White Paper

ixia

Network Security Testing

26601 Agoura Road, Calabasas, CA 91302 | Tel: 818.871.1800 | Fax: 818.871.1805 | www.ixiacom.com | 915-1785-01 Rev C January, 2011

Table of Contents

Security is a discipline concerned with protecting networks and computer systems against threats such as exploits, malware, data leakage, spam, and denial of service (DoS) attacks, as well as ensuring trusted access through mechanisms such as IPsec or SSL. Enterprises have deployed security devices of all types to defend against threats, and to prevent unintended data leakage.

Network security devices consist of one or more security functions, including firewall, intrusion prevention/detection systems (IPS/IDS), data leakage prevention (DLP), and content security filtering functions (e.g. anti-spam, antivirus, URL filtering). Those functions have increasingly been integrated into Unified Thread Management (UTM) system or Next Generation Firewalls. Every security device requires continuous testing to ensure that the devices are effective, accurate, and productive, while simultaneously maintaining acceptable performance.

It is essential that homes, government organizations, and enterprises of all sizes maintain secure networks. The number and types of attacks continues to grow at an alarming rate. The devices used to defend against them are necessarily complex.

"In 2010, [hackers] have created and distributed one third of all viruses that exist. This means that 34% of all malware ever created has appeared ... in the last twelve months."

The Current State of Network Security

There has been an explosion of security threats in recent years. According to the 2010 Annual Report from Panda Labs: "In 2010, [hackers] have created and distributed one third of all viruses that exist. This means that 34% of all malware ever created has appeared ... in the last twelve months."

The breakdown of the types of malware programs found by Panda Labs is shown in Figure 1. These categories are explained in this paper.

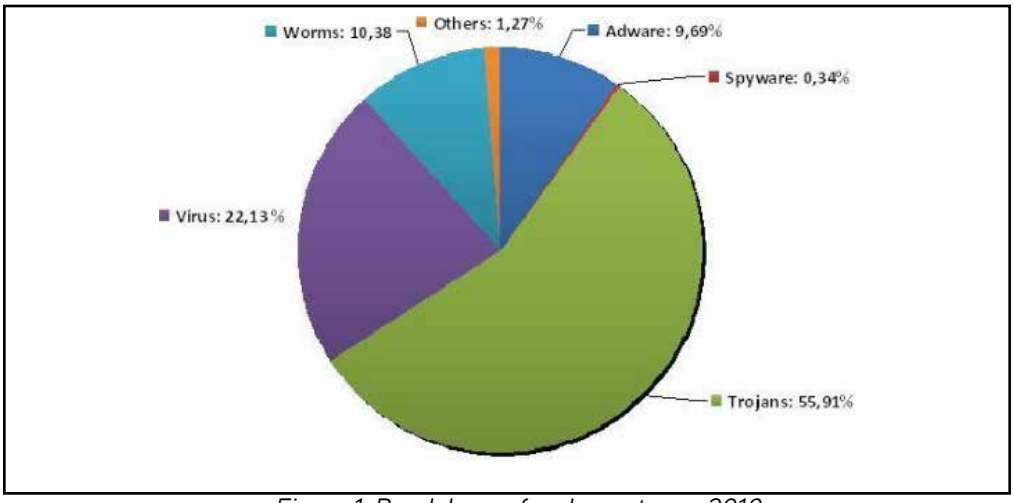

Figure 1. Breakdown of malware types, 2010

Hacking has mutated from a hobby to a successful business. 78% of malware attacks export user data, and 70% of the targets were banks. It is estimated that companies lose between 0.5 and 2.5% of their revenues because of security-related losses and downtime.

From September 2009 through March 2010, the Ponemon Institute conducted a survey of reported data breaches in the United States, United Kingdom, Germany, France and Australia. The average loss from the surveyed companies was USD 3.425 million per breach; an average per capita cost of USD 142. The biggest threats were from employees who had been laid off and attacks from outside the company.

During the last few years, the cumulative number of vulnerabilities has increased dramatically, as shown in Figure 2 from PandaInsights.com.

