A Summary of Hacking Organizations, Conferences, Publications, and Effects on Society

Alisha Cecil [acecil19@yahoo.com]

Abstract

Since the early 1970's, hackers have been prevalent throughout the computing world. Two main categories of Hackers have evolved: the Open Source and Free Software group and the Security Hackers group. This paper details some of the more notable groups and individuals of each 'category' of hackers, the effects of hacking on society, as well as conferences and publications that they are responsible for that have contributed to the modern hacking world.

Table of Contents

1.0 Introduction

Since the early 1970's, hackers have been prevalent throughout the computing world. They come in all shapes,

sizes, and colors. Some act with good intentions, others with ill intentions, and yet others with a mixture of both. No matter what the intentions were, the outcomes of their actions affected the world in some way. New organizations, such as Microsoft and Apple were founded and a new 'open and free' attitude towards software development evolved. However the good came along with the bad. Some hackers were more interested in their own personal gain and strived to circumvent security measures that existed. The rest of this paper details some of the more notable groups and individuals of each 'category' of hackers, the effects of hacking on society, as well as conferences and publications that they are responsible for that have contributed to the modern hacking world. Figure 1 below provides a timeline of the notable events that are discussed in this paper.

Before beginning the discussion on the different groups, it is first important to be aware of the different styles of hacking that exist.

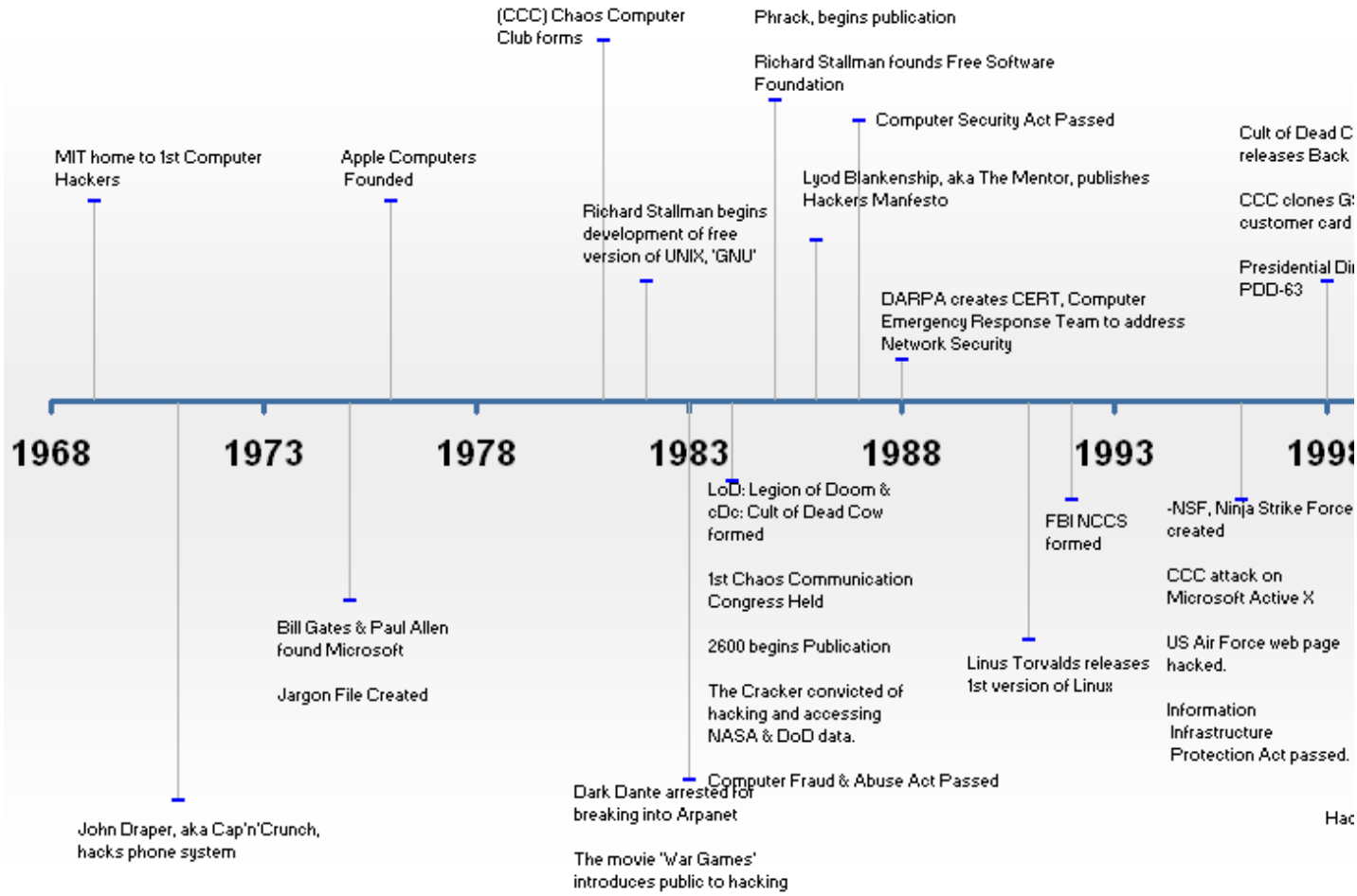

Figure 1: Hacking History [Timeline07]

