

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

Contents

Part 2 10 Major Security Threats	1
Attacking Techniques Become More and More Sophisticated.....	1
Threats to Organizations	2
【1st】 Threat of DNS Cache Poisoning [1st Overall]	2
【2nd】 Sophisticated Targeted Attacks [3rd Overall].....	4
【3rd】 Information Leakage Occurring on a Daily Basis [5th Overall].....	6
Threats to Users	8
【1st】 Diversified Infection Routes for Computer Viruses and Bots [4th Overall]	8
【2nd】 Threats Arising from Vulnerable Wireless LAN Encryption [6th Overall]	10
【3rd】 Never Decreasing Spam Mails [8th Overall].....	12
【4th】 Threats Arising from Using the Same User ID and Password [10th Overall]	14
Threats to System Administrators/Developers	16
【1st】 Threats of Attacks via a Legitimate Website [2nd Overall].....	16
【2nd】 Actualized Passive Attacks [7th Overall].....	18
【3rd】 Potential Vulnerability in Embedded Systems/Devices [9th Overall]	20
【Appendix A】 Relations among 10 Major Security Threats	22
【Appendix B】 Correlation Diagram of 10 Major Security Threats.....	23
【Appendix C】 References.....	24
【Appendix D】 Information Security Overview for FY 2008 (10 Topics)	25

This document is a translation of Part 2 & 10 Topics of the original Japanese edition of the Information Security White Paper 2009. The entire English translation will be released in the subsequent issue.

Please be advised that most of the references referred to in this document are offered in Japanese only.

Both English and Japanese editions are available for download at:

<http://www.ipa.go.jp/security/english/third.html> (English web page)

<http://www.ipa.go.jp/security/vuln/10threats2009.html> (Japanese web page)

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

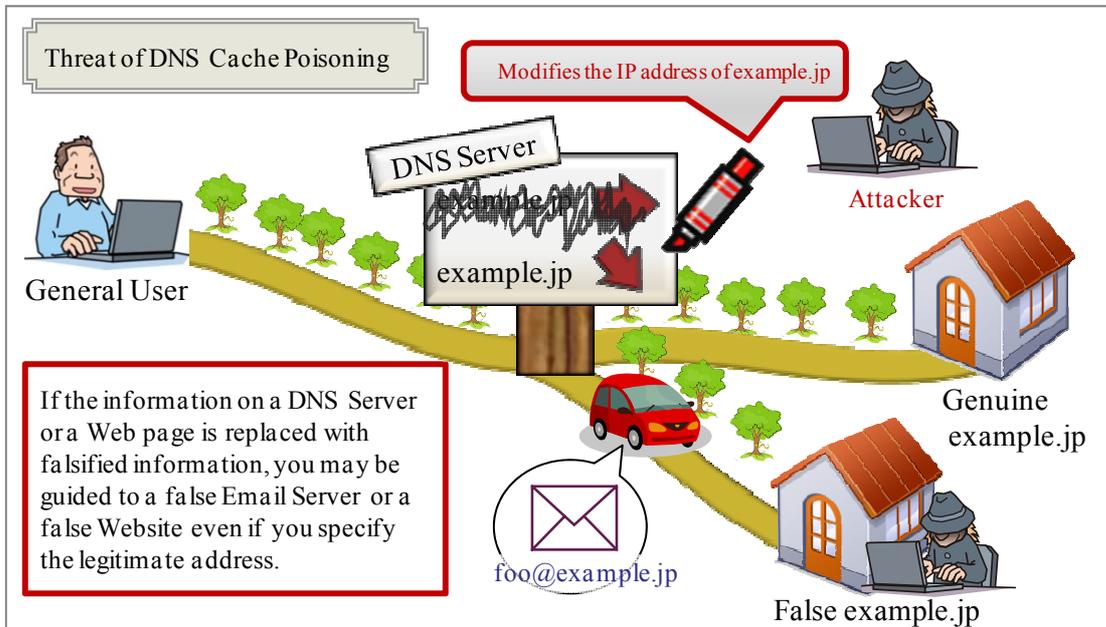
- [1st] Diversified Infection Routes for Computer Viruses and Bots
- [2nd] Threats Arising from Vulnerable Wireless LAN Encryption
- [3rd] Never Decreasing Spam Mails
- [4th] Threats Arising from Using the Same User ID and Password

■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]



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.jpccert.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

Email Software
_ □ ×

← Back → 🏠

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)

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

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

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 through 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.

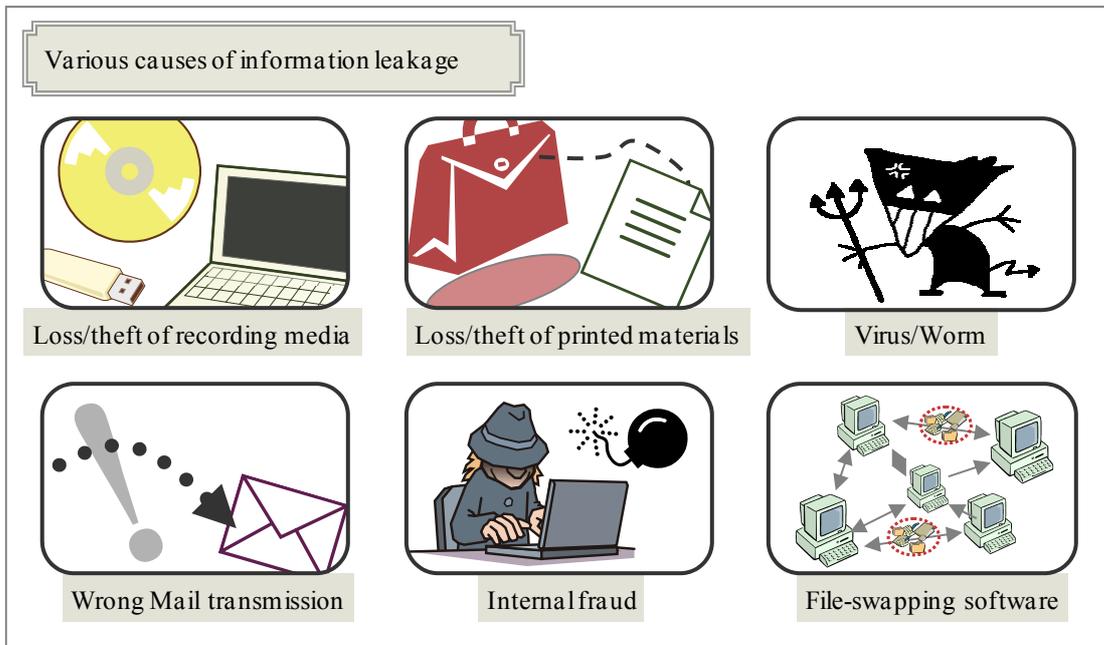
References

- 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]



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 identify 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)