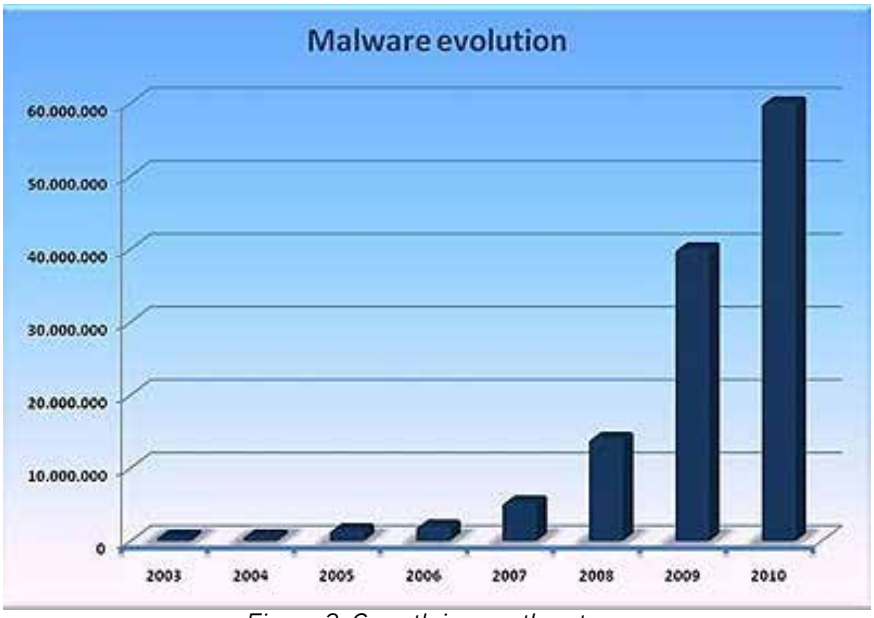

Figure 2. Growth in new threats

It is estimated that companies lose between 0.5 and 2.5% of their revenues because of security-related losses and downtime.

The number of vulnerabilities discovered in applications is far greater than the number discovered in operating systems. As a result, more exploitation attempts are recorded on application programs. The most popular exploitation targets tend to change over time because the rationale for targeting a particular application often depends on factors such as prevalence or the inability to effectively patch. Browsers and client-side applications that can be invoked by browsers seem to be consistently targeted, taking advantage to the current trend wherein trusted Web sites are converted into malicious servers.

Zero-day vulnerabilities are those not found until a service is deployed. There has been a significant increase worldwide over the past several years in the number of people discovering zero-day vulnerabilities, as measured by multiple independent teams discovering the same vulnerabilities at different times.

The Source of the Problem

But who is to blame for the vulnerabilities that malware takes advantage of? The Internet is something that we all want—the ability to publish and find information, the ability to buy and sell products, the ability to communicate with others. The vast interconnection made possible by the Internet, however, provides the avenue for malicious action.

It's possible for any of us to let the invaders in by running flawed software. That is, software that is outright broken or sloppily written. Flaws are classified as either known or unknown, zero-day vulnerabilities. Known vulnerabilities are published, allowing authors to issue fixes and security vendors to update software. Zero-day vulnerabilities are potentially more harmful, associated with newly published programs or offered Web services. Such vulnerabilities may be visible for days or weeks until patched.

Network, server, and client misconfiguration offers another avenue for hacking. Network elements, such as routers and home gateways, come with a default administrator password, passwords that often never change. A hacker with access to a router can cause all traffic through the router to be sent through its own server, allowing "person-in-the-middle" attacks.

Similarly, misconfigured servers can allow hackers to disable or modify Web sites, inserting code of its own choosing. Such code is usually intended to steal data from associated databases.

Misconfigured servers can allow hackers to disable or modify web sitess, inserting code of its own choosing.

The Damage

The damage from successful network security attacks can take many forms:

- **Theft of data.** This consists not only of financial data, such as credit card numbers, but can also include customer lists, intellectual property, and product development and marketing plans.
- **Loss of time.** It can take a great deal of time to recover from a security attack, or even from the suspicion of an attack. Data may need to be recovered or reconstructed and systems extensively checked.
- **Monetary loss**. This is often preceded by the theft of data.
- **Disabled or crippled services.** Protesters and some governments may seek to disable offending Web sites. Hackers may be purely malicious in their intent.
- **Legal exposure.** Any of the previous items may expose an enterprise to law suits for loss of data or money entrusted to them.

Classification of Security Attacks

User-Involved Attack Mechanisms

Innocent computer users are involved in most security breaches. The most frequent methods include:

- **E-mail.** In addition to spam, e-mails can contain attachments that are malicious executable programs or links to infected Web sites. This is currently the primary initial infection vector used to compromise computers that have Internet access.

- **Web.** Those same client-side vulnerabilities are exploited by attackers when users visit infected Web sites. Simply accessing an infected Web site is all that is needed to compromise the client software. Web sites can be dangerous in several ways:
  - Masquerading as valid Web sites collecting financial and personal information.
  - Infected through content injected from associated Web sites.
  - Present false information. For example, a Web page advertisement might suggest that a user's computer is infected with a virus, inviting the user to click on a virus scanning program, which actually infects the computer.
- **FTP.** FTP is frequently used to download executable programs. Internet access.
- **Instant Messaging (IM).** Instant messaging programs now provide mechanisms for passing executable programs and Web links, providing a means of infecting computers and revealing information.
- **Peer-to-peer (P2P).** P2P environments are often used to share software, which may be similarly infected.
- **Gaming.** Social interaction with other players may invite e-mail or IM communications.
- **Software updates.** Software vendors are increasingly updating their software over the Internet, using Web pages, or dedicated, resident programs. Malicious parties may substitute their own software, or infect the updates before they are downloaded.
- **People.** End-users are frequently at fault for the following reasons:
  - Poor passwords
  - Inconsistently updating their software
  - Getting too personal
  - Being too trusting
  - Inconsistent application of security software
  - Engaging in wishful thinking

Web vulnerabilities comprise 49% of the total number of those reported.

