Information Security White Paper 2009 Part 2

10 Major Security Threats

Attacking Techniques Become More and More Sophisticated

& Appendix D

Information Security Overview for FY 2008（10 Topics）

June 2009

IT SECURITY CENTER (ISEC)
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Part 2 10 Major Security Threats

Attacking Techniques Become More and More Sophisticated

This document was compiled by the "Information Security Study Group", which consists of 111 people, including those participating in the "Information Security Early Warning Partnership", information security researchers and those responsible for information security.

We conducted a vote to rank "threats to the secure use of the Internet" that arose in 2008 by asking voters "What threat struck you most?", "What threat do you think had a significant impact on the society?" etc., and selected 10 major security threats.

This year, we classified respondents into three groups: "organizations", "users" and "system administrators/developers". Associated threats were assigned to each group and then compiled information - including the summary of the incident, how it happened, the extent of the damage and how it was dealt with, and what measures were taken.

In recent years, attacking techniques have become diversified (e.g., DNS Cache Poisoning, sophisticated Targeted Attack, diversified viruses and bots that attack unspecified number of people indiscriminately, defacing legitimate Websites to attack site visitors, etc.).

■Threats to Organizations

[1st] Threat of DNS Cache Poisoning
[2nd] Sophisticated Targeted Attacks
[3rd] Information Leakage Occurring on a Daily Basis

■Threats to Users

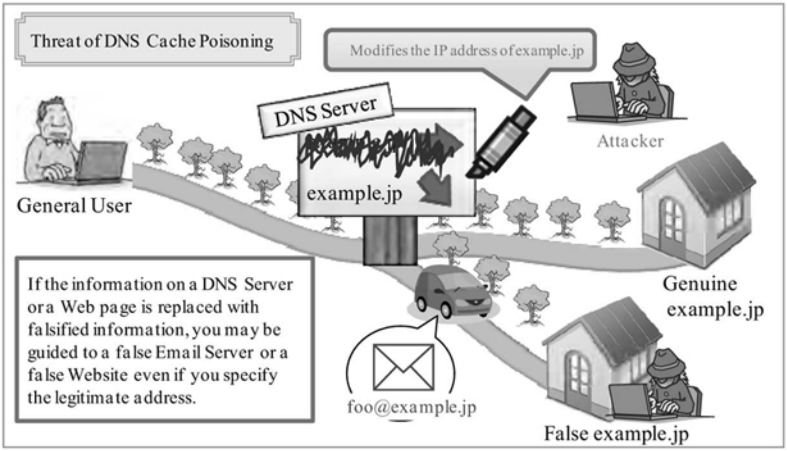
[1st] Diversified Infection Routes for Computer Viruses and Bots
[2nd] Threats Arising from Vulnerable Wireless LAN Encryption
[3rd] Never Decreasing Spam Mails
[4th] Threats Arising from Using the Same User ID and Password

■Threats to System Administrators/Developers

[1st] Threats of Attacks via a Legitimate Website
[2nd] Actualized Passive Attacks
[3rd] Potential Vulnerability in Embedded Systems/Devices

Threats to Organizations

【1st】 Threat of DNS Cache Poisoning [1st Overall]


Threat of DNS Cache Poisoning
Modifies the IP address of example.jp
DNS Server
example.jp
Attacker
General User
If the information on a DNS Server or a Web page is replaced with falsified information, you may be guided to a false Email Server or a false Website even if you specify the legitimate address.
Genuine example.jp
foo@example.jp
False example.jp

In July 2008, vendors all together released an upgraded version of, and patches for, DNS-related Software. These were intended to provide tentative countermeasures against the new DNS Cache Poisoning Vulnerability discovered by Mr. Dan Kaminsky.

<Outline of the Problem>

Domain Name System (DNS) is a mechanism that provides mapping information for associating host names (e.g., www.ipa.go.jp) and IP addresses (e.g., 202.229.63.242). Because many network services on the Internet are designed to use DNS, DNS is thought to be an underlying service for the Internet.

When exploited for attacks, DNS Cache Poisoning Vulnerability might allow attackers to replace legitimate information on DNS Servers (which provide DNS services) with false information. Users of the DNS Server whose original information has been replaced with false information could have the following problem: Even though they enter a legitimate URL or e-mail address, they might be guided to a falsified Website or Mail Server provided by an attacker and possibly become the victim of a phishing scam or information leakage.

The presence of DNS Cache Poisoning Vulnerability has been known for a long time, but in the case of an attack exploiting this vulnerability, a waiting period is required between the first attack (sending a falsified response) and the subsequent attack. So, this sort of attack is considered an inefficient attack method. Mr. Dan Kaminsky discovered an attack method that can eliminate this waiting time, demonstrating that most DNS servers are highly vulnerable.

