SAND--98-8497C

Security Incidents on the Internet, 1989 - 1995

CONF-980723--

John D. HOWARD, Ph.D.

Sandia National Laboratories
Box 969, MS-9214, Livermore, CA 94551 USA
johnhoward@earthlink.net or jdhowar@sandia.gov

RECEIVED
MAY 1 1 1998
OSTI

Abstract

This paper presents an analysis of trends in Internet security based on an investigation of 4,299 Internet security-related incidents reported to the CERT® Coordination Center (CERT®/CC) from 1989 through 1995. Prior to this research, our knowledge of actual Internet security incidents was limited and primarily anecdotal. This research: 1) developed a taxonomy to classify Internet attacks and incidents, 2) organized, classified, and analyzed CERT®/CC incident records, 3) summarized the relative frequency of the use of tools and vulnerabilities, success in achieving access, and results of attacks, 4) estimated total Internet incident activity, 5) developed recommendations for Internet users and suppliers, and 6) developed recommendations for future research.

With the exception of denial-of-service attacks, security incidents were found to be increasing at a rate less than Internet growth. Estimates showed that most, if not all, severe incidents were reported to the CERT®/CC, and that more than one out of three above average incidents (in terms of duration and number of sites) were reported. Estimates also indicated that a typical Internet site was involved in, at most, around one incident (of any kind) per year, and a typical Internet host in, at most, around one incident in 45 years. The probability of unauthorized privileged access was around an order of magnitude less likely. As a result, simple and reasonable security precautions should be sufficient for most Internet users.

1. Introduction

This paper presents a summary of trends in Internet security based on an investigation of 4,299 Internet security-related incidents reported to the CERT®/CC from 1989 through 1995. The CERT®/CC (originally known as the Computer Emergency Response Team Coordination Center) provides the Internet community a single organization for coordinating responses to security incidents [HoR91:25]. The CERT®/CC is located at Carnegie Mellon University's Software Engineering Institute, Pittsburgh, Pennsylvania, USA (http://www.cert.org/).

Prior to this research, the CERT®/CC was unable to release specific Internet security incident information. Our knowledge of actual security incidents on the Internet was therefore limited and primarily anecdotal. This paper is organized into the following sections:

- A taxonomy of Internet attacks and incidents
- A summary of CERT®/CC incident records
- A summary of the relative frequency of attack taxonomy categories
- Estimates of total Internet incident activity
- Recommendations for Internet users and suppliers

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

- Recommendations for future research
- Current research activities
- References

2. Internet Attack and Incident Taxonomy

Development of agreed upon terminologies and principles of classification (a taxonomy) is a necessary prerequisite to systematic studies in any field of inquiry [McK82:3]. Development of comprehensive taxonomies in the field of computer security has been an intractable problem of increasing interest [Amo94:31]. In this section, I present the taxonomy I developed based on my experience in classifying actual Internet attacks and incidents.

The terms *attack* and *incident* are often used interchangeably in computer security literature, which results in considerable confusion. In order to classify actual Internet incidents, a distinction must be made between these terms. An *attack* I defined to be a single unauthorized access attempt, or unauthorized use attempt, regardless of success. An *incident*, on the other hand, I defined to be a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing.

The taxonomy I developed is in two parts. First is a "full" taxonomy for Internet *attacks*. This attack taxonomy is broader in scope than most previous taxonomies, because I did not attempt to enumerate all computer security flaws, or methods of attack, but rather attempted to provide a broad, inclusive framework. My intention was to reorient the focus of the taxonomy toward a *process*, rather than a single classification category, in order to provide both an adequate classification scheme for actual Internet attacks, and also a taxonomy that would aid in thinking about computer and network security.

The complete *attack* taxonomy is shown in Figure 2.1, which depicts a simplification of the path an attacker must take in order to accomplish the attacker's objectives. To be successful, an attacker must find one or more paths that can be connected, perhaps simultaneously. This taxonomy suggests that computer security is preventing attackers from achieving objectives by making any complete connections through the six steps depicted.

2.1. Attackers and Their Objectives - *People* attack computers. They do so through a variety of methods and for a variety of objectives. What I found to distinguish the categories of attackers was a combination of who they are, and their objective (what they want to accomplish). Based on their objectives, I have divided attackers into the following six categories:

1. Hackers - break into computers for challenge and status
2. Spies - break into computers for information to be used for political gain
3. Terrorists - break into computers to cause fear for political gain
4. Corporate raiders –employees break into computers of competitors for financial gain
5. Professional Criminals - break into computers for personal financial gain
6. Vandals - break into computers to cause damage

These six categories of attackers, and their four categories of objectives, are shown in the leftmost and rightmost blocks of Figure 2.1. These serve as the two ends of the operational sequence of computer and network attacks. In between are the "tools, vulnerabilities, access, and results" which link attackers to their objectives.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