Back to Table of Contents

2.0 Hacking Styles

When you hear the word HACKER you typically think of a person who has gained access to a system they do not have permission to access. It is generally perceived with a negative connotation. A hacker can in fact be a person who acts in a legal or illegal way. According to Wikipedia, three categories of hackers exist. A White Hat hacker is a person who engages in ethical hacking. These include members of the open source and free software movement as well as home computer hobbyists. White Hat hackers do not participate in illegal activities, as opposed to a Black Hat hacker who illegally engages in computer trespassing. Black Hat hackers

generally have a malicious intent and carry out activities that will negatively affect others. The third category of hackers that has evolved is the Grey Hat hacker. Grey Hat hackers are a hybrid of white and black hat hackers. They sometimes act legally with good intentions, while other times illegally for their own personal gain. [Hacker07]

Now that the different styles have been described, it is important to understand the high-level theories to which there actions can be derived.

Back to Table of Contents

3.0 Hacker Etiquette & Ethics

Hacker Ethic is a term that was first used in *Hackers: Heroes of the Computer Revolution* written by American journalist Steven Levy in 1984. The ideology behind hacker ethics came from the values of the hackers at the MIT Artificial Intelligence Laboratory. The key points are as follows: [Hacker07]

- "Access to computers - and anything which might teach you something about the way the world works - should be unlimited and total. Always yield to the Hands-on Imperative!"
- "All information should be free."
- Mistrust authority- promote decentralization."
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position."
- "You can create art and beauty on a computer."
- "Computers can change your life for the better."

The difference between how these principles are put to use is all in how they are construed. For example Black Hat hackers may read the first principle, access to computers, as right to obtain access in any way possible from any system in the world at any cost.

The Jargon File, a glossary of hacker slang created in 1975 from multiple technical cultures, also provides a definition of hacker ethic [HackerEthic].

- 1. "The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing open-source code and facilitating access to information and to computing resources wherever possible."
- 2. "The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality."

Most hackers accept the term hacker ethic as in number one above. There are a few groups, such as GNU, that go further and believe all information should be free and any proprietary control of it is bad. Definition two is a bit more controversial. Some see the act of cracking as unethical, while others believe that 'ethical' cracking excludes destruction and therefore see themselves as harmless crackers. With this view they see it as a good thing that they can break into a system and then notify the administrator exactly how the system was compromised and how they can fix it.

More generally, hacker ethic "is that almost all hackers are actively willing to share technical tricks, software, and possibly computing resources with other hackers" [HackerEthic]. The groups and individuals discussed below have done exactly that. They have shared knowledge in the form of new software suites, vulnerability detection, as well as general computing information with the rest of the world.

Back to Table of Contents

4.0 Hacking Groups & Individuals

There are two main categories of hackers: Computer Security hackers and Open Source and Free Software hackers.

4.1 Open Source & Free Software Hackers

Hackers who fall in the open source and free software category are white hat hackers who see software design as an art form and build programs lightheartedly. This group was developed in the 1960's by academic hackers working with minicomputers and in the computer science field. In the 1990's it became more of what we know as the free software and open source movement. Hackers in this group typically work in the open and go by their real name. They often look down on security hackers and refer to them as crackers.

Programmers working in the academic culture will modify existing code or resources to achieve their end goal. Major contributors to this group include Linus Torvalds, creator of Linux, as well as Dennis Ritchie and Ken Thompson, creators of the C Programming Language. Richard Stallman, founder of the GNU project, is also a contributor to this group. Stallman also founded the Free Software Foundation in 1985. Table 4.1 below is a list of some of the more popular free software products that exist. To view a complete list of products visit http://directory.fsf.org/.

Table 4.1: Abbreviated Free Software List [FreeSoftware]

Free Software	Description
GNU	OS
Linux	OS
SAMBA	File-sharing
Radius	Remote authentication and accounting system
Eclipse	Java based Integrated Development Environment
EMACS	Extensible, real-time editor
OpenSSH	Free implementation of SSH1 protocol
Mozilla	Internet Browser
FireFox	Lightweight Browser
Wireshark	Network Protocol Analyzer
Thunderbird	Redesign of Mozilla mail component
Open Office	Complete office suite
MySQL	Relational database management system

In the late 1970's, with the availability of the MIT's Altain, hobby hacking became popular. Members of this home computing genre, Hobbyists, focus mainly on commercial computer and video games, software cracking, and modification of computer hardware and other electronic devices (modding). The creator of Apple I and II series computers, Steve Wozniak, and the co-founder and chairman of Microsoft, Bill Gates are two individuals that prospered in this era [Hacker07].

All of these individuals worked under the realm of definition one of the Hacker Ethic of the Jargon File, unlike their counterparts the security hackers who more closely followed definition two.

