For the Year 2011

10 Major Security Threats

- Attacks are fast evolving...Is your security good enough? -

IPA

Information-technology Promotion Agency, Japan

March 2011

Contents

This document is available for download at the following URL:

For the Year 2011

10 Major Security Threats – Attacks are fast-evolving… Is your security good enough? –

http://www.ipa.go.jp/security/english/vuln/10threats2011_en.html

10 Major Security Threats for the Year 2011

Attacks are fast evolving… Is your security good enough?

Introduction

This report summarizes 10 major security threats for the year 2010. It was produced by the 10 Major Security Threats Committee of 127 members, which consist of those involved with the Information Security Early Warning Partnership, information security practitioners and researchers, and other collaborators.

In this document, the term "threat" refers to any events that cause loss or damage to an organization; "risk" refers to a possibility of an organization suffering loss or damage or encountering dangers that are caused by "threat"; "business impact" refers to the impact of "risk" on an organization's business and/or service continuity.

Based on their Business Continuity Management (BCM) concept, the organizations should analyze and assess the business impact brought about by the existing threats, and then take appropriate security measures based on the analysis and assessment results. IPA hopes this report will help to understand the current circumstance surrounding information security and improve security threats.

Organization of this Report

This report consists of 3 chapters.

Chapter 1 looks at the business impact on organizations that were caused by the actual security incidents during the year 2010.

Chapter 2 outlines 10 major security threats for the year 2010 in terms of their great social impact and strong impression. 10 Major Security Threats were ranked as Table 1 according to the vote of the Committee members.

Chapter 3 presents the points and approaches towards information security.

Summary of 10 Major Security Threats for 2011

In 2010, same old, new and various security incidents occurred, such as the Advanced Persistent Threats (APT) that combines multiple attacking methods, information leakage caused by mismanagement of information assets, viruses targeting smartphones and attacks targeting the users of microblogging services.

Especially, the Advanced Persistent Threats (APT) that combines multiple attacking methods, such as Stuxnet, shows that control systems are no longer off-limits in cyber space.

In the recent web development where people can easily send out information, information leakage caused by “people”, such as by taking out the internal information from the premises without permission or misplacing information media like PC, made the importance of information management highlighted once again. For example, the statistical data, such as the number of information leakage incidents and the assumed amount of total compensation payments in the first half of 2010, are shown in Table 2 and the number of people affected per incident is shown in Table 3.

Other than that, the viruses targeting

fast-spreading smartphones, cross-site scripting vulnerability exploitation in the microblogging services and the use of short URLS to redirect the users to malicious websites were noticeable.

Attacks targeting information assets have been becoming more and more sophisticated and advanced, and past security measures may not protect the assets anymore. The organizations should analyze existing “threats”, what “risk” they pose and how much “impact” they have on the organization, and then consider and implement appropriate countermeasures.

Table 1：For the Year 2011 10 Major Security Threats

Ranking	10 Major Security Threats
1st	Information leakage caused by "people”
2nd	Unstoppable! Attacks through websites
3rd	Attacks exploiting vulnerability in standard software
4th	Attacks targeting smartphones on the rise
5th	Advanced Persistent Threats (APT) that combines multiple attacking methods
6th	Troubles caused by inadequate security measures
7th	Security issues in mobile phone websites
8th	Hard-to-detect targeted attacks
9th	Security issues in cloud computing
10th	Attacks targeting users of microblogging service and SNS

Table 2：First Half 2010 – Data on Personal Information Leakage

Number of People Affected	1 1,270,383
Number of Incidents	684
Assumed Amount of Total Compensation Payments	¥36,437,050,000
Number of People Affected per Incident	1,951
Amount of Compensation Payment per Incident	¥55,970,000
Amount of Compensation Payment per People Affected	¥40,823

Ref.: JNSA: 2010 Information Security Incidents [First Half Flash Report]

Table 3：First Half 2010 – Number of People Affected by Information Leakage

No.	Number of People Affected	Sector	Cause
1	201,414	Academics, Specialized and Technical Service Providers	Mismanagement
2	197,907	Information and Communications	Theft
3	170,325	Finance and Insurance	Mismanagement
4	100,000	Information and Communications	Loss, Misplacement
5	90,700	Finance and Insurance	Mismanagement
6	63,805	Service	Theft
7	51,300	Finance and Insurance	Mismanagement
8	33,600	Finance and Insurance	Mismanagement
9	27,998	Finance and Insurance	Mismanagement
10	15,521	Finance and Insurance	Mismanagement

Ref.: JNSA: 2010 Information Security Incidents [First Half Flash Report]

Classification of 10 Major Security Threats

10 major security threats observed in 2011 were divided into the following three categories. The result is shown in Figure 1.

(1) Threats of external attacks

(2) Threats of information leakage

(3) Threats caused by design, implementation or operation of information system

Attacks that threaten information system via external network or through electronic media are categorized into (1). Threats where information held by an organization (e.g. confidential information, personal information) is exposed due to loss or theft are categorized into (2). Issues caused by inadequate security measures and handling of security problems for outsourced applications are categorized into (3).