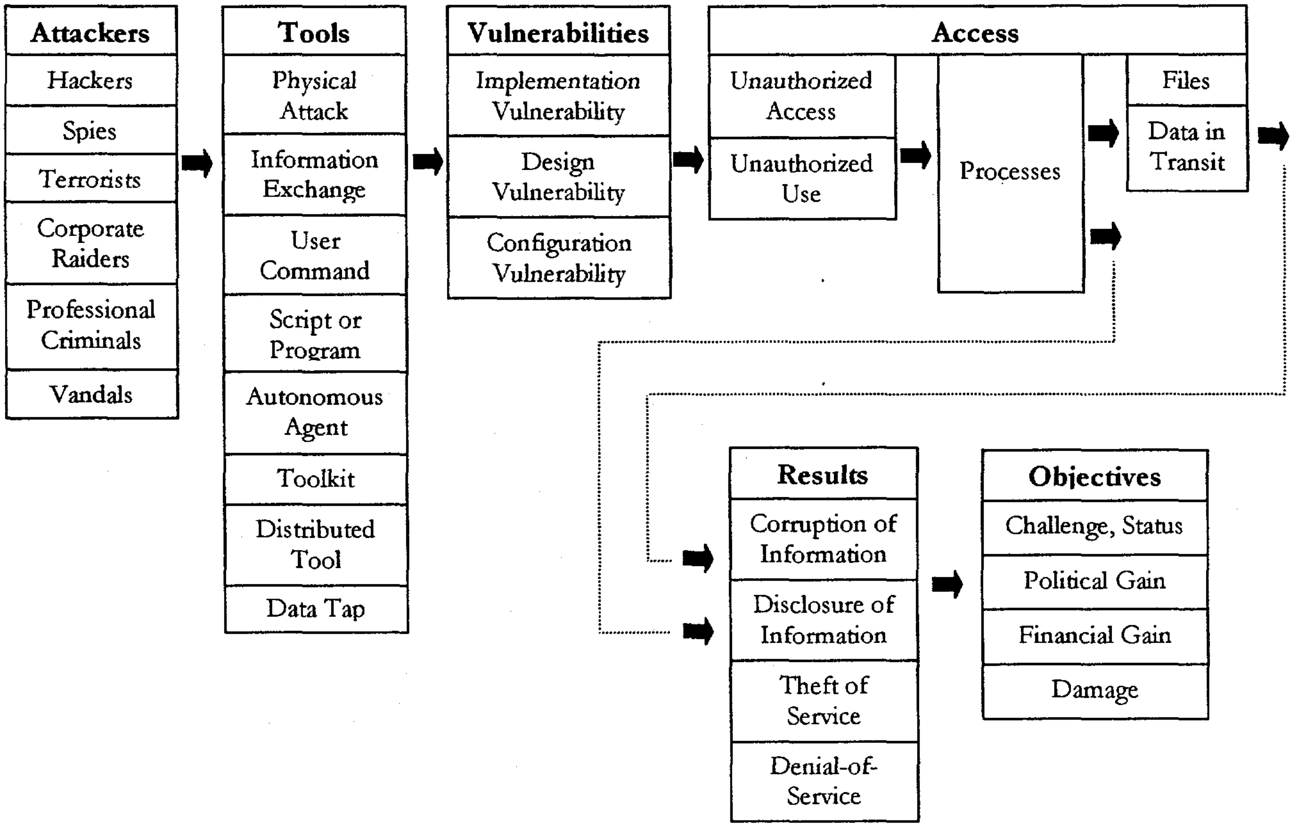

Figure 2.1. Computer and Network Attack Taxonomy

2.2. Access – In order to successfully accomplish an objective, an attacker must either obtain unauthorized access to a computer or network, or, if authorized to have access, must use that access in an unauthorized way. This is shown in the left side of the access block of Figure 2.1. The unauthorized access or use is to *processes*, or to files or data in transit *through processes*. These are depicted in the right side of the access block (Figure 2.1).

2.3. Vulnerabilities – In order to reach the desired process, an attacker must take advantage of a computer or network *vulnerability*, which is a flaw allowing an unauthorized access or use [Amo94:2]. A vulnerability may arise in three ways:

Implementation Vulnerability - the design is satisfactory, but an error has been made in its implementation in software or hardware

Design Vulnerability - the vulnerability is inherent in the design, and therefore even a perfect implementation in software or hardware will result in a vulnerability.

Configuration Vulnerability - system configured in such a way as to result in a vulnerability, such as system accounts with default passwords, "world write" permission for new files, and vulnerable services enabled [ABH96:196].

2.4. Results - Between obtaining access and the attacker's objectives, I conceptualized the *results* of attack. At this point in the sequence of an attack, the attacker has access to the desired processes, files, or data in transit. The attacker is now free to exploit this access to alter files, deny service, obtain information, or use the available services. Figure 2.1 depicts these results of attack, which are defined as follows [Amo94:3-4,31; RuG91:9-10; Coh95:55-56]:

Corruption of Information - any unauthorized alteration of files stored on a host computer or data in transit across a network.

Disclosure of Information - the dissemination of information to anyone who is not authorized to access that information.

Theft of Service - the unauthorized use of computer or network services without degrading the service to other users.

Denial-of-service - the intentional degradation or blocking of computer or network resources.

2.5. Tools - The final connection to be made in the operational sequence that leads attackers to their objectives is the *tools* of attack. This is also the most difficult connection to make because of the wide variety of methods available to exploit vulnerabilities in computers and networks. When authors make lists of methods of attack, often they are actually making lists of tools. The approach taken here was to established the following categories (see Figure 2.1):

Physical Attack - The attacker is physically at the computer and attacks the system physically.

Information Exchange - The attacker obtains information either from other attackers (such as through a hacker bulletin board), or from the people being attacked (commonly called social engineering).

User Command - The attacker enters commands at a command line or graphical user interface. An example is entering Unix commands through a telnet connection.

Script or Program - Scripts and programs initiated at the user interface to exploit vulnerabilities. Examples are a shell script to exploit a software bug, a Trojan horse login program, or the password cracking program *crack*.

Autonomous Agent - The attacker initiates a program, or program fragment, which operates independently from the user to exploit vulnerabilities. Examples are computer viruses or worms.

Toolkit - The attacker uses a software package which contains scripts, programs, or autonomous agents that exploit vulnerabilities. An example is the widely available Internet toolkit called *rootkit*.

