

“Holes in the Net: Security Risks for the E-Consumer”

Testimony of Dr. Vinton G. Cerf

before the

Space, Science, and Technology Subcommittee

of the

U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

Senator Ron Wyden (Oregon) –Chairman

July 17, 2001

“Holes in the Net: Security Risks for the E-Consumer”

Introduction

As a historical matter, the Internet and its predecessor systems were developed in a largely academic environment focused on research, information and resource sharing and a general atmosphere of cooperative enterprise. For over twenty years, from 1969 to 1990, the Internet research program and user population benefited from this academic setting. However, by 1990, the environment began to change. For one thing, Internet services were just beginning to be made available on a commercial basis. As the cross section of users changed from its academic and military origins to encompass the business sector and the general public, a far broader range of behaviors were manifest in the Internet world. Various kinds of vandalism and other deliberate attacks increased in incidence.

If not daily, then more often than one would like, one reads reports about a variety of network vulnerabilities, hacker attacks, unintended information releases and other frailties on the Internet. For the most part, these problems center on the computers that serve users on the Internet, but a good number also reflect vulnerabilities of the network itself. The network vulnerabilities are a primary concern for the Internet Service Providers who have responsibility for keeping the Internet in operation 24 hours per day, 365 days per year. It is also worth observing that many of the operational problems arising on the Internet have little to do with deliberate attacks. Rather, these problems arise simply from the complexity of the system, the proclivity of Murphy's Law to take effect at any moment,¹ bugs in the software, human errors and things that simply break down. While network-related problems are a consumer concern, to the extent that they interfere with access and use of Internet services, the more critical concerns revolve around the serving computers (so-called Internet hosts) through which all online services are implemented, the client computers (desktops, lap-tops, personal digital assistants, internet-enabled cellular phones, and so on) and the policies of companies that provide services through the Internet. I will concentrate my testimony, therefore, on the end-points of the Internet: hosts, client devices and the companies that provide Internet-based services.

Consumers are particularly vulnerable to weaknesses in application software. Email can carry attachments that harbor so-called “viruses” that can “infect” the rest of the software in the user's computer. Web pages can deliver software that is interpreted by the user's browser and may cause damage to the user's information or interfere with proper operation of the user's computer. This topic is explored in more detail later in this paper.

Host Vulnerabilities

Among the most visible of the consumer-affecting problems are denial-of-service attacks aimed at interfering with the normal operation of one or more servers on the net. These attacks are sometimes very hard to distinguish from legitimate overloads, such as the

famous Victoria's Secret Lingerie webcast that drew a reported 1.5 million viewers whose attempts to download streaming video completely outstripped the server's ability to deliver traffic. The server simply could not respond to all the user requests for data. Such problems are analogous to overloaded emergency service centers that cannot accept all the telephone calls made during a crisis.

If the overload comes from a single source or a small number of sources, ISPs sometimes can track down the source and filter out the offending packets as they enter the network. However, hackers have developed distributed denial-of-service (DDOS) attack tools that harness tens to hundreds of thousands of computers in the Internet. Each of these may send only a small amount of traffic but the aggregate may overwhelm the target. Such attacks are much harder to defend against and to track down. A principal reason that such distributed attacks are even possible is that many hosts on the Internet are unprotected from break-ins and become unwitting "hosts" for so-called "Trojan horse" software that can be activated remotely and used to originate traffic towards the target. The irony of this situation is that the unprotected hosts often contain no information or provide no services that are considered critical in nature. They might be serving computers and workstations in an academic setting. They might even be laptops or desktops that are connected to the Internet by dedicated links (such as Digital Subscriber Loops or cable modems). If these platforms can be found by methodical probing of the net, they may be subsequently "infected" with "zombie" software that can later be used in a DDOS attack. But because these computers might not be thought to contain critical or valuable information, they may not be as protected from invasion as they might otherwise be.

These vulnerable resources may not be configured by their operators to be resistant to the exploitation of vulnerabilities. The systems may be operating with "default" passwords that come with the manufacturer's "standard" configuration – such passwords are widely known (especially among the hacking crowd) and should be changed by the operator before going online. Desktop machines (and operating systems) that were designed to be used mostly as client computers, may become more vulnerable when they participate in so-called "peer-to-peer" operations. Examples of such applications include Instant Messaging, file transfer services, Internet telephony and so on, in which the computer behaves both as a client and as a server.

Apart from a variety of denial-of-service risks associated with host machines on the net, e-consumers run a variety of risks of information compromise in which data they consider private could be exposed to unauthorized view. The least technical and most common avenue for such exposure is a consequence of corporate policies that simply do not protect consumer privacy. User names, addresses, telephone and fax numbers, email identifiers, account numbers, social security numbers, credit card numbers and any of a variety of other data might well be released, deliberately, by a corporation that does not have a consumer privacy protection practice and chooses to share this information for business purposes. The same data might be released unintentionally by the operator of a host who has failed to protect an online system from exploitation.

One of the more ironic scenarios occurs when the user's client computer establishes an encrypted channel over the Internet to a server machine, transmits private information to that machine, and the information, so carefully protected while in transit, is exposed to unauthorized parties either by business practice or by negligence in configuring the server from invasive attack.

Rip Van Wrinkle

Consumers are sometimes surprised by the unexpected consequences of well-intended service features. For example, a few months ago, I suddenly received a barrage of messages from my email correspondents who reported that a batch of message they had sent me nearly two years ago had suddenly emerged on the Internet accompanied by rejection notices saying that these messages had not been delivered. A back-up email server had received and recorded these messages and awakened from its slumbers (for reasons never quite clear) to realize that from its perspective, this cache of messages had not been delivered in two years. The machine dutifully set out to notify every sender of this fact and included a copy of the "undelivered" message.

