Author:

David "Conundrum" Condrey

Public Relations Representative; United Technologies, Inc.

Date: November 08, 2001

"To follow the path:
look to the master,
follow the master,
walk with the master,
see through the master,
become the master."
- Unknown

Introduction

In the past two decades hacking has seemed to become an ever more present plague amongst the internet. Through the Hollywood aspect it has drawn several hundred's of new users to an imaginary world of hacking which is in fact not at all what hacking is about nor even closely related to the actual everyday actions of a professional or even hobby hacker.

This book is not to teach you how to be a hacker… This book was written only as a means of helping to basically explain and introduce the basic concepts as a reference to security professionals and/or a basic introduction to the true work of hacking to the new legitimate hacker.

Many heard the famous speech given by Al Gore about the "Information Superhighway" that will bring a gift bag of ill-defined, nonspecific treasures to households across the country and the world. But sadly, many persons understanding ends there. Everybody's talking about the Internet, but nobody seems to be saying anything. It seems as if the facts of the Internet were written in a language that can only be decoded by the few people who already know all about the Internet.

This book was written so both those whom may have never touched a computer or those who've had a keyboard on their fingertips since they could read may understand the basic concepts they revolve in.

This book does not go as far as to teach you how to use the Internet or, for that matter, how to use a computer or network. This book simply provides on overview of the basic construct and culture behind the technology. And hopefully by the time you have reached the last page of this document you may have a better understanding of the complexity of what once seemed so simply with the flick of a button, and the cultures and emotions which inhabit the new world of exploration both good and bad. I wrote this book in hopes that it would become a unending work. This first version shall show you the basic concepts of the hacker culture and past. However, you may expect every growing versions of this book as time progresses with, like the world, changing information, more indepth notes. I will also begin going more indepth to the actual technology and programming that makes the internet revolve and is the main aspect of a hackers mind.

If nothing more this book should help to relinquish the endless questions on "Can you teach me how to hack?" from the ignorant kid who's seen a Hollywood hackers movie and wants to break into their school computers or hack a bank, or "Hackers are evil cyber terrorists." From those unknowing people around the world who don't have a basic grasp of anything more than what they are told, or what they see from those illegal hackers arrested endlessly. For you will soon learn that hackers are not evil by the salvation of our technological future… That hacking is not something you learn, but something which grows inside from the early infant stages of life… We are not your cyber terrorist; I will not teach you how to hack… I will teach you how to be a hacker.

The History of Hacking

The internet would not have ever been created if not for hackers. There is; however, some controversy on this subject and most will argue that it was not hackers but the government whom created the internet. This is correct; although you miss one major point… that those in the government whom worked on the creation of the first network protocols to later fuel what we call the internet today where hackers.

The internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The internet is a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location, race or ethnic background. Like no other the internet has united humanity in an overwhelming exchange of ideas and thoughts. However, it is still the most major factor in a hackers life today.

In the 60's and 70's hackers worked to bring the internet together and form a long held dream… Today we undergo a totally different set of goals. As the internet has already been formed, now we work towards the influencing to strengthen the internetwork community and bring a true unification between hackers as a truly seen culture of minds.

In this chapter we will discuss the development and evolution of the Internet from the early years of Arpanet and MaBell phone phreaks to the later years we hold today and where we hope to move in the future.

The internet today is a widespread information infrastructure, the initial prototype of what is often called the National (or Global) Information Infrastructure. Its history is complex and involves many aspects of technology, organizational involvement, communities and culture… And its influence reaches not only to the technical fields of computer communications but throughout society as we move towards increasing use of online tools to accomplish electronic commerce, information acquisition, and community operations.

ARPANET - INTERNET

The first written development regarding what we now call the Internet (or InterNetwork) could be considered as a series of memo's written by J. Licklider whom was working at MIT during the time period around August 1962 discussing his "Galactic Network" concepts. In his papers, he envisioned a globally interconnected computer system to which everyone around the world could quickly and easily access data and programs from any other location. In concept, his ideals were in fact much like the internet as it is today.

Licklider later became the first head of the computer research program at ARPA (The Advanced Research Projects Agency) of the United States government which began in

October of 1962 (In 1971, ARPA changed it's name to DARPA, The Defense Advanced Research Projects Agency, then back to ARPA in 1993 and back to DARPA once again in 1996).

While at ARPA, Licklider was able to convince his predecessors, Ivan Sutherland, Bob Taylor, and Lawrence Roberts who was also a MIT researcher during the same time of Licklider, of the importance of his network concepts. These three people would later become some of the most important personal for the development of the internet.

At this same time the United States Air Force was recruiting the RAND Corporation to do research on how to maintain its command and control over its missiles and bombers after a possible nuclear attack. Baran, the lead director of RAND at the time, was able to complete a document on how this objective could be reached which included the use of a packet switched network which was the first implementation of this kind in history.

Later, in 1964, Leonard Kleinrock, also working on research at MIT, published his first book on his theories of packet switching as a follow up of the short paper on the subject he wrote in July of 1961. While working together in research, Kleinrock was able to further convince Lawrence Roberts of the theoretical feasibility of communications using packets rather than the ideas of using circuits which before then had been the unanimous idea. This was the first major step towards computer networking… The next step would be seen in getting computers to talk to each other which would come in 1965.

In 1965, working with Thomas Merrill, Roberts was able to connect the TX-2 computer in Massachusetts to the Q-32 in California with a low speed dial-up telephone line creating the first wide-area computer network ever created. The result of this project was to provide proof to the legitimacy of the original theories of packet switching and computer networking.

By the end of the following year Roberts was recruited to DARPA to work on developing the computer network concepts and quickly putting together his own plan for the "ARPANET" (This was later published in 1967). At the conference where Roberts presented his paper on ARPANET there was also a following paper on packet network concepts from Donald Davies and Roger Scantlebury. Scantlebury told Roberts about the NPL work as well as that of Paul Baran and others at RAND. As it happened the work at MIT, RAND, and NPL had all proceeded in parallel without any of the researchers knowing about each others work… At this conference the word "packet" was adopted from the work at NPL and the proposed line speed to be used in the ARPANET design was upgraded from 2.4 kbps to 50 kbps.

Two years later in August 1968, after Roberts and DARPA had refined the overall structure and specifications for the ARPANET, an RFQ was released by DARPA for the development of one of the key components, the packet switches called IMP's or Interface Message Processors. Four months later, in December, a group headed by Frank Heart at Bolt Beranek and Newman (BBN) won the RFQ and began working on the IMP's with Bob Kahn playing a major role in the overall design architecture of the ARPA Network.

The network topology and economics were designed and optimized by Roberts, working with Howard Frank and his team at the Network Analysis Corporation. The network measurement system was prepared by Kleinrock and his team at UCLA.