4.2 Security Hackers

Hackers in the security hacking category are mostly black hat hackers working with ill intentions. Some groups and individuals however could better be categorized as grey hat hackers. This category of hackers prefers to be secretive and will often use an alias to conceal their true identity. Their actions will frequently circumvent security measures that have been put in place. This group was initially developed in the context of phreaking, the subculture interested in the public telephone networks, during the 1960's and the microcomputer bulletin board system (BBS) scene of the 1980's. "The BBS is a computer system running software that allows users to dial into the system over a phone line and using a terminal program, perform functions such as downloading software and data, uploading data, reading news, and exchanging messages with other users" [Bulletin07].

With the release of the movie *War Games*
in 1983, public awareness was raised to the idea that national security could indeed be compromised by computer security hackers. This concern materialized when a group of teenage hackers in Milwaukee, WI, known as the 414's, broke into computer systems across the United States and Canada. The 414's received extensive news coverage, which in turn caught the attention of Congressman Dan Glickman. As a result, he called for an investigation and for laws to be established in the area of computer hacking. On Sept 26, 1983 a member of the 414's, Neal Patrick, was called before the US House of Representatives to testify about the dangers of hacking. In turn, six bills on computer crime were introduced by the House later in the year [Hacker07].

The groups below have been major influencers to the security hacking environment and to those which are entering the hacking scene.

4.2.1 Chaos Computer Club (CCC)

Created in 1981, the Chaos Computer Club is one of the biggest and most influential hacker organizations in the world. CCC is based in Germany and is still active today. They became world famous after they hacked the German Bildschirmtext computer network and proceeded to infiltrate a bank in Hamburg. After breaking into the bank, they proceeded to make a deposit into their account of DM 134,000. The following day, with press present, the money was returned. They are more widely known for their public demonstrations of security risks. In 1996 they demonstrated an attack against Microsoft's ActiveX. In 1998 they were able to clone a customer card on the GSM (Global System for Mobile Communications) network. In order to do this they had to circumvent the A10 encryption algorithm.

Aside from their security risk demonstrations, CCC also hosts Europe's largest annual hacker conference known as the Chaos Communications Congress. In addition to the Congress, they also host a Chaos Communication Camp every four years in a city that is near Berlin (cities change each camp). Other undertakings of CCC include the quarterly magazine, Datenschleuder ("data catapult"), and a monthly radio show in Berlin called ChaosRadio [CCC07].

While CCC is an international hacking organization that contributed to the hackers of today, the US was also home to some of the more influential groups as well.

4.2.2 Legion of Doom (LoD)

Legion of Doom (LoD), a hacking organization active from 1984-1990, was founded by a individual going by the name of Lex Luthor. The membership LoD originally comprised of phone phreaks. LoD's name is a taken from the cartoon series "Superfriends," in which Lex Luthor, Superman's arch rival, led a group by the same name. Throughout its existence, LoD was split into LoD and LoD/LoH (Legion of Doom/Legion of Hackers) for the members that were more skilled at hacking than pure phone phreaking [LoD07]. The group itself was more of a state of mind than anything else. During its heyday, if you were hacking it was assumed that you were a member of LoD.

They gained their fame from their creation of the first invitation only hacking based BBS. The BBS had a security system that caused the system to remain idle until a primary password was entered. LoD's BBS was also the first to engage in behaviors such as social engineering. To ensure the high quality of message content, access was only allowed to highly knowledgeable users. The members of the group also tried to stay very low key and therefore only traded info to select BBSs and via personal telephone conversations.

Like the CCC, LoD published a semi-regular electronic magazine, The Legion of Doom Technical Journal, which contained files and other items of interest to the hacking community. Copies of the Technical Journals can be found at http://www.textfiles.com/magazines/LOD. Its name is a parody of the ancient and honored AT & T Technical Journal [Sterling]. Only three journals were ever published. During the making of the fourth issue several members were raided by the Secret Service and similar organizations, which put a halt to its publication.

A couple different opinions of the LoD have evolved over the years. One opinion is that in its years of operation, the LoD may have entered tens of thousands of systems, and peeped into credit histories and monitored telephone calls, but caused no direct harm to the phone systems or networks they took over [Phrack-LoD]. On the other hand, many members were raided and sometimes successfully prosecuted for causing damage to systems and reprogramming phone company computers [LoD07]. Among the members arrested was Loyd Blankenship, who went by the alias of The Mentor.

4.2.3 The Mentor

Loyd Blankenship, aka The Mentor, was a member of the LoD, Extasy Elite, Racketeers, and the PhoneLine Phantoms. Loyd was arrested when he was 21 and wrote The Conscience of a Hacker (Hacker Manifesto) on Jan 8, 1986 while in jail. It was published in the 7th issue of Phrack, http://www.phrack.org/archives/7/P07-03 [Blankenship00].

The manifesto gives an insight into the psychology of early hackers. It is said to have shaped the hacker community's view of itself and its motivations. In the manifesto, hacking is explained as a way to learn when you are bored in school and smarter than other students. It is more than just selfishness or the desire to exploit and harm others, it is a technology that should be used to expand the horizons and try to keep the world free [Manifesto07].