Distributed Tool - The attacker distributes tools to multiple hosts, which are then coordinated to anonymously perform an attack on the target host simultaneously after some time delay.

Data tap - The electromagnetic radiation from a cable carrying network traffic, or from a host computer is "listened" to by a device external to the network or computer.

With the exception of the physical attack, information exchange and data tap categories, each of the tool categories may contain the other tool categories within them. For example, toolkits contain scripts, programs, and sometimes autonomous agents. So when a toolkit is used, the scripts and programs category is also included. User commands also must be used for the initiation of scripts, programs, autonomous agents, toolkits and distributed tools. In other words, there is an order to some of the categories in the tools block, from the simple user command category to the more sophisticated distributed tools category. What made these categories mutually exclusive when actually applied to the CERT®/CC records was that I classified attacks according to the *highest* category of tool used.

2.6. Classification of Incidents - Data were extracted from each incident after the incidents were reconstructed from the CERT®/CC records. These data were used to classify each incident according to reporting date, starting date, ending date, number of sites, number of messages, reporting site names, other site names, level of attack, methods of operation, corrective actions, and CERT® tracking numbers. "Level of attack" and "methods of operation" consisted of keywords describing the types of attacks in the incident, based on the attack taxonomy. The level of attack was the highest "level" of access the attacker achieved (access block of the taxonomy, Figure 2.1).

3. Summary of CERT®/CC Incidents

A total of 4,567 incidents over this 7 year period were reconstructed from the CERT®/CC records. This included 268 false alarms (6%), and 4,299 actual incidents (94%) ranging from login attempts to large incidents involving break-ins at the root level. The number of incidents increased each year at a rate between 41% (1991 to 1992) and 62% (1993 to 1994). The exception to this took place between 1994 and 1995 when the number of incidents reported decreased slightly.

As stated in Section 2, the center of the connection between attackers and their objectives is the attacker's requirement for unauthorized access or unauthorized use. Most of the CERT®/CC incidents (89%) were unauthorized access incidents: *root break-ins* (28%), *account break-ins* (24%), and *access attempts* (38%). Relative to the growth in Internet hosts, each of these access categories was found to be *decreasing* over the period of this research: root-level break-ins at a rate around 19% less than the increase in Internet hosts, account-level break-ins at a rate around 11% less, and access attempts at a rate around 17% less.

Of the 4,299 actual incidents reported to the CERT®/CC, 458 (11%) were classified as unauthorized use incidents: *denial-of-service attacks* (2.4%), *corruption of information incidents* (3%), and *disclosure of information incidents* (5%). The growth in total unauthorized use incidents was around 9% per year *greater* than the growth in Internet hosts. Based on reporting date, the 4,299 incidents are plotted in Figure 3.1, grouped by month.

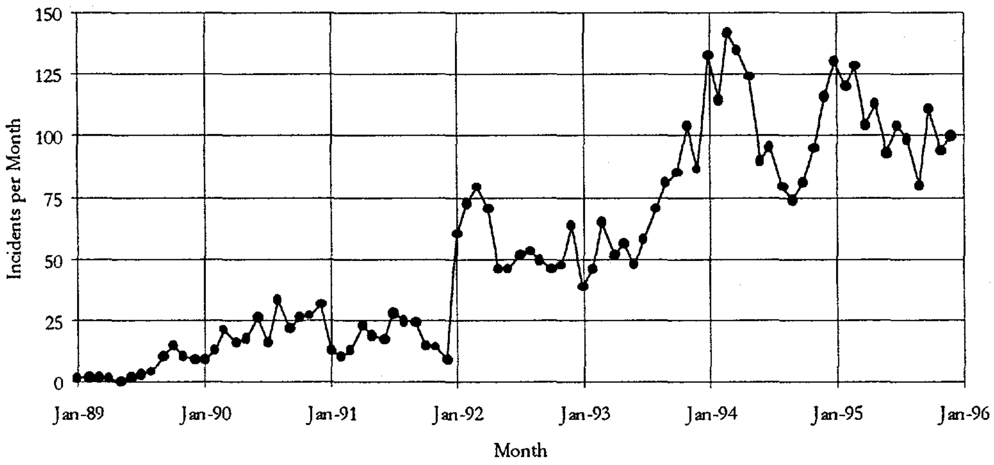

Figure 3.1. CERT®/CC Incidents by Month, 1989 - 1995

The number of incidents reported to the CERT®/CC, as shown in Figure 3.1, is actually not a good indication of either the activity at the CERT®/CC, nor of the state of Internet security because 1) the incidents are presented according to reporting date, which is an inaccurate representation of the incidents in *time*, 2) the incidents are not comparable due to wide variations in duration, in the number of sites involved, and in the severity or success of the attack, and 3) the number of incidents is not compared to the growth of Internet hosts.