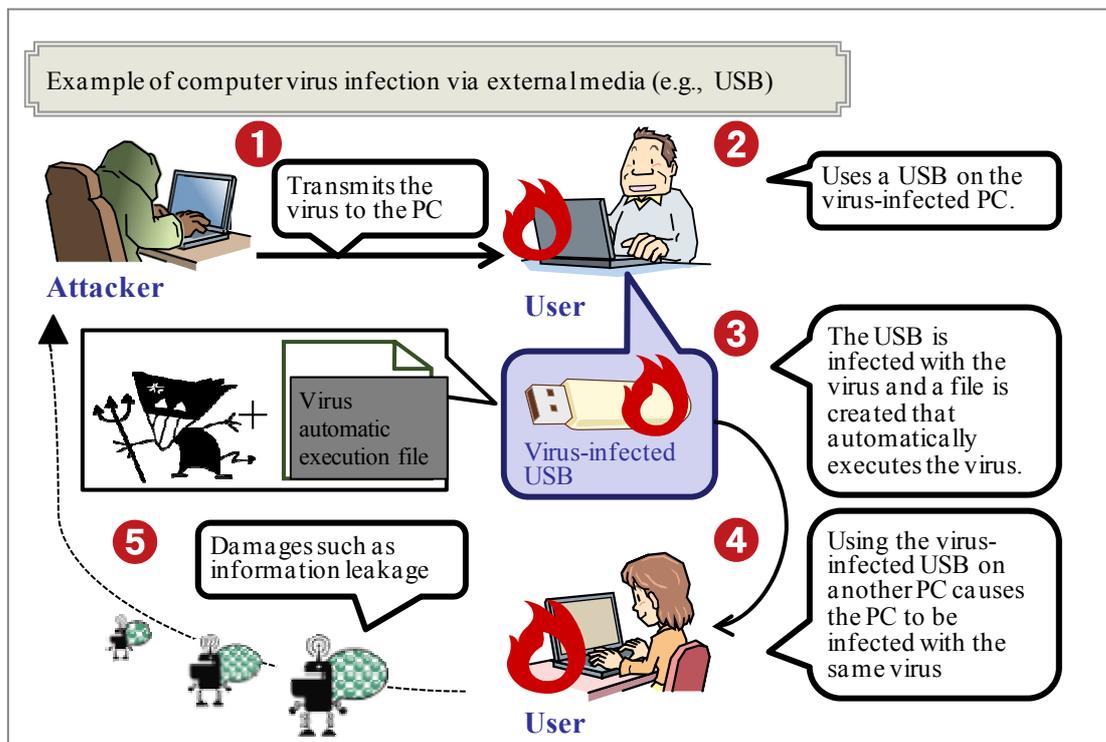
IPA: 情報漏えいインシデント対応方策に関する調査

<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]



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)

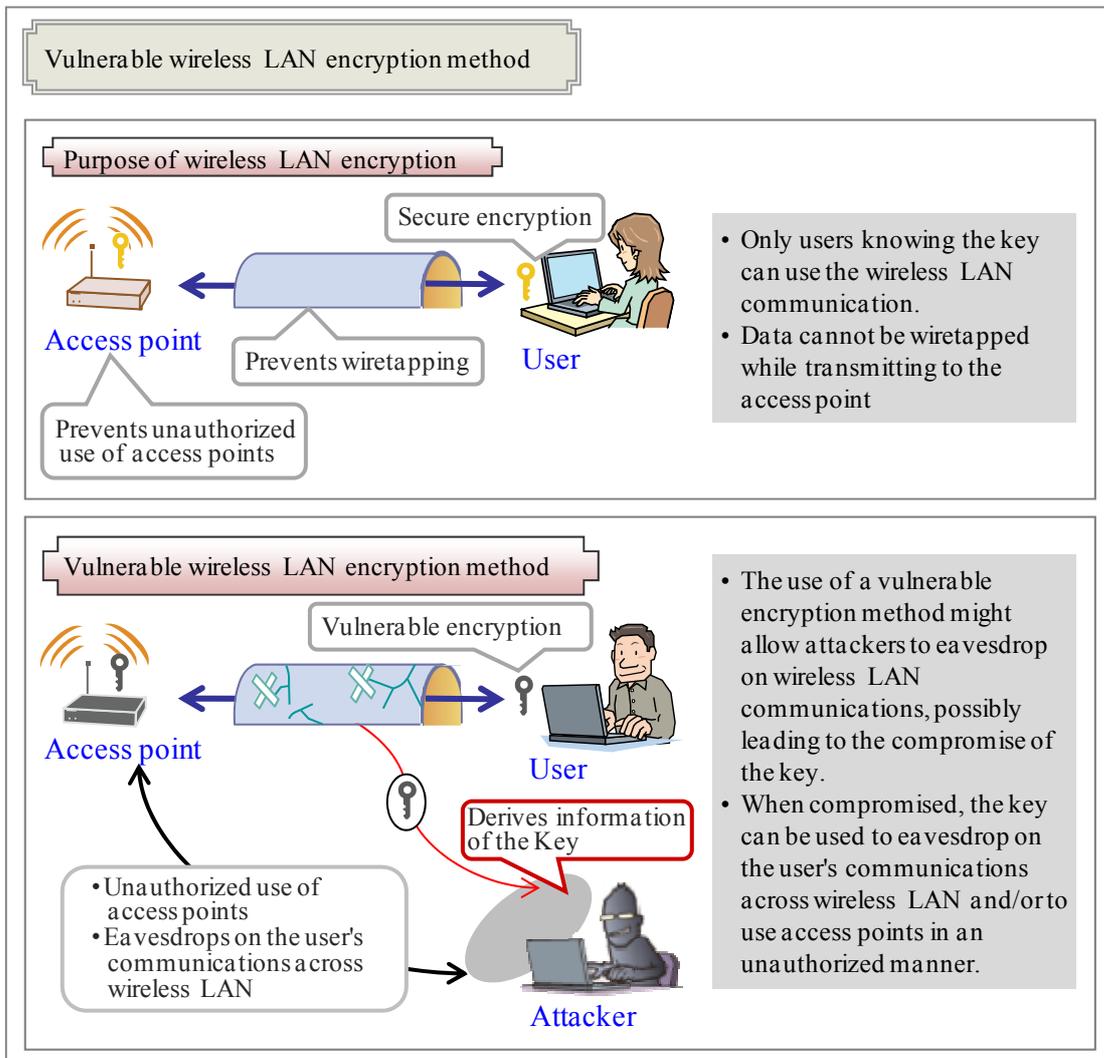
IPA: Computer Virus / Unauthorized Computer Access Incident Report [Summary]

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]



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)