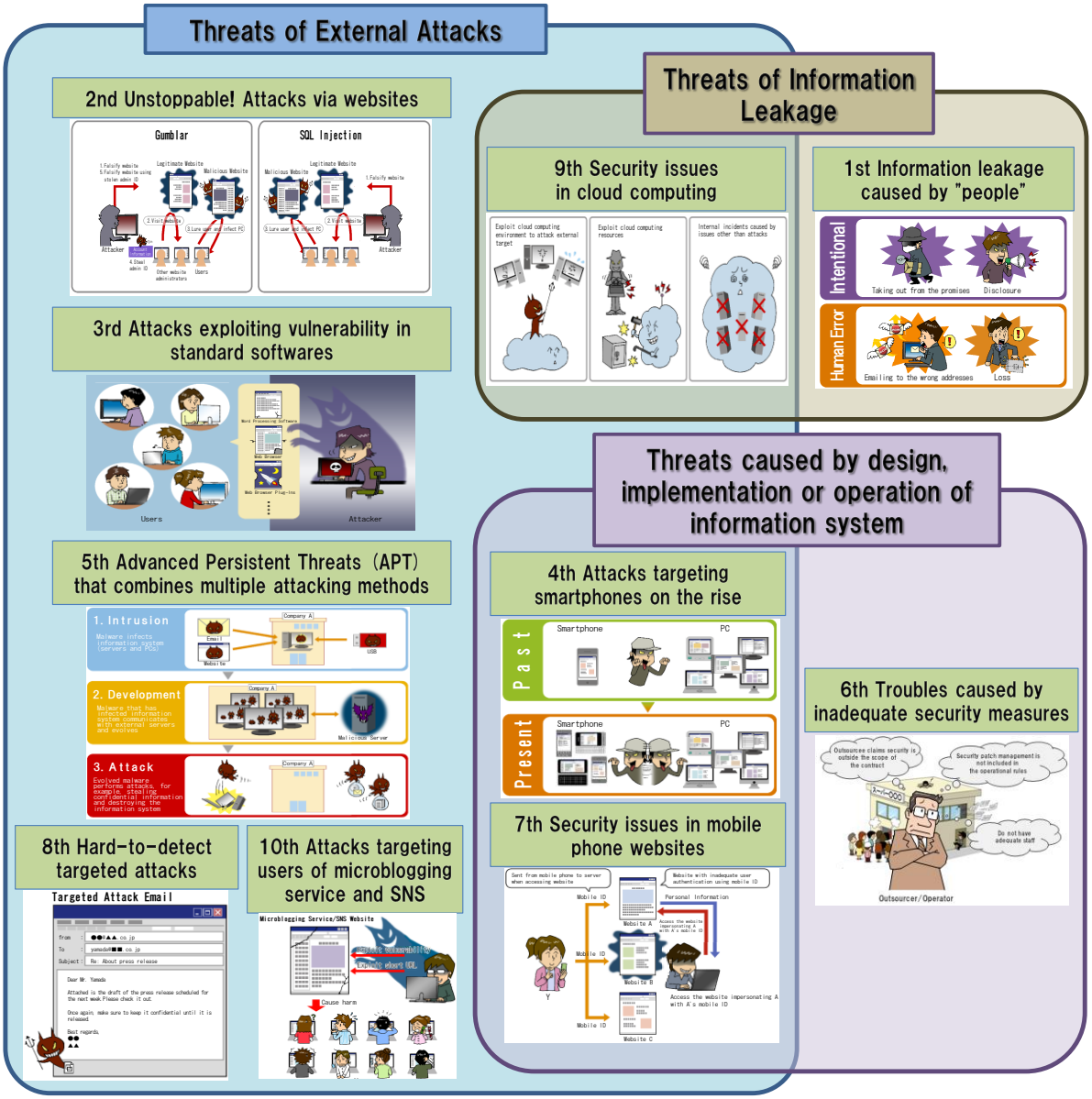


Figure 1: Classification of 10 Major Security Threats

This page intentionally left blank.

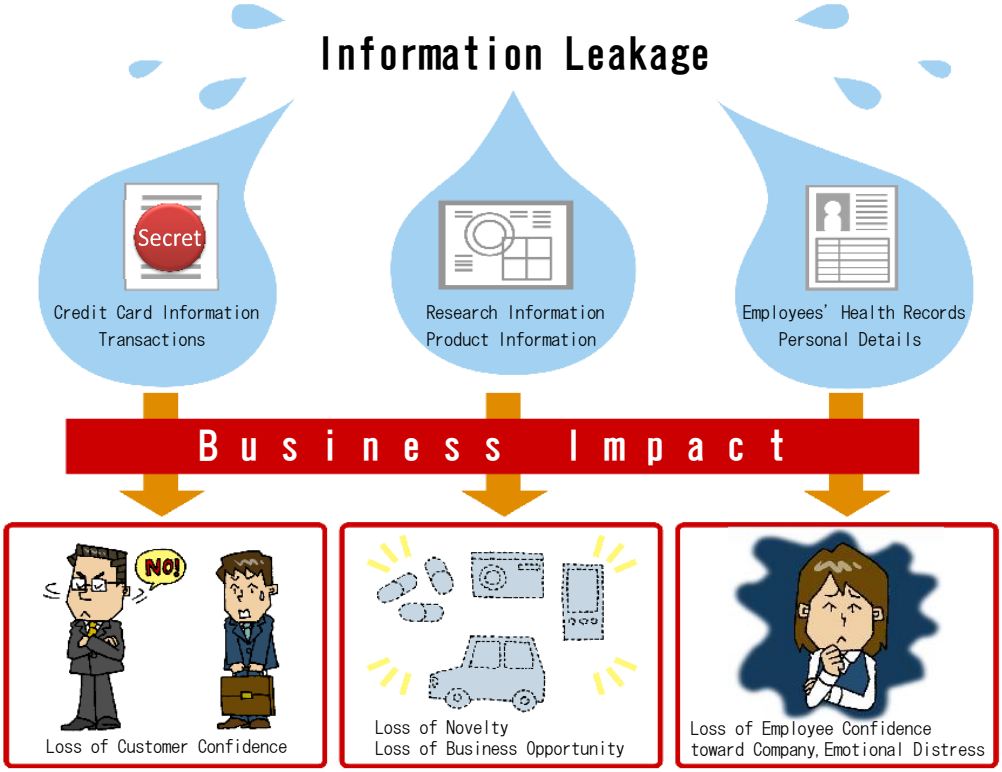
Chapter 1 Business Impact on Organizations in 2010

In 2010, security incidents that directly threaten the business, such as information thefts and system shutdowns, occurred both in Japan and overseas. If a security incident happens, it will have a great impact on the business management, such as the loss of revenue and social confidence, inconvenience to the users and degradation of employee motivation. In addition, the theft of intellectual property and research and development data are now a reality and it could pose a serious risk to business continuity to the manufactures.

In this chapter, we look at 3 typical security incidents: “information leakage”, “system shutdown” and “website falsification”. Then, we analyze and assess their business impact, and consider organizational issues based on the real security incidents.

1.1 Business Impact of Information Leakage

～Multiple Businesses Were Attacked and Intellectual Property Was Stolen～



1.1.1 Threats and Risks of Information Leakage

Threats of information leakage are mainly categorized into two: “information disclosure” caused by an organization’s inadequate information management, human error or intentional disclosure, and “information theft” where an external attacker intentionally steals the organization’s information assets. In this chapter, information leakage means and includes both.

“Information leakage” is ranked top in the 10 Major Security Threats for 2011 and has been increasing its social impact year after year. In recent years, there were the cases where employees intentionally steal or disclose internal information and it is becoming a great risk to the

businesses. Attacks by external attackers to steal internal information assets for financial gain are also a big threat.

Impact of information leakage depends on the importance of the leaked information. For example, some information may cause financial damage to those involved or if it is personal information, the incident may develop into the business's social responsibility issue and affect its business management. If privacy information such as academic results is leaked, the people affected will suffer distress and it may develop into a risk of being sued for compensation.

When information leakage occurs, the business must investigate the extent of the leakage and prevent the damage from spreading as quickly as possible.

1.1.2 Business Impact

•Leakage of Credit Card Information

If credit card accepting stores are negligent and the credit card information is leaked or stolen, needless to point out the loss of social confidence, it will not only cost the business compensation fee to people affected by the incident, money to improve security and recover corporate image, but also impact the business strategy for the future.

For example, in Japan, a security incident happened where an online shopping website was attacked from the outside and more than 70,000 credit card data were said to be disclosed. In 2009, a major insurance company was attacked also from the outside and more than 30,000 credit card data were disclosed. Moreover, 5,000 credit card data were about to suffer unauthorized charge.

•Leakage of Research and Development Information

In January 2010, 30 businesses, including Google, Adobe Systems, Symantec and Yahoo, were attacked and intellectual property information was stolen and the actual harm was done.