Countermeasures against DNS Cache Poisoning Vulnerability released by vendors are tentative. As a concrete measure, you can use DNSSEC (DNS Security Extension), which is an extended DNS specification to enhance DNS security; however, DNSSEC is not a commonly-used technology. A fundamental solution to address this threat is discussed by such groups as the Internet Engineering Task Force (IETF), which is working on the standardization of Internet-associated technology.

<Progress of the Problem>

Information on DNS Cache Poisoning Vulnerability was released in 2008 by Mr. Kaminsky. At first, detailed information was to be publicized after the release of the patches to overcome the vulnerability, but in July of that year, almost as soon as vendors released countermeasures, a potential attack method was publicized and the attack actually carried out, making the issue more serious.

<Situation of Damage and Countermeasures>

There was a report that a DNS Cache Server operated by an ISP in the U.S. received an attack in which its users were guided to other Websites than the originally-intended one.

By the end of 2008, the number of reports on DNS Cache Poisoning Vulnerability that had been submitted to IPA based on "Early Warning Partnership" had reached 792. Of those cases, only 108 cases had been solved (through methods such as applying patches) by the end of January, leaving 684 cases unsolved.

<How to Address This Problem>

To reduce damages caused by this problem, system administrators should apply the upgraded version of DNS-related Software that addresses this problem and then take the following steps:

- Make sure that the Contents Server's recursive inquiry feature is disabled;
- Ensure that the Cache Server allows recursive inquiries only from authoritative sources by using a firewall's packet-filtering feature or any other means;
- When using one server as both the Contents Server and Cache Server, the issuance of recursive inquiries should be allowed only from the networks within the organization or, if not feasible, the Contents Server and Cache Server should be separated physically.

References

JPCERT/CC: 複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性
http://www.jpcert.or.jp/at/2008/at080013.txt (in Japanese)

IPA: Security Alert for DNS Cache Poisoning Vulnerability
http://www.ipa.go.jp/security/english/vuln/200809_DNS_en.html

IPA: Second Security Alert for DNS Server Vulnerability
http://www.ipa.go.jp/security/english/vuln/200812_DNS_en.html

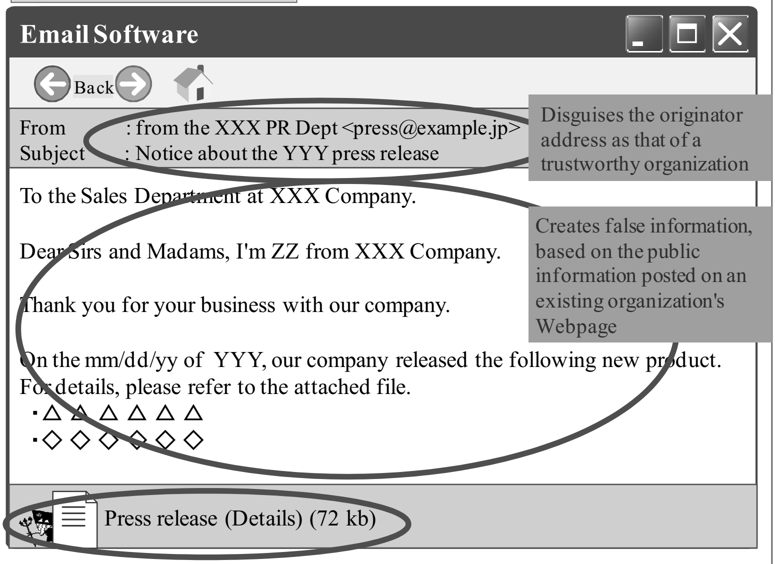
IPA: DNSキャッシュポイズニング対策
http://www.ipa.go.jp/security/vuln/DNS_security.html (in Japanese)

Threats to Organizations

【2nd】Sophisticated Targeted Attacks [3rd Overall]

Case example of Targeted Attacks

Examples of Attacks



From : from the XXX PR Dept <press@example.jp>
Subject : Notice about the YYY press release

To the Sales Department at XXX Company.

Dear Sirs and Madams, I'm ZZ from XXX Company.

Thank you for your business with our company.

On the mm/dd/yy of YYY, our company released the following new product.
For details, please refer to the attached file.
・△ △ △ △ △ △
・◇ ◇ ◇ ◇ ◇ ◇

Press release (Details) (72 kb)

Disguises the originator address as that of a trustworthy organization

Creates false information, based on the public information posted on an existing organization's Webpage

Attaches a virus-contaminated file that infects the user's system when opened

Targeted Attack is an attack whose target is limited to a specific organization or person. In 2008, a sophisticated attack method appeared that distributes a computer virus through the exploitation of vulnerability in software products, such as by using "Social Engineering - a technique to illicitly obtain people's personal information by exploiting an off-guard state in their mind and behavior (For details on the viruses, please refer to "[1st] Diversified Infection Routes for Computer Viruses and Bots" in "Threats to Users").