Web Vulnerabilities

Web vulnerabilities comprise 49% of the total number of those reported. The cumulative number of reported Web vulnerabilities is more than 20,000. Attacks against Web applications constitute more than 60% of the total attack attempts observed on the Internet.

Three types of vulnerabilities predominate:

- **Cross-site scripting (XSS).** This type of exploit inserts HTML or other Web content into Web pages before they are displayed to the user.
- **SQL injection.** This type of exploit extracts information from a database.

- **File includes.** This vulnerability is similar to SQL injection in that it takes advantage of unchecked user input. Such input may be used with Web sites that use PHP or Java.

Figure 3 shows the most common malicious software in common Web downloads.

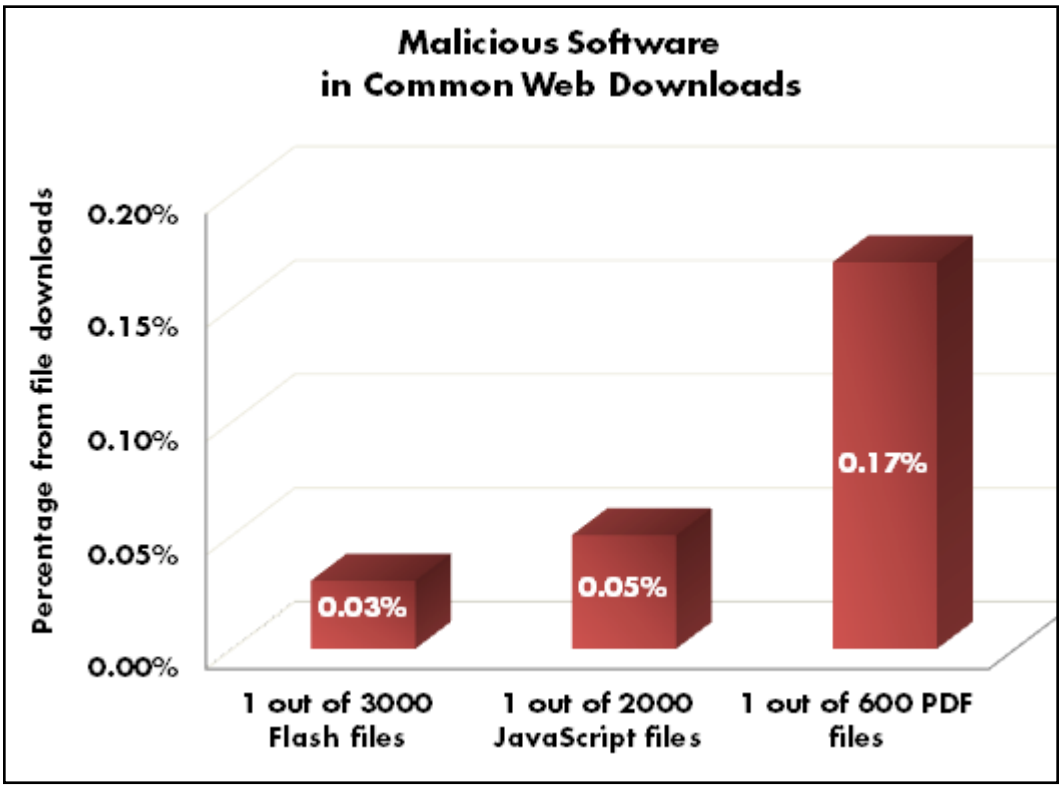

Figure 3. Malicious software in common Web downloads

Sites that offer their users remote access may rely solely on user passwords. Automated "robots" may try long lists of possible passwords in order to gain access.

Web application vulnerabilities, such as SQL injection and cross-site scripting flaws account for more than 80% of the vulnerabilities reported. Despite the enormous number of attacks and despite widespread publicity about these vulnerabilities, most Web site owners fail to scan effectively for the common flaws.

Network-Level Attack Mechanisms

A number of attacks are mounted without user involvement. The Internet depends on a number of services accessible to everyone: Web, DNS, FTP, SMTP, POP, IMAP, and SIP to name just a few. The server software used for these services, plus the many plug-ins that are used in conjunction with the services, are an attractive target for hackers.

Sites that offer their users remote access may rely solely on user passwords. Automated "robots" may try long lists of possible passwords in order to gain access.

Denial of service attacks are another network-level threat in which the attacker uses large numbers of hijacked computers to send malicious traffic to a Web or other server. The purpose of the attack is to disable the service partially or completely.

Sources of Vulnerabilities

Vulnerabilities are a result of software flaws, flaws that fail to anticipate all possible conditions, especially unusual user input.

Nevertheless, the problem of discovering and verifying new vulnerabilities is a very large industry problem. Some security companies receive more than 55,000 new samples per day.

Malware

Malware is the term used to describe the entire gamut of malicious software. For the purpose of this discussion, we will break them down into six categories:

- Viruses
- Worms
- Trojans
- Rootkits
- Spyware
- Malicious adware/scareware

Although we can distinguish these types, modern malware is very often hard to categorize—blending multiple types of attacks.

Vulnerabilities are a result of software flaws, flaws that fail to anticipate all possible conditions, especially unusual user input.

