.com/articles/op/xml/00/08/07/000807opbiggs.xml. 17 Feb 2003.
[35] Biggs, Maggie.
[36] International Biometric Industry Association. Facts About Biometrics, the Biometric Industry, and IBIA. 29 Feb 2000. URL: http://www.ibia.org/understa.htm. 17 Feb 2003.

devices involved with computers and more hacking techniques are developed to crack the different encipherment algorithms it is clear the today's network defenses will not be enough to safeguard the information of the future. It is the IT professional's responsibility to develop and implement more innovative and stronger security measures on the future networks.

Other Authorities

Angermiller, Daniel, Bauer, Casey, Patel, Paula, and Turner, Mike. Security and Hacking Group Project. URL: http://webpages.acs.ttu.edu/dangermi/FriendsofClyde-SecurityandHacking.doc. 1 Jan 2003. 6

Biggs, Maggie. InfoWorld. "Fraud, negative ROI to lead businesses to embrace emerging biometric techniques." URL: http://archive.infoworld.com/articles/op/xml/00/08/07/000807opbiggs.xml. 17 Feb 2003..... 8

Department of Defense, *Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, National Computer Security Center, Ft. Meade, MD 20755 (Dec. 1985). Also known as the "Orange Book." URL: http://csrc.nist.gov/publications/history/dod85.pdf..... 6

Devitt, Michael. Online Technology. "A Brief History of Computer Hacking." 2002. URL: http://www.chiroweb.com/columnist/devitt/. 21 Aug 2002 2

Hoyle, Michelle A. Computers: From the Past to the Present. "The Difference Engine." 1994 – 2002. URL: http://www.eingang.org/Lecture/difference.html. (25 Nov 02). 1

International Biometric Industry Association. Facts About Biometrics, the Biometric Industry, and IBIA. 29 Feb 2000. URL: http://www.ibia.org/understa.htm. 17 Feb 2003..... 8

LaMorte, Christopher and Lilly, John. "Computers: History and Development." Jones Telecommunications & Multimedia Encyclopedia. 1999. URL: http://www.digitalcentury.com/encyclo/update/comp_hd.html (16 Nov 02). 1

Trigaux, Robert. St. Petersburg Times Online. "A History of Hacking." 2000. URL: http://www.sptimes.com/Hackers/history.hacking.html. 1 Jan 2003..... 5