<Outline of the Problem>

The biggest threat of Targeted Attack is that users do not notice it is an attack, as it effectively employs "Social Engineering." For example, users could be deceived by an e-mail whose sender address is spoofed as a trustworthy business partner or a reliable person and contains credible information. Furthermore, document files or compressed files attached to this sort of mail may contain a computer virus that exploits vulnerability in systems or software products. Because they look like ordinary files, users might open them without precaution. When opened, the virus-contaminated files might show documents as they would be in a normal state, but in reality, the user’s systems might be infected with other viruses or information on the systems may be compromised in a way that users do not notice it.

<Progress of the Problem>

Targeted Attack was acknowledged as a problem after relevant material was published in 2005 by US-CERT. In response to this, JPCERT/CC announced a Security Alert about Targeted Attack "Security Alert about Trojan Horse". In 2006, news reports that the National Police Agency in Japan had received a Targeted Attack and the security alert on e-mail whose sender address was spoofed as the Defense Agency (currently the Ministry of Defense) become the topic of conversation.

Even now, it is not easy to establish a complete measure, but in 2008, JPCERT/CC announced the "Report on the Survey on Measures and Techniques for Preventing Targeted Attack", while IPA released "Research and Surveys on Targeted Attack in Recent Years." In this way, various fact-finding surveys on Targeted Attack were conducted in Japan.

<Situation of Damage>

In the spring of 2008, a Targeted Attack was carried out by using e-mail whose sender address was spoofed as IPA or the "Information Processing Society of Japan's Computer Security Symposium 2008." For the IPA-spoofing Targeted Attack, information posted on IPA's Website (such as Security Alerts, texts on research surveys, attached files, etc.) was abused. When opened, those attached files caused the user’s systems to be infected with computer viruses though the exploitation of multiple vulnerabilities. In 2008, there also was a news report that a corporate manager in the U.S. received Targeted Attack.

<How to Address This Problem>

For Targeted Attack, general antivirus measures can be used as an effective method to prevent virus-infection. Among such general measures are: keeping up-to-date operating systems, applications, plug-ins (such as ActiveX), and virus definition files of antivirus software.

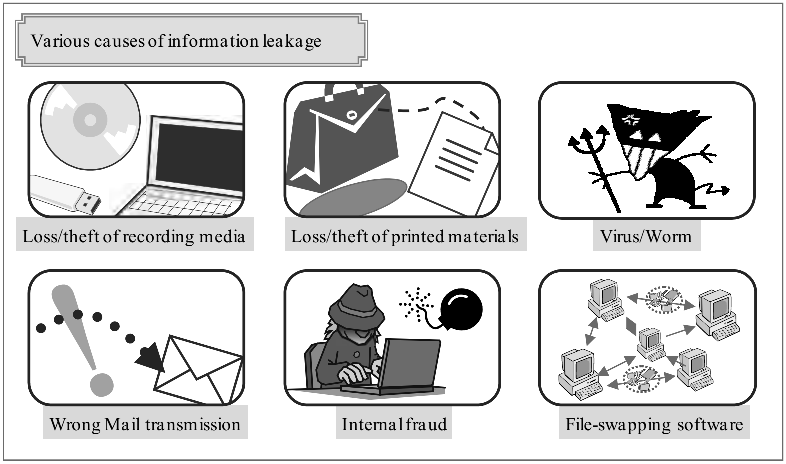
In the case of the IPA-spoofing Targeted Attack, the viruses that had entered into the user’s systems attempted to communicate with external devices, waiting for commands from the attacker. In this case, system administrators could use firewall to block unnecessary communications or only allow HTTP/HTTPS access via a proxy server with authentication feature, which would effectively prevent the spread of the damages.

References

PC Online:国内企業を狙った「標的型攻撃」を確認、手口を変えて毎週攻撃
http://pc.nikkeibp.co.jp/article/news/20081218/1010634/ (in Japanese)
TECHWORLD：企業の経営層を標的にした巧妙な詐欺メールがまん延
http://www.techworld.jp/channels/security/101778/ (in Japanese)

Threats to Organizations

【3rd】Information Leakage Occurring on a Daily Basis [5th Overall]


Various causes of information leakage
Loss/theft of recording media
Loss/theft of printed materials
Virus/Worm
Wrong Mail transmission
Internal fraud
File-swapping software

Almost every day, we hear the news on incidents concerning the leakage of various types of information (such as personal information and technical information). In 2008, such incidents occurred frequently in many places. Information leakage is an issue of high priority that is discussed every year in the "Information Security White Paper."