As a member of the LoD, he ran a BBS known as The Phoenix Project from his home. It was a local meeting place for elite members of the LoD. It became one of the most infamous BBSs due to its involvement in the E911 Case. For more information on the E911 case visit, http://everything2.com/index.pl?node=the%20E911%20Case. The Phoenix Project was a target in the E911 investigation due to its reputation in the underground hacking scene and due to Loyd's prior hacking arrest. On March 1, 1990, after the Secret Service raided Loyd's house and workplace and confiscated equipment and computers, the BBS was effectively forced offline [Phoenix05]. Blankenship has since retired and now works as a freelance game developer and electronic musician.

Just as Loyd Blankenship and LoD were well known for their participation in the BBS community, cDc Communications also made an appearance in the BBS scene as well.

4.2.4 cDc Communications

cDc Communications was founded in 1984 in Lubbock, Texas. It is the parent organization of Cult of the Dead Cow, http://www.cultdeadcow.com. Their goal was 'Global Domination Through Media Saturation'. They are well known in the BBS scene for their underground ezine, a publication released periodically that discusses anything the publisher deems newsworthy [Ezine07], also known as Cult of the Dead Cow. They are also well known for several different tool creations such as Back Orifice and SMBRelay among others. See Table 4.2.4

below for an abbreviated list of tools created by cDc Communications. For a full list visit: http://www.cultdeadcow.com/cms/apps.php3.

Table 4.2.4: cDc Communications Abbreviated Tool List

Creation Year	Tool	Creator	Description	Link
2007	eCoderRing	Flack	"Fun, friendly, easy to use program that allows two people to send secret messages to one another. While eCoder Ring is intended for entertainment purposes only, if used correctly eCoder Ring is capable of producing nearly unbreakable ciphers"	http://www.robohara.com/software/
2006	Torpark (XeroBank Browser)	Steve Topletz	Anonymous web browser. Allows users to securely and anonymously surf the internet, bypassing firewalls and website censorship.	http://www.hacktivismo.com/projec
2006	VM Detect	Danny Quist (& Offensive Computing)	Detects Virtual Machines.	N/A
2003	Six/Four System	Mixter	"The Six/Four System is a flexible framework consisting of a formally specified Peer-To-Peer protocol. This protocol is best described as a trust-enhanced anonymous tunneling protocol, and meant to provide people with anonymous, secure access to public data."	http://www.hacktivismo.com/projec
2002	Camera/Shy	The Pull	"Utilizing LSB steganographic techniques and AES-256 bit encryption, this application enables users to share censored information with their friends by hiding it in plain view as ordinary gif images. Camera/Shy is the only steganographic tool that automatically scans for and delivers decrypted content straight from the Web."	http://www.hacktivismo.com/projec
2001	SMBRelay	Sir Dystic	TCP level SMB man-in-the-middle relay attack.	http://www.xfocus.net/articles/2003
2000	NBName	Sir Dystic	NetBIOS DoS Tool	http://www.cultdeadcow.com/tools/
1999	BackOrifice 2000	DilDog	Built on basic BackOrifice, it puts administrators "in control of the system, network, registry, passwords, file system, and processes."	http://www.bo2k.com/

1998	BackOrifice	Sir Dystic	"Back Orifice is a remote administration system which allows a user to control a computer across a tcpip connection using a simple console or GUI application."	http://www.cultdeadcow.com/tools/
1998	ButtSniffer	DilDog	"Packet sniffer and network monitor for Win95, Win98 and also Windows NT 4.0."	http://www.cultdeadcow.com/tools/

Back Orifice was designed for remote system administration. Its name is a pun of Microsoft's BackOffice Server. The user can control a computer running Windows from a remote location. It was debuted at DEF CON 6 on Aug 1, 1998. Its purpose was to demonstrate the lack of security in Microsoft's OS Windows 98. cDc later debuted Back Orifice 2000, in 1999 at DEF CON 7. Despite its legitimate purposes, there are other factors that make it suited for more malicious activities. The server is capable of hiding itself from the users of the system. It can be installed without user interaction, and can be distributed as the payload of a Trojan Horse. Once installed it will not show up in any task or program lists and is rerun every time the computer is started. Some of its features include logging keystrokes, monitoring network packets and logging plaintext passwords that pass, the ability to redirect incoming TCP or UDP ports to other addresses and ports, as well as any other capability that the user sitting at the machine has [BackOrifice][cDc07].

The other popular tool, SMBRelay was released on March 21, 2001 at the @tlantacon convention. They claimed it took less than two weeks to write SMBRelay. It performs TCP level SMB man in the middle attacks on Windows. It was created to prove that when Microsoft continues to use protocols that have known issues for backwards compatibility, they leave their customers at risk. It has the ability to handle multiple connections at once. It collects password hashes and stores them in a text file using a L0phtcrack compatible format, so that they can be cracked at a later time. They also created SMBRelay2, which is a variation of SMBRelay that works at the NetBIOS level and uses NetBIOS names rather than IP addresses [SMBRelay] [cDc07].

In 1996 cDc Communications created Ninja Stike Force (NSF). NSF is a group dedicated to achieving the goals of cDc both online and offline. Membership is obtained by individuals who stand out in their support of the cDc and its ideals. They are recognized as being the best of the best in their skills. NSF launched its own website, http://www.ninjastrikeforce.com/, in 2006 [cDc07].