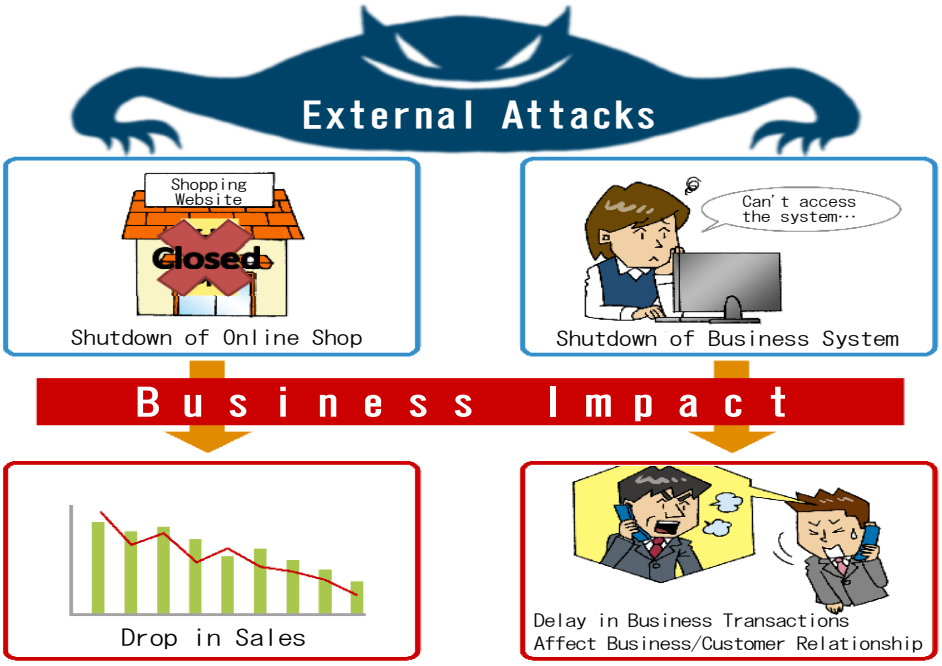
For the manufacturers who develop and produce a product, there is a big risk that research or design data are stolen, obtained and exploited by a rival manufacturer. Should such a case happen, the new product can be put on the market by the rival manufacturer on ahead and the first manufacturer loses a business opportunity. If the rival manufacturer obtains a patent first and makes the first manufacturer unable to sell its new product, the investment to the new product goes to naught and it will affect the first manufacturer's business strategy significantly. Also, if confidential information such as design secrets is disclosed, it will harm the manufacturer's advantage and reduce its competitive power.

•Leakage of Health Records or Personal Details

Other than business information, a business has personal information on the employees. Personal information includes highly sensitive information that should be kept private, such as health records and personal details. If such privacy information is disclosed, it will not only violate the privacy but also cause mental harm to the affected individuals. Moreover, it could have an indirect impact, for example, degrading employees' motivation. The employee motivation is critical to the business's growth and could have a big impact on the business continuity.

1.2 Business Impact of System Shutdown

～DDoS Attack and Virus Rendered Multiple Businesses Temporarily out of Service～



1.2.1 Threats and Risks of System Shutdown

A system shutdown caused by external attack is common in the world these days. In Japan, online game websites or hosting service servers suffered temporary service shutdown due to the DDoS attack against them and caused communication problems. In other countries, a case was reported where a nuclear power facility was halted for a certain period of time due to a computer virus brought in from the outside.

The business impact of system shutdown depends on the importance of the service that is affected. For the online businesses, “system shutdown” may directly lead to “halt of the business”. The business should understand the impact of shutdown of each business system and implement the security measures to mitigate the risk of external attacks.

1.2.2 Business Impact

•In the Case of Web Services

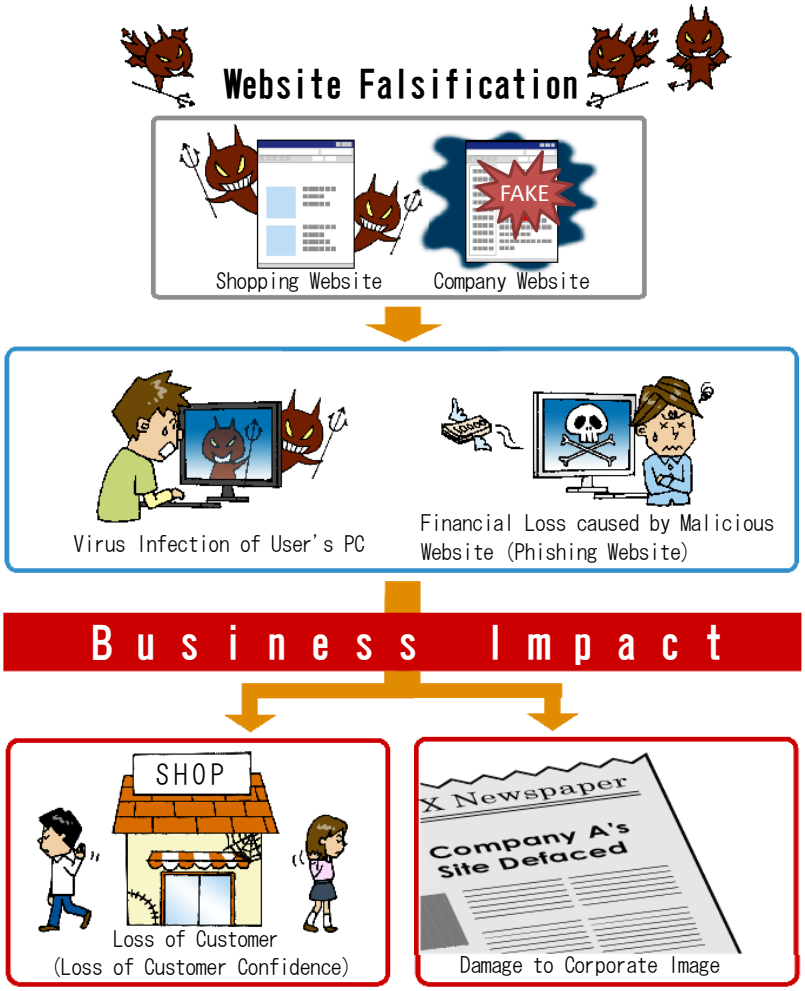
For the businesses that operate online shopping websites, system shutdown has a direct impact and means they cannot continue their business during the shutdown. In addition, they may lose the customer and social confidence because of the service disruption as an indirect damage.

•In the Case of Business Systems

It is common to hear of the incidents where a business system is infected with a virus and people are unable to use the business applications or email system. Since the current office environment is based on the information systems, if the business system is shut down, it affects the daily business significantly. For example, the employees cannot communicate with the business partners via email or if the order placement system shuts down, it may cause troubles such as the delay of the delivery and lead to complaint from the business partners or worse, the loss of business with them.

1.3 Business Impact of Website Falsification

～Website of Big Names Were Falsified and Their Corporate Image was Damaged～



1.3.1 Threats and Risks of Website Falsification

Since 2009, website falsification incidents are kept reported due to the widespread of Gumblar. Website falsification was ranked 2nd in the 10 Major Security Threats for 2011 and is still wrecking havoc. For example, there was a case where a server used for the Internet advertisement service was falsified and the users who accessed the websites using said service were redirected to the malicious websites and infected with viruses.

In the past, website falsification was a joke but its purpose and motivation have been shifted to financial gain. Attackers aim to steal the Internet users' personal information or credit card information by luring them to the phishing websites or infect their PC. The business websites are used as a stepping stone to take part in a cyber crime without the website administrator's knowledge. This could lower their corporate image and affect their business.

1.3.2 Business Impact

•In the Case Of Shopping Websites

If a hopping website is falsified, the loss of customers is expected as a business impact. To guess the customers' feeling, if they feel that they

may become a victim of cyber crime, they will hesitate to shop at the compromised website. It is also possible that the customers who experienced harm may take revenge by posting negative and slandering feedback about the shopping website to the message boards. In this case, the image of the shopping website will be damaged and it may lose the customers.

•In the Case of Corporate Websites

In the current Internet era, a corporate website represents its image. When a corporate website is hacked and falsified, people who get interested in the corporation could be lead to the virus-infected websites or phishing websites and become victim of financial crime. In this case, In addition to the loss of customer confidence, the fact that it has taken part of cyber-attacking the users through its falsified website will lower its customer and social impression and could impact its business.

This page intentionally left blank.

Chapter 2 10 Major Security Threats

[1st] Information Leakage Caused by "People"

Information leakage is by no mean a new threat but it is becoming to pose a bigger risk as PCs and the Internet become more common and people are gotten used to send out information easily.