<Outline of the Problem>

There are various causes of information leakage such as:

- Theft/Loss of recording media or printed materials
- Virus-infection
- e-mail transmission error
- Unlawful acts by the staff within the organization
- Use of File-Sharing Software
- Wrong Settings on Web Servers, improper operations
- SQL Injection Vulnerability and other vulnerabilities in web applications (For details, please refer to "[1st] Threats of Attacks via a Legitimate Website" in "Threats to System Administrators/Developers")

It is not easy to prevent every information leakage incident, but organizations can implement technical measures and establish, and enforce, organizational rules as a precaution against such incidents and to raise employees' awareness of information security.

<Progress of the Problem>

The Private Information Protection Law, which was enacted in 2003 and fully enforced in 2005, drew people's attention on information leakage incidents, prompting enterprises to establish a framework for complying with the law. As a countermeasure against information leakage incidents, some organizations apply a rule to limit the computers that can be taken out of the organization's premises, or a rule to prohibit the use of removal media (such as USB flash drive), which in turn could lower the convenience of information equipment. On the other hand, even if such computers (the ones taken out of the organization's premises) were lost or stolen, information stored on them could be protected if the HDD was equipped with cryptic functionality. This sort of technical approach is in progress as it enables the secure use of computers outside the organization's premises without compensating convenience.

<Situation of Damage>

According to the "Information Leakage Incident Report for the First Half of 2008 (Advance Report)" released by the Security Victimization Survey WG of Japan Network Security Association (JNSA), in 2008, the number of people whose information was leaked decreased significantly in comparison to the previous year. However, the number of information leakage cases for the first half of 2008 amounted to 683, and the total number of such cases for 2008 might exceed the record high of 1,032 marked in 2005. Human error such as wrong operations and loss of equipment (e.g., computers, media, etc.) accounted for over half of the causes of information leakage.

<How to Address This Problem>

Management should, by referring to such documents as "Information Security Management and PDCA Cycle" published by IPA, sort out the organization's policy about information security and communicate them to all personnel within the organization. They should also examine what risks are being posed, what measures should be taken, and what can be achieved by implementing those measures. Then they need to formulate rules, establish a framework, and enforce those rules.

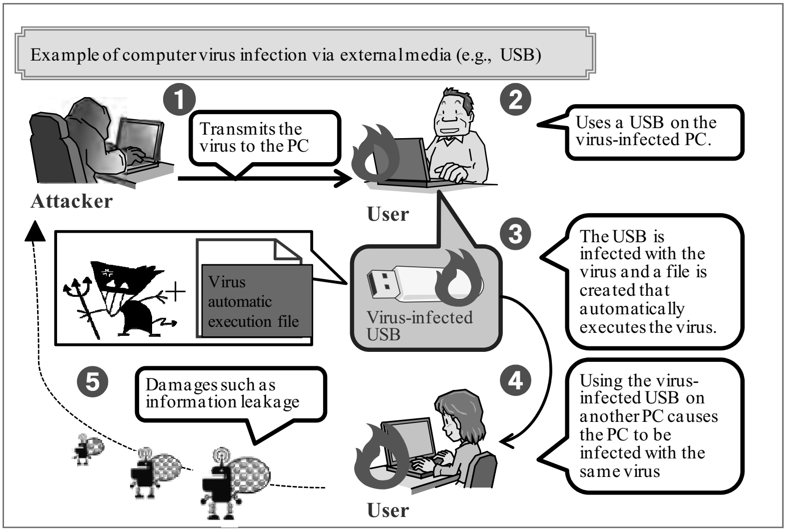
Based on the security standard set up by the management personnel, system administrators should establish specific procedures to follow the standard. Once established, procedures should be reviewed as needed; through the reviews, system administrators should identity what should be modified and consider how to deal with potential new threats.

References

JNSA:【速報版】2008年上半期　情報セキュリティインシデントに関する調査報告書(Ver. 1.0)
http://www.jnsa.org/result/2008/pol/incident/ (in Japanese)
IPA: 情報漏えいインシデント対応方策に関する調査
http://www.ipa.go.jp/security/awareness/johorouei/index2.html (in Japanese)

Threats to Users

【 1st 】 Diversified Infection Routes for Computer Viruses and Bots [4th Overall]


Example of computer virus infection via external media (e.g., USB)
1
Transmits the virus to the PC
Attacker
2
Uses a USB on the virus-infected PC.
User
3
Virus automatic execution file
Virus-infected USB
The USB is infected with the virus and a file is created that automatically executes the virus.
4
Using the virus-infected USB on another PC causes the PC to be infected with the same virus
5
Damages such as information leakage
User

In 2008, we saw more sophisticated virus-infection methods.