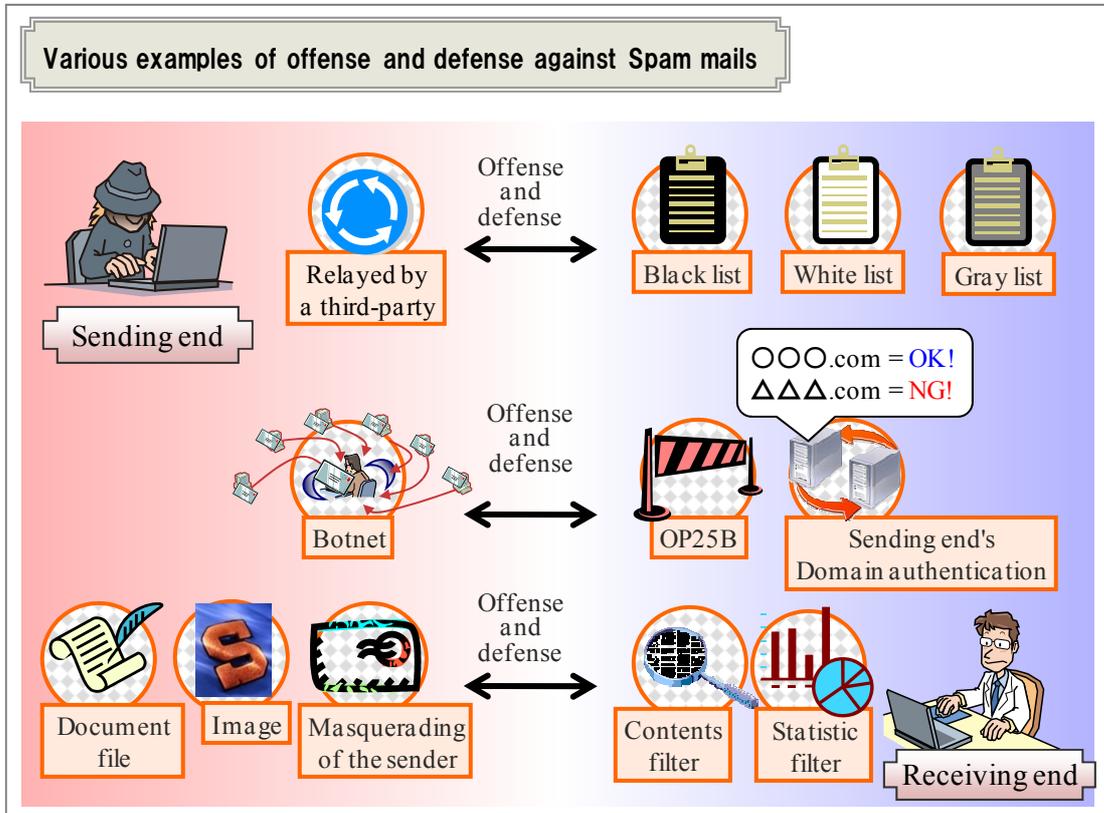
Practical attacks against WEP and WPA,

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

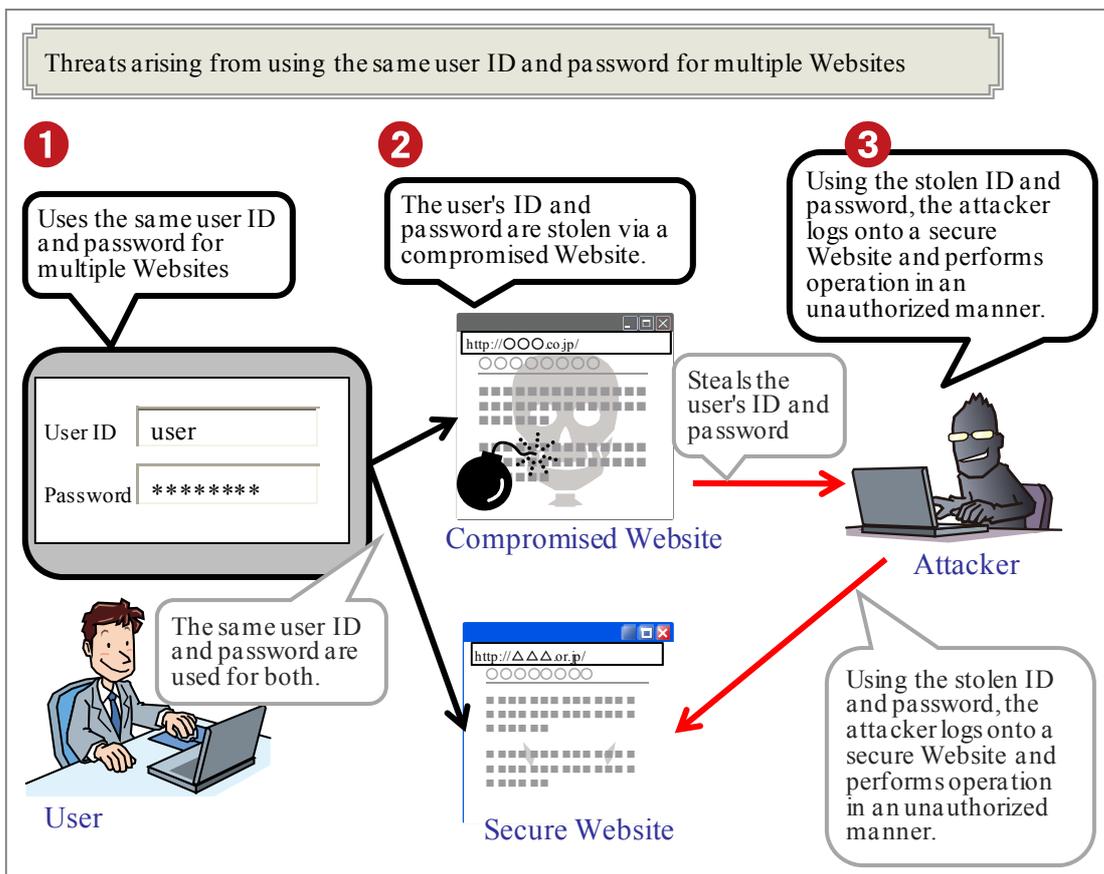
<http://www.itmedia.co.jp/enterprise/articles/0901/30/news032.html> (in Japanese)

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]



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)

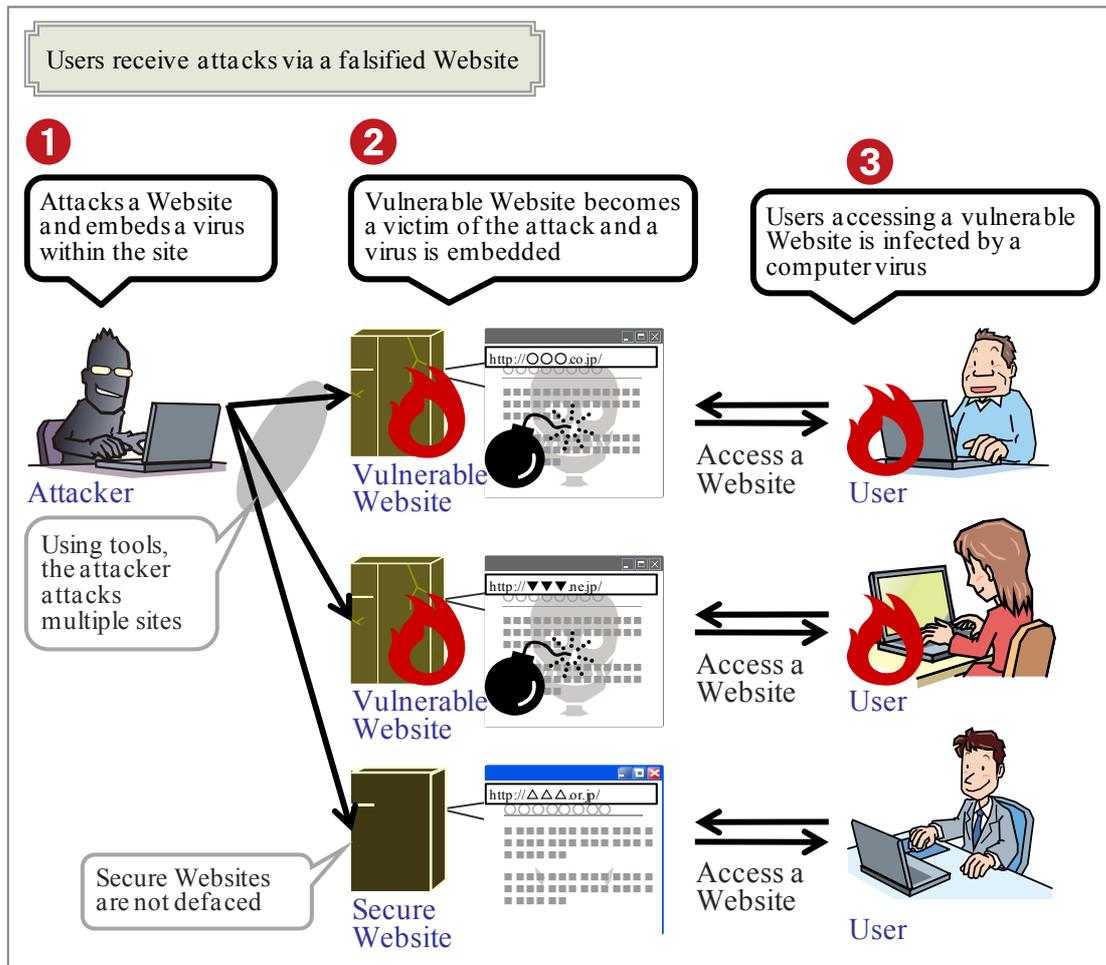
Yahoo! Japan セキュリティセンター: サイトごとに違うパスワードを!