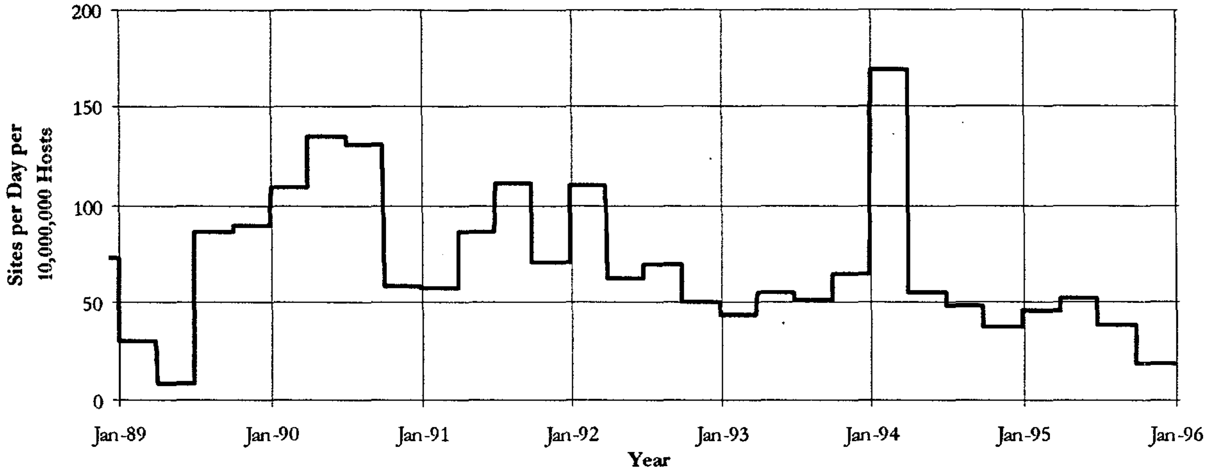

Figure 3.2. CERT®/CC Sites/Day /10,000,000 Hosts - Root and Account Break-ins, Averaged Over Quarters

A more informative method of presenting Internet incident information is to use the total average sites per day for each category of attack. This can be derived by summing the average sites per day from each incident in a category using each starting date, ending date and the total number of sites involved.

	Report date	Start date	Middle date	End date	Days duration	# of sites	Sites/day	# of messages
1	2-Apr-90	2-Apr-90	24-Mar-91	14-Mar-92	713	383	0.54	158
2	18-Jun-92	9-Jun-92	19-Jul-92	28-Aug-92	81	162	2.00	227
3	16-Jun-92	12-Jun-92	16-Sep-92	21-Dec-92	193	107	0.55	458
4	28-Jul-92	28-Jul-92	25-Oct-92	22-Jan-93	179	66	0.37	229
5	2-Mar-93	1-Feb-93	18-Apr-93	4-Jul-93	154	264	1.71	486
6	29-May-93	5-Mar-93	22-Jul-93	9-Dec-93	280	93	0.33	476
7	12-Jul-93	12-Jul-93	11-Sep-93	11-Nov-93	123	141	1.15	288
8	11-Aug-93	25-Jun-93	12-Oct-93	29-Jan-94	219	113	0.52	141
9	13-Aug-93	12-Aug-93	31-Oct-93	19-Jan-94	161	164	1.02	918
10	20-Oct-93	20-Oct-93	11-Dec-93	1-Feb-94	105	248	2.36	648
11	5-Feb-94	5-Feb-94	20-Mar-94	3-May-94	88	155	1.76	89
12	27-May-94	27-May-94	22-Jul-94	17-Sep-94	114	62	0.54	167
13	3-May-94	3-May-94	28-Aug-94	24-Dec-94	236	103	0.44	367
14	16-Jul-94	28-Jun-94	25-Sep-94	23-Dec-94	179	130	0.73	394
15	18-May-94	1-May-94	11-Oct-94	24-Mar-95	328	112	0.34	118
16	2-Sep-94	2-Sep-94	28-Nov-94	24-Feb-95	176	100	0.57	192
17	15-Sep-94	15-Sep-94	4-Jan-95	26-Apr-95	224	515	2.30	1907
18	7-Dec-94	7-Dec-94	22-Jan-95	9-Mar-95	93	85	0.91	215
19	19-Jan-95	19-Jan-95	17-Apr-95	15-Jul-95	178	166	0.93	548
20	27-Jan-95	26-Jan-95	19-Apr-95	11-Jul-95	167	108	0.65	340
21	8-Apr-95	8-Apr-95	18-May-95	28-Jul-95	82	154	1.88	329
22	7-May-95	7-May-95	28-Jul-95	18-Oct-95	165	267	1.62	909
23	26-Jul-95	26-Jul-95	9-Sep-95	24-Oct-95	91	81	0.89	118
24	11-Oct-95	20-Aug-95	1-Dec-95	14-Mar-96	208	237	1.14	741
25	29-Sep-95	29-Sep-95	31-Dec-95	2-Apr-96	187	81	0.43	320

Table 3.1. Summary of Root Break-in Incidents With ≥ 79 Days Duration, ≥ 62 Sites, ≥ 87 Messages

For these 25 incidents, a three-phase process of attack was consistently used: 1) gain access to an account on the target system, 2) exploit vulnerabilities to gain privileged (root) access on that system, and 3) use this privileged access to attack other systems across the network.