<Outline of the Problem>

Major cases of the 2008 virus infection are as follows:

- Virus-infection via PDF or Microsoft Office Word files that are in electronic document file format
- Virus-infection via USB flash drive or other removable media

Traditional computer viruses infected computers when connected to a network. But in 2008, a new virus appeared that uses the automatic execution feature of removable media (when such media is connected to a computer, its contents are automatically executed and the computer becomes infected with a virus). If the removable media containing a computer virus was used on other computers, they would also be infected with that virus even if they were not connected to a network. Even if the virus-infected computer was on an isolated network that has no Internet connection, the virus could spread across the isolated network.

Bots have also exercised an overwhelming influence. A bot is a program designed to infect computers and acts in accordance with commands from a command server that are sent across external networks. Once infected, the user's computer might be used to transmit a large amount of spam mails or as the source of DOS attacks against a specific Website.

SANS, a U.S. private entity specializing in information security, speculates that the more-than-4-fold increase in the number of bot-infected computers in the three months from June 2008 to August 2008 was due to the increase in the virus infection via a bot-embedded Website - a Website on which "Bot Infection Trap" is set by attacks such as SQL Injection Attack (For details, please refer to "[1st] Threats of Attacks via a Legitimate Website" in "Threats to System Administrators/Developers"). According to the activity reports of Cyber Cleaning Center (CCC), operated under the cooperation of the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI), the average number of bots samples collected by honeypot per month fluctuates between 300,000 and 650,000.

<Progress of the Problem>

Around the year 2000, cases of diskette- and e-mail-based virus-infection stood out. But around the year 2001, we faced an increasing threat of worms that exploit vulnerability in Servers to spread infection. Around the year 2002 to 2003, bots appeared in the world, and in 2004 bots became an issue in Japan. Bots evolved further, making it difficult to observe their behavior and applying redundant configuration of command servers. Year after year, bots' attacking techniques are becoming more and more sophisticated, making it difficult for enterprises to establish appropriate countermeasures. Moreover, the objective of virus creators shifted from "crime for pleasure" to "taking someone's money without their noticing it."

<How to Address This Problem>

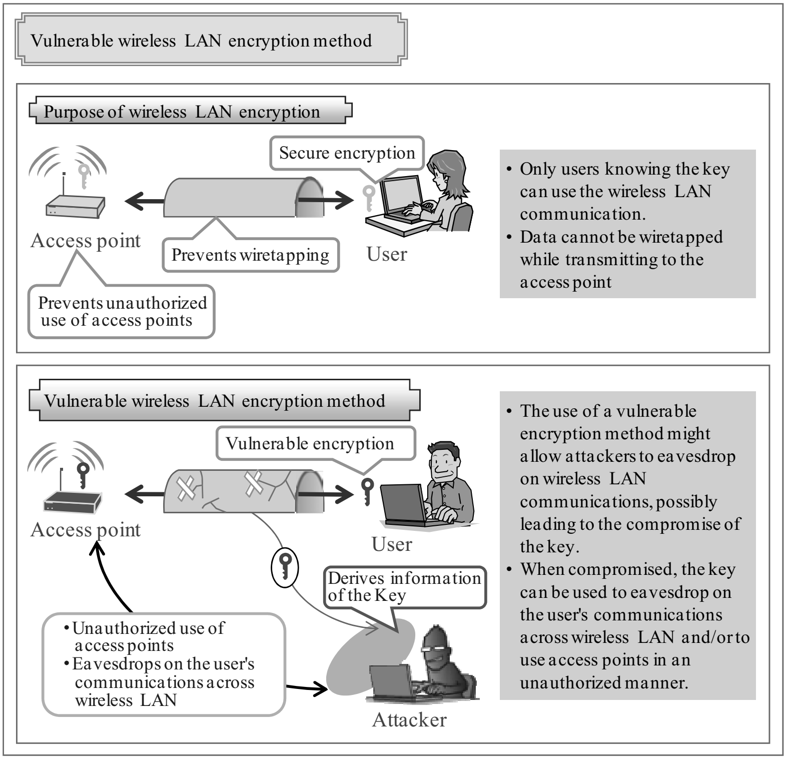
For this threat, you can apply traditional measures such as keeping up-to-date operating systems, applications, plug-ins (such as ActiveX) and virus definition files of antivirus software. You can also use a Bot Removal Tool (CCC Cleaner) provided by Cyber Cleaning Center to check your computer for bot-infection and remove it if detected. You should also refrain from connecting removable media of unknown origin to your computer and letting the media automatically execute its contents.