<Threats>

Information leakage could bring down critical damage to the business. It is important for the business not only to take preventive measures but also get ready for possible incidents.

One of characteristics of information leakage is that it is caused by behavior of “people“. A reason why information leakage cannot be eliminated is because the current information systems require the involvement of “people” to make a judgment over things that cannot be controlled by computers when we handle and manage information.

The causes of information leakage by “people” are mainly categorized into two: “intentional” acts and “human error”. The following sections address typical cases of information leakage for each cause.

[Intentional Information Leakage]

⑴ Taking out Data from the Premises

There is a case where an employee or ex-employee stores the customer list in external storage media such as a USB memory stick or CD-ROM and intentionally takes out from the premises and sells it to the buyers. The cause of this behavior can be the retaliation to the employer who fired him or her, or financial gain by selling the list to the buyers.

⑵ Disclosure to Outsiders

There is a case where a person intentionally posts the information obtained as an insider on a public website to disclose the information. In 2010, disclosure of the government’s classified information on an overseas information disclosure website was one of the hottest news. In Japan, there was a case where an individual disclosed an organization’s sensitive information on a website without really thinking anything about it. Behind these trends are the development of web services that enable people to publish information more and more easily.

[Information Leakage by Human Error]

⑴ Emailing to Wrong Addresses

The most typical case of information leakage

due to human error is sending an email to the wrong address. A difficulty of preventing this misoperation is that the only person who can judge the correct recipients and prevent the incident is the sender him- or herself. Education to reduce mistakes is effective to some extent but eliminating human error is hard to achieve.

⑵ Loss and Theft

Information leakage by loss of information means a case where classified information is disclosed due to the loss of PC or external storage media such as USB memory stick or CD-ROM. The fact that the reduced size and large capability of data storage media have made transfer of large amount of data ever so easy has increased the risk of data loss. Information can be disclosed through the theft as well.

<Impact>

The impact of information leak on the organization depends on the kind of industry and the information disclosed.

For example, in the case of the business which directly trades with the customers, such as general retailers or online shopping websites, leakage of the customer information may result in not only the loss of customer confidence but also a lawsuit. In such a case, it will cost the business a lot of money to respond to and recover from the incident, in addition to the impact of lost revenue. In the worst case scenario, the incident will threaten its business continuity. For the business whose strong point is the novelty of its products, if trade secrets such as the product's design information or research information are disclosed, it will have a significant impact on the business strategy.

If information leakage occurs, various works must be done, such as investigation of the cause of the leakage, announcement and apology to people affected, report to the authority, compensation to people affected, and rebuilding of customer and social confidence. How quickly the business can return to its normal state is the key in the incident response. The organizations should consider how to respond to an incident in advance and get ready for it, not to mention implementing the preventive measures to prevent information leakage from happening.

〈Statistics for the Year 2010〉

According to the Report on Information Security Incidents published by JNSA (Japan Network Security Association), the number of people affected by personal information leakage during the first half of the year 2011 is 1,270,000. The number of incidents is 684. "misoperation" (sending email to the wrong addresses) accounts for 37 % of the causes and "mismanagement" (lack of internal rules) follows second with 30%.

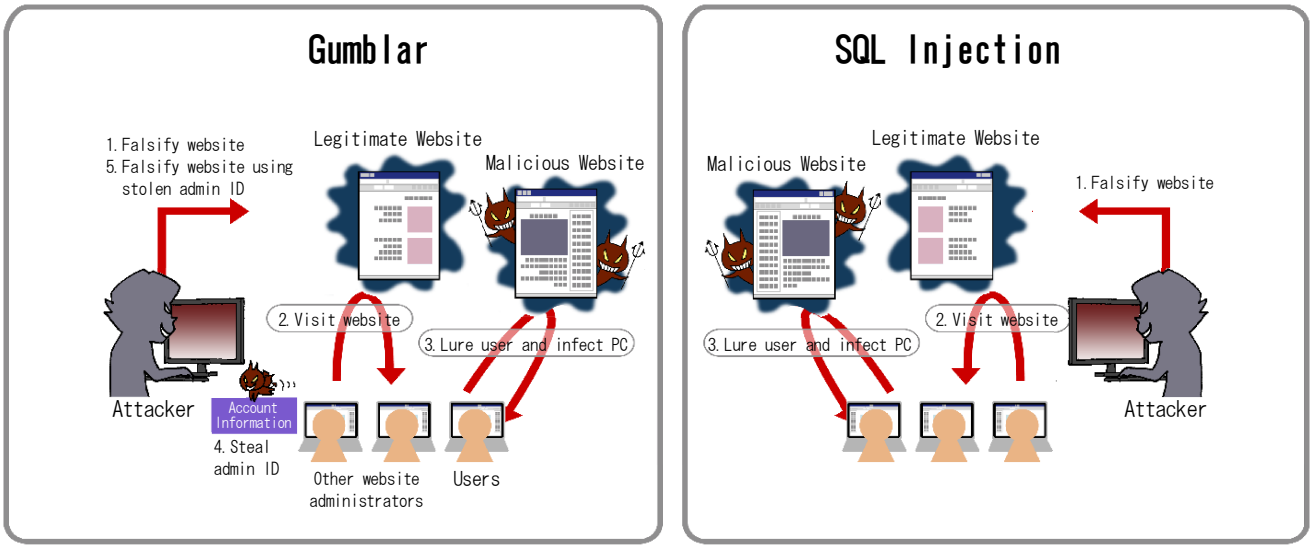
An example of the real incidents is that a temporary employee took out the list of 460,000 shopping website customers from the premises and sold it to a buyer. At an information system vendor, an employee lost a PC that stored the information on 100,000 customers on the way home and disclosed the information.

References (All in Japanese)

JNSA: http://www.jnsa.org/result/incident/data/2010fp_incident_survey_sokuhou_v1.0.pdf

SecurityNext：http://www.security-next.com/cat_cat25.html

[2nd] Unstoppable! Attacks through websites



Attacks through websites continue to be popular in 2010. Attacks that exploit websites affect both the organizations and the users.

<Threats>

By attacks through websites, a popular, well-trusted website can be maliciously used as a stepping stone in cyber crimes. As a result, the users' computer can be infected with virus without their knowledge and become victim of information theft.

The typical attacks through websites are those with Gumblar and attacks that exploits SQL injection vulnerability. The threats and characteristics of each method are summarized in the following.

[Website Falsification by Gumblar]

A Gumblar attack follows the steps below.

(1) An attacker falsifies a legitimate website to redirect its user to a malicious website where virus is ready to infect the users' PC..

(2) A user visits the legitimate website.

(3) The user's PC is infected with virus at the malicious website the user was redirected to.

(4) The virus starts to steal data, such as the account information (ID, password), transfer data to the attacker, and spread the virus to other PCs on the network.

(5) If an infected PC has the administrator account information of other websites, the attacker then falsifies those websites using the obtained information.

Infected websites can grow exponentially and that is one of the biggest threats of the Gumblar attacks.

However, the step (5) needs to meet the following requirements.

- The vulnerability management is not done with the website administrator's PC.
- The website can be updated from anywhere, such from home or Internet cafés.

[Website Falsification by SQL Injection]

Website falsification in an SQL injection attack is performed by manipulating the database for the website.

There are two conditions for the SQL injection attack to successfully falsify the website.

- The website contains SQL injection vulnera-

bility.

- The website dynamically generates a web page using the data stored in the database.

If the website satisfies these conditions, it is possible that an SQL injection attack falsifies the website and injects virus into it. As a result, the user's PC will be infected. In addition to falsify the website, the SQL injection attack poses a threat where the information stored in the database may be stolen.