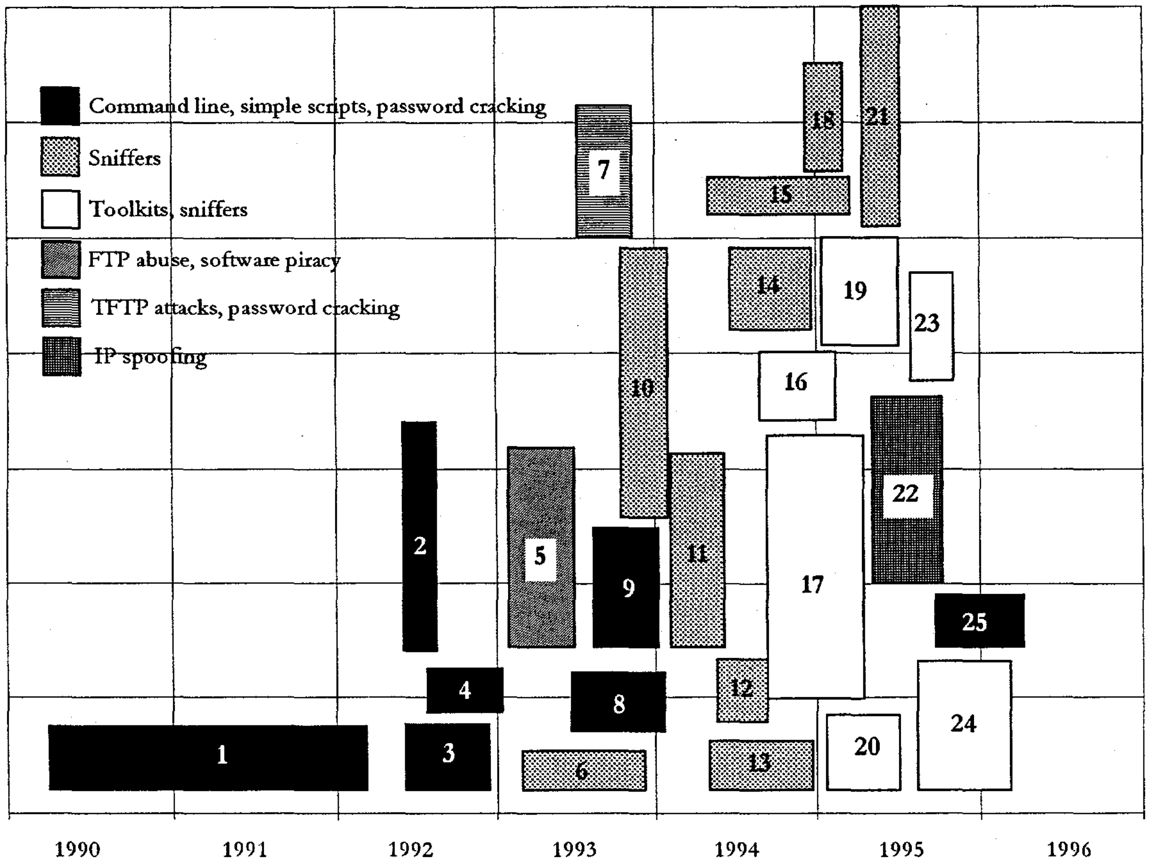

Figure 3.3. Sites per Day versus Duration for 25 "Severe" Incidents
(Note: Numbers in each block indicate the order of the incident according to middle day as shown in Table 3.1, and the vertical dimension is average sites per day, one division = one site/day)

Although the absolute number of incidents generally grew, the sites per day data showed there was a steady *decline* in security activity reported to the CERT®/CC, *compared to the size of the Internet,* since peaking in 1990. The slope of the growth in all sites per day for all incidents, and for root and account-level break-ins (Figure 3.2) were both around 7% *less* than the growth rate in the number of Internet hosts ($\alpha = 1\%$, $R^2 = 9.4\%$).

In order to identify the most severe incidents in the CERT®/CC records, a criteria was developed from this research as follows: root break-ins, ≥ 79 days duration, ≥ 62 sites, and ≥ 87 messages to/from the CERT®/CC. This selected 25 incidents with an average of 190 days duration, 164 sites, and 433 messages in the CERT®/CC record, as summarized in Table 3.1.

The distribution of these incidents over time is presented in Figure 3.3 which plots a rectangle representing each incident. The horizontal dimension of each incident corresponds to the duration, and the height corresponds to the average sites per day as listed in Table 3.1.

There were two predominant trends seen in the 25 severe incidents. First, the sophistication of intruder techniques progressed from simple user commands, scripts and password cracking, through the use of tools, such as sniffers (1993) and toolkits (1994), and finally to intricate techniques that fool the basic operation of the Internet Protocol (1995). The second trend was that intruders became increasingly difficult to locate and identify. In the early incidents, the attackers tended to be a few individuals confined to a specific location or group of locations, and as a consequence, tended to be easily identifiable. As intruder tools became more sophisticated and the size of the Internet grew, the severe incidents involved more attackers operating in many different locations. The newest and most sophisticated techniques allowed the attackers to obtain nearly total obscurity.

4. Summary of the Relative Frequency of Attack Taxonomy Categories

Recording of attack taxonomy categories in the CERT®/CC records was not systematic or complete. As a result, this information is incomplete. Some valuable information, however, can be obtained by determining the relative frequency that various attack taxonomy categories appear in the CERT®/CC incident records. In the CERT®/CC records, more information was found about *Tools*, *Vulnerabilities*, and *Access*, than the other categories of the taxonomy. Very little information was in the records about the beginning and ending categories, *Attackers* and *Objectives*.

A total of 778 incidents (18% of all incidents) reported the use of some tool. From these records, the largest category of tools was scripts or programs (15%). These consisted primarily of *Trojan horses* (11%) and *sniffers* (6%). The two general categories of toolkits were tools designed to exploit privileged or root access (1.2%), and *scanners* (2.6%). These tools appeared relatively late in the CERT®/CC records. The CERT®/CC records contain very few references to autonomous agents such as *worms*, and *viruses*. There was no mention in any of the CERT®/CC records of the use of *Data taps*, or *Distributed tools*. Data taps are physical taps and not attacks across the Internet, which makes them much less likely to be reported to the CERT®/CC. Distributed tools do not appear in the CERT®/CC records until after the period of this research.

Nearly half of the incidents in the CERT®/CC records mention specific vulnerabilities (45%). The most frequently recorded vulnerabilities involved various problems with passwords (22%). Most of the password vulnerabilities were in three categories: *password files*, which indicated that a password file had been copied (14%), *password cracking*, generally indicating that passwords had been determined by the operation of a password cracking tool (10%), and *weak passwords*, which could be easily guessed (4%).