In 1999, cDc created a third spin off, known as Hactivisimo, http://www.hacktivismo.com/news/. Hactivismo is dedicated to the creation of anti-censorship technology in furtherance of human rights on the internet [cDc07]. The mission statement on their website is "To conduct and publish scientific research in the areas of information technology, communications and electronic media; and, to assist (where possible) non-governmental organizations, social justice groups and human rights entities in the use of advanced information technologies for the furtherance of their works" [Hactivismo].

Although the organizations discussed above were very influential to those interested in hacking and eye opening to those who's systems they hacked, those outside of the technology realm probably were not aware of what was going on behind closed doors. The organization known as Shadow Crew changed all that and made hacking an issue that everyone had to worry about.

4.2.5 Shadow Crew

Shadow Crew surfaced from the underground site conterfeitlibrary.com in early 2002. It was an international crime message board that shared information with carders or "hackers". The information on the site was used to trade, buy, and sell anything from stolen personal information to hacked credit card numbers and false

identification. It was created by several people; the most notable individual going by the name of Kidd, the real name is unknown. The other two individuals responsible for its creation were MacGyver (Kim Taylor), and CumbaJohnny.

The Shadow Crew site was a great success from 2002-2004. Although as early as April 2003, federal agents found CumbaJohnny. From that time on CumbaJohnny was working alongside the feds, assisting in gathering, entrapping, and monitoring the site and those that accessed it un-renounced to the users themselves. There were many ways that users could access the site. One was through a secure VPN set up by CumbaJohnny. Those who utilized the VPN were watched closer than others. After long secretive and careful investigation, on Oct 26, 2004, the secret service with the cooperation of police from around the world raided 28 members of the Shadow Crew (most were those that accessed via the CumbaJohnny's VPN) [ShadowCrew07].

It was estimated that at its peak, Shadow Crew had as many as 4000 members. They also had possession of nearly 1.5million credit card numbers, 18 million e-mail accounts and lots of identification documents that were being sold to the highest bidder. More than $4 million in losses was suffered by card issuers and banks worldwide [McCormick05].

Back to Table of Contents

5.0 Hacker Conferences

There are many different conferences that are held around the world that unite all persons that have an interest in the hacking community and its works, positive or negative. The attendees of these conferences range from hacking groups such as those mentioned above, to hacking hobbyists and even federal agents. Anyone that is a computer enthusiast is invited to attend. It offers a chance for people to get together, talk face-to-face, and swap information about innovations, trends, practices, and rumors in the field of computer security. Many of the organizations above host the conferences listed below.

5.1 Chaos Communication congress

The Chaos Communication Congress is Europe's largest annual hacker conference. Started in 1984, it is held at the end of each year in Berlin by the Chaos Computer Club [CCCongress07]. The event itself is separated into four different areas: the Conference, the HackCenter, Art and Beauty, and the Phone Operation Center.

The conference encompasses the main portion of the Congress and is divided into 5 main topic categories.

- 1. Hacking- focuses on current technological development and research regarding hardware and software.
- 2. Science- focuses on the current state of research, and the basic facts of nature, science, and math that affect the initiatives of the hacking community.
- 3. Community- offers a space for meetings of the activist groups attending and developer conferences.
- 4. Society- includes any topics that are affecting the general and free software development society.
- 5. Culture- tries to present unknown things or well-known things in a different light.

The Hackcenter offers a large lab where people can tinker with and evaluate their own modern technology hardware and software. It also allows them to present the project to others in attendance at the congress.

The motto of Art and Beauty is "you can create art and beauty with a computer". It is described as a workshop, installation, and a happening.

The last area of the congress is the Phone Operation Center. It is a DECT, Digital Enhanced Cordless

Telecommunications, system and phone infrastructure. Participants are allowed to bring their own DECT phone equipment and register it at the conference, so they can contact other participants at the conference free of charge [ChaosCC05].

While Chaos Communication Congress is the oldest hacker convention in Berlin, SummerCon is one of the oldest conventions in the United States started only 3 years after the Berlin convention.

5.2 SummerCon

SummerCon started in 1987 and has set a precedent for more modern conferences such as H.O.P.E. and DEF CON. It was originally run by the underground ezine, Phrack. It was held annually in St. Louis, MO until 1995. After 1995 it was run by Legion of Doom and was moved to Atlanta, GA. It has since been held in other cities such as Washington D.C., Pittsburgh, PA, and Austin, TX [Summercon07].

Just as SummerCon was led by the infamous LoD and paved the way for H.O.P.E. and DEF CON, HoHoCon was led by cDc Communications and also helped pave the way for the more renowned conventions.

5.3 HoHoCon (or XmasCon)

HoHoCon was a conference that took place around Christmas time in Houston, TX from 1990-1994. It was sponsored by Drunkfux and Cult of the Dead Cow. Phrack also helped to sponsor the forth and fifth conferences. It is credited as being the first "modern" hacker con. It also helped to inspire DEF CON and H.O.P.E. [HoHoCon07].