<Impact>

If a website is falsified, there is a possibility that the user's PC may be infected with virus or the web services may be temporarily shutdown. Consequently, social confidence toward the organization that operates the website can be damaged. The more popular the website is, the bigger the social impact is, and the possibility that its users will become victim to the attack increases.

Some viruses pose as a security software and induce the user to enter the credit card information to buy a paid version of the software to remove the virus. If the user's PC is infected with this type of virus, the user may suffer financial loss.

To prevent these from happening, both the website administrators and users must implement security measures.

<Statistics for the Year 2010>

As compared to 2009, the news coverage of the attacks through websites was fewer in 2010. However, the attacks and the damage they caused continued to be reported in 2010.

According to a report published by a antivirus software vendor in 2010, the number of incidents of virus infection was more than 100 businesses in October 2010 alone. Another report says that among the top 10 viruses reported to the said vendor, 4 viruses are those that exploit websites like Gumblar. These facts suggest that attacks through websites did not calm down.

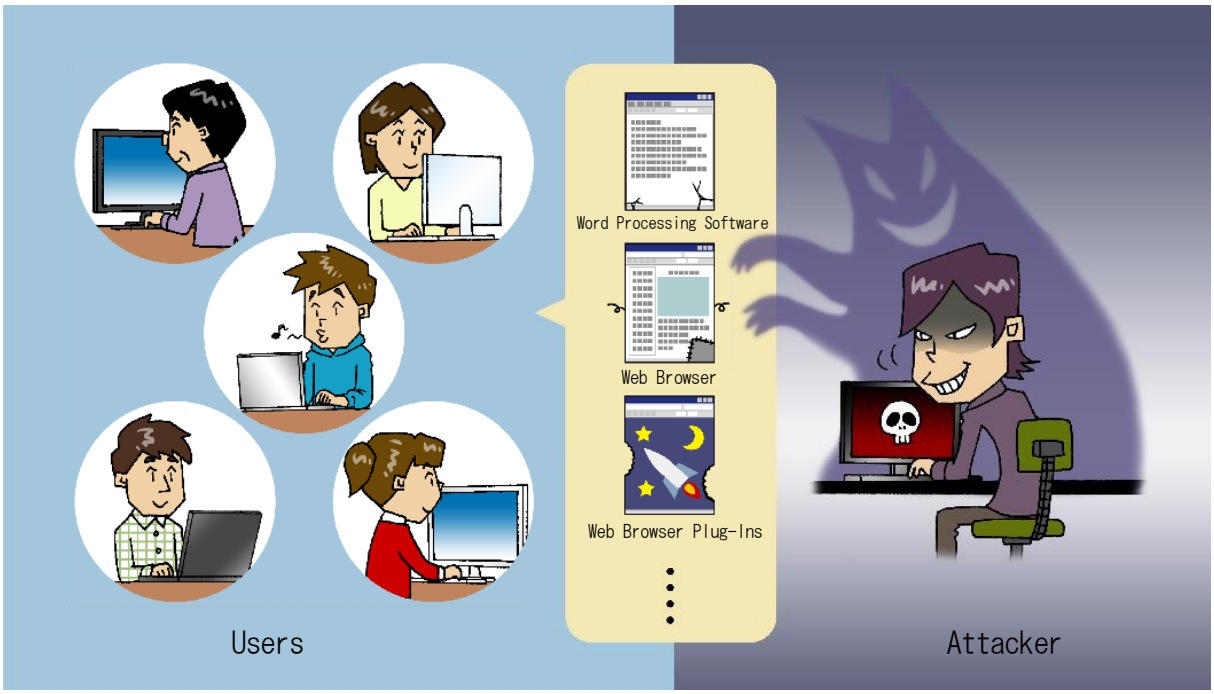
References (All in Japanese)

JPCERT/CC: http://www.jpcert.or.jp/at/2010/at100001.txt

Mycom Journal: http://journal.mycom.co.jp/articles/2010/11/05/trendmicro/index.html

Trend Micro: http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20101217082311.html

[3rd] Attacks Exploiting Vulnerability in Standard Software Applications



Among software applications, there are so-called standard softwares used by a large number of people. Attacks that exploit vulnerability in those standard softwares never cease.

<Threats>

On a computer, various software applications are running. If they contain vulnerability, attackers may exploit it in attack. Especially, the software applications used by a large number of people like the standard softwares are prime target.

One of the reasons why the standard softwares are targeted by attackers is not only its large user base but also the assumption that quite a number of their users do not update the softwares to fix vulnerabilities. That makes many users sitting ducks for attackers if vulnerability is found in the standard softwares.

Many attacks that exploited vulnerability in the standard software were reported to IPA in 2010. When the existence of the attack that exploits vulnerability in a widely used software is confirmed and the security patch to fix the vulnerability is available, IPA publishes a security alert. In 2010, IPA issued 15 security alerts.

Softwares for which the security alerts are released are the following.

- Internet Explorer
- Adobe Reader, Adobe Acrobat
- Java Runtime Environment (JRE)
- Java Development Kit (JDK)
- Ichitaro Series
- Adobe Flash Player
- Windows Shell

<Impact>

When attackers target the standard softwares, they use various attacking methods such as websites and email. Among the 10 Major Security Threats for 2011, the 2nd “Unstoppable! Attacks

through Websites" and the 8th "Hard-to-Detect Targeted Attacks" also exploit vulnerability in the standard softwares.

By attacks, information stored on the PC may be stolen or the PC could be used as a stepping stone to attack others.

To prevent the attacks, it is effective to update the standard softwares to the fixed version. Most operating systems and accompanying software applications have an update function that updates them automatically and periodically. Other software applications often have a similar automatic update function or a notification function that alerts the users that the new version is available.

Attackers try to compromise the users' PC in various ways such as via websites and email. The users should accustom themselves to checking if the standard softwares on their PC are up to date. Some of the standard softwares can be checked with IPA's MyJVN Version Checker.

<Statistics for the Year 2010>

According to IPA's "Report on Awareness Survey on Information Security Threats for 2010", those who said yes to whether "they update the security patch using the Windows Update" was 69.4%. For Adobe Reader, it was 55.6%. Others answered that they did not update.

Windows Update distributes the security patch for Internet Explorer, one of the most used web browsers, as well. The survey result suggests that the users are not accustomed to update the standard softwares like Internet Explorer and Adobe Reader.

According to a U.S. security vendor, among top 15 most-exploited vulnerabilities, 5 are related to Internet Explorer and 4 are related to Adobe Reader. Those vulnerabilities were found in 2006. The fact that they are still exploited in attack suggests that many Internet Explorers and Adobe Readers out there are not updated, and old vulnerabilities are waiting to be exploited.