The reputation of *sendmail* and other mail transfer agents for being "plagued with security problems" was confirmed in the CERT®/CC incident records, which contain numerous references to *sendmail* (10%), *SMTP* (0.4%) and *mail* (8%). Problems with implementation of trusted hosts (such as the *hosts.equiv* or *.rhosts* file) was recorded in a significant number of incidents (6%), as was *configuration* (6%), *TFTP* (6%), *NIS* and *YP* (4%), *FTP* (4%), and *NFS* (3%).

The CERT®/CC records contained 419 incidents with some information about the *results* category of the taxonomy (10%). The largest category of these results was *theft of service* (7%), which primarily consisted of *FTP abuse* (6%). *Disclosure of information* was another large category of *results* (6%), which consisted primarily of *software piracy* (5%). *FTP abuse*, *software piracy*, and *warez* are all related, so it makes sense that they were recorded in a similar number of incidents.

There were 170 incidents in the CERT®/CC records that gave information about *corruption of information* (4%), which primarily consisted of *modifying or deleting logs* (2%), or *deleting files* (2%).

Little information was found in the CERT®/CC records for some of the categories of the attack taxonomy. One likely cause was that only certain categories of information were necessary for the mission of the CERT®/CC, such as *vulnerabilities* and *access level.* Other possible reasons were that the information was assumed (and therefore not recorded), or that the CERT®/CC does not view itself as actually being responsible for *all* security problems on the Internet. For example, the *VIRUS-L* moderated mailing list had a focus on computer virus issues, which may explain the lack of virus information in the CERT®/CC records.

5. Estimates of Total Internet Incident Activity

Since attacks make up incidents, total Internet security *activity* could be measured by either the total Internet *attack* activity or the total Internet *incident* activity. In order to estimate the number of *attacks*, some sample of Internet activity is required. Vulnerability studies by U.S. Defense Department agencies can be used for such an estimate. A vulnerability analysis by the U.S. Defense Information Systems Agency (DISA) showed that the probability of an individual attack being reported was around 1 out of 140 (0.7%). In a different study, the U.S. Air Force Information Warfare Center (AFIWC) estimated this probability to be 1 out of 8 (12.5%). Table 5.1 summarizes the estimates of total Internet attack activity based on these studies.

Source of Estimate	**Estimate of Total Attacks per Year**
DISA [GAO96:18]	2.5 million
DISA (corrected for 500 reported attacks)[see How97:176]	700,000
AFIWC (using estimated 500 reported attacks) [WhK96]	40,000

Table 5.1. Estimates of Total Internet Attacks per Year in 1995

These widely varying estimates indicate that currently we cannot accurately estimate the number of *attacks*. The same is not, however, true for estimations of the number of *incidents*. Estimates of the rate of reporting of attacks, and of the number of attacks per incident, could be used to estimate the total number of Internet incidents as follows:

$$N_t \cong \frac{N_r}{P(I)} \cong \frac{N_r}{1 - [1 - P(A)]^{\alpha}}$$

where N_t = the total number of Internet incidents

N_r = the number of Internet incidents reported

$P(I)$ = the probability (percentage) that an *incident* will be reported

$P(A)$ = the probability that an *attack* will be reported

α = the number of attacks per incident

The DISA and AFIWC studies give us a low and a high estimate of the probability of an attack being reported [*P(A)*]. The number of attacks per incident was estimated to be between 10 and 1,000 when all CERT®/CC data was considered together. Better estimates were obtained when the types of incidents were considered separately. Table 5.2 summarizes the estimates of total Internet incident activity made by estimating attacks per incident, or from Site A projections. "Site A" is one Internet site that reported all their incidents to the CERT®/CC. These estimates are for one year in 1995.

Estimates of Total Internet Incidents per Year in 1995		
Source	**Low Estimate**	**High Estimate**
Based on Incidents per Host estimates at Site A	16,800	22,800
Based on attacks per incident 10 to 1,000, and DISA probability	1,200	17,350
Based on attacks per incident 10 to 1,000, and AFIWC probability	1,200	1,630
Based on DISA probability	2,500	15,800
Based on AFIWC probability	1,400	2,400

Table 5.2. Summary of Estimates of Total Internet Incident Activity

With respect to severe incidents, using the DISA probability of reporting an attack, the probability of any severe incident *not* being reported to the CERT®/CC was between 0% and 4%. Using the AFIWC probability of reporting an attack, the probability of any severe incident *not* being reported to the CERT®/CC was essentially zero. This confirms the impression the reports themselves give: that it is hard to conceive that a severe Internet security incident would not be reported to the CERT®/CC.

There were 394 incidents in the CERT®/CC records (9.2%) that were *above average* both in terms of duration (above 16.5 days) and in terms of the number of sites (above 6.5 sites). When these incidents were isolated and analyzed, it showed that if we assume the DISA probability of report, then a minimum of around 1 out of 2.6 of the above average incidents were reported to the CERT®/CC (and nearly all of them may have been reported). If we assume the AFIWC probability, then it was estimated that more than 96% of these incidents were reported to the CERT®/CC.

6. Recommendations for Internet Users and Suppliers

Security is a problem on the Internet. The thousands of successful break-ins described in this research are a testimony to that. Numerous authors -- scholars and sensationalists alike -- go even farther by describing the Internet as a "dangerous place" in terms of security.