Due to Kleinrock's early development of packet switching theory and his focus on analysis, design and measurement, his Network Measurement Center at UCLA was selected to be the first node, or system, on the ARPA Network. All this came together in September 1969 when BBN installed the first IMP at UCLA and the first host computer was connected. Doug Engelbart's project on "Augmentation of Human Intellect" at SRI (Stanford Research Institute) provided a second node.

SRI supported the Network Information Center, lead by Elizabeth Feinler and included functions such as maintaining tables of host names to address mapping as well as a directory of the FRS's.

The following month, when SRI was connected to the ARPANET, the first host-to-host messages were sent from UCLA to SRI. Two more nodes were then added at the University of Santa Barbara and Utah. These last two nodes made it possible to incorporate application visualization projects.

Glen Culler and Burton Fired of UCSB investigated methods for display of mathematical functions using storage displays to deal with the problem of refresh over the net. Robert Taylor and Ivan Sutherland at Utah investigated methods of 3-D representations over the network.

During the following years, computers were quickly added to the ARPANET and work proceeded on completing a complete host-to-host protocol and other network software.

In 1969, a key step was also taken by Crocker at UCLA in the establishment of the Request for Comments (RFC) series of notes. These memos were intended to be an informal fast distribution way to share ideas with other network researchers. At first the RFC's were printed on paper and distributed via normal U.S. mailing. As the File Transfer Protocol (FTP) came into use, the RFC's were prepared as online files and accessed via FTP servers.

The effect of the RFC was to create a positive feedback loop within the community and provide a base for ideas or proposals presented in one RFC triggered another RFC with additional ideas, and so on… when some consensus had come together a specific document would be prepared.

In 1972, October, Kahn organized a large, and as it turns out, very successful, demonstration of the ARPANET at the International Computer Communication Conference. This was also the first public demonstration of this new network technology to the public. It was also in 1972 that the initial use of electronic mail was introduced.

In March of the same year, Ray Tomlinson at BBN wrote the first basic email message send and read software. In July, Roberts expanded its utility by writing the first email utility program to list, selectively read, file, forward, and respond to messages. From there forward email took off as the largest network application used.

DARPA left three contracts to Stanford, BBN, and UCLA to implement the TCP/IP protocol. The Stanford team, led by Vinton Cerf, produced the detailed specification and a year later there were three independent implementations of TCP that could interoperate.

This was the beginning of a long term development project to evolve the Internet concepts started by the ARPANET. Beginning with the ArpaNetwork, Packet Radio, and Packet Satellite, the experimental environment grow to incorporate essentially every form of network and formed a broad-based research and development community with each expansion being a new challenge. This was the first true realization of the original dreams lectured by Licklider in the early 60's.

The early implementations of TCP were done for large time sharing systems such as Tenex and TOPS 20. When desktop computers first appeared, it was thought that TCP was too big and complex to run on a personal computer.

David Clark and his research group at MIT then set out to show that a compact and simple implementation of TCP was possible to be used on any personal computer. They first produced an implementation with the Xerox Alto and then the IBM PC.

Once compact implementation of the TCP/IP protocol was made available, the development of local area networks (LAN) began to spring up around the United States and flourish what would become the Internet. Ethernet technology was also developed by Bob Metcalfe at Xerox in 1973 allowing coaxial cable to quickly move data.

A major shift occurred as a result of the increase in scale of the Internet and its associated management issues. To make it easier for people to use the network, hosts were assigned names, so that it became unnecessary to remember the numeric addresses. Originally, there were a fairly limited number of hosts so it was feasibly to maintain a single table of all the hosts and their associated names and addresses. The shift to having a large number of independently managed networks meant that having a single table of hosts was no longer feasible and the Domain Name System (DNS) was invented by Paul Mockapetris at the University of Wisconsin to permit a scalable distributed mechanism for resolving hierarchical host names into an internet address.

In 1976 the SATNET (Atlantic Packet Satellite Network) was also born. This network was able to link the United States with Europe using INTELSAT satellites owned by a consortium of several different European countries.

The increase in the size of the internet also challenged the capabilities of routers. Originally, there was a single distributed algorithm for routing that was implemented uniformly by all the routers in the Internet… As the number of networks in the internet grew, this initial design could no longer expand as necessary. This made it necessary to replace the original routing algorithms with a model of hierarchical routing with an Interior Gateway Protocol (IGP) used inside each region of the internet, and an Exterior Gateway Protocol (EGP) to be used to tie the regions together. This design permitted different regions to use a different IGP, so that different requirements for cost, rapid reconfiguration, robustness and scale could be accommodated. Not only the routing algorithm, but the size of the addressing tables, stressed the capacity of the routers.

Around this period of the, in 1979, USENET, created by Steve Bellovin, came into use along with BITNET ("Because it's Time" Network), created by IBM, for the use of email and listservs.

As the internet began to evolve, one of the major challenges was how to propagate the changes to the software… particularly the host software. DARPA then decided to support the Berkeley research labs to investigate modifications to the UNIX operating system, including the incorporation of TCP/IP into the OS. Although Berkeley later rewrote the BBN code for the protocols to more efficiently fit into the UNIX system and kernel, the incorporation into the Unix BSD system release provide to be a critical element in dispersion of the protocols to the research community. Much of the CS research community began to use Unix BSD for their day-to-day computer environment.

One of the more interesting challenges was the transition of the ARPANET host protocol from NCP to TCP/IP as of the first of January, 1983 after Barry Leiner had taken over management of the Internet research program at DARPA. This required that all hosts must convert simultaneously or be left behind. This transition was carefully planned within the community over several years before it actually took place and in the end went surprisingly smoothly.

Three years earlier in 1980 the TCP/IP standards were adopted as a defense standard. This enabled defense to begin sharing in the DARPA internet technology base and led directly to the eventual partitioning of the military and non-military communities. By 1983, ARPANET was being used by a significant number of defense research and development and operational organizations. The transition from NCP to TCP/IP then permitted it to be split into a MILNET supporting operational requirements and ARPANET supporting research needs.

The following year in 1981, (the year I was born as a matter of fact), the National Science Foundation created a backbone known as CSNET with 56 kbps networking (while ARPANET was currently using 50 kbps networking) for institutions that did not currently have access to the ARPANET. Vinton Cerf later proposed a plan for internetworking the ARPANET and CSNET.

In 1984, a contract was given to MCI from CSNET to help in several upgrades. New circuits were made to be T1 lines, 1.5 Mbps. IBM also helped provide advanced routers and Merit would manage the network. After upgrades, the CSNET was changed to be called NSFNET (National Science Foundation Network) and the older lines remained as the original CSNET. NSFNET was finally completed in 1988.

At this time the ICCB was also disbanded by Leiner and Clark after recognizing that the continuing growth of the Internet community demanded a restructuring of the coordination mechanisms. The ICCB was then replaced by a structure of Task Forces, each focused on a particular area of the technology be it routers, end-to-end protocols, etc… The Internet Activities Board (IAB) was the first department formed from the Task Force. Coincidently the chairmen of the Task Forces ended up remaining as the same people as the members of the previous ICCB, David Clark continued to act as the senior member.