At the time HoHoCon was the largest gathering of those in, related to, or wishing to know more about the computer underground. Attendees were often some of the more notable members of the "hacking" and "telecom" communities [HHC94].

Although HoHoCon was only held for four years it led the way for what is now the world's largest hacker convention, DEF CON which is still active today.

5.4 DEF CON

DEF CON holds the title of world's largest annual hacker convention. It was first held in Las Vegas, NV in 1993 and continues today. Attendees include a wide range of personalities interested in the hacking world, general interest groups, federal government employees, lawyers, and hackers. Its focus ranges from computer and hacking related subjects, social events, and contests such as creating the longest wi-fi connection to cracking computer systems to non-related computer contests. The best known contest is Capture the Flag where teams of hackers attempt to attack and defend computers and networks. The last conference was attended by over 7000 people [DEFCON07].

Besides DEF CON, H.O.P.E is the other conference that is held annually till this day.

5.5 Hackers On Planet Earth (H.O.P.E)

H.O.P.E. is a conference series sponsored by the hacker magazine 2600: The Hacker Quarterly. Conferences have been running since 1994. Attendees include hackers, phone phreaks, net activists, government spooks, and any other person that has an interest in hacking. It is a three day conference that takes place in July at the Hotel Pennsylvania in New York City. There have been six conferences to date with the seventh being scheduled for 2008 [HOPE07].

The conferences began by occupying only a small amount of a hotel and grew in size to occupy more than an

entire floor of a hotel at its most popular events. The H.O.P.E. conferences are heavily invested in the social and political agendas that motivate and support hacker activity. At H2K2, the second H.O.P.E. conference Loyd Blankenship gave a reading of his Hacker Manifesto and provided additional insight into his writing. The list of HOPE conferences can be found at http://www.2600.com/hopes.html.

5.6 Black Hat Briefings

The Black Hat company was founded in 1997 by Jeff Moss. The goal of the company was to provide advanced education to security professionals within global corporations and federal agencies. Black Hat Briefing takes place in Las Vegas, NV immediately before DEF CON. There are also other forums that occur around the world in places such as Amsterdam, Tokyo, Singapore, and a special even dedicated to federal agencies occurs in Washington D.C. [BlackHat07].

They also provide training that provides hands on experience with the latest security threats and countermeasures. To find more out about the Black Hat Company go to http://www.blackhat.com.

Back to Table of Contents

6.0 Hacker Publications

As previously mentioned above, many of the hacker organizations have some sort of publication they produce to share beliefs and accomplishments with dedicated followers. Two of the more widely known publications, *2600: Hacker Quarterly*
and Phrack are described in more detail below. Both of these publications also are sponsors of at least one hacker convention.

6.1 *2600: Hacker Quarterly*

2600: Hacker Quarterly (2600:), http://www.2600.com/, is an American publication that publishes technical information on a variety of topics such as telephone switching systems, internet protocols and services, general news concerning the computer "underground" and libertarian issues. It first entered print in 1983 and continues to be printed on a quarterly basis. It is noted as being a Grey Hat hacker's magazine. The magazine is also responsible for establishing the H.O.P.E. conferences. 2600: has been known to have been caught up in many court cases, those of which included Universal vs. Reimerdes, a case that involved the distribution of the DVD copy protection tool DeCSS [2600].

2600: also sponsors meetings around the world. These meetings act as forum for anyone interested in technology to meet and discuss events in the world of technology, to learn and to teach others. The meetings are open to all age and skill levels. They take place on the first Friday of every month from 5pm to 8pm local time unless noted [2600Meeting].

2600: was the only hacker publication available for its first two years in print, until 1985 when Phrack began producing an underground ezine. Unlike 2600:, Phrack was originally available via an electronically distributed magazine (ezine) on the Metal Shop BBS and was not available in print form.

6.2 Phrack

Phrack, http://www.phrack.org/, began as an underground ezine made for and by hackers on Nov 17, 1985. It is open for contributions on the subjects of security, hacking, phreaking, lock picking, anarchism, cryptography, spying, radio broadcasting, coding, conspiracy, and world news.

The last issue, #63, was scheduled for release on July 29, 2005 in conjunction with the DEF CON and What the Hack Conventions. Issue #63 was going to be a hardback version to be distributed at DEF CON but when the printer discovered they were printing a hacking book they refused to print it. Two other individuals stepped up and were able to print copies in time for the conference. Within issue #63 they announced they would continue to release new issues. The most recent issue was released on May 28, 2007 and a call for papers has been put of for future releases.

There is only one official Phrack, however the name phrack has become a symbol for the entire hacking underground and is often reused by other groups to help them gain credibility [Phrack07].