Denial of Service Attacks

Denial of service (DoS) and distributed denial of service (DDoS) attacks are the oldest methods of disabling IP networks. While those methods are well-known and have been studied for years, they continue to remain one of the most effective ways to impact the performance of IP networks or services, or completely restrict access to a network, service, or application for legitimate users.

By definition, the intent of a DoS/DDoS attack is to partially restrict or completely deny access of legitimate users to resources provided by a victim's network, computer, or service. When this attempt is initiated from a single host, the attack is called a DoS attack. While DoS attacks can be successful mounted using a single host with limited resource, the majority of the attacks require a group of malicious hosts that flood the victim's network with an overwhelming amount of attack packets. This type of attack is called distributed DoS.

According to Internet World Stats, the worldwide Internet population in June of 2010 was close to 2 billion users. Many of the Internet users browse the Internet without appropriate security software, or by using operating systems and software that is not properly updated. Attackers use automated techniques to discover such systems and use known vulnerabilities to install DDoS tools on those system. Such infected computers are called Zombie computers.

Zombie computers report back to a command and control center (C&C). After they are logged on, they become part of a remotely controlled botnet. The most common C&C servers are Internet Relay Chat (IRC) servers, but in some cases, can be Web servers.

Relying on hundreds to thousands of infected computers that have been previously infected with worms or trojans that facilitate remote control for an attacker, large DDoS attacks can be coordinated. Larger botnets can exceed 100,000 zombie computers, which can generate aggregated traffic from 10 Gbps to 100 Gbps – more than most ISPs can handle.

McAfee's third quarter 2010 report indicates 18 million new zombies were created in the third quarter of 2010, an average of 200,000 new zombies per day. The zombie computers were primarily used to generate spam, but their purpose could be easily changed by the botnet controller to generate DDoS attacks.

To increase the effectiveness of the attack, vulnerabilities are often used to obtain control of Web servers for the purpose of installing trojans or worms that add the server to the controlled botnet. Server machines have the advantage of better computing resources and higher available bandwidth. Further, attack traffic is generated from trusted IP addresses.

To increase the effectiveness of the attack, vulnerabilities are often used to obtain control of Web servers for the purpose of installing trojans or worms that add the server to the controlled botnet.

A large number of DDoS enabling tools are available on the Internet. The most common ones include Tribe Flood Network (TFN) and its newer version TFN2K, Trinoo (Trin00), Stacheldraht, myServer,

Unexpected Peak Hours

DDoS attacks can be the unintentional result of an overwhelming number of legitimate users accessing Web sites with hot news or events that interest millions of users in a short time interval. One of the most publicized examples is when Google mistook millions of search queries for "Michael Jackson died" for a distributed DoS attack.

Collateral damage

We've now witnessed two salvos in the WikiLeaks cyber war. The first was fired by the group Anonymous at Mastercard, Amazon, PayPal and Visa – each of whom had withdrawn support for WikiLeaks. This brought about a counter attack from parties unknown against the WikiLeaks web sites. The attacks against the commercial sites seems to have paused for the moment and the WikiLeaks data has been copied to hundreds of "mirror" sites, but the cyber war is a chilling reminder of how vulnerable we are.

Both engagements used relatively unsophisticated distributed denial of service (DDoS) attacks to overwhelm the targeted web sites.

DDoS Methods of Attack

DDoS attacks can be classified as follows:

- **Resource starvation**
- **Alteration or destruction of system configurations**
- **Hardware damage**

The most common denial of service methods are based on overwhelming the victim's computer or network with useless data that result in overutilization of the following:

- **Network bandwidth**
- **CPU utilization**
- **Memory consumption**
- **Disk and storage**

Based on the resources targeted, the attacks can be further classified as:

- **Bandwidth consumption.** One of the easiest ways to deny access to a resource is by consuming the bandwidth available between the ISP and the victim's network.
- **System resource starvation.** These attacks focus on consuming system resources such as CPU time and memory. CPU time is usually consumed with packets used to initiate new connections. Memory starvation can be achieved with legitimate connections that are maintained active after a connection is established.
- **DoS attacks targeting protocol and software flaws.** These attacks exploit software design-flaws (for example, Ping of Death and Land attack).
- **Storage.** As a general rule, anything that allows data to be written to disk can be used to execute a DoS attack, assuming that no protection is set on the amount of data that can be written.
- **Alteration or destruction of system configurations.** These types of attacks require access to the victim's computer. Exploits based on known vulnerabilities in the operating system or applications may allow attackers to get root access to the system. By altering key configuration aspects of the server, an intruder may prevent users to access the compromised computer or network.

  Routing-based DoS attacks target modification of the routing table, preventing the victim from properly sending or receiving legitimate traffic.

  To simplify the use of network addressing, name systems such as Domain Name Servers (DNS) provide a way to map the user-friendly name for a computer or service to the IP address associated with that name.
- **Hardware damage.** Attackers that get root access to systems may destroy the hardware permanently. As an example, attempting to update the firmware of a device with a corrupted image may result in permanent damage.