References

トレンドマイクロ: USBメモリで広まるウイルスへの対策
http://jp.trendmicro.com/jp/threat/solutions/usb/ (in Japanese)
サイバークリーンセンター(CCC): ボットの駆除対策手順
https://www.ccc.go.jp/flow/index.html (in Japanese)
IPA: Computer Virus / Unauthorized Computer Access Incident Report [Summary]
http://www.ipa.go.jp/security/english/virus/press/200812/E_PR200812.html

Threats to Users

【2nd】Threats Arising from Vulnerable Wireless LAN Encryption [6th Overall]


Vulnerable wireless LAN encryption method
Purpose of wireless LAN encryption
Secure encryption
Access point
Prevents wiretapping
User
Prevents unauthorized use of access points
• Only users knowing the key can use the wireless LAN communication.
• Data cannot be wiretapped while transmitting to the access point
Vulnerable wireless LAN encryption method
Vulnerable encryption
Access point
User
Derives information of the Key
•Unauthorized use of access points
•Eavesdrops on the user's communications across wireless LAN
Attacker
• The use of a vulnerable encryption method might allow attackers to eavesdrop on wireless LAN communications, possibly leading to the compromise of the key.
• When compromised, the key can be used to eavesdrop on the user's communications across wireless LAN and/or to use access points in an unauthorized manner.

In October 2008, at the "Information Processing Society of Japan's Computer Security Symposium 2008", a paper on vulnerability in Wired Equivalent Privacy (WEP) was presented. The paper said WEP, a wireless LAN encryption standard, could be decrypted in a short time in a general environment.

<Outline of the Problem>

Wireless LAN is a Network environment that enables telecommunications between wireless LAN access points and devices with wireless LAN capability. It allows for wireless communications within the range reached by radio waves, even if an obstacle was placed.

It is convenient, but unlike wired LAN that uses a physical line, it can allow a malicious person to capture the communications without having to break into an office or house. So when wiretapping, wireless LAN could provide more opportunities for attackers to gain unauthorized access than wired LAN.

To make it difficult for attackers to intercept wireless LAN communications, an encryption scheme called WEP can be used. But a paper on its vulnerability was released, saying that in a general environment, WEP-encrypted texts can easily be decrypted in a short time (e.g., 10 seconds for the 20 MB communication)

In the past, WEP-encrypted texts could be decrypted in a short time only under certain conditions, but now no condition is required. Users may think that, even if their wireless communications were intercepted, specific contents would remain uncovered as they were properly encrypted. But this is not the case with WEP. As mentioned earlier, WEP-encrypted texts can easily be decrypted, possibly leading to the leakage of communication messages or unauthorized use of wireless access points. In addition to WEP, TKIP (Temporal Key Integrity Protocol), which is employed by WPA (Wi-Fi Protected Access), was found to allow some of the information to be decrypted. From a futuristic perspective, it is recommended to use AES (Advanced Encryption Standard) for WPA2 (Wi-Fi Protected Access 2)-based wireless communication.

<Progress of the Problem>

Since WEP was established in 1999 as a wireless LAN encryption standard, researchers have been trying to decrypt WEP-encrypted texts. Amid the advancement of code-breaking techniques, it has become clear that WEP does not provide adequate communications security. As its successor, WPA was established in 2003 and WPA2 in 2004. In the past, it was advised not to use WEP as it had a known vulnerability, which then became more obvious in 2008.

<How to Address This Problem>

When using wireless LAN, use WPA2's AES instead of a vulnerable encryption scheme (such as WEP, WPA-TKIP). When setting up a wireless access point at your home or on your organization's premises, it is possible to mitigate risks by, if feasible, limiting the accessible area (such as by enforcing limited electric wave emission).

If the products being sold are equipped with WEP, developers should instruct users not to use WEP as it has a known vulnerability. For products that have no alternative encryption scheme available, developers should modify their programs so they can apply other encryption schemes aside from WEP (e.g., WPA2)