After some minor changing of membership on the IAB, Phil Gross became the chair of the revitalized Internet Engineering Task Force (IETF), which at the time was only a section of the IABTF.

By 1985, the Internet was already well established as a technology supporting a broad community of researcher and developers and was beginning to be used by other communities for daily computer communications. Electronic mail was being used broadly across several areas.

In 1990, MERIT, IBM, and MCI formed a non-profit corporation, the Advanced Network and Services Corporation (ANS) to conduct research into high speed networking. Soon, they were able to come up with concepts for the T3 43 Mbps lines. NSFNET quickly adopted the new network and was fully upgraded by the end of the following year.

As the T3 lines were being incorporated in the NSFNET, the United States decided to disband the original ARPANET for lack of the fact that the ARPANET was quickly becoming out of date. As ARPANET was disbanded, it was replaced by the NSFNET backbone on the new T3 connections. Four years later, NSFNET upgraded once again to the Asynchronous Transmission Mode (ATM) backbone providing 145 Mbps transfer

The following year, CSNET, consisting of 56 kbps lines, was also disbanded. And the NSF established a new network named NREN, the National Research and Education Network, to conduct high speed networking research along with the Advanced Network and Services Corporation.

By 1992, yet another reorganization took place. In 1992, the Internet Activities Board was reorganized and renamed to the Internet Architecture Board operating under the auspices of the Internet Society which was formed in the same year. A relationship was formed between the IAB and IESG, with the IETF and IESG taking a larger responsibility for the approval of standards in this new technology.

The World Wide Web (WWW) was also released by CERN created by Tim Berners-Lee first designed to help in development for the large high-energy physics collaborations of corporate America having a demand for instantaneous information sharing between physicists working in different universities around the country and institutes all over the world.

Berners-Lee, along with Robert Cailliau, wrote the first WWW browser running under NeXTStep, along with the first WWW server and communications software, defining URL, HTTP, and HTML.

A new coordination organization was also formed, the World Wide Web Consortium (W3C). Initially led from MIT's Laboratory for Computer Science by Tim Berners-Lee and Al Vezza, W3C had taken on the responsibility for evolving the various protocols and standards associated with the Web.

Media Overflow

When our country was first formed, there was one thing that controlled the government. Along with the Executive, Judicial, and House branches the one thing that policed them all was the media. The media press was, and remains as, the one thing that always keeps us informed of the news we need in order to make our own decisions. When you have a third party giving you your news on which to base decisions then is the decision truly your own…? The press reports on when something wrong is happening, or when an event has occurred. One example being in the late 1960's we were shown raw footage of soldiers getting killed in Vietnam despite the attempts of the armed forces to censorship. However lucky, we like to believe things today our different… that we're a free country, with free ideas, and we've fixed all our previous mistakes.

Now, thanks to several acts passed by the Reagan, Bush, and Clinton, administrations, corporations are able to easily merge, buy and sell, and commence hostile takeovers. One example of this being NBC, which is now owned by General Electric, one of the largest missile industries in our "free" country. Thus, they have editorial control of what goes over the network. "Isn't this war great…? Our missiles work perfectly. We have no choice but to blow North Korea back into the stone-age."… as of the fact that all the other opinions and options have been omitted… Also, it seems more and more that our country's politicians are now being funded by corporations. Why? Because hopefully the government will not mess with all of our illegal activities taking place… Several of the largest funders ironically enough consist of the Tobacco, Liquor, and automotive industries…

We like to believe that we are all in control of our own lives. Truly, the fact is we are controlled in everything we do by the corporations that surround us on a day to day basis. From the food we eat, the soda we drink, the clothes we wear…

Radio

From the early days of the invention of the telegraph and telephone to radio communications in the late 19th century, the media has had our complete attention in making us think… what they want us to think.

As with most innovations, there was a lag between the development of broadcasting, and formal recognition of its existence by the government regulators.

As radio technology advanced, public fascination multiplied in quadruple intervals. New American patents improved on Marconi's wireless telegraph, bring in live radio music and voice… The Navy bought receivers and transmitters encouraging research and development into even more advanced technologies. But of course one sure way to make money in radio was to sell stock…

Hackers, in those days weren't even called hackers yet, but simple amateurs, tinkerers. These were people who would buy parts to concoct receivers and transmitters. The trendy technology attracted young men most of all with woman coming soon after with the movement of woman's rights and the desire to make a stand. Colleges and home garages were important centers of tinkering. There was exciting listening to snippets of Morse code, and the occasional music or voice. Response by radio or even mail at the time was a thrill.

Amateur radio traffic grew enough to interfere with naval operations. So by law, when the United States entered World War I in 1917, all amateur radio equipment was ordered to be shut down and the Navy took over all commercial ship-to-shore stations. The Navy and Army bought most all receivers and transmitters.

All along, patents were crucial. AT&T, interested in amplifying voice along thousands of wire miles, bought rights to signal amplification patents. General Electric, maker of light bulbs, developed high vacuum tubes and an advanced alternator. American Marconi held its original patents.

By 1920 the federal government, mostly the Navy, was radio's 900-pound gorilla. It controlled ship and store stations, manufacturing, research and development, and man power. Many tinkerers advanced their radio capabilities… but while in uniform. By the end of the massive World War it was only sensible that the Navy was able to push on Congress its ideas of radio future…

With patents being ever more crucial, AT&T, GE, and RCA, had a complex deal about which could do what with the others' patents. Westinghouse, a major radio manufacturer for the government during the time, saw itself shut out. It scrounged for patents from other inventors, and came up with a few key ones. Then it had the cool idea to operate a powerful transmitter on the roof of it Pittsburg plant. Station KDKA was an immediate hit. In 1922 modern broadcasting was born…

Westinghouse was admitted to the patent-sharing deal. The new business model was clear: AT&T, GE, RCA, and Westinghouse would operate broadcasting stations to give listeners their news, education, and entertainment on a daily routine. Every home would have its own set. Radio would uplift our people and inform our democracy. Broadcast advertising was out of the question. Profits would come from making and selling radios and their parts.

Colleges spent money to set up stations because radio was about education, and was the leading edge technology. They had to be in the game too… Department stores set up stations at their premises to attract customers, by letting them witness, first hand, live broadcasts. They had to be in the game too…

Still, no one really knew how broadcasting would pay. A few stations tried soliciting checks without much success. AT&T went headlong into toll-broadcasting. It set up stations to operate as public phone booths, where citizens who had something to say to the world could pay for a brief broadcast on the air. It also considered using its infrastructure to broadcast to homes by wire, instead of wireless, but saw no future in it…

AT&T's New York toll-broadcasting station, WEAF, became a trailblazer. Connected to other stations by telephone wires, enabling simultaneous identical broadcasts, WEAF had the first real network. The big taboo, the unthinkable moral violation in this new, pure instrument of democracy, was blatant paid advertising. So first there were paid educational talks, actually infomercials as we'd call them today. Then, there were concerts at GB department stores. Regularly scheduled, sponsored entertainment programs starting with the Eveready Hour… Sponsors were not allowed ugly, direct advertising for that would be such a blunt violation of human rights… Rather, they bought consumer goodwill by sponsoring fine entertainment with short reminders of who was paying for the broadcast.