The most common denial of service methods are based on overwhelming the victim's computer or network with useless data that result in overutilization.

Common DoS/DDoS Attacks

- **Address Resolution Protocol Flooding attack**. This attack constantly sends address resolution protocol (ARP) requests to a gateway or to another host within the same sub-network, thus tying up the attacked gateway or host. The attack is achieved by tricking the hosts of a LAN into generating a constant storm of ARP requests by providing them with wrong MAC addresses for hosts with already-known IP addresses.

- **TCP SYN Flooding attack**. TCP SYN flooding is one of the most common DDoS attack. A typical TCP connection requires a three-way handshake in which the client computer requests a new connection by sending a TCP SYN packet to its remote peer. In response, the TCP SYN/ACK packet is sent by the remote peer and the TCP connection request is placed in a queue, waiting for the TCP ACK packet, which completes the handshake.

  To accomplish this attack, the attacker sends a storm of TCP SYN packets to the victim's IP address, initiated from a large number of spoofed IP addresses, forcing the victim to open a huge number of TCP connections with a SYN/ACK response.

- **UDP Flooding attack**. A UDP flooding attack relies on a large number of attackers sending multiple UDP packets to the victim's computer, saturating its bandwidth with useless UDP packets. The attack packets can target both open and closed ports. When the packets target ports on which the victim's computer is not listening, ICMP destination unreachable packets may be sent by the victim to the spoofed IP address in each UDP packet.

- **PING Flooding attack**. This threat floods the victim with multiple ICMP echo request (PING) packets, thus saturating its bandwidth. This is a very standard attack that can be done with utilities, such as PING, included with any operating system.

- **Smurf attack**. Smurf is another type of PING attack. The attack exploits improperly configured networks that allow external packets from the Internet to use an IP broadcast address as a destination address. By sending a storm of PING packets with the address spoofed with the intended victim's address, all the PING requests are reflected back to all computers of the local network, resulting in an amplified number of replies destined to the victim's computer.

- **PING of Death attack**. Similar to the Ping attack, the Ping of Death also sends an ICMP Echo request to the victim. In this case, however, it is sent in the form of a fragmented message, which, when reassembled, is larger than the maximum legal size of 65,535 bytes. This might cause the attacked host to crash or to stop responding.

- **ICMP Destination Unreachable attack**. On receipt of an ICMP Destination Unreachable packet, the recipient will drop the corresponding connection immediately. This behavior can be exploited by an attacker by simply sending a forged ICMP Destination Unreachable packet to one of the legitimate communicating hosts.

- **ICMP Host Unreachable attack**. The ICMP Host Unreachable packet is another ICMP packet type that can be used to break the communication of two hosts.
- **ICMP "Time Exceeded" attack**. The Time Exceeded Message is an ICMP message that is generated by a gateway to inform the source of a discarded datagram because of the time to live field has reached zero.
- **Land attack**. This attack attempts to drive the victim crazy by sending it special-crafted TCP packets with the source IP address and source port number identical to the victim's IP address and port number. This causes the attacked host to think that it 'speaks to itself' and will often cause it to crash.
- **Teardrop attack**. This is a fragmented message where the fragments overlap in a way that destroys the individual packet headers when the victim attempts to reconstruct the message.
- **FIN Flood attack**. This threat floods a user specified target with TCP packets from randomized, spoofed addresses, where the FIN (final) flag has been turned on. The FIN flag is sent by a user to designate that it is no longer sending packets.
- **RST attack**. This vulnerability allows an attacker to create a DoS condition against existing TCP connections, resulting in premature session termination. Because an attack uses a random IP as the source IP, it is possible that the source IP or computer (if it exists) will send a reset packet (RST/ACK) back to the server that says it did not make the connection request. All this creates incomplete or half-open connections.
- **Application Level DoS and DDoS attack**. Flaws in software implementations can be exploited to cause buffer overflow, consume all memory and CPU, crash the application stack, make the computer to stop responding, or reboot the computer.
- **HTTP GET Flooding attack**. The attack sends an overwhelming number of HTTP GET or HTTP POST requests to the targeted HTTP server, depleting the victim's resources. The requests have legitimate contents and they originate over valid TCP connections. By serving those requests as normal requests, the server ends up exhausting its resources.
- **DNS Flooding attack**. This threat attacks a DNS server by sending a high number of DNS requests that looks like they are initiated from the victim's IP address. The small queries sent by the zombie computers are amplified by the recursive DNS servers that are used as intermediaries to resolve the domain, which generate in response larger UDP packets, overwhelming the victim's computer.
- **SIP Flooding attacks**. This class of attacks floods the victim with a significant number of SIP messages, including REGISTER, INVITE, OPTIONS, MESSAGE, BYE, SUBSCRIBE, NOTIFY, ACK, and PING. The messages are sent from spoofed IP addresses and targets depletion of victim's resources by forcing the victim to process useless SIP messages.