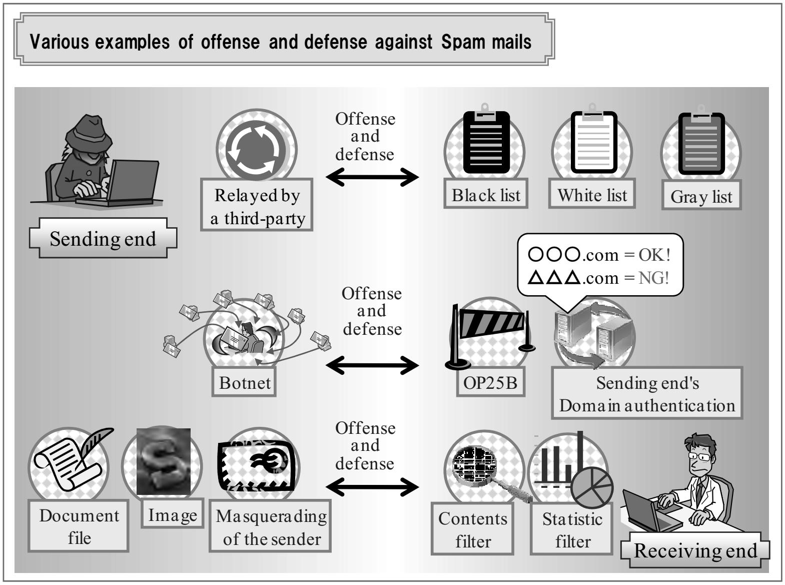
References

ITmedia:「WEPを一瞬で解読する方法」を研究者グループ発表　プログラムも公開予定
http://www.itmedia.co.jp/news/articles/0810/14/news020.html (in Japanese)

Practical attacks against WEP and WPA,
Martin Beck, Erik Tews, TU-Dresden, Germany, November 8, 2008
http://dl.aircrack-ng.org/breakingwepandwpa.pdf

Threats to Users

【3rd】Never Decreasing Spam Mails [8th Overall]



Spam mail is also called unsolicited commercial e-mail (UCE) or unsolicited bulk e-mail (UBE). Generally, attackers send a large amount of spam mails to unspecified people for the purpose of advertisement, phishing scam, or virus-infection, impeding the use of e-mail systems for their original purpose.

<Outline of the Problem>

Due to a large amount of spam mails sent, legitimate mails that should be received by the recipients might be buried in the spam mails, or if anti-spam measures were in place, recipients might not be able to receive e-mail addressed to and meant to reach them due to an adverse effect of such measures. Furthermore, in some cases, a computer virus is attached to spam mails, so the recipient's computer could be infected with the virus.

As an anti-spam measure, a new technology was developed in which mail text is analyzed to check for spam, but attackers attempt to avoid detection by attaching image or PDF files to their mail or by using other means. While ISPs and anti-spam software are taking some measures, attackers are developing a method to avoid detection, so the reality is; they are playing a cat-and-mouse game.

<Progress of the Problem>

Spam mails have been acknowledged as a problem since a long time ago. Old-type spam mails were sent by exploiting vulnerability in mail servers or by causing recipients to execute a computer virus attached to an e-mail.

In Japan, around 2001, spam mail transmission aimed at mobile phones became a serious problem as the recipients had to pay the communication fees for the unsolicited packets. To address this issue, mobile phone companies announced that they had strengthened anti-spam measures in 2003 and, since then, the number of spam mails sent to mobile phones has reduced significantly.

However, the number of spam mails sent to PCs did not decrease; rather, it increased drastically in 2004. This may be due to the increase in the use of bots for spam mail transmission. In 2008, there was a news report that, in abroad, the network communication of an operator hosting the sending of a large amount of spam mails was shut down by an ISP, which effectively reduced spam mail transmission. However, there also was a report that the number had increased again, so the reality is, no complete measure has been reached against spam mails.

<Situation of Damage>

According to the statistics by a security vendor abroad, more than 90 percent of e-mail transmitted over the Internet is spam mails.

<How to Address This Problem, Precaution>

Users should take measures such as not replying to spam mail received or not clicking URLs contained in them. Once you respond to the spam mail, the sender would assume that his mail was successfully accepted and might send much larger amounts of spam mails. Users can also use anti-spam services provided by ISPs or implement spam-mail-filtering to reduce opportunities for spam mails to reach their PCs.

System administrators should consider using SPF (Sender Policy Framework - a technology for Sender Domain Authentication), SenderID, DomainKeys, or S/MIME (a standard for e-mail encryption and digital signature). These technologies are not for directly reducing spam mail transmission, but can be used to improve the reliability of mail sources and are expected to reduce spam mails in the long run.