Within a few years, sponsored entertainment evolved into direct advertising. Radio would clearly become a much bigger business than envisioned under any prior business model. The patent deal, not written for this new world, strained as its members rushed for a piece of the pie. All this led the AT&T, RCA, GE, and Westinghouse to start the National Broadcasting Company (NBC) which then bought WEAF from AT&T.

It was 1926. One could see elemental patterns of the radio business popping up everywhere. Hardware makers, signal movers, content creators… And so many interfaces with ordinary people and non-radio specific businesses that in a sense, the whole world consisted of listeners, consumers, or advertisers.

The strength of the media was only increased with the further invention of television. First, as a simple tool for entertainment. Television quickly became the replacement that radio had once been. Bringing news on a daily basis from around the world, to other entertainment broadcasts.

If you were listening to radio in 1931, you probably had a lot on your mind besides music. Sixteen percent of the country was unemployed and the Great Depression was showing no signs of letting up. President Herbert Hoover was being blamed with increasing frequency. 1931 was the year that inventor Thomas Edison died. It was also the year organized crime figure, Al Capone, was sentenced to an 11 year prison sentence for income tax evasion. RCA's Victor Talking Machine Company introduced their 33 1/3 rpm plastic records bringing a new age of recorded entertainment instead of in the past when the only available options to the public were to tune in to their local radio stations if you were lucky enough to have a local radio broadcaster.

Experimental televisions were also just starting to take off with 15 stations on the air. Although few Americans had the money for a television receiver. By the end of 1931, CBS, known as W2XAB at the time, began some minor television broadcasting although, by large, the nation's loyalty still belonged mainly to radio…

1931 saw a new magazine make its debut. On October 15, "Broadcasting" appeared, being published twice a month in its early days. At the time of "Broadcasting's first issue, there were 608 different radio stations on the air in the United States. The census of 1930 said that 12 million of the country's 30 million homes owned at least one radio. While despite the looming depression, there was no lose in radio listening.

As the depression was dying down, in 1937 it was estimated that over 80% of the population had a radio and were even starting to put them in their cars. This was also the year when Americans first truly saw the power of the radio and news with the tragic crash of the Hindenburg. WLS and NBC announcer Herb Morrison had come to New Jersey to do a routine voice-over for a newsreel when before his eyes he became totally aware of an airship exploding and bursting into flames only a few hundred yards from where he stood. Morrison ended up reporting something far from routine and showed the world how important radio truly was for the first time. Television had yet to show any truly moving advantages over radio…

Film & Television

The first working device for analyzing a scene to generate electrical signals suitable for transmission was a scanning system proposed and built by Paul Nipkow in 1884. The scanner consisted of a rotating disc with a number of small apertures arranged in a spiral, in front of a photo-electric cell. As the disc rotated, the spiral of 18 holes swept across the image of the scene from top to bottom in a pattern of 18 parallel horizontal lines.

The Nipkow disc was capable of about 4,000 pixels per second. The scanning process analyzed the scene by dissecting it into picture elements. The fineness of picture detail that the system was capable of resolving was limited in the vertical and horizontal axes by the diameter of the area covered by the aperture in the disc. For reproduction of the scene, a light source controlled in intensity by the detected electrical signal was projected on a screen through a similar Nipkow disc rotated in synchronism with the pickup disc.

Despite subsequent improvements by other scientists (J. L. Baird in England and C. F. Jenkins in the United States) and in 1907 the use of Lee De Forest's vacuum-tube amplifier, the serious limitations of the mechanical approach discouraged any practical application of the Nipkow disc.

Nevertheless, Nipkow demonstrated a scanning process for the analysis of images by dissecting a complete scene into an orderly pattern of picture elements that could be transmitted by an electrical signal and reproduced as a visual image. This approach is, of course, the basis for present-day television.

Nipkow lived in Berlin, although he was of Russian birth. The U.S.S.R. claims a Russian invented television, not because of Nipkow, but another man who experimented with the Nipkow disc in 1905 in Moscow. The Germans, English and Japanese also claim their share of the fame for inventing television.

No one argues, however, that credit for the development of modern electronic television belongs to two men: Philo T. Farnsworth and Vladimir Zworykin. Each spent their lives perfecting this new technology.

A Russian immigrant, Vladimir Zworykin came to the United States after World War I and went to work for Westinghouse in Pittsburgh. During his stay at the company from 1920 until 1929, Zworykin performed some of his early experiments in television. Zworykin had left Russia for America to develop his dream: television. His conception of the first practical TV camera tube, the Iconoscope in 1923, and his development of the kinescope picture tube formed the basis for subsequent advances in the field. Zworykin is credited by most historians as the father of television.

Zworykin’s Iconoscope (Greek for "image" and "to see") consisted of a thin aluminum-oxide film supported by a thin aluminum film and coated with a photosensitive layer of potassium hydride. With this crude camera tube and a CRT as the picture reproducer, he had the essential elements for electronic television.

Continuing his pioneering work, Zworykin developed an improved Iconoscope six years later that employed a relatively thick, 1-sided target area. He had, in the meantime, continued work on improving the quality of the CRT and presented a paper on his efforts to the Eastern Great Lakes District Convention of the Institute of Radio Engineers (IRE) on November 18, 1929. The presentation attracted the attention of another former Russian immigrant, David Sarnoff, then vice president and general manager of RCA. Sarnoff persuaded Zworykin to join RCA Victor in Camden, NJ, where he was made director of RCA's electronics research laboratory. The company provided the management and financial backing that enabled Zworykin and the RCA scientists working with him to develop television into a practical system.

Both men never forgot their first meeting. In response to Sarnoff's question, Zworykin, thinking solely in research terms, estimated that the development of television would cost $100,000. Years later, Sarnoff delighted in teasing Zworykin by telling audiences what a great salesman the inventor was. "I asked him how much it would cost to develop TV. He told me $100,000, but we spent $50 million before we got a penny back from it."

By 1931, with the Iconoscope and CRT well-developed, electronic television was ready to be launched and Sarnoff and RCA were ready for the new industry of television.

The only competitor RCA had in this new market venture was a young teenager at the age of 19 in Idaho.

Legend has it that Philo Farnsworth conceived of electronic television when he was a 15 year old high school sophomore in Rigby, Idaho, a small town about 200 miles north of Salt Lake City. Farnsworth met a financial expert by the name of George Everson in Salt Lake City when he was 19 years old and persuaded him to try and secure venture capital for an all-electronic television system.