Making money from malware

Successful malware attacks can result in a number of unpleasant effects:

- **Botnets:** Formed from infected computers under remote control. Botnets are used for generating spam and for distributed denial of service attacks.
- **Stolen data:** Eventually leading to stolen money, either through fraudulent credit card transactions or banking transfers.
- **Disabled or damaged computers:** Requiring significant amounts of time to restore or rebuild.
- **Partially or completely disabled services:** Such as e-mail or Web commerce.

Criminals are reaping benefits through the following ways:

- Unauthorized bank and credit card transactions.
- Advance fees, as in the Nigerian scam that requests money to cover the transfer of millions of 'unclaimed' funds.
- Product sales from scareware and Web-based enticements.
- Criminal services that allow the creation and use of malware.
- Resale of stolen credit card and bank account information.
- CAPTCHA-breaking services. CAPTCHA is a technique that presents an image with an embedded word or number, as shown in Figure 9. This ensures that a human is involved in the interaction. Criminal elements are now offering software, services, and personnel to defeat this interaction.

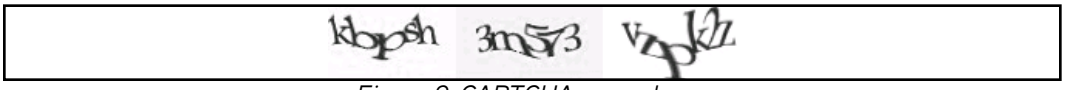

Figure 9. CAPTCHA examples

- Virus testing services. These are online services that determine whether a candidate virus/malware file will be detected by 40 or more anti-virus programs.
- Search redirection. These are services that poison Google and other search engine lookups so that they direct users to target Web sites.
- Legal institutions may be perceived as insecure by their customers.

Network Security Testing

Network security is a critical concern for enterprises, government agencies, and organizations of all sizes. Today's advanced threats demand a methodical approach to network security. In many industries, enhanced security is not an option. U.S. federal regulations such as Sarbanes-Oxley, HIPAA, GLBA, and others require organizations, including financial institutions, health care providers, and federal agencies, to implement stringent security programs to protect digital assets.

The layered approach represents the best practice for securing a network. It requires appropriate security measures and procedures at five different levels within a network:

1. Perimeter
2. Network
3. Host
4. Application
5. Data

Network security professionals speak in terms of "work factor" – the effort required by an intruder to compromise one or more security measures. A network with a high work factor is difficult to break into, while a network with a low work factor can be compromised relatively easily. If hackers determine that a network has a high work factor, they are likely to move on and seek networks that are less secure.

Figure 10 details the accepted security levels, along with the types of security tools used at each level. Ixia tests products and software at the perimeter and network levels, the subject of this paper.

Network security is a critical concern for enterprises, government agencies, and organizations of all sizes.

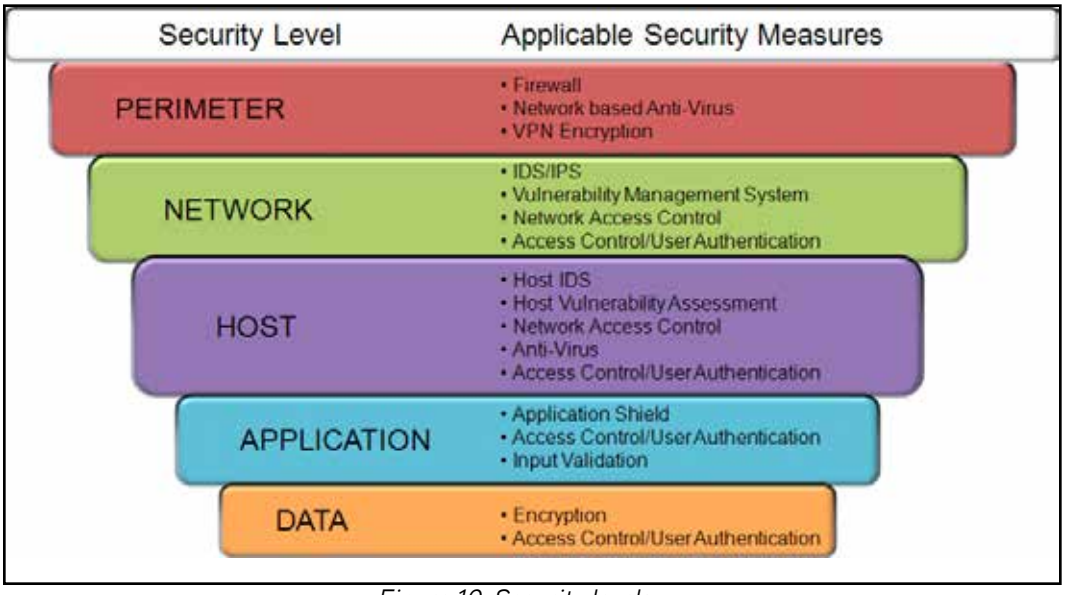

Figure 10. Security levels

Network Security Devices

- **Firewalls**. Firewalls were the first independent security devices used with external network connections. The purpose of the original firewalls was to ensure that only those connections that were required were allowed into the enterprise network. This typically includes services offered to the public: e-mail, Web, FTP, DNS, and a few others. Firewalls are also used to limit the types of services that internal computers may access outside the enterprise. This serves to somewhat limit malware from contacting external servers.