<http://security.yahoo.co.jp/attention/password/> (in Japanese)

Threats to System Administrators/Developers

[1st] Threats of Attacks via a Legitimate Website

[2nd Overall]



As in the previous year, we also saw the spread of "Attacks via a Legitimate Website" in 2008, in which a legitimate Website is defaced and users accessing it suffer from certain damages.

<Outline of the Problem>

For an attack aimed at those visiting a legitimate Website, the first objective of an attacker is to attempt to deface the Website. While various methods can be used for Website forgery, SQL Injection Attacks that exploit SQL Injection Vulnerability in web applications were most commonly seen in 2008. SQL Injection Attacks are designed to attack databases used for Websites (e.g., compromising, falsifying or deleting the information contained in

the database). In some cases, defaced Websites are used as the source of subsequent attacks. Attackers are said to be using a tool that automatically carries out those attacks.

<Progress of the Problem>

In Japan, SQL-Injection-driven information leakage incidents occurred in 2005 caused the issue of SQL Injection Attacks to appear frequently on the news. Originally, this attack was designed to steal the information on databases used for Websites but, around 2007, it began to change its form and, nowadays, it is designed to embed a computer virus into a legitimate Website so that the Website visitors would catch that virus. This sort of attack method has become prominent, producing further damages (For details, please refer to "[1st] Diversified Infection Routes for Computer Viruses and Bots" in "Threats to Users").

According to the observation by security vendors in Japan, the number of SQL-Injection-driven incidents in 2007 was higher than the previous year and the number increased at an accelerating pace in 2008. Moreover, cases surfaced in which user IDs and passwords that were stolen on a Website were used illicitly to use other site's services, as the users had been using the same User ID and password for multiple Websites (For details, please refer to "[4th] Threats Arising from Using the Same User ID and Password" in "Threats to Users").

<How to Address This Problem>

One of the reasons why SQL Injection attacks are on the rise is, while a Website that interacts with a database has become common, there still are many sites whose countermeasures against SQL Injection attacks are insufficient.

When using a database for the Website, system administrators and Web application developers should incorporate SQL Injection countermeasures into their programs during the design and development phase. Developers should strive to improve Website security by referring to document such as "How to Secure Your Website", published by IPA. They also need to consider Website vulnerability scan and system renovation programs.

References

ラック:改ざんされたWebサイト閲覧による組織内へのボット潜入被害について

<http://www.lac.co.jp/news/press20081222.html> (in Japanese)

NRI Secure Technologies: セキュリティ診断結果の傾向分析レポート2008年版を公開

<http://www.nri-secure.co.jp/news/2008/0728.html> (in Japanese)

IPA: Security Alert for SQL Injection Attacks

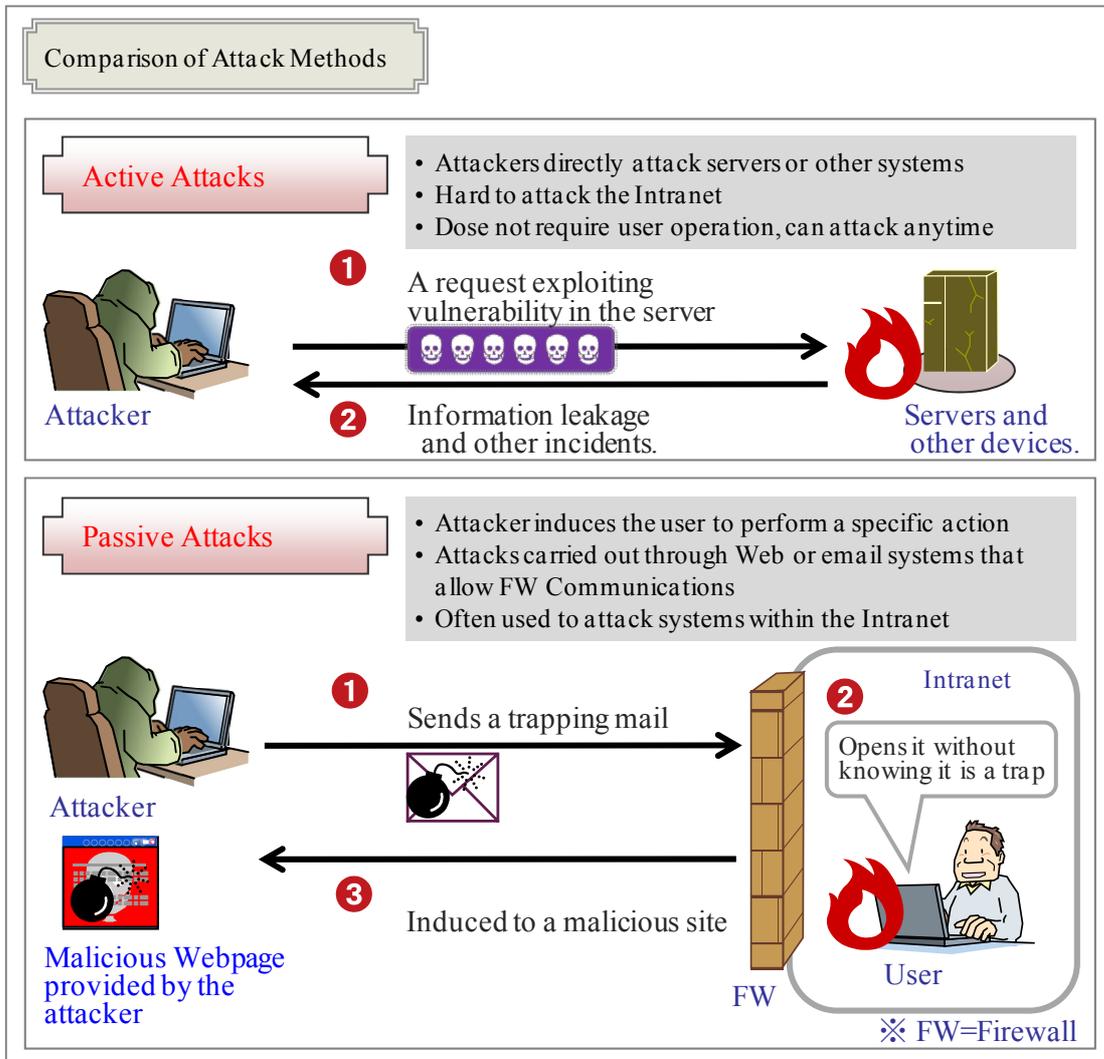
http://www.ipa.go.jp/security/english/vuln/200805_SQLInjection_en.html

IPA: How to Secure Your Web Site 3rd Edition Released

http://www.ipa.go.jp/security/english/vuln/200806_websecurity_en.html

Threats to System Administrators/Developers

[2nd] Actualized Passive Attacks [7th Overall]



There have been an increasing number of incidents caused by "Passive Attack"¹ - an attack in which users are induced or directed to the phony Website containing false information that is created by an attacker exploiting a vulnerable legitimate Web server.

<Outline of the Problem>

"Passive Attack" is attacks where the attacker induces the user to view a vulnerable Website or a trapping-mail. Examples of passive attack are: "Targeted Attack" and an attack that exploits cross-site scripting Vulnerability or other vulnerabilities in Web browsers (For details, please refer to "[2nd] Increasingly-Sophisticated Targeted Attacks" in "Threats to Organizations").

¹ Passive Attacks: Attacks where the attacker induces or directs the user to perform a specific action.