But just how much of a problem is security on the Internet? What this research shows is a mixed message. On the positive side, this research clearly shows that the state of Internet security is not as bad as some authors have proposed. Both in terms of the absolute numbers of incidents, and in the growth of these incidents, the numbers are lower than reported in popular literature and in the Press. More importantly, response teams and researchers are not as unaware of Internet security activity as some authors have argued. As shown in Section 5, the most serious incidents on the Internet *are* reported. In addition, none of the incidents were tremendously destructive. In fact, very few instances were recorded of destructive attacks. Most attacks were in the category of a nuisance (although some were a *big* nuisance), and not something more destructive or harmful.

Nevertheless, on the negative side, security incidents were clearly not dropping to zero. As shown in Section 3, the rate of growth of Internet incidents was less than the growth of Internet hosts by 7%. But, stated another way, this means that the growth of Internet incidents in absolute terms was nearly at the *same* pace as the growth of the Internet.

To put this in perspective, we can use the estimates of total Internet incident activity in Section 5 to see how likely we are to be involved in an Internet incident. This yields the very rough estimates in Table 6.1.

	Low Estimate	**High Estimate**
Individual Site Involved	1 time in 15 years	1 time in 0.8 years
Individual Host Involved	1 time in 850 years	1 time in 45 years

Table 6.1. Estimated Rate that an Internet Site or Host was Involved in an Incident in 1995

This table shows that, according to these estimates, a typical Internet site is involved in *no more* than around *one incident per year.* In terms of hosts, the estimates of Table 6.1 show that a typical Internet host is involved in *no more* than around *one incident every 45 years.* The CERT®/CC records show that some sites and hosts are apparently more attractive because they were involved in many incidents each year. This means that for the average, less attractive, sites and hosts, the probability of being involved in an incident is even lower.

In addition, as shown by this research, many of the Internet incidents are minor and often do not involve successful break-ins. As such, the rate at which sites and hosts are involved in *serious* incidents is even lower. For example, at one site that reported all their incidents to the CERT®/CC (Site "A"), only 7% of incidents involved root break-ins. If this were similar throughout the Internet, then the *maximum* rate that any one *site* would be involved in a root break-in would be around once in 10 years, and any individual *host* around once in 540 years.

Risk	**Estimated Rate Risk Occurs**
Root Break-In, Internet Site	1 out of 10 years
Root Break-In, Internet Host	1 out of 540 years
Convenience Store Robbery	1 out of 1.5 years
Hard Disk Failure	1 out of 75 years
100 Year Flood	1 out of 100 years
Serious Structural Fire, NY City	1 out of 220 years
Death Due to Breast Cancer	1 out of 6,224 years
Death in Motor Vehicle	1 out of 6,250 years
Death Due to Fire, NY City	1 out of 40,000 years

Table 6.2. Comparison of Estimated Rates That Risks Occur
[Pik97, USB96:Chart Nos. 129, 138, 318, 1263, NYC97a, NYC97b]

These rates of occurrence are similar to other risks that we take reasonable precautions for. Table 6.2 compares several example risks with Internet security risks. The conclusion we can draw from this is that, because there is a steady, but relatively small, level of Internet security incidents, Internet users should take reasonable security precautions, just as they would take for other risks in their lives. In addition, Internet suppliers should produce and distribute products that provide users with reasonable security.

The following sections discuss these implications in more detail.

6.2. Implications for Internet Users

This year, any specific individual will most likely *not* be the victim of a violent crime, have their house robbed, or their car stolen. But they might. Because of this, they are likely to take reasonable precautions to protect themselves and their property.

This research shows the same is true of the Internet. Unlike what some authors have proposed, an individual Internet user is most likely *not* going to be the victim of an Internet attack this year. But they might. Because of this, they should take reasonable precautions to protect the files on their computer, and to protect their data as it transits the Internet.

Two analogies illustrate this point. Take, for example, convenience stores. They get robbed sometimes. This could clearly be prevented with a "fortress" security system of physical barriers and armed guards. But then how convenient would that store be to shop in? Instead of ensuring *no* risk of robbery, the convenience store owner typically takes reasonable precautions against robbery in order reduce that risk, but accepts some risk in order to ensure the store is still convenient to shoppers.

An Internet user can be perfectly secure from Internet attack by simply disconnecting from the Internet. But then, this user would no longer be an Internet user. Instead of taking this "no risk" strategy, it is probably more appropriate to take reasonable precautions and accept a level of risk that depends on that user's individual needs.

A second analogy is the mail system. We view the mail system as generally being secure enough to send a personal letter, or to send a check to pay a bill. On the other hand, most people do not send cash or valuables through the mail unless special precautions are taken. We also don't usually send sensitive personal information on a post card, and instead, we enclose it in an envelope. Sometimes a letter is lost, but not often.

In some ways, the Internet is a less secure system than the U.S. Postal Service ("snail mail" in the computer vernacular). E-mail is usually sent across the Internet in clear text that could be read by other users. On the other hand, Internet e-mail is usually a lot quicker, and perhaps more convenient and inexpensive. As such, users may be willing to accept the higher security risk when using the Internet in order to have the capabilities.

Prudent users of the Internet, however, should take precautions in two ways. First, they should take reasonable precautions to protect their files stored on their local computer or stored on the network. And second, they should take reasonable precautions to protect their data in transit on the Internet. For each user of the Internet, the *reasonable* level of precautions may be different, and it depends on that user's needs.

This research shows the following basic security precautions should be sufficient for most users:

1. Back up important files.

2. Use a good password for network access controls.

3. Ensure permissions are set properly on files that can be accessed by others.

4. Encrypt, or store off-line, files that are particularly sensitive.

5. Do not send sensitive user identifications, such as a social security number, address, phone number, personal data, or credit card number across the Internet unless it is encrypted at the source (prior to being sent across the Internet).