  Firewalls initially operated by filtering connections based on a 5-tuple

  - TCP or UDP
  - Source IP address
  - Source port number
  - Destination IP address
  - Destination port number

  Firewall rules are applied against connections attempted through the firewall, either inbound or outbound, to determine whether the connection is allowed or not. This worked well for a number of years, but as services and their protocols multiplied and applications began to use HTTP's port (80) as their transport mechanism, the ability of firewalls to meaningfully control traffic diminished.

  To handle this, firewalls began to use a technique, one of which is known as deep packet inspection (DPI) In addition to using the 5-tuple information included in layers 2, 3, and 4 of a packet, DPI looks into layer 7 application information to determine exactly the service that is being used. This additional information is then used in firewall rules.

Work factor is defined as the effort required by an intruder to compromise one or more security measures, which in turn allows the network to be successfully breached.

- **VPN gateway**. VPN gateways are used to securely connect multiple sites within an enterprise, remote and roaming employees, and business partners. Two protocols are commonly used:

  - **SSL.** This protects and encrypts traffic, while providing a Web-based interface for information access.
  - **IPsec**. This is network-level security that encapsulates and encrypts all traffic between the gateways. IPsec is described in detail in the VPN Test Methodologies section.

- **Intrusion Detection and Prevention Systems (IDS/IPS)**. Intrusion detection systems are an older technology that passively monitors network traffic, looking for particular malicious patterns, such as repeated attempts to log on to an account. When they notice a pattern, they send alerts to administrators and sometimes modify firewall rules to restrict access from the offending IP address.

  Intrusion prevention systems are logically in line with traffic. That is, all traffic from the firewall's external link is sent through the IPS. It is responsible for identifying and stopping suspected traffic. Specific IPS rules and signatures are used to control how many flows are watched and for how long so as to ensure that the IPS does not significantly diminish the overall traffic flow. IPSs are complex systems, attempting to minimize the number of false positives.

- **URL Filtering**. URL filtering seeks to keep users away from a restricted set of Web sites. These sites are generally classified as follows:
  - **Offensive content**: pornography or other objectionable material.
  - **Harmful content**: containing malicious code.
  - **Inappropriate content**: pages deemed not proper to view at work, such as games or sports.

  The list of Web sites used with the first two categories is often distributed as a service from a security vendor, based on the experience of all of its customers. IT managers create and maintain the last category, often based on lists from the security vendor.

- **Anti-Virus**. Network anti-virus software, located on the firewall or UTM system, serves to identify and filter all forms of malware. It does this by looking at the network connections associated with protected services: e-mail, Web, FTP, IM, and others. The data within the stream is examined using a number of techniques that identify malware. Depending on the particular software, the connection or transfer may be aborted or the offending malware removed from the stream.

  Each vendor has a set of proprietary techniques that they use to identify malware. A common technique is the use of signatures, which are particular unique sequences or bits of data that identify the malware.

- **Anti-Spam**. Anti-spam network software has a great deal in common with anti-virus software, and is often bundled together. Spam is a growing problem, with more and more sophisticated, customized messages being delivered. List-based approaches often miss such messages. Users must remain skeptical and vigilant with respect to 'special' offers.

- **Data Loss and Leakage Prevention**. Data loss/leakage prevention (DLP) is different than other security precautions in that it looks at outbound versus inbound information. DLP seeks to keep company and client proprietary information from leaving the organization, either innocently or maliciously.

  Outbound information flows, such as e-mail, Web form data, FTP, IM, and other channels are filtered. A list of rules, keywords, and policies are applied to determine whether the communication should be rejected or allowed. Such filtering is very tricky. For example, a brokerage company might disallow any account number to be sent to a customer, who may be frustrating for the broker and customer.

- **Evasion Techniques**. Security devices have a tough job—operating on large traffic volumes and keeping up with an ever changing set of threats. An additional complication is the ability of hackers to disguise their attack through evasion techniques. A few examples are as follows:
  - **URL obfuscation**. URLs filtering may be confused by the use of backslashes instead of forward slashes, or the use of % escape characters instead of 'normal' letters.
  - **Fragmentation**. IP packets are broken up into many smaller pieces, making it more difficult to identify.

- **Stream segmentation**. An attack taking place over one connection, e-mail for example, might be interspersed with other traffic, potentially over a long period of time. Security appliances may need to stop looking at the original connection for lack of internal memory.

Testing Security Devices

Testing of network security devices requires a number of techniques, which will be discussed in the next few sections:

- Known vulnerabilities
- Massive denial of service
- Realistic multiplay traffic with comprehensive quality of service metrics
- Encrypted traffic
- Data leakage tests

Known vulnerability testing is the cornerstone of network security device testing.

Known Vulnerability Testing

Known vulnerability testing is the cornerstone of network security device testing. Attacks are mounted against the security device by using a large database of known malware, intrusions, and other attacks. A number of organizations exist to maintain this list. One leading organization is the U.S. National Vulnerability Database maintained by the National Institute of Standards and Technology (NIST). The Mitre Corporation provides access to this database, called the CVE—Common Vulnerabilities and Exposures. As of May 2010, more than 42,000 vulnerabilities are listed, with more than 15 added on a daily basis.