Cross-site scripting is an attack method that exploits vulnerability in web applications to attack Website users. In this attack, a malicious script is executed on users' browsers when they visited a vulnerable Website, causing damages such as phishing scam or information leakage. There are many Websites whose countermeasures against cross-site scripting are insufficient, and many reports on vulnerable Websites are submitted to IPA.

In a passive attack that exploits vulnerability in browsers, the user's PC might be infected with a computer virus by just accessing a malicious Website.

The characteristic of passive attack is that, it exploits a network available for general use within the organization. This is because there aren't many networks attackers can directly attack. Nowadays, it has become common for enterprises to install firewall. Meanwhile, for software products that were vulnerable to active attacks, source programs were modified to reduce the vulnerabilities that can be exploited for active attacks. This may account for the decrease in active attacks and the increase in passive attacks.

<Progress of the Problem>

Passive attack has been known since a long time ago. Cross-site scripting Vulnerability became widely known to the public through the information provided by CERT/CC and Microsoft in February 2000. Meanwhile, a number of vulnerabilities in Web browser were detected and some of those vulnerabilities were exploited for malicious purposes. At that time, however, only active attacks were emphasized while passive attack was barely grasped. But the threat of passive attack was gradually recognized by the public as "Targeted Attack" appeared and an attack that exploits vulnerability in Web browsers was carried out. Nowadays, passive attack is acknowledged as one of the most serious problems.

<Situation of Countermeasure>

By the end of 2008, the number of reports on cross-site scripting Vulnerability that had been submitted to IPA based on "Early Warning Partnership" had reached 1,024. Of those cases, only 314 cases had been solved by the end of January (such as by applying patches), leaving 710 cases unsolved.

<How to Address This Problem>

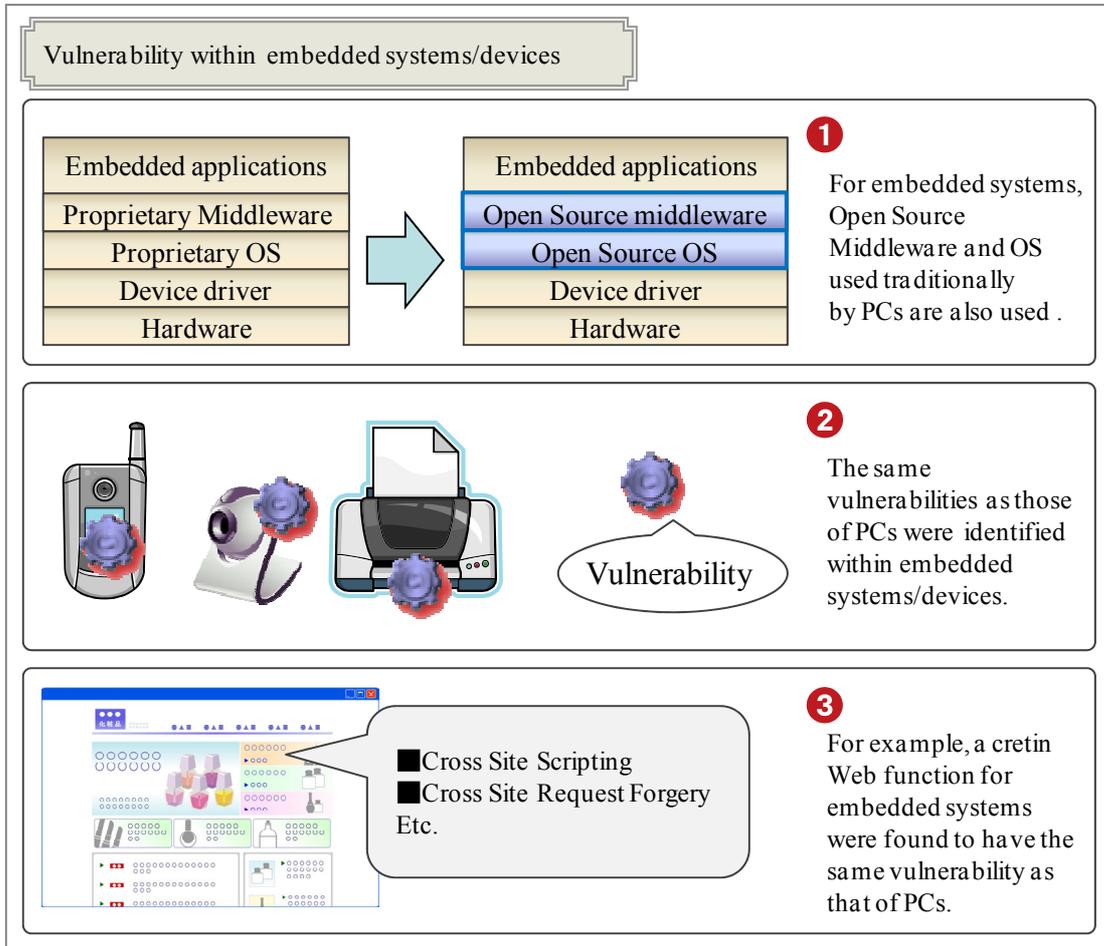
System administrators and web application developers should take note of cross-site scripting Vulnerability and other vulnerabilities that may become the cause of passive attack. This is an issue developers should take care of as users can do nothing about it. Developers should incorporate countermeasures into their systems from the design phase, making sure that no security hole is introduced. They should take necessary steps by referring document such as "How to Secure Your Website", published by IPA.

References

IPA: Reporting Status of vulnerability-related information
http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html

Threats to System Administrators/Developers

[3rd] Potential Vulnerability in Embedded Systems/ Devices [9th Overall]



Network environment for embedded systems/devices are improving and an increasing number of embedded systems/devices are using open source operating systems and middleware. This means that, any vulnerability in embedded system/device, as in other systems, could be exploited for an attack.

<Outline of the Problem>

Development of information and communication technology made it easy to add a communication feature to embedded systems/devices, enabling the use of network anywhere at any time.

When exploited, vulnerability in embedded systems/devices could allow attackers to steal information as they would on computers connected to the Internet or to perform operation on those systems/devices in an unauthorized manner. In recent years, we saw an increasing

number of embedded systems/devices using open source operating systems and middleware and having the Internet connection capability. For this reason, the same problem arose as that for computers connected to the Internet.

In 2008, vulnerability was detected in popular mobile phones in Japan and security alert was issued on an attack in which silent phone calls are made to IP telephones. Furthermore, JVN (Japan Vulnerability Notes) released information about vulnerabilities in the mobile phones, portable music players and small terminals that were used widely in Japan. Some of Internet-capable embedded-systems/devices have Web Interface functions. These functions might also have Web application vulnerability. Among eight embedded-system-related vulnerabilities reported on JVN in 2008, four cases were related to Web Interface functions. As with web applications, we need to promote security measures for embedded devices' Web interfaces.

<Progress of the Problem>

Up until a few years ago, there had been only a few embedded systems/devices with the Internet connection capability, so for most embedded systems/devices, update feature was unavailable. But now, embedded systems/devices, in particular, those having the Internet connection capability are equipped with update capability, enabling users to update systems to overcome the vulnerability detected.

<How to Address This Problem>

When developing an embedded system/device to be connected to a network, developers should take precaution so as not to create security holes in their systems/devices from the design phase. It's best to provide a mechanism for users to update programs in an easy-and-secure manner should any vulnerability be detected. As with other systems, embedded systems/devices should be developed with information security in mind. Developers should strive to improve Website security by referring to document such as "How to Secure Your Website", published by IPA.