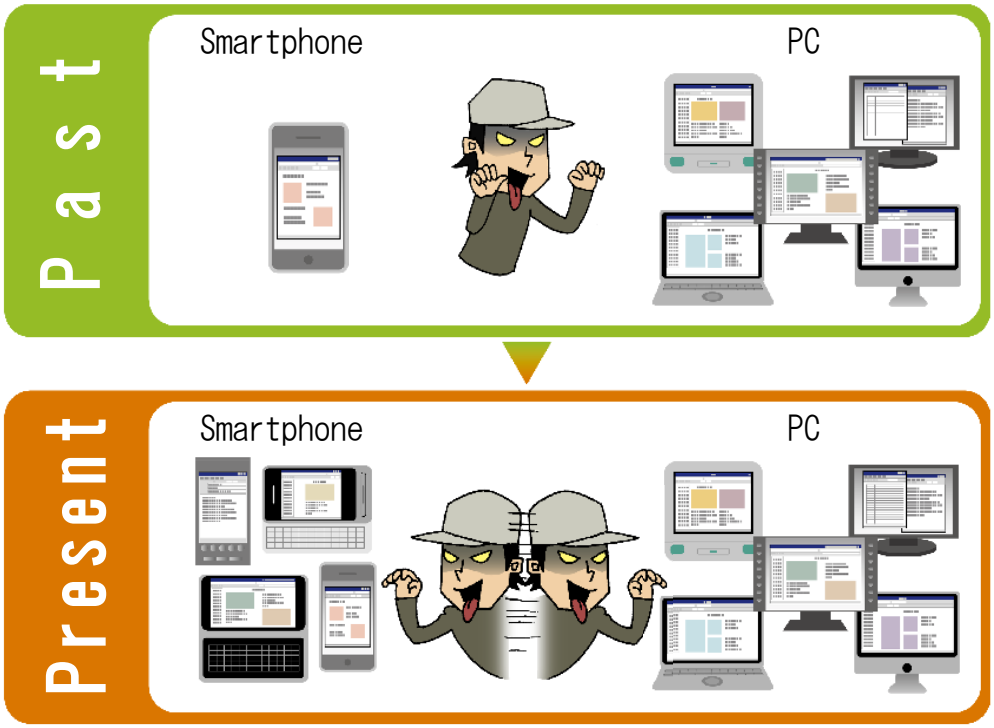
References

ITMedia: http://www.itmedia.co.jp/enterprise/articles/1007/16/news013.html (in Japanese)

IPA Security Alerts: http://www.ipa.go.jp/security/english/index.html

IPA: http://www.ipa.go.jp/security/fy22/reports/ishiki/index.html (in Japanese)

[4th] Attacks Targeting Smartphones on the Rise



Smartphones are quickly becoming a mainstream mobile option. With that, the security issues concerning smartphones have also become evident.

<Threats>

A smartphone is a mobile information terminal with the function of both cell phone and personal digital assistance (PDA). It stores personal information such as an address book and the functions can be enhanced flexibly by installing applications. Things that were unavailable with cell phones are available with smartphones by just enhancing the functions. The user base is increasing yearly and attacks targeting smartphones have emerged. For example:

(A) Attacks that exploit vulnerability in software applications accompanying smartphones.

(B) Attacks that induce the users to install virus posing a legitimate application.

(A) targets smartphones that contain vulnerability and infects them by leading the users to visit the malicious websites or open malicious files.

(B) induces the users to install virus into smartphones, posing as a legitimate application. With the method (B), regardless of the existence of vulnerability in smartphone applications, the smartphones will be infected once the user installs the bogus application (virus).

Although smartphones are getting as capable as PCs, it is difficult to implement the same level of security as PCs into smartphones at this point. Vulnerability should be fixed but it takes time for smartphone vendors to provide security patch and it does not help that there is no established standard to determine whether an application is legitimate or not.

Considering the increase of the user base, flexible scalability and poor security, the factors that encourage attackers are in place and the likelihood of attacks against smartphones is expected to increase.

<Impact>

Since smartphones are now on the attacker's target list, the users need to take care of security of smartphones as well as that of PCs. There are threats like information leakage of personal information stored in email and an address book, being tracked by the position information using GPS and being used as a stepping stone to attack others. Depending on the operating system, antivirus software is available.

To start with, it is important for the smartphone users to know the security issues and countermeasures to mitigate the risks.

If smartphones are supplied to staff in an organization, make sure to establish appropriate operation practice, taking into account the current and future smartphone environment, such as increasing functionality and user base and expected threats, in addition to establishing the operation rules.

〈Statistics for the Year 2010〉

According to a report by a marketing research firm, the number of smartphones shipped domestically is expected to reach 6.75 million in 2010 It is 2.9 times as many as the previous year (2.34 million), showing the rapid growth of smartphones.

In 2010, a practice that enabled to cancel the restrictions on smartphones by exploiting vulnerability in iOS used for iPhone/iPod and touch/iPad, and the viruses that targeted Android OS were observed and confirmed.

To be specific, a practice (Jailbreak) removed the restrictions set up on the smartphone terminals by exploiting vulnerability in Safari, a web browser software accompanying iOS. The point in this story is that it was done by exploiting vulnerability.

By removing the restrictions, smartphones become more vulnerable to attacks. There was a case where a smartphone was infected with virus that targeted jailbroken smartphones at an academic institution.

As for viruses for Android OS, 3 types – Trojan horse, spyware and bot – have been confirmed. Android applications are available not only at Android Market set up by Google, but also at software distribution websites run by the third parties or even personal websites. Check out IPA's "Security Alert for Viruses Targeting Android OS" and see if the software distributors are trustworthy by checking if the access permission list displayed when installing the software includes suspicious access permission, and judge whether the software is safe to install.

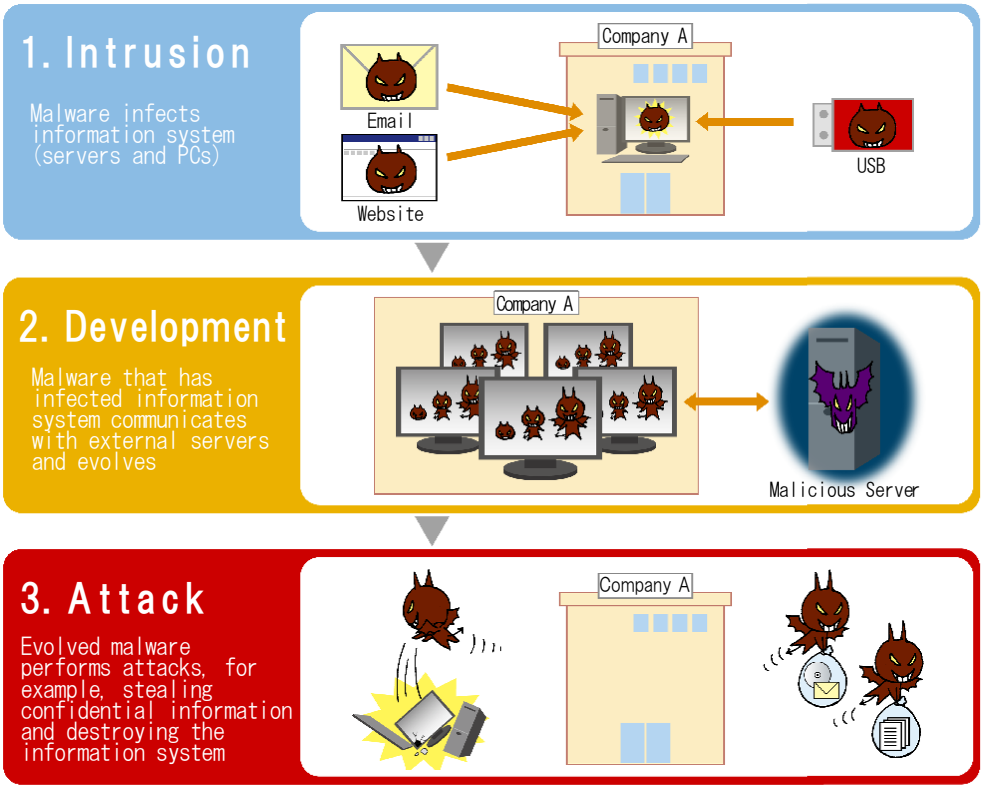
References (All in Japanese)

MM Research Institute Ltd.: http://www.m2ri.jp/newsreleases/main.php?id=010120101216500

Keio University ITC: http://www.hq.itc.keio.ac.jp/topics/topics61.html

IPA: http://www.ipa.go.jp/security/topics/alert20110121.html

[5th] Advanced Persistent Threats (APT) That Combines Multiple Attacking Methods



In 2010, a term “APT (Advanced Persistent Threats)” has become popularly used mainly in the U.S. and Europe to indicate a cyber attack that targets a specific organization. APT is a general name for the attacks that exploit vulnerability in software applications and targets specific organizations and individuals through social engineering, supported by the combination of multiple attacking methods.