More generally, email services often make backup copies of the email so as to recover from a catastrophic failure of a primary server. From time to time, email users are surprised to discover that email they thought they had long since deleted has been retained in backup files and has been released by accident or has become discoverable in a legal proceeding or is accessible under appropriate warrants. This is perhaps a specific case of the more general case of record keeping, such as is done in the consumer telecommunications service industry. Detailed billing records of calls (telephone number called, originating telephone number, date and time of day of call) are often kept for periods ranging from three months to a year to resolve subsequent disputes. Anyone who uses a major credit card that provides a report annually on their use can confirm that the credit card industry knows a great deal about specific consumer activities in the form of detailed transaction records.

Passwords

One of the more serious consumer risks arises in the use of access-controlled services requiring user authentication. The most common method of authentication is to associate a "password" with a user identifier (ID). These passwords are often fixed and reused repeatedly. Users are notorious for the poor choices of passwords and their unwillingness to change them regularly. Passwords can often be guessed (birthdate, pet's name, spouse's name, the current year, anniversary date, social security number, telephone number, address). Password files at the service hosts are usually one-way encrypted² but if a hacker can get a copy of the encrypted password file it is possible to run a "reverse dictionary attack" to try to find the password. In a reverse dictionary attack, all the words in the dictionary are encrypted and then compared with each of the encrypted passwords taken from the target computer. A match exposes the password. Such tools are very commonly available. Good password practices dictate at the least that reusable passwords be changed regularly, contain more than just alphabetic characters, be 6-10 characters

long and not contain common words found in the dictionary. An example of such a password is “SOLIPIKU98.”

There are a number of alternatives to these so-called “reusable” passwords. Some of these require the use of a device that introduces a constantly changing password. Others authenticate by means of a challenge and an encrypted response that can be verified.

Risks

The July 2, 2001 edition of TIME Magazine carried a cover story devoted to online privacy risks faced by consumers. Identity theft is one of the most critical and increasing risks faced by consumers. Information about consumer use of Web services can be collected in each user’s personal computer by Web service providers in small caches of information called “cookies.” The Web service providers can use this information to tailor services provided to individual users. However, this data might contain personal information that could be linked with data obtained through other sources and possibly even re-sold to third parties for marketing purposes. Consumers are at risk if companies that collect this data make use of it in ways that consumers do not expect or would not approve. It is this concern that led to requirements for companies to report their privacy protection practices to consumers on a regular basis.

Not all web sites are what they seem and some may appear to offer products or services but may in fact simply be “fronts” for purposes of capturing personal information, credit card numbers and the like. This is outright fraud. It is illegal and actionable.

Public access to government records may expose a considerable amount of personal information to public view. Details of court records, registrations, building permits and designs, home addresses and phone numbers, traffic violations are all potentially available. This is through no weakness in the design of the Internet and its applications but a consequence of state or local policy with regard to access to “public” records.

So-called “data brokers” obtain personal information from a variety of sources, often government sources, and amass databases of personal information which they then resell to the public for a fee. There is often considerable debate about the legality of making such information accessible, even if it is obtained by legitimate means from legal sources.

Software can be put into your computer by someone with physical access to it that will provide a record of virtually everything you do with your machine. Similar software might be ingested over the Internet as an attachment to an email message or possibly as a consequence of loading a web page and executing “applets” (written in programming languages such as Java). Such “Trojan horse” software can expose all of your personal computer’s data and activity to view. The recent wave of interest in dedicated, high speed access to Internet using Digital Subscriber Loops (DSL) or cable modems creates a new risk for consumers. If their computers are online all the time, with fixed Internet addresses, they may become subject to hacker attacks, just as the web servers and other Internet hosts are exposed today.

Consumers may be misled by email, chat room or instant messaging exchanges into believing things about their correspondents that are not true. This works both ways. A person may misrepresent himself or herself deliberately or you may be the target of an attack against you by someone pretending to be you. Such terms as “cyberstalking” have entered the language to account for this kind of behavior.

Reactions

Consumers can respond by being far more careful about the information they provide to online service providers. They can avoid downloading, opening or executing attachments on email messages until they confirm their origin. They can purchase, use and frequently update virus detection software. Even if you use secure web sites, the protection extends only to the delivery of personal information to the web site. The web service provider’s privacy protection policies determine whether the data provided is propagated further to third parties. Consumers should make a point of learning company privacy protection policies.

Companies seeking to protect their own computing assets and networks can install firewalls and make use of encryption methods to protect employee access to corporate networks via the public Internet. Software manufacturers need to pay closer attention to the potential abuses their software can support – not simply focus on the constructive functionality they offer. Internet service providers need to configure their networks to increase resistance to various forms of hacking. And legislators may be able to help law enforcement agencies by providing tools for combating criminal use of online systems. There is a tension in the latter response because it is possible to erode privacy in severe ways in the process of trying to assist in law enforcement.

The Internet has the potential to be an enormously powerful, positive and constructive force in our society. It is also a potential source of serious abuse. As a society, we are challenged to find a balance between protecting the society from abusive practices and protecting individuals from abuse by various state, local and federal government agencies. The next decade will surely be filled with unexpected twists and turns as we learn how to apply online technologies to our daily needs. One can only hope that out of all the experience will come wisdom and the will to apply it.

¹ Murphy’s Law reads, “If anything can possibly go wrong, it will.” A corollary suggests that Murphy was an optimist!

² “one-way” means that the original password is encrypted in such a way that even if you know the encryption algorithm, you cannot directly decrypt the password. However, one could use a dictionary, encrypt its words, then look for encrypted text in the dictionary that matches the one-way encrypted password.