References

IPA: 複数の組み込み機器の組み合わせに関するセキュリティ調査報告書

<http://www.ipa.go.jp/security/fy19/reports/embedded/> (in Japanese)

IPA: Security Alert for Vulnerability in Multiple YAMAHA Routers

http://www.ipa.go.jp/security/english/vuln/200801_Yamaha_press_en.html

IPA: Security Alert for Vulnerability in Multiple I-O DATA Wireless LAN Routers

http://www.ipa.go.jp/security/english/vuln/200803_iodata_press_en.html

IPA: Security Alert for I-O DATA DEVICE HDL-F Series Vulnerability

http://www.ipa.go.jp/security/english/vuln/200811_iodata_en.html

IPA: Security Alert for Vulnerability in Sony SNC Series Network Camera

http://www.ipa.go.jp/security/english/vuln/200902_sonysnc_en.html

[Appendix A] Relations among 10 Major Security Threats

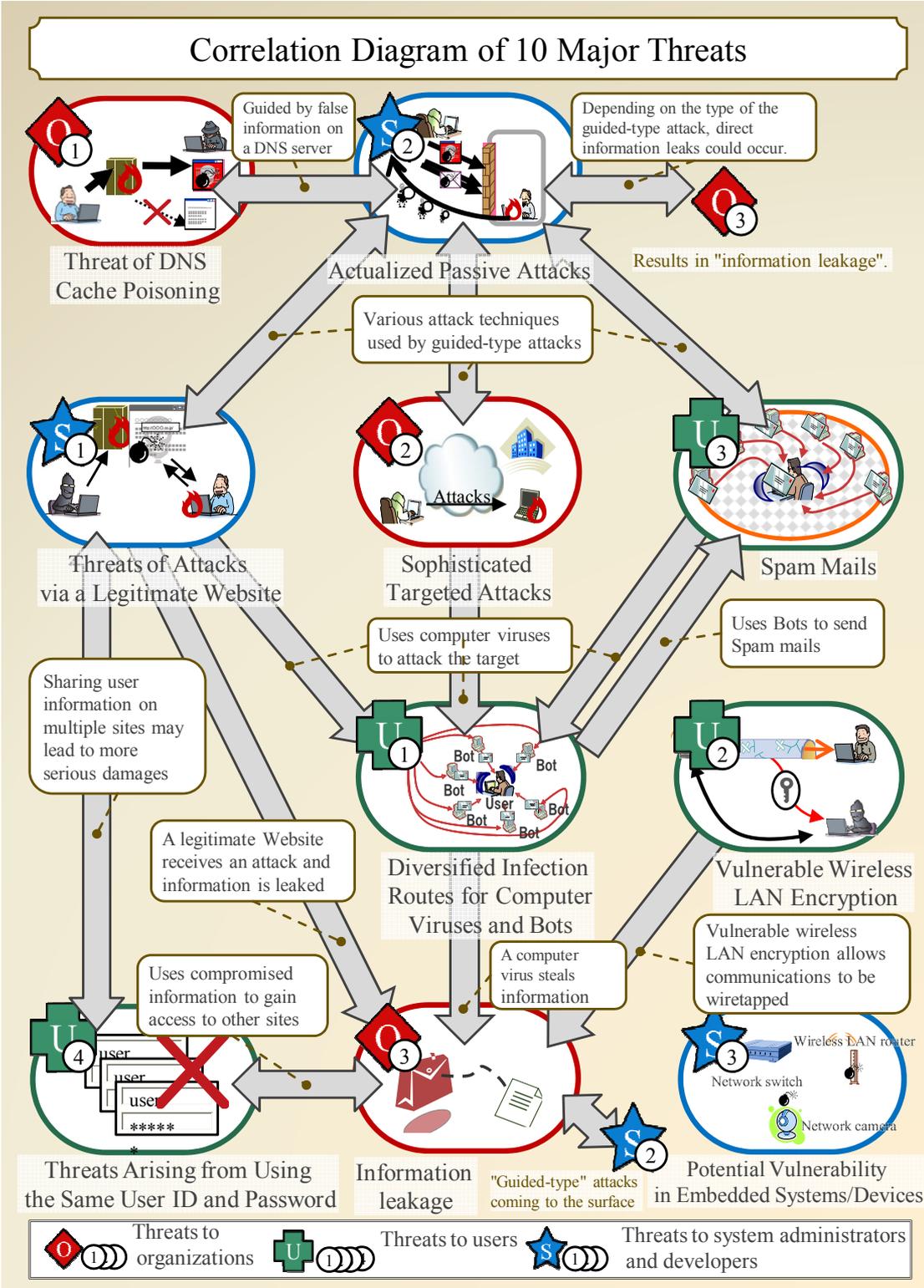
**Appendix Table 1. 10 Major Security Threats
Overall Rankings and Those who Need to Take Measures**

10 Major Security Threats		Those who Need to Take Measures				Ranking [2009]	Previous Ranking [2008]
		Management	Users	System administrators	Developers		
Threats to Organizations							
1st	Threat of DNS Cache Poisoning			⊙		1st (Up)	—
2nd	Sophisticated Targeted Attacks	⊙		⊙		3rd (Up)	4th
3rd	Information Leakage Occurring on a Daily Basis	⊙		○		5th	3rd
Threats to Users							
1st	Diversified Infection Routes for Computer Viruses and Bots		⊙	○		4th (Up)	6th
2nd	Threats Arising from Vulnerable Wireless LAN Encryption		⊙	○	○	6th (Up)	—
3rd	Never Decreasing Spam Mails		⊙	○		8th (Up)	9th
4th	Threats Arising from Using the Same User ID and Password	○	⊙	○		10th (Up)	—
Threats to System Administrators/Developers							
1st	Threats of Attacks via a Legitimate Website	○		⊙	○	2nd	2nd
2nd	Actualized Passive Attacks			○	⊙	7th	1st
3rd	Potential Vulnerability in Embedded Systems/Devices				⊙	9th (Up)	10th

⊙ : Those who should take measures ○ : Those who should take measures on an as-needed basis
(Up) : Those ranked higher than the previous year level

Appendix Table 1 shows overall rankings of 10 major security threats and who needs to take measures. Among the new threats ranked in Top 10 in this year are: "Threat of DNS Cache Poisoning" and "Threats Arising from Vulnerable Wireless LAN Encryption." Among the threats ranked higher than the previous year level are: "Diversified Infection Routes for Computer Viruses and Bots" and "Increasingly-Sophisticated Targeted Attacks."

[Appendix B] Correlation Diagram of 10 Major Security Threats



Appendix Table 2. Relations among 10 Major Security Threats

【Appendix C】References

[For Organizations]

- (1) ソーシャル・エンジニアリングを巧みに利用した攻撃の分析と対策, Feb. 2009
<http://www.ipa.go.jp/security/vuln/report/newthreat200902.html> (in Japanese)
- (2) 近年の標的型攻撃に関する調査研究—調査報告書—, Mar. 2008
<http://www.ipa.go.jp/security/fy19/reports/sequential/> (in Japanese)
- (3) 知っていますか？脆弱性(ぜいじゃくせい), Jul. 2007
http://www.ipa.go.jp/security/vuln/vuln_contents/ (in Japanese)
- (4) 情報漏えい発生時の対応ポイント集, Sep. 2007
<http://www.ipa.go.jp/security/awareness/johorouei/> (in Japanese)

[For System Administrators]

- (5) 安全なウェブサイト運営入門, Jun. 2008
<http://www.ipa.go.jp/security/vuln/7incidents/> (in Japanese)
- (6) ウェブサイト運営者のための脆弱性対応ガイド, Feb. 2008
http://www.ipa.go.jp/security/fy19/reports/vuln_handling/ (in Japanese)
- (7) Vulnerability Information Portal Site JVN
<http://jvn.jp/en/>
- (8) Vulnerability Countermeasure Information Database JVN iPedia
<http://jvndb.jvn.jp/en/>
- (9) Filtered Vulnerability Countermeasure Information Tool MyJVN
<http://jvndb.jvn.jp/en/apis/myjvn/>
- (10) SQL インジェクション検出ツール iLogScanner, Apr. 2008
<http://www.ipa.go.jp/security/vuln/iLogScanner/> (in Japanese)
- (11) DNS キャッシュポイズニング対策, Jan. 2009
http://www.ipa.go.jp/security/vuln/DNS_security.html (in Japanese)