<Threat>

The APT has the following characteristics.

(1) Tactful use of social engineering
(2) Exploitation of zero-day vulnerability
(3) Infection via network/USB memory stick
(4) Communication with external command and control server
(5) Customization to each target

These are known attacking tactics and not novel. People may think that if they are known attacks, the organizations that set up with decent security can prevent them. Truth is, it is not that simple. Each attack is combined tactfully to bypass the computer’s security mechanism and tuned for each target. That enables to attack the computer systems which had been considered impossible to attack.

An attack has 3 phases, “1. intrusion”, “2. development” and “3. attack”, and multiple attacking methods are used in each step.

[1. Intrusion]

An attacker compromises the system through targeted email using social engineering or external storage media such as an USB memory stick. One of the attack’s characteristics is that it often exploits multiple vulnerabilities including zero-day security holes, making it difficult to prevent with

ordinary antivirus measures.

[2. Development]

The virus sets a backdoor in the compromised PC, communicates with the command and control server, download other viruses, spread itself by infecting others or enhance its functions. Before launching the final attack, it downloads a program specially customized for the compromised system.

[3. Attack]

The virus launches attacks against the target, for example, steal information or destroy the system.

<Impact>

In the overseas incidents, serious, actual damages have been reported, such as impact on the control systems and theft of highly classified information. APT is observed mainly overseas and it may be giving a false assumption that they have no affect on the control systems in Japan. However, it may be that the systems in Japan are just not targeted yet and could be done against a lot of in Japan.

One reason this attack is successful is that it takes advantage of the traditional network design which assumes the data transmission from the inside network is not a threat. The network design should be reviewed and enabled to prevent the virus that has infected the system from sending out the information.

〈Statistics for the Year 2010〉

Major examples of the APT are the attacks called “Operation Aurora” and the attacks by the “Stuxnet” virus.

“Operation Aurora” was the attacks that targeted the multiple information system vendors including Google. The attacks exploited a zero-day vulnerability in Internet Explorer and stole the user information.

“Stuxnet” is a virus that is said to target Iranian nuclear facilities and contains the codes that seem to manipulate the control systems of the nuclear facilities. If executed, the control systems may have shut down. The virus is designed to infect other systems exploiting the multiple vulnerabilities, including those for which security patches were not available yet.

In both cases, zero-day attacks are used and it shows that it is difficult to prevent the attack at the point of intrusion. At the end, the information targeted by the attacker may be stolen and the critical systems may be shut down. Such attacks are a huge threat to the organization.

References

IPA: http://www.ipa.go.jp/about/technicalwatch/20101217.html (in Japanese)

McAfee: http://www.mcafee.com/japan/about/prelease/pr_10a.asp?pr=10/06/18-1 (in Japanese)

issa-sac: Advanced Persistent Threat

http://www.issa-sac.org/info_resources/ISSA_20100219_HBGary_Advanced_Persistent_Threat.pdf

[6th] Troubles Caused by Inadequate Security Measures

In case security of web systems and applications is breached, it is important to establish an operation framework and procedures to respond to the incidents in advance. If neglected, it may cause a significant damage to the organization's business continuity.

<Threats>

In general, information systems like web applications are released after security measures are implemented in their developmental stage and a number of tests are done. If security is not well considered in the development or operation phase, or new attacking methods are discovered, the risk of security breach increases.

As a result, the website may lose information through unauthorized access, be used to infect its visitors or rendered inaccessible.

Since the lifecycle of an information system is long, its security, including how to maintain and manage security level, should be considered not only at the design and development phase but also from the planning phase.

<Impact>

If security issues are found in the publically available information systems or business systems and the organization cannot respond to them adequately, the following impact may be inflicted.

- Service disruption or rumor may hinder the business or threaten the continuity of business.
- As a result of the continuous use of the information system that lacks security, it may be used as a stepping stone to attack others and cause a big trouble and damage to the society.

Some of the inadequate security responses are often seen in the case where system development or operation is outsourced. When using outsourcing, the liability and responsibility for in-

cidents is often unclear and become a cause of trouble.

In other cases, some systems have been used without applying security patch since their platform or applications are old. Flowering cloud computing could also have the same issues.

The following is some important points to avoid such troubles.

- When outsourcing the system development, consider well about non-functional requirements (system qualities).
- Making sure that vulnerability management of the system and its components are available.
- When outsourcing the system operation, clarify to what extent the outsourcee is liable and responsible for vulnerability response in the contract.

〈Statistics for the Year 2010〉

In accordance with the Information Security Early Warning Partnership, IPA collects report on vulnerability in products and systems. As a part of it, IPA notifies the website operators of their vulnerability reported by the public and urges to fix it.

However, vulnerabilities in many websites are still unfixed regardless of vulnerability notification. Among the vulnerabilities being handled by IPA, there are 218 websites that have been left untreated for more than 2 years as of December 2010. Among those websites' vulnerability, 111 are cross-site scripting, (51%), 64 are SQL injection (29%), 22 are publication of wrong files (10%) and 21 are for other vulnerability and causes (10%). Even high-risk SQL injection vulnerability is left neglected. The operators of those unfixed websites often mention that they cannot reach the vendors or the programmers with necessary skill are not available at the vendors, beside the lack of development cost.

In the case of Okazaki City Library, its website became temporarily unavailable due to its implementation flaw. The website operator and development vendor's inadequate response expanded the impact of the incident and allowed it to grow into a social issue.