The main concern of the financial investors whom Everson was able to persuade to put up money for this unproven young man with unorthodox ideas, was that no one else was investigating an electronic method of television. Obviously, many people were interested in capturing the control over patents of a vast new field for profit. If no one was working on this method, then Farnsworth had a clear field. If, on the other hand, other companies were working in secret without publishing their results, then Farnsworth would have little chance of receiving the patent awards and the royalty income that would surely result. Farnsworth and Everson were able to convince the financial backers that they alone were on the trail of a total electronic television system.

Farnsworth established his laboratory first in Los Angeles, and later in San Francisco at the foot of Telegraph Hill. Farnsworth was the proverbial lone basement experimenter. It was at his Green Street (San Francisco) laboratory that Farnsworth gave the first public demonstration in 1927 of the television system he had dreamed of for six years.

Farnsworth was quick to develop the basic concepts of an electronic television system, giving him an edge on most other inventors in the race for patents. His patents included the principle of blacker-than-black synchronizing signals, linear sweep and the ratio of forward sweep to retrace time. Zworykin won a patent for the principle of field interlace.

In 1928 Farnsworth demonstrated a non-storage electronic pickup and image scanning device he called the Image Dissector. The detected image was generated by electrons emitted from a photocathode surface and deflected by horizontal and vertical scanning fields (applied by coils surrounding the tube) so as to cause the image to scan a small aperture. In other words, rather than an aperture or electron beam scanning the image, the aperture was stationary and the electron image was moved across the aperture. The electrons passing through the aperture were collected to produce a signal corresponding to the charge at an element of the photocathode at a given instant.

The limitation of this invention was the extremely high light level required because of the lack of storage capability. Consequently, the Image Dissector found little use other than as a laboratory signal source. Still, in 1930, the 24-year-old Farnsworth received a patent for his Image Dissector, and in the following year entertained Zworykin at his San Francisco laboratory.

Farnsworth's original "broadcast" included the transmission of graphic images, film clips of a Dempsey/Tunney fight and scenes of Mary Pickford combing her hair (from her role in the “Taming of the Shrew”). In his early systems, Farnsworth could transmit pictures with 100- to 150 line definition at a repetition rate of 30 lines per second. This pioneering demonstration set in motion the progression of technology that would lead to commercial broadcast television a decade later.

Farnsworth held many patents for television and through the mid-1930s remained RCA's fiercest competitor in developing this new technology. Indeed, Farnsworth's thoughts seemed to be directed toward cornering patents for the field of television and protecting his ideas. In the late 1930s, fierce patent conflicts between RCA and Farnsworth flourished. They were settled in September 1939 when RCA capitulated and agreed to pay continuing royalties to Farnsworth for the use of his patents. The action ended a long period of litigation. By that time Farnsworth held an impressive list of key patents for electronic television.

Farnsworth died in 1971 and is credited only slightly for the giant industry that he helped create.

There were other attempts to the development of television however unsuccessful, such as the Farnsworth Image Dissector, for studio applications. The most ambitious was the Allen B. DuMont Laboratories' experiments in the 1940's with an electronic flying-spot camera. The set in the studio was illuminated with a projected raster frame of scanning lines from a cathode-ray tube. The light from the scene was gathered by a single photo-cell to produce a video signal.

The artistic and staging limitations of the dimly-lit studio are all too obvious. Nevertheless, while useless for live pickups, it demonstrated the flying-spot principle, a technology that is widely used today for television transmission of motion picture film and slides.

General Electric also played an early role in the development of television. In 1926, Ernst Alexanderson, an engineer at the company, developed a mechanical scanning disc for video transmission. He gave a public demonstration of the system two years later. Coupled with the GE experimental TV station, WGY in Schenectady, New York, Alexanderson's system made history on September 11, 1928, by broadcasting the first dramatic program on television. It was a 40-minute play titled, “The Queen's Messenger”. The program consisted of two characters performing before three simple cameras.

There was a race to see who could begin bringing television programs to the public first. In fact, the 525 line 60 Hz standards promoted in 1940 and 1941 were known as "high definition television," as compared with some of the experimental systems of the 1930's. The original reason for the 30 frame per second rate was the simplified receiver design that it afforded. With the field scan rate the same as the power system frequency, ac line interference effects were minimized in the reproduced picture. Both Zworykin and Farnsworth were members of the committee that came up with proposed standards for a national system. The standard was to be in force before any receiving sets could be sold to the public.

The two men knew that to avoid flicker, it would be necessary to have a minimum of 40 complete pictures per second; this was known from the motion picture industry. Although film is exposed at 24 frames per second, the projection shutter is opened twice for each frame, giving a net effect of 48 frames per second. If 40 complete pictures per second were transmitted, even with 441 lines of horizontal segmentation (which was high definition TV prior to WWII), the required bandwidth of the transmitted signal would have been greater than the technology of the day could handle. The interlace scheme was developed to overcome the technical limitations faced by 1940s technology.

Solid-state imaging devices using a flat array of photosensitive diodes were proposed as early as 1964 and demonstrated publicly in 1967. The charge voltage of each sensor element was sampled in a horizontal and vertical, or X-Y, addressing pattern to produce an output voltage corresponding to readout of the image pixels. The resolution capability of these first laboratory models did not exceed 180-by-180 pixels, a tenth of that required for television broadcasting applications. Nevertheless, the practicability of solid-state technology was demonstrated.

In the first solid state camera system, a video signal was generated by sampling the charge voltages of the elements of the array directly in an *X* and *Y* (horizontal and vertical) scanning pattern. In the early 1970s a major improvement was achieved with the development of the *charge-coupled device* (CCD), in operation a charge-transfer system. The photosensitive action of a simple photodiode was combined in one component with the charge-transfer function and metal-oxide capacitor storage capability the CCD. The photo-generated charges were transferred to metal-oxide semiconductor (MOS) capacitors in the CCD and stored for subsequent readout as signals corresponding to pixels.

Thus, rather than sampling directly the instantaneous charge on each photosensitive picture element, the charges were stored for readout either as a series of picture scanning lines in the interline-transfer system, or as image fields in the *frame-transfer* system.

The early CCD chips were interline-transfer devices in which vertical columns of photosensitive picture elements were alternated with vertical columns of sampling gates. The gates in turn fed registers to store the individual pixel charges. The vertical storage registers were then sampled one line at a time in a horizontal and vertical scanning pattern to provide an output video signal. This approach was used in early monochrome cameras and in three-sensor color cameras. It was also used with limited success in a single-tube color camera wherein cyan, green, and yellow stripe filters provided three component color signals for encoding as a composite signal. The interline system is of only historical interest. Frame-transfer technology is now used in all professional-quality cameras.