[For Developers]

- (12) セキュアプログラミング講座
<http://www.ipa.go.jp/security/awareness/vendor/programmingv2/> (in Japanese)
- (13) How to Secure Your Web Site 3rd Edition Released, Jun. 2008
http://www.ipa.go.jp/security/english/vuln/200806_websecurity_en.html
- (14) TCP/IP に係る既知の脆弱性に関する検証ツール, Jan. 2009
http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html (in Japanese)
- (15) SIP に係る既知の脆弱性に関する検証ツール, Apr. 2009
http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html (in Japanese)
- (16) Vulnerability Disclosure Guideline for Software Developers Released, Jul. 2007
http://www.ipa.go.jp/security/english/vuln/200807_announce_manual_en.html
- (17) 自動車と情報家電の組み込みシステムのセキュリティに関する調査報告書, Mar. 2009
<http://www.ipa.go.jp/security/fy20/reports/embedded/index.html> (in Japanese)

【 Appendix D 】 Information Security Overview for FY 2008 (10 Topics)

In this section, we outline 10 topics selected from what happened in the field of information security in the fiscal year ending in March 2008.

1. Information leakage in FY 2008:

"File-Sharing Software" was ranked 1st. "Unauthorized Access" was also notable
As the major cause of information leakage, "(anonymous) File Sharing Software" was ranked 1st in FY 2008, in comparison to "Loss/Theft" in FY 2007. As a result, an unreasonable situation arose, in which second-leakers received no punishment, while users who fell victim of information leakage incident by disclosure viruses in their computers were slapped by social sanction (in some cases, legislative measure such as copyright law was enforced). "Second-leakers" intentionally upload the leaked information in a file-sharing network, after the initial information leakage incident has quieted down. Concerned bodies submitted a petition to the government calling for legislation on this issue. The Japanese society is now being asked: "Which is more important, the privacy of the second-leaker's communications or the privacy of the owner of the leaked information?" (Figure 1)

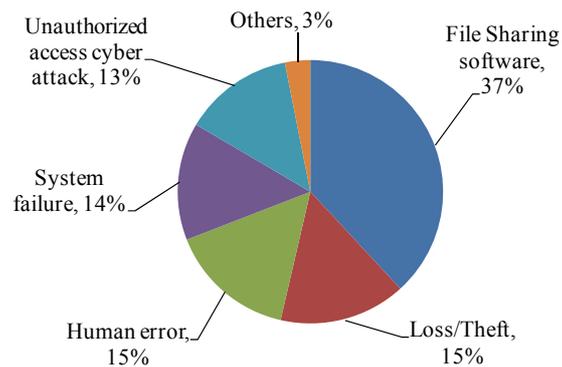


Figure 1. Cause of Information Leakage

2. The Second Stage of Japan's overall plan:

Making a new Information Security Basic Plan

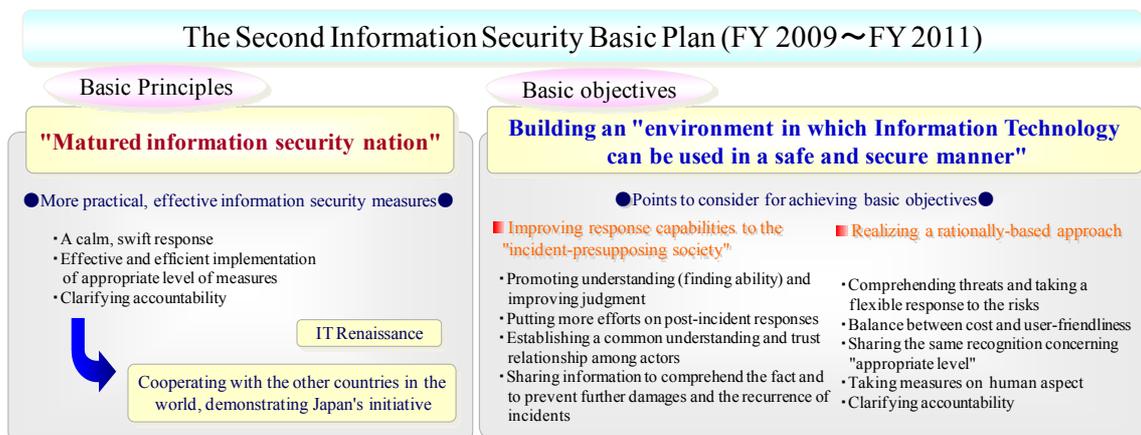


Figure 2. Basic Principles and Objectives of the Second Information Security Basic Plan

Japan's information security policy has been implemented based on "The First Information Security Basic Plan (Target period: FY 2006 to FY 2008)", but on February 3, 2009, the government formulated "The Second Information Security Basic Plan"(Target period: FY 2009 to FY 2011), as the next stage in the national plan. In addition to "Proactive Defense" and "Protection" addressed in the prior plan, the Second Basic Plan covers issues such as improving response capabilities to the "incident-presupposing society", balancing cost and user-friendliness, and realizing a rationally-based approach (e.g., clarifying accountability.) (Figure 2)

3. Vulnerability in Domain Name Servers:

Cache Poisoning has become a topic of global interest

Information on a vulnerability named "Cache Poisoning", along with patch programs to remedy it, was released by experts around the world in July 2008.

DNS is an important server that provides the basis for the use of e-mail and Websites, and JPCERT/CC and relevant

organizations in Japan were acting to keep the public informed about vulnerabilities identified. Among the vulnerability reports submitted to IPA in the second half of 2008, "DNS Cache Poisoning" accounted for a large proportion. Even now, no measures have been taken for most DNS Servers, and immediate action is strongly urged. (Figure 3)

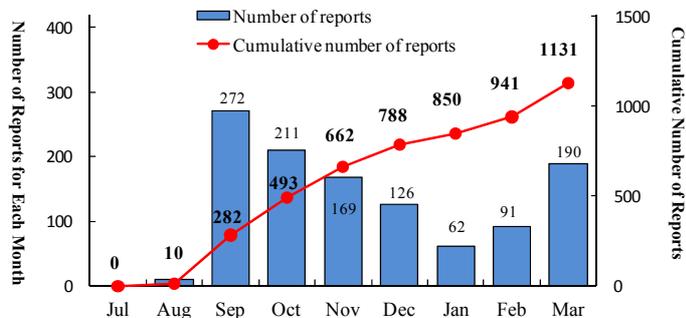


Figure 3. Changes in Number of Reported DNS Cash Poisoning Vulnerability

4. A study on cipher generation transition has started

In February 2009, a guideline was publicly released for soliciting cryptography, which is recommended for the e-Government systems that are expected to adopt new cryptography in 2013. Official public offering is scheduled in the autumn of 2009, following the security evaluation of the new cryptography proposed. The release of the guideline marked the start of new cryptography research by the related community in Japan. New cryptography that can be used worldwide is expected, rather than just adding it to the recommended cryptography list for e-Government.