Proper security testing requires that a number of known vulnerabilities be applied to security devices at a significant percentage of line rate. The device under test (DUT) should properly reject all such attacks, while maintaining a reasonable rate of transmission of 'good' communications.

In addition, known vulnerabilities must be applied using the wide variety of evasion techniques. The combination of thousands of known vulnerabilities and dozens of evasion techniques requires that a subset of all possibilities be used for testing. Test tools offer representative samples, including special cases for newly published vulnerabilities.

Distributed Denial of Service

Denial of service attacks often use large numbers of computers that have been taken over by hackers. Those computers use dozens of attack techniques designed to overload network and security devices. This type of testing requires test equipment capable of simulating thousands of computers.

The DUT must be tested to ensure that none of the denial of service attacks, singly or in combination, is able to disable the device. In addition, the ability of the DUT to accept new connections and can provide an acceptable level of performance must be measured.

Line-Rate Multiplay Traffic

Not only must security devices fend off attacks, but they must pass non-malicious traffic at the same time. To ensure this, testing for defense against attacks must be done with a background of real-world multiplay traffic. That is, a mix of voice, video, data, and other services that constitute normal traffic should be applied to the DUT such that the sum of the malicious and normal traffic is the maximum for the device's interfaces.

The quality of experience for each of the normal services must be measured to ensure that the end users' satisfaction will not be sacrificed. For example, voice over IP requires very little bandwidth, but latency and jitter impairments are immediately heard by the human ear.

Encrypted Traffic

As enterprises move to connect their multiple sites and mobile and remote users together into a corporate VPN, data encryption is becoming increasingly important. Data encryption ensures both privacy and authentication of the sending party through the use of certificates or other techniques.

The process of establishing an encrypted link, and then subsequent encryption and decryption can be a significant load for a security device. It is essential that a realistic mix of encrypted traffic be mixed with clear traffic during performance testing. The rate at which encrypted connections can be established is particularly important, representing how quickly a network can resume normal operation after an outage.

Data Leakage Testing

Data leakage testing involves transmission of data from the 'inside-out' to determine if data loss prevention devices will detect the leakage of proscribed information. All outbound means must be tested, including e-mail, e-mail attachments, Web-based mail, Web form data, FTP, and IM.

Enterprises must create test cases for each of the rules, keywords, and policies that they use in the security device, including tests that should not be flagged. Network equipment manufacturers (NEMs) have a more difficult job—requiring a more extensive set of test cases that exercise each type of rule and policy, along with a sampling of keywords.

There are literally hundreds of protocols associated with modern Internet systems. Each operating system vendor and network equipment manufacturer implements each protocol in its own way.

Ixia's IxLoad-Attack

IxLoad-Attack is a complete network security testing solution, offering extensive tests for all types of network security applainces and systems, including:

- Firewalls
- VPN gateways
- Unified threat management (UTM) systems
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Anti-virus (AV) systems

IxLoad-Attack – provides an extensive of more than 6,000 known vulnerabilities, which are applied selectively against security systems. The vulnerabilities are listed in the Common Vulnerabilities and Exposures (CVE) list, and are well indexed for ease of selection. Selected vulnerabilities are applied in parallel or sequentially to discover security flaws. In addition to the vulnerabilities, numerous evasion techniques are available for masking attacks. Together with the extensive set of vulnerabilities, millions of security attacks can be applied by IxLoad-Attack.

IxLoad-Attack includes DDoS – provides approximately 30 denial of services attack types. These attacks may be spread over powerful Ixia test ports to provide line-rate attacks at any volume recovered.

In addition, **IxLoad-IPsec** creates up to thousands of IPsec encapsulated tunnels for application and vulnerability traffic of all types. Encapsulation of vulnerability traffic is a unique capability of IxLoad-IPsec, injecting attack traffic over secure IPsec tunnels. This simulates malware existing at remote sites, which may infect all other sites if not protected. Ixia's powerful Xcellon-Ultra-XTS platform provides up to 20 Gbps of encrypted traffic.

Of particular significance is that IxLoad's other capabilities – of generating real-world multiplay traffic: voice, video and data traffic at line-rate. This is used to evaluate a critical security measure: will network security solutions still provide adequate "normal" service, even when under attack? This is essential. After all, what good is a security solution that stops attacks, but won't allow "good" traffic to pass in sufficient volume?

Please visit Ixia's Security Solution page at

http://www.ixiacom.com/solutions/testing_security

for more information.

Ixia Worldwide Headquarters

26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)

1.877.367.4942

(Outside North America)

+1.818.871.1800

(Fax) 818.871.1805
www.ixiacom.com

Other Ixia Contacts

Info:	info@ixiacom.com
Investors:	ir@ixiacom.com
Public Relations:	pr@ixiacom.com
Renewals:	renewals@ixiacom.com
Sales:	sales@ixiacom.com
Support:	support@ixiacom.com
Training:	training@ixiacom.com