Milestones in the development of CCD devices for professional applications include the introduction in 1979 by Bosch of the FDL-60 CCD-based telecine, the NEC SPC-3 CCD camera in 1983, and the RCA CCD-1 camera in 1984.

From the start of commercial television in the 1940s until the emergence of color as the dominant programming medium in the mid-1960s, virtually all receivers were the direct-view monochrome type. A few large-screen projection receivers wire produced, primarily for viewing in public places by small audiences. Initially the screen sizes were 10 to 12-inch diagonal.

The horizontal lines of the two fields on a receiver or monitor screen are produced by a scanning electron beam which, upon striking the back of the picture tube screen, causes the phosphor to glow. The density of the beam, and the resultant brightness of the screen, is controlled by the voltage level of a video signal applied between the controlling aperture and the cathode in the electron gun.

In the old days, viewers were advised to sit at least one foot away from the screen for every inch of screen size as measured diagonally. Thus, if you had a 25-inch screen TV set, you were supposed to sit 25-feet away. In those early days the electron beam scan of the CRT phosphor revealed with crisp sharpness the individual scanning lines in the raster. In fact, the focus of the electron beam was sometimes purposely set for a soft focus so the scan lines were not as easily seen.

All color television picture displays synthesize the reproduction of a color picture by generating light, point by point, from three fluorescent phosphors, each of a different color. This is called an additive system. The hue of each of color light source is defined as a primary color. The most useful range of reproduced colors is obtained from the use of three primaries with hues of red, green, and blue. A combination of the proper intensities of red, green and blue light will be perceived by an observer as white.

Utilizing this phenomenon of physics, color television signals were first produced by optically combining the images from three color tubes, one for each of the red, green and blue primary transmitted colors. This early Trinescope, as it was called by RCA, demonstrated the feasibility of color television. The approach was, however, too cumbersome and costly to be a practical solution for viewing in the home.

The problem was solved by the invention of the shadow-mask picture tube in 1953. The first successful tube used a triad assembly of electron guns to produce three beams that scanned a screen composed of groups of red, green and blue phosphor dots. The dots were small enough not to be perceived as individual light sources at normal viewing distances. Directly behind the screen, a metal mask perforated with small holes approximately the size of each dot triad, was aligned so that each hole was behind an R-G-B dot cluster.

The three beams were aligned by purity magnetic fields so that the mask shadowed the green and blue dots from the beam driven by the red signal. Similarly, the mask shadowed the red and blue dots from the green beam, and the red and green dots from the blue beam.

As television technology began to grow so did the commercialization. Both NBC and CBS took early leads in paving the way for commercial television. NBC, through the visionary eyes of David Sarnoff and the resources of RCA, stood ready to undertake pioneering efforts to advance the new technology. Sarnoff accurately reasoned that TV could establish an industry-wide dominance only if television set manufacturers and broadcasters were using the same standards. He knew this would only occur if the FCC adopted suitable standards and allocated the needed frequency spectrum. Toward this end, in April 1935, Sarnoff made a dramatic announcement that RCA would put millions of dollars into television development. One year later, RCA began field testing television transmission methods from a transmitter atop the Empire State Building.

In a parallel move, CBS, after several years of deliberation, was ready to make its views public. In 1937, the company announced a $2 million experimental program that consisted of field testing various TV systems. It is interesting to note that many years earlier, in 1931, CBS put an experimental TV station on the air in New York City and transmitted programs for more than a year before becoming disillusioned with the commercial aspects of the new medium.

The Allen B. DuMont Laboratories also made significant contributions to early television. While DuMont is best known for CRT development and synchronization techniques, the company's major historical contribution was its production of early electronic TV sets for the public beginning in 1939.

It was during the 1939 World's Fair in New York and the Golden Gate International Exposition in San Francisco the same year that exhibits of live and filmed television were demonstrated on a large scale for the first time. Franklin Roosevelt's World's Fair speech on April 30, 1939, marked the first use of television by a U.S. president. The public was fascinated by the new technology.

Television sets were available for sale at the New York Fair's RCA pavilion. Prices ranged from $200 to $600. Screen sizes ranged from 5-inches to 12-inches. Because CRT technology at that time did not permit wide deflection angles, the pictures tubes were long. So long, in fact, that the devices were mounted vertically. A hinge-mounted mirror at the top of the receiver cabinet permitted viewing.

At the San Francisco Exposition, RCA had another large exhibit that featured live television. The models used in the demonstrations could stand the hot lights for only a limited period. The studio areas were small, hot and suitable only for interviews and commentary. People were allowed to walk through the TV studio and stand in front of the camera for a few seconds. Friends and family members were able to watch on monitors outside the booth. It was great fun, the lines were always long and the crowds enthusiastic. The interest caused by these first mass demonstrations of television sparked a keen interest in the commercial potential of television broadcasting.

The early planners of the U.S. television system thought that 13 channels would more than suffice for a given society. The original channel 1 was from 44MHz to 50MHz, but was later dropped prior to any active use because of possible interference with other services and only 12 channels remained.

Bowing to pressure from various groups, the FCC revised its allocation table in 1952 to permit ultra high frequency (UHF) TV broadcasting for the first time. The new band was not, however, a bed of roses. Many people went bankrupt building UHF stations because there were few receivers available to the public. UHF converters soon became popular. The first converters were so-called matchbox types that were good for one channel only. More expensive models mounted on top of the TV receiver and were tunable.

Finally, the commission issued an edict that all TV set manufacturers had to include UHF tuning in their receivers. This move opened the doors for significant market penetration for UHF broadcasters. Without that mandate, UHF broadcasting might still be in the dark ages.

The klystron has been the primary means of generating high power UHF-TV signals since the introduction of UHF broadcasting. The device truly revolutionized the modern world when it was quietly developed in 1937. Indeed, the klystron may have helped save the world as we know it. And, more than 50 years after it was first operated in a Stanford University laboratory by Russell Varian and his brother Sigurd, the klystron remains irreplaceable, even in this solid-state electronic age.

With the commercialization of television, customers were quick to grow. At the time you were lucky to be able to own a television set, much like was the radio during its early years.

<u>Rebels with a Cause</u>

"The computer underground is both a life style and a social network. As a lifestyle, it provides identity and roles, an operational ideology and guides daily routine. As a social network, it functions as a communications channel between persons engaged in one of three basic activities: Hacking, phreaking, and pirating. Each subgroup possesses an explicit style that includes an ethic and "code of honor", cohesive norms, career paths, and other characteristics that typify a culture."[2]

Hacking, in fact, has been around for over a century… In 1878 they weren't called hackers yet but several teenagers hired to run the switchboards became notorious for disconnecting and misdirecting calls were thrown off the United States brand new Bell telephone system.

One of the first "phreakers" was an MIT student by the name of Steward Nelson. In 1964 Nelson learned how to make the MIT computer generate the frequencies that would allow him to freely make long distance telephone calls.