Back to Table of Contents

7.0 Hackers Effects On Society

Hackers have been responsible for both good and bad incidents in society. As a result of White Hat hackers we have foundations such as the Free Software Foundation that have made it possible for computer users to use, study, copy, modify, and redistribute computer programs freely. Grey Hat hackers have also had positive effects on society by working to find vulnerabilities in popular software products with the intentions of notifying the creators so they can fix the problems before a Black Hat hacker can come along and exploit the flaw. However during the prime time of hacking in the mid 90's Black Hat hackers caused all sorts of ruckus. "The NY Times reported that in 1997, there were more than 1900 hacker websites and more than 30 hacker publications." In 1998, 418 cases were given to federal prosecutors. That was 43% more than the previous year. In the first & second quarter of 1999, businesses were said to have lost $7.6 billion as a result of viruses. Also in 1999, corporations spent $7.1 billion on security and were estimated to spend a total of $17 billion in a matter of four years. Over 1400 web hacks were reported as of July 1999 [CyberSpace02]. One can assume that from 1999 to 2007, these numbers have more than doubled. Table 7 below lists the organizations & laws that have come about as a result hacking in society.

Table 7: Hacking Organizations & Laws

Creation Year	Organization or Law	Description
1984	Computer Fraud & Abuse Act	Laws passed with the intent of reducing "hacking" of computer sys
1985	FSF- Free Software Foundation	Non-profit corporation founded to support Free Software Movemer
1987	Computer Security Act	Congresses attempt at improving the security and privacy of sensiti Federal computer systems. Designates the National Institute of Star Technology (NIST) as the lead government agency for computer se
1988	CERT CC- Computer Emergency Response Team Coordination Center	Created by DARPA, it is the major coordination center in dealing v security problems.
1992	NCCS- FBI's National Computer Crime Squad	Investigates violations of the Federal Computer Fraud and Abuse A
1996	National Information Infrastructure Protection Act	Amended the Computer Fraud & Abuse Act.
1998	Presidential Directive PDD-63 (CIP- Critical Infrastructure Protection)	National program to assure the security of vulnerable and interconr infrastructures of the US.

2001	US Patriot Act	Increased the scope of the penalties defined in the Computer Fraud
2004	CAN-SPAM Act	Establishes requirements for those who send commercial email, spe for spammers and companies whose products are advertised in spar the law, and gives consumers the right to ask emailers to stop spam

Big businesses are not the only ones that feel the wrath of Black Hat hacking. Anyone who uses a computer suffers from their works. Hackers use mechanisms such as social engineering and phishing to gather personal information from unknowing victims in an effort further their control. According to Javelin Strategy and Research, in 2005 11.6% of all identity thefts were obtained through online means. Based on the latest 2007 data, the average fraud amount per victim was $5, 720 and the average resolution time was 25 hours [Javelin07]. Computer users also spend time and resources dealing with SPAM. In 1996, a user received an average 2,200 SPAM messages a year, and spent an average of four to five seconds on each message. 28% of the people responded to a SPAM message and 8% of people purchased a product. Time and money spent on SPAM is an ever increasing number, in 2007 alone, the amount of SPAM is estimated to increase by 63% [SpamStats06].

Back to Table of Contents

8.0 Summary

As stated above, there are numerous hacking organizations, conferences, and publications throughout the world, and this paper has just begun to touch on the groups that exist out there. The information above discusses some of the more notorious groups that have had a significant impact on hacker society, and continue to influence the ideologies of new hackers that are entering the marketplace. Many popular software applications such as Microsoft, Linux, and the GNU project may not exist without the achievements of the Open Source and Free Software Hacking group. Furthermore, despite the typical mal-intentions of Security Hacking groups, several groups such as cDc and CCC have detected vulnerabilities in Microsoft applications that may have gone unnoticed without their efforts and resulted in numerous other security breaches. Black Hat hackers as a group have cost society billions of dollars and have resulted in an undetermined number of hours in time fixing the problems that have resulted from the hackers actions. In the end, regardless of what a group or individual's aspirations may be, numerous hacking conferences allow for all conglomerations of people to gather and share their knowledge. There are thousands of other hackers, black, white, or grey, out there working diligently to shape technology as we know it, and the numbers continue to grow. They continue to evolve and discover new ways of doing things, and new ways to interpret their principles of operation.

Back to Table of Contents

Acronymns

BBS	Bulletin Board System
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act
cDc	Cult of Dead Cow
CCC	Computer Chaos Club
CERT CC	Computer Emergency Response Team Coordination Center
CIP	Critical Infrastructure Protection
DARPA	Defense Advanced Research Projects Agency

DeCSS	DVD-Video disc encrypted using the Content-Scrambling System (CSS)
DECT	Digital Enhanced Cordless Telecommunications
DM	Deutsche Mark (German Mark)
DoS	Denial of Service
ezine	Electronic Magazine
FSF	Free Software Foundation
GNU	Gnu's Not Unix
GSM	Global System for Mobile Communications
H.O.P.E	Hackers on Planet Earth
LoD	Legion of Doom
LoD/LoH	Legion of Doom/Legion of Hackers
MIT	Massachusetts Institute of Technology
NCCS	National Computer Crime Squad
NSF	Ninja Strike Force
OS	Operating System
SMB	Server Message Block (protocol)
VM	Virtual Machine

Back to Table of Contents

References

1. [Hacker07] "Hacker", Wikipedia, 11/8/2007 http://en.wikipedia.org/wiki/Hacker

2. [Ethic07] "Hacker Ethic", Wikipedia, 11/3/2007, http://en.wikipedia.org/wiki/Hacker_ethic