References

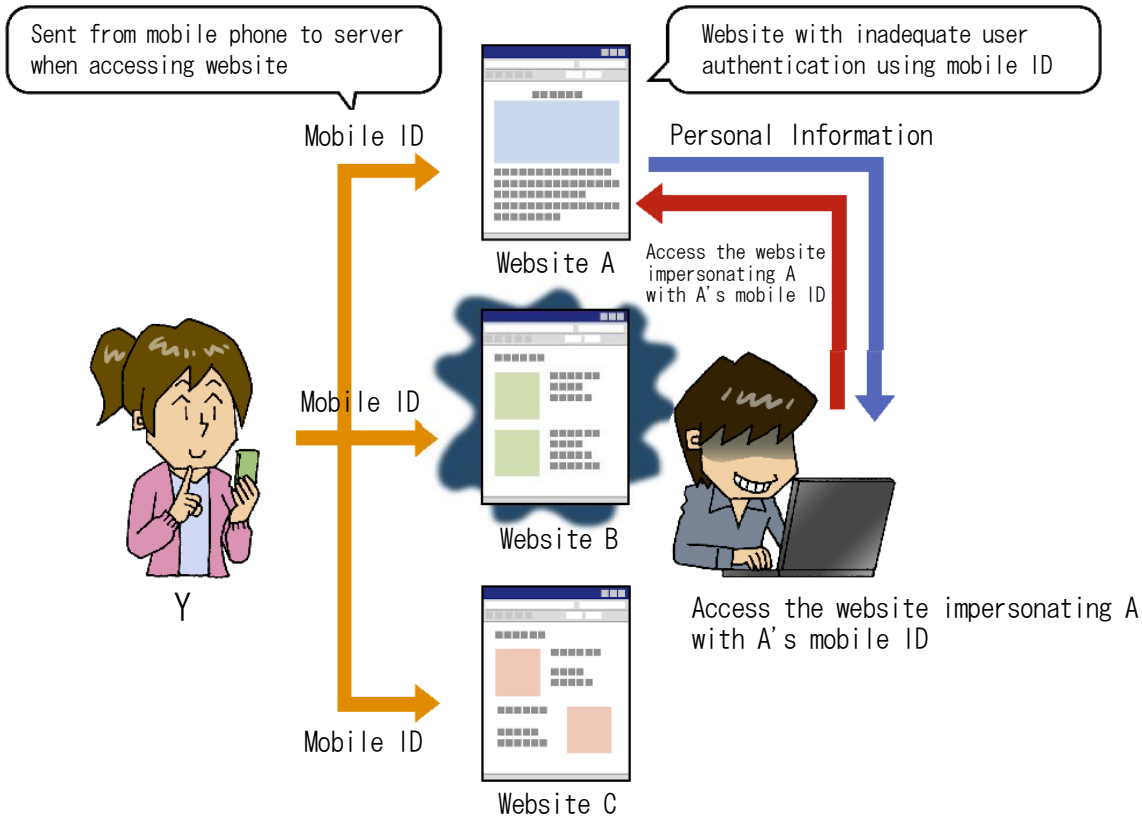
IPA: http://sec.ipa.go.jp/reports/20100416.html (in Japanese)

IPA: http://www.ipa.go.jp/security/fy20/reports/sme-guide/index.html (in Japanese)

IPA: Reporting Status of Vulnerability-related Information about Software Products and Websites: 4th Quarter of 2010 (October – December) http://www.ipa.go.jp/security/vuln/report/vuln2010q4-e.pdf

Okazaki City Library: http://www.library.okazaki.aichi.jp/tosho/about/files/20110225.html (in Japanese)

[7th] Security issues in mobile phone websites



There are mobile phone websites that use the information specific to each mobile phone. Some of the websites that have been built based on the know-hows unique to mobile phones may be unsecure.

<Threats>

Traditional mobile phones, excluding smartphones, lack web browser functions compared to PCs. For example, web browsers in some models do not support cookies. Considering the existence of those models, implementing a specific web function into mobile phones in the same way as into PCs is not possible.

Because of that, some websites use a mobile phone's identifier (hereafter called the "mobile ID") related to the mobile phone service user or the device for user authentication to access mobile websites or session management. However, this implementation method (hereafter called the "easy login") is basically valid only when the requirements below are met. Otherwise, it may cause security problems.

(A) Access to the mobile phone websites is made only through the mobile phone and access from other type of devices is distinguishable by the website.

(B) The mobile phone user cannot alter the HTTP header in the HTTP request.

For example, access control with the source IP address can be performed to meet the requirement (A), but if implementation is wrong, ID spoofing can be done in the following way. Let's say that the website A has a problem with IP address-base access control.

(1) Y accesses the website A and B.
(2) Y sets up for the easy login service at the website A.
(3) The administrator of the website B accesses the website A from his or her PC using Y's mobile ID.

When accessing multiple websites from a single mobile phone, the same mobile ID is sent to all of them. For that, the mobile ID is not a secret information. If a website's authentication mechanism solely depends on the mobile ID, a third party can easily spoof it. As mentioned before, some of the websites that have been built based on the know-hows unique to mobile phones may be unsecure.

Most new models are advanced and support cookies or even JavaScript. This requires the mobile phone websites to implement the same level of security as those for PCs. The mobile phone website developers should be aware of the changes in technological advancement of mobile phone, update their know-hows and build secure mobile phone websites.

<Impact>

Through ID spoofing, personal information may be leaked or data may be altered. If personal information is leaked, even though the direct victims are the affected users, the website operators will suffer indirect damage by losing customer confidence.

The easy login is an authentication method available for the mobile phones that do not support cookies, but it can be very vulnerable in some environment. Defect in user authentication can directly affect the safety of personal information. Thus, an authentication method must be considered carefully. It is desirable to adopt the same authentication methods as PCs, such as password and cookies. If mobile phone service providers offer the secure authentication methods, use them.

〈Statistics for the Year 2010〉

In 2010, some security alerts concerning the flaw in the easy login implementation were issued and the actual incidents occurred where a third party spoofed other user and succeeded to log in.

OpenPNE, a social network service development software, had a flaw in the easy login implementation. Its access control with IP address had a security flaw and allowed a third party to log in from PC as other user.

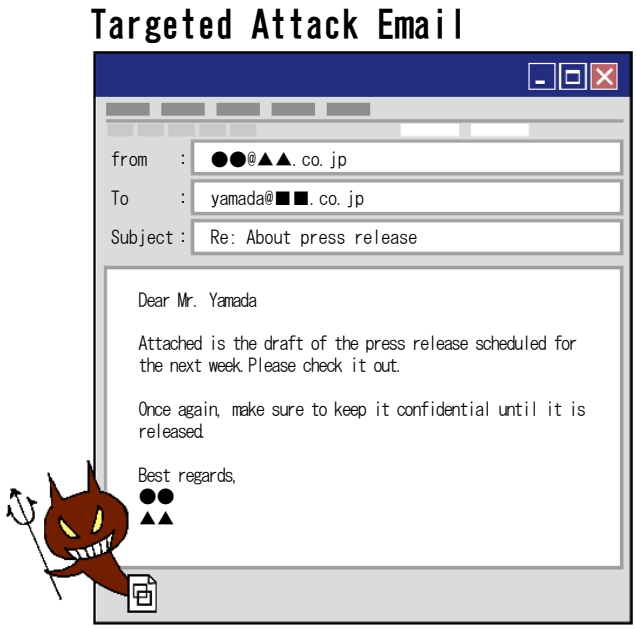
Also, the Kuroneko Members Web Service had the same easy login implementation issue and a third party could log into the service as other user under some specific conditions.

Both services properly notified the users and the issues have been fixed.

References

IPA: Security Alert for Vulnerability in OpenPNE
http://www.ipa.go.jp/security/english/vuln/201003_openpne_en.html
OpenPNE: http://www.openpne.jp/archives/4612/ (in Japanese)
Yamato Transport: http://www.kuronekoyamato.co.jp/info/info_101025.html (in Japanese)

[8th] Hard-to-detect targeted attacks



Targeted attack is an attacking technique that targets specific persons or organizations to steal information by impersonating people the targets know or their business acquaintance and sending an email that is attached with a virus-infected file or contains a link to a malicious website.

<Threats>

Most of targeted attacks infect the target's PC by sending emails that attract the interest of target persons or organizations and leading them to open the attachment or click the link within the email body. The virus then begins to steal information stored in the targets' PC and cause harm to other systems via network. The virus distributed through email lies hidden within the PC, acting like a spy and downloading other viruses via network.

Targeted attacks first emerged in 2005. It has been s several years but it is still difficult to take effective countermeasures unlike other attacking methods. Behind this problem is that the attacks use social engineering that exploit human psychology and often succeed to deceive the victims. For example, if the email shown in the figure above is sent under the name of an real business acquaintance, it would be difficult to tell whether the email is a targeted attack or genuine email. A skeptic person may suspect its authenticity but most people more likely open the file considering it is an important email from their business partners. As such, the characteristic of targeted attack is