One of the stranger entries in the phreaking scene was "Joe the Whistler" in 1969. Born blind, he had the unique ability to whistle a perfect 2600 Hz tone. It is this tone that allowed him to access the long distance telephone system. It is rumored that phreakers used to call Joe so they could tune their blue boxes. It was another blind man, Dennie, who gave rise to one of the most famous phreakers, John Draper, also known as Cap'n Crunch.

In 1971, unknown John Draper received an anonymous call from a kid that called himself "Dennie" who showed him how he could make free long distance calls with the simple use of Cap'n Crunch cereal whistles. When the third hole was taped over, this whistle would generate a perfect 2600 Hz tone thus giving one access to the long distance phone system. Cap'n Crunch was also one of the first people to successfully create the blue box which was a home made tool used to automate phreaking with the 2600 Hz tone.

Cap'n Crunch later was able to make blue boxes that would generate several different tones to access different parts of the telephone system or dial internal telephone company numbers. First schooled in the art of phreaking by Dennie, John Draper followed suit by schooling two soon to be famous students in the art of phone phreaking, Steve Jobs and Steven Wozniak, the founders of Apple Computer. John Draper first met Steve Wozniak at UC Berkeley in the winter of 1971 when Wozniak had searched Draper down as an idle to ask him how to use the infamous blue box after reading an article in the Esquire Magazine entitled "Secrets of the Little Blue Box" published in October of that same year. At this time Draper also introduced Wozniak into the Peoples Computer Company (PCC) which later became more organized and turned into the Home Brew Computer Club (HCC).

The new found underground world of phreaking came to the general public's attention in the 1971 article in Esquire Magazine. This article outlined the methods by which a small, group of individuals were outsmarting the American telephone systems in order to make free phone calls around the globe.

John Draper became the idol of phreakers around the world. Draper took phreaking to another level. The focus of his work was not attempting to obtain free phone calls, but rather to access and manipulate the computer system which lay behind the phone system to place even more complex calls with each new attempt.

Prior to the advent of the personal computer, hacking was limited to the activities of phreaking or to those who had access to mainframe computers. As a result, it did not become a widespread activities until the early 80's with the release of personal computers such as the Commodore 64. Hacking was also helped along with such Hollywood representations as the movie "War Games" in 1983.

As the popularity of hacking grew so too did the subculture. Bulletin Board Systems (BBS) grew in profusion. These served as electronic meeting places, where hackers could exchange stories and techniques. Access to a board would be granted or denied based on your technical proficiency or the fame of your exploits. Electronic newsletters and USENET groups also surfaced. One of the first magazines was "2600: The Hacker Quarterly" which started in 1984 and remains today one of the most popular publications.

Part of gaining acceptance in the hacker community was adopting a handle, as phreakers had done in the 1970's. Handles could be based on high-tech allusions or they could be dark and violent descriptions. Nonetheless, lurking behind these grandiose names was often a young teenager with the overwhelming thirst only for knowledge.

Some hackers formed more cohesive communities or groups. One of the first was the 414 Group, named after an area code in Wisconsin. There was also the Legion of Doom, one of the most famous groups, which sprung to life in 1984 with a hacker by the handle of Lex Luthor. The Legion of Doom also helped in the formation of Masters of Deception created by one of the original members of LOD, Phiber Optik.

In these early days, most hackers were united in their goals and desires. The primary goal was to explore the wide world of technology that was opening up.

Sadly, even through the golden years of blooming hackers, hacking did not escape the notice of authorities. Pat Riddle, or Captain Zap, was the first hacker to be prosecuted by the US government in 1981 for theft of goods and phone service. Zap had regularly invaded the Department of Defense computers for several years. Deficiencies in the criminal code meant that an individual could not be prosecuted simply for breaking into a system. This was however remedied in 1985 through amendment to the Computer Fraud and Abuse Act in the United States. Amendments to the Criminal Code of Canada were also made in 1986.

An increasing number of hackers in the late 80's were no longer satisfied with simply looking around at system. Many were using their skills for more criminal pursuits and created the first black-hat hackers and warez. The distribution of pirated software and games was commonplace. Some of the early hackers felt that a new generation had entered the scene, a generation that cared little for the original hacker ethics of exploration but not destruction, which cared little for the principle of freedom of technology but were rather more interested in individual profit.

True hackers began to separate themselves from what they termed the black-hats, lamers, and warez and script kiddies: more derogatory terms to identify these new groups of illegal software traders, and hackers whom were unwilling to abide by the hacker ethics.

The first known virus attack also occurred at the University of Delaware during this period in 1987. It caused some minor system errors but no permanent damage. The following year in November, another virus was released on the ARPANET system which spread through the government and university computer systems within a few hours. The virus was actually a worm created by Robert Morris Jr., the son of one of the lead researchers at the National Computer Security Center. Apparently Morris had been motivated by curiosity and had not envisioned that his program would in fact cripple the entire network for weeks. He was later tried and convicted by the US government, but his sentence was reduced as it was alleged that "no fraud or deceit was actually intended.

Since the late 80's, viruses have become a favorite weapon of attack among black-hats and successfully formed several multi-million dollar organizations for the development of anti-virus/anti-worm/anti-trojan software and programs. However, an ever increasing fear of viruses and their effects have contributed in the attack against all hackers good and evil by government authorities and the general public and media alike.

The Newbie Guide

"Welcome to the 21st Century. You are a Netizen (Net Citizen), and you exist as a citizen of the world thanks to the global connectivity that the Net makes possible. You consider everyone as your compatriot. You physically live in one country but you are in contact with much of the world via the global computer network. Virtually you live next door to every other single netizen in the world. Geographical separation is replaced by existence in the same virtual space."[3]

A 'newbie' is actually simply the term hackers give to other hackers whom have just started learning and still do not have much knowledge. Often times, it is often also give to hackers who have entered a new organization or bulletin board where they are not known yet. It is not meant as a title of disgrace or disrespect but simply one of many titles in the hacker culture. As a newb it is your one goal to learn.

To become a hacker, you must first learn that… learning is not what will make you a good hacker. To be a hacker you must first understand that you are already a hacker. What makes a hacker who they are? Simply… the desire. The desire to learn, the desire to explorer and expand, to ask the questions no one else is asking.

The hacker mind-set is not confined to the software/hardware systems that most people think of. Hackers apply there attitude to all nature of things, music, art, science…

You must also learn and understand that there is another group of people who openly call themselves hackers… but aren't. These are people who get a fun out of breaking into a computer simply to crash it, or phreaks the phone system to call the Pope. Real hackers call these people 'lamers' or 'script-kiddies' or 'cracker'. You must understand, the ability to break security does not make you a hacker any more than being able to hotwire a car make you a car thief. Unfortunately, many journalists have been masked into using the work 'hacker' in unison with 'lamer' or 'cracker'.