5. IC Card security issue raised in Europe and the United States:

Japan is also building a framework for security evaluations

IC cards are used for transportation cards, credit cards, electronic passports, etc., serving as a foundation for the lives of people around the world. In June 2008, university researchers in the Netherlands demonstrated that the "Oyster Card", which has 17 million issued copies in Europe, can be replicated by a special technique analyzing its electronic circuit, and used

illegally in the London Underground. A similar demonstration was done with a pass-permit card used in the Boston subway. In Japan, there is increasing demand for information security measures that are applied for IC Card/Card Reader hardware and their operating systems. For this reason, the "IC Systems Security-Round Table", a private association to build a framework for IC Card security evaluation in Japan, was established in March 2009.

6. U.S. New President Obama's Information security policy:

Given the first priority

On January 21, 2009, The Obama Administration announced the outline of a new strategy for cyber security, saying that cyber security is one of the first priorities for his administration. Since he made a campaign speech in the summer of 2008, President Obama has been addressing cyber security as the top priority of his Administration.

The new strategy consists of 6 pillars, including building a cyber infrastructure as the nation's strategic asset and reinforcing the U.S. government's leadership in the field, leading next generation of R&D, protecting IT infrastructure, preventing corporations from cyber-espionage, minimizing crime opportunity gain, protecting personal information and releasing information on incidents concerning information leakage. Further, the position of "National Cyber Adviser," who reports directly to the President and is responsible for making federal policies regarding cyber security, will be established. (Figure 4)



Figure 4. One of the Policy Proposals That Became the Basis for the President Obama's Information Security Policy

7. Enterprises' investment in information security:

The impact of financial crisis has become visible, particularly in regional towns and cities

As the biggest challenge in implementing information security is "expenditures necessary for information security measures", the IPA's surveys in many parts of Japan revealed that this tendency has become more prominent, particularly in regional nucleated cities. The next challenge is "expenditure to have staff with specialized expertise." Amid the global financial crisis that is also affecting Japan's economy, small and medium-sized enterprises in Japan are challenged to raise funds. This problem seems to affect enterprises' investment in information security measures.

Many large Japanese corporations had completed major information security-related investment by 2008 and such investment was reduced drastically in 2008, compared to 2007. Further support is required for small and medium-sized enterprises that have limitation on business resources.

8. E-government:

A study on how to improve services moved into high gear

A study on a mechanism which allows multiple administrative services to be completed at one site (e.g., next generation administrative services, social security cards, “electronic post-office box (tentative naming)”, etc.) moved into high gear in April, 2008. During the study session, system architecture is examined, taking into account information security and privacy, such as how to identify and authenticate users (citizens), and how to utilize and control information. It is important to build a social system, which is rational and convenient for people's living and economic activities. For this reason, the construction of common platforms and IDs is gathering momentum.

Private organizations also are making efforts to promote the shared use of IDs on multiple sites. Among them are "Open ID Foundation Japan", which was established in October 2008, and "Liberty Alliance".

9. Amendment of the Unsolicited Commercial E-mail Prevention Law, Opt-In system started in December 2008

In December 2008, the Unsolicited Commercial E-mail Prevention Law was amended to adopt an "Opt-In" system that prohibits sending commercial e-mail unless prior consent is obtained from recipients. Unsolicited commercial e-mail occupies a large portion of Internet bandwidth, slowing down transmission speed. Furthermore, they may allow computer viruses to be embedded in them and/or guide users to malicious websites containing computer viruses. Unsolicited commercial e-mail is often sent from abroad. Outside Japan, under the cooperation of concerned organizations, the network of a malicious ISP hosting the sending of unsolicited commercial e-mail was shut down in August 2008, proving to be an effective measure. Deeper international cooperation will be required in the future.

10. Chinese Standard Expected to Harmonize with International Standard:

Concerns in the China Compulsory Certification system

The Chinese government has implemented the China Compulsory Certification system (CCC) since 2002, for the purpose of maintaining national security and ensuring the safety of products. In January 2008, the government announced that it would add 13 information security products to target products of CCC in May 2009. The Chinese government is purportedly planning to apply an ISO/IEC15408 (Common Criteria)-like standard for CCC. While major countries in the world join the international mutual recognition framework of Common Criteria, CCC is deemed to be a vehicle for China to not accept products certified in other countries, which became major concerns to the international community. For this reason, Japan, the U.S., European countries and South Korea are negotiating with China at WTO and other meetings. Continuous efforts should be made to come to an appropriate settlement.

(*) On April 29, 2009, the Chinese government announced that it would reschedule to May 1, 2010 and confine to products in government procurement. However, on May 4, 2009, the U.S. and Japan rendered a message requesting China to withdraw CCC.

Information Security White Paper 2009 Part 2

10 Major Security Threats

Attacking Techniques Become More and More Sophisticated

[Publication]	Mar. 24, 2009	First Printing
	May 25, 2009	Second Printing
	Jun. 25, 2009	English Translation First Printing

[Editor] Information Security Study Group,
IT Security Center,
Information-technology Promotion Agency, Japan

How to Report Information Security Issues to IPA

Designated by the Ministry of Economy, Trade and Industry, IPA IT Security Center collects information on the discovery of computer viruses and vulnerabilities, and the security incidents of virus infection and unauthorized access.

Make a report via web form or email. For more detail, please visit the web site:

URL: <http://www.ipa.go.jp/security/todoke/> (Japanese only)

Computer Viruses

When you discover computer viruses or notice that your PC has been infected by viruses, please report to IPA.

Software Vulnerability and Related Information

When you discover vulnerabilities in client software (ex. OS and browser), server software (ex. web server) and hardware embedded software (ex. printer and IC card), please report to IPA.

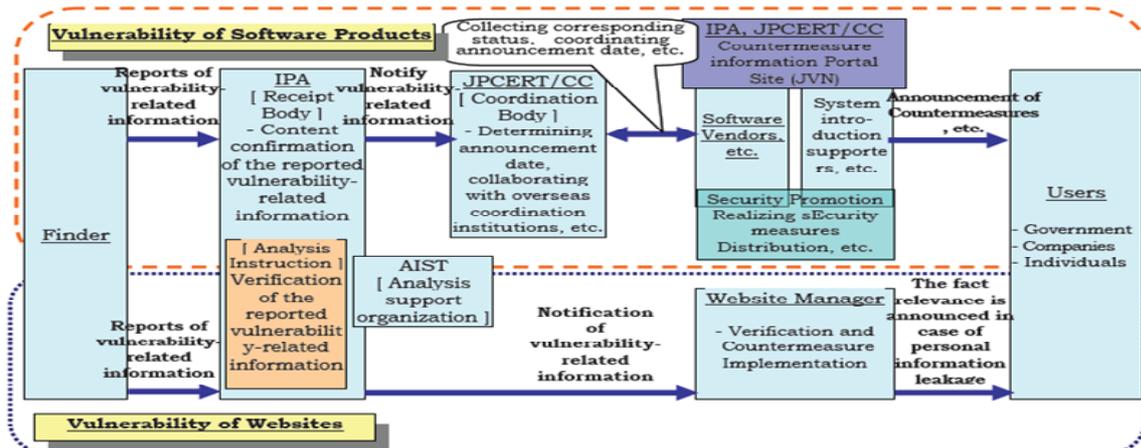
Unauthorized Access

When you detect unauthorized access to your network, such as intranets, LANs, WANs and PC communications, please report to IPA.

Web Application Vulnerability and Related Information

When you discover vulnerabilities in systems that provide their customized services to the public, such as web sites, please report to IPA.

Framework for Handling Vulnerability-Related Information ~ Information Security Early Warning Partnership ~



JPCERT/CC: Japan Computer Emergency Response Team Coordination Center, AIST: National Institute of Advanced Industrial Science and technology



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591 JAPAN
<http://www.ipa.go.jp/index-e.html>

IT SECURITY CENTER
Tel: +81-3-5978-7527 FAX: +81-3-5978-7518
<http://www.ipa.go.jp/security/english/>