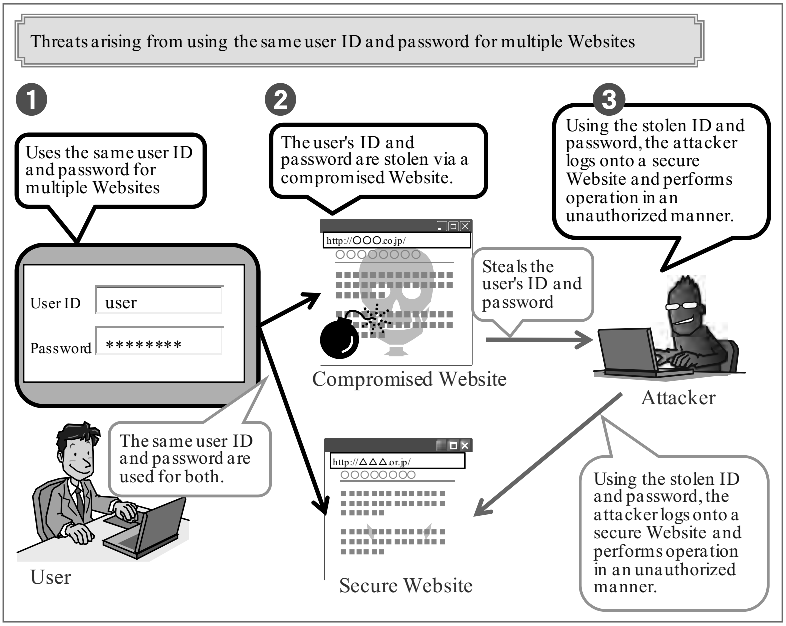
References

ITmedia: 企業に届く正規メールは1割以下に
http://www.itmedia.co.jp/enterprise/articles/0901/30/news032.html (in Japanese)

nikkei BP net: 2008年のスパム·メール、悪質業者の摘発にもかかわらず前年比25%増
http://www.nikkeibp.co.jp/it/article/NEWS/20090127/323513/ (in Japanese)

Threats to Users

【4th】Threats Arising from Using the Same User ID and Password [10th Overall]


Threats arising from using the same user ID and password for multiple Websites
1
Uses the same user ID and password for multiple Websites
User ID
user
Password
****
The same user ID and password are used for both.
User
2
The user's ID and password are stolen via a compromised Website.
http://○○○.co.jp/
○○○○○○○○
Compromised Website
Steals the user's ID and password
http://△△△.or.jp/
○○○○○○○○
Secure Website
3
Using the stolen ID and password, the attacker logs onto a secure Website and performs operation in an unauthorized manner.
Attacker
Using the stolen ID and password, the attacker logs onto a secure Website and performs operation in an unauthorized manner.

If the same User ID and password were used for multiple Websites' online services, information leakage on one of those sites might allow the attacker to log onto another site using the compromised information (User ID and password).

<Outline of the Problem>

There was a news report that a User ID and password stolen from a Website through SQL Injection were used illicitly by the attacker to log onto another Website. It can be assumed that the user of the stolen ID and password were using the same ID and password for multiple sites.

Various Websites use User ID and password to identify and authenticate their users. Accordingly, users are required to set a User ID and password on each site. However, they tend to use the same ID and password for multiple sites as it is difficult for them to manage different IDs and passwords. Meanwhile, websites that manage User IDs and passwords to provide services do not know if the same ID and password are used for other sites. So it is not easy to establish a technical measure to address this issue

<Progress of the Problem>

Since before 2008, Web users had been alerted not to use the same User ID and password for multiple sites. Security incidents that occurred in 2008 due to the same User ID and password being used brought to the surface that users do find it difficult to manage different IDs and passwords per service. In 2008, a security alert was issued to warn against the use of the same User ID and password for multiple online services.

<How to Address This Problem>

Users should take measures such as not setting the same User ID and password on multiple Websites by using a tool that provides adequate password management (e.g., Password Management Software). It is also important to use a hard-to-guess password.

System administrators should instruct system users not to use the same User ID and password for multiple purposes, reminding them of the seriousness of this problem and raising their awareness of information security. In addition to not using the same User ID and password, it is also important to use a strong password. One example of measures for web applications is to store passwords not in plain text but in the form of hash value. By doing so, even if the information was compromised by an attacker, he would only know the hash value and not the password itself, which would minimize the damage.

As a simple authentication management method, you can use OpenID, for which major Websites announced their participation in 2008. However, while OpenID provides users with convenience, the reliability of its authentication server has yet to be improved.

Should user IDs and passwords be compromised (such as through the exploitation of vulnerability in the Website), the site operator should inform users of the information leakage and explain the associated risks. By doing so, secondary damage can be prevented.

References

日経ネットプラス: ネット利用、パスワード「使い回し」8割超す
http://netplus.nikkei.co.jp/netnavi/tozai/toz081021.html (in Japanese)
Yahoo! Japan セキュリティセンター: サイトごとに違うパスワードを！
http://security.yahoo.co.jp/attention/password/ (in Japanese)