3. [HackerEthic] "Hacker Ethic", The Jargon File, version 4.4.7, http://www.catb.org/jargon/html/H/hacker-ethic.html

4. [FreeSoftware] "Free Software Directory", FSF, http://directory.fsf.org/

5. [CCC07] "Chaos Computer Club", Wikipedia, 9/20/2007, http://en.wikipedia.org/wiki/Chaos_Computer_Club

6. [LoD07] "Legion of Doom (hacking)", Wikipedia, 10/12/2007, http://en.wikipedia.org/wiki/Legion_of_Doom_%28hacking%29

7. [Sterling] Sterling, Bruce, "Law and Disorder of the Electronic Frontier", The Hacker Crackdown, http://www.chriswaltrip.com/sterling/hackcrck.html

8. [Phrack-LoD] "The History of the Legion of Doom", Phrack Vol 3, Issue 31, Phile #5 of 10, http://www.phrack.org/issues.html?issue=31

9. [Blankenship00] "Loyd Blankenship", Everything2, 5/23/2000,

http://www.everything2.com/index.pl?node_id=565219

10. [Manifesto07] "Hacker Manifesto", Wikipedia, 11/3/2007, http://en.wikipedia.org/wiki/Hacker_Manifesto

11. [Phoenix05] "The Phoenix Project", Everything2, 2/26/2005, http://everything2.com/index.pl?node=The%20Phoenix%20Project

12. [cDc07] "Cult of the Dead Cow", Wikipedia, 10/28/2007, http://en.wikipedia.org/wiki/CDc_communications

13. [SMBRelay] "SMBRelay", http://www.xfocus.net/articles/200305/smbrelay.html.

14. [BackOrifice] "BackOrifice, The Worst Case Scenario", http://www.cultdeadcow.com/tools/bo.php

15. [ShadowCrew07] "ShadowCrew", Wikipedia, 9/25/2007, http://en.wikipedia.org/wiki/ShadowCrew

16. [McCormick05] McCormick, John & Gage, Deborah, "Shadowcrew: Web Mobs", Baseline, 3/7/2007, http://www.baselinemag.com/article2/0,1397,1774393,00.asp

17. [CCCongress07] "Chaos Computer Congress", Wikipedia, 9/5/2007, http://en.wikipedia.org/wiki/Chaos_Communication_Congress

18. [ChaosCC05] "Chaos Computer Club Events", 22C3, 2005, http://events.ccc.de/congress/2005/overview.en.html

19. [SummerCon07] "Summercon", Wikipedia, 10/19/2007, http://en.wikipedia.org/wiki/Summercon

20. [HoHoCon07] "HoHoCon", Wikipedia, 11/20/2007, http://en.wikipedia.org/wiki/HoHoCon

21. [HHC94] "The Fifth Annual HoHoCon", Cult of the Dead Cow, 12/26/1994, http://www.cultdeadcow.com/news/h-con94.txt

22. [DEFCON07] "DEF CON", Wikipedia, 10/13/2007, http://en.wikipedia.org/wiki/DEF_CON

23. [HOPE07], "H.O.P.E.", Wikipedia, 9/13/2007, http://en.wikipedia.org/wiki/H.O.P.E

24. [BlackHat07] "Black Hat Briefings", Wikipedia, 10/9/2007, http://en.wikipedia.org/wiki/Black_Hat_Briefings

25. [2600] "2600: The Hacker Quarterly", Wikipedia, 11/7/2007, http://en.wikipedia.org/wiki/2600:_The_Hacker_Quarterly.

26. [2600Meeting] "2600 Meetings", 2600: The Hacker Quarterly, 2007, http://www.2600.com/meetings/

27. [Phrack07] "Phrack", Wikipedia, 11/8/2007,

http://en.wikipedia.org/wiki/Phrack

28. [Phreaking07] "Phreaking", Wikipedia, 11/5/2007, http://en.wikipedia.org/wiki/Phreaking

29. [Bulletin07] "Bulletin Board System", Wikipedia, 11/8/2007, http://en.wikipedia.org/wiki/BBS

30. [Ezine07] "Underground Ezine", Wikipedia, 10/20/2007, http://en.wikipedia.org/wiki/Underground_ezine

31. [Timeline07] "Timeline of computer security hacker history", Wikipedia, 11/29/2007, http://en.wikipedia.org/wiki/Timeline_of_hacker_history

32. [CyberSpace02] "Hacking Into Cyberspace", 4/18/2002, http://www.units.muohio.edu/psybersite/cyberspace/security/focus3.shtml

33. [Javelin07] Javelin Stategy & Research, "How Many Identity Theft Victims are There? What is the Impact on the Victims?", PrivacyRights.org, 2007, http://www.privacyrights.org/ar/idtheftsurveys.htm

34. [SpamStats06] "Spam Statistics 2006", http://spam-filter-review.toptenreviews.com/spam-statistics.html

Back to Table of Contents

Last Modified: Dec 02, 2007.

Note: This paper is available on-line at .