6. Use an encryption program, such as Pretty Good Privacy (PGP) or S-MIME, if you want e-mail to be private.

An additional recommendation for commercial Internet users is:

7. Conduct some form of risk analysis to determine the cost effective level of security needed.

There was no indication in this research that these simple precautions would not be effective in preventing most Internet attacks.

There were very few references to viruses in the CERT®/CC records. As such, this research did not indicate that virus protection was required. This research did not, however, examine problems *within* local area networks. Viruses can be a considerable problem within LANs, particularly for LANs with personal computers (PCs and MacIntoshes). As such, an additional precaution that users on LANs with PCs and MacIntoshes should take is to use virus protection software that is frequently updated.

6.3. Implications for Internet Suppliers

Internet suppliers include both commercial vendors that supply hardware and software used to access the Internet, and organizations such as the Internet Society and its member organizations that help establish standards for Internet protocols. As noted in the previous sections, this research gave no indication that simple precautions would not be effective in preventing most Internet security problems. Suppliers of Internet products should, therefore, ensure their protocols and products conveniently provide Internet users with capability to take these simple precautions as described it the previous section. In addition, the CERT®/CC incident records clearly indicate specific problem areas with respect to Internet security that should be corrected by Internet suppliers.

The recommended corrections are as follows:

1. Provide protocols and software that encrypt user name, password and IP address combinations at the source, or provide an alternative system that does not require passwords to be sent in the clear across the Internet.

2. Provide protocols and software that prevent access to files of encrypted passwords, or provide an alternative system that does not require encrypted passwords to be stored in files on systems accessible across the Internet.

3. Deliver systems to customers in a secure state.

4. Develop protocols and programs with reasonable protections against denial-of-service attacks.

5. Accelerate development of protocols and programs that provide reasonable privacy for such user programs as e-mail.

7. Recommendations for Future Research

This research was only a preliminary analysis of the data derived from the CERT®/CC incident records during 1988 to 1995. Both the complete report of this preliminary analysis [How97], and the data set itself, can be obtained from the CERT®/CC [http://www.cert.org/] or from the author [johnhoward@earthlink.net]. Possible research opportunities with this data set are as follows:

1. Analysis of additional trends in the data over time

2. Comparison of incident trends to other events

3. Implications of trends in the distribution of operating systems across the Internet

The findings of this research could be validated or extended through additional data. This could be accomplished as follows:

4. Validation and extension through 1996 and later CERT®/CC data

5. Validation and extension through data from other response teams

Experience during this research has also indicated there are important areas of related research that remain largely unexplored. Among these are:

6. Development of a heuristic for determining the scope of an incident

7. Refinements of the taxonomy

8. Research into behavior of attackers

9. Better sampling of Internet activity

8. Current Activities

The CERT®/CC, with the cooperation of the Sandia National Laboratories, is currently 1) developing "common language" to describe Internet incidents and vulnerabilities, 2) entering incident and vulnerability information into a "knowledge" database, and then 3) making this information available to the Internet community. It is hoped that similar methods will be adopted by other incident response teams. The ultimate objective is for the Internet community to have comparable incident and vulnerability information available near real time. For more information, contact the CERT®/CC [http://www.cert.org/] or the author [johnhoward@earthlink.net].

9. References

References in this paper are placed within brackets at the end of the referenced passage. The reference starts with three letters that identify the author(s), followed by a two digit number for the year, a colon, and specific page numbers.

[ABH96] Derek Atkins, Paul Buis, Chris Hare, Robert Kelley, Carey Nachenberg, Anthony B. Nelson, Paul Phillips, Tim Ritchey, and William Steen, *Internet Security Professional Reference*, New Riders Publishing, IN, 1996.

[Amo94] Edward G. Amoroso, *Fundamentals of Computer Security Technology*, Prentice-Hall PTR, Upper Saddle River, NJ, 1994.

[Coh95] Frederick B. Cohen, *Protection and Security on the Information Superhighway*, John Wiley & Sons, New York, 1995.

[GAO96] . . . ., *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD-96-84, Government Accounting Office, Washington, DC, May, 1996.

[HoR91] P. Holbrook, and J. Reynolds, editors, *Site Security Handbook*, RFC 1244, available on the Internet from the Internet Engineering Task Force (IETF), and at numerous other sites.

[How97] John D. Howard, *An Analysis of Security Incidents on the Internet, 1989 - 1995*, Ph.D. Dissertation, Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, PA, April, 1997. Available on-line at http://www.cert.org/.

[McK82] McKelvey, Bill, *Organization Systematics: Taxonomy, Evolution, Classification*, University of California Press, Berkeley, CA, 1982.

[NYC97a] Fire Department, City of New York, *Facts About the FDNY*, World Wide Web Site, http://www.ci.nyc.ny.us/, April, 1997.

[NYC97b] Department of Buildings, New York City, *Home Page*, World Wide Web Site, http://www.ci.nyc.ny.us/, April, 1997.

[Pik97] Frank Pikelner, *Hard Drive Specs*, World Wide Web Site, http://www.ariel.cs.yorku.ca/~frank/hd-specs.html, April, 1997.

[RuG91] Deborah Russell and G. T. Gangemi, Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., Sebastopol, CA, 1991.

[USB96] U.S. Bureau of the Census, *Statistical Abstract of the United States: 1996 (116th Edition)*, Washington, DC, 1996.

[WhK96] Richard White and Greg Kincaid, *Information Warfare: An Overview of AFIWC Operations*, version 2.3, briefing at the USAF Academy, CO, February, 1996