The basic difference: hackers build things…, crackers break them…

Hackers solve problems, build, and expand on ideas. For the most part, they believe in freedom of information, and voluntary mutual help. To be accepted as a hacker, you must not only behave as though you have this similar attitude, but you must live it, feel it. A hacker is not a word, but a person, a culture.

Becoming the kind of person who believes in these things is important to *you*, for helping you learn. As with all creative arts, the most effective way to become a master is to imitate the mind set of masters… not only intellectually but emotionally as well.

Creative brains are a valuable, limited resource. They should not be wasted on reinventing the wheel when there are so many other more fascinating new problems waiting to be solved.

One of the most important aspects of becoming a successful hacker is to learn to research. This is probably the single most important quality to any hacker. Although hackers, for the most part, are always willing to help another; we can only open the doors. You are the one who must walk through and explore. Asking a question that can easily be answered on your own, or has already been answered is probably one of the worst things a hacker could do.

Contrary to popular belief, you don't have to be a *nerd* to be a hacker.

The Community

Joining a community or hacker organization is natural for any hacker to do. As a hacker you will often find that you have been classified by the media as an outcast and may have a hard time finding friends. However, the culture of hacking offers numerous outlets for hackers to join together to either collate on a project, to discuss theory or politics, or just chat as friends.

Like most cultures without a money economy, the world revolves around reputation. You solve an interesting problem or help another, how interesting they are, and how well you did the work is what will give you status in a community.

Accordingly, when you work as a hacker, you may learn to tally the score of your reputation in your head on a scale of those around you and what they think of you. This is simply another aspect to the desire to surpass each other…

Specifically, "hackerdom" is what anthropologists would call a gift culture. You gain status and reputation in it not by domination, beauty, or by what you have, but what you give others. Specifically, giving away your time, creativity, and intellect.

Hackers also like to judge others on not how they look, what color or race they are, what religion they hold dear, but how they act. These can be seen in a variety of different aspects: Your debate and discussion skills, how well you hold a conversation with others, how willing you are to help, and most importantly your written English… You will be surprised how many hackers, may write code quite well, but will often misspell or miss-punctuate when writing.

The Final Do's & Don't

Once you know what a hacker is, you must learn to abide the rules of the culture or you will quickly find yourself an outcast of your own.

Do’s

? Learn to program as soon as possible.
? Get involved with a community to help you learn and earn status within.
? Read.

Don’ts

? Do not choose a stupid or over-used handle (name). Your handle should be something that best describes your character or past.
? Do not get into ‘flame-wars’ with others.
? Do not think that you are an elite hacker because you read this book or some other text. There is always someone better…
? Do not write with bad grammar or spelling errors.
? Do not post your own website whenever you talk to someone. Advertising is often despised by others, also known as *spamming*.

Why was this the smallest chapter in the book...? Because as a hacker you must learn to be a true hacker on your own. No one can tell you how to fully be a hacker. You learn and experience, and someday you may look in the mirror and call yourself a real hacker. No one can truly tell you who a hacker is or how they act. All we can do is guess; because being a hacker is not something you can see or feel but something that is in your heart.

Security… Guide to

On top of everything, security *is* the single most important aspect to an intellectual hacking career. It can be argued, that a hackers main purpose is security. We infiltrate a network so as we can find holes in the secure and become better enlightened to fixing the problems and advancing the technologies. However, before you can advance on the current technology for stopping the attacks you must learn, in and out, what the attacks are, how they operate, and then how they can be stopped…

The Attacks

There are several different types of computer security attacks that are used across the internet. However, probably the most common of these would be the famous “Denial of Service” attacks (or DoS).

Denial of Service

A Denial of Service (DoS) attack is not a virus but method illegitimate hackers (aka. Cracker aka. Script Kiddie) use to prevent or deny legitimate users access to a computer.

DoS attacks are typically executed using a variety of pre-programmed tools that can send many request packets to a targeted Internet server using html, ftp, or mail servers which flood the server's resources, making the system unusable. Any system that is connected to the Internet and is equipped with TCP-based network services which have not already been protected from these attacks is subject to them.

Denial of Service attacks are the most common infliction upon the internet today. Because of the fact that these attacks are probably the easiest to inflict, not to mention the variety of pre-programmed applications that can easily automate these attacks, “script-kiddies” as well call them, have taken up DoS’ing as a favorite new past-time.

It is difficult to trace the origin of the request packets in a DoS attack, especially if it is a distributed DoS attack. It is impossible to prevent all DoS attacks, but there are simple precautions server administrators can take to reduce the risk of being compromised by a DoS attack. For example, disabling ICMP response to protect from a Smurf-type attack or configuring a router to filter and check if an IP coming from the outside has an external IP to avoid a TFN type attack.

The Buffer Overflow

The most typical, and used, type of DoS attack is the buffer overflow attack. These attacks work by simply sending more traffic to a network address than the data buffers can handle. Some basic examples of this could be sending email messages with 256 character file attachments, sending oversized ICMP packets, or simply sending an email with an extremely large subject line.

The SYN Attack

Not quite as common as the buffer overflow attack, but still often used, is the SYN attack. When a session is initiated between the TCP client and the server in a network, a very small buffer space exists to handle the usually rapid handshake exchange of messages that set up the session. The session establishing packets include a SYN field that identifies the sequence in the message exchange. As you can see, an attack can easily send a number of connection requests very rapidly and then fail to respond to the reply. This will then cause the first packet to remain in the buffer and leaving the server unable to accommodate other, legitimate, connection requests. Although the packet in the buffer is dropped after a certain period of time without a reply, the effect of many of these fake connection requests is to make it difficult for legitimate requests to get established.

Teardrops Falling

The next attack we will discuss is the “Teardrop” attack which exploits the way that an IP requires a packet that is too large for the next router to be divided into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. In the teardrop attack, the attacker’s IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it will thus cause the system to crash.

Smurf, Infamous… not Famous
Next is the ever famous Smurf. Here, the perpetrator sends an IP ping request to a receiving site. The packet then specifies that it be broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service. The result will be an excessive number of ping replies flooding back to the system and thereby spoofing the host. If the flood was successful, the spoofed host will no longer be able to receive or distinguish real traffic.

Credits

Written & Edited by: *David “Conundrum” Condrey*
Graphics by: *David “Conundrum” Condrey*
Published by: *The United Technologies Network*
PDF Exported by: *David “Conundrum” Condrey*

Bibliography

[1] ”Corporate Earth: A rant by Amp Divorax” (edited for content by David Condrey)
Original document
[2] ”A Postmodernist Interpretation of the Computer Underground”
[3] ”The Net & Netizens: The Impact the Net has on People’s Lives”
The Internet Society
The World Wide Web Consortium
CERN
The Internet Engineering Task Force
The Internet Architecture Board
The Internet Research Task Force
The RAND Corporation
USENET
The Living Internet

Further Reading

United Technologies
Fate Research Labs
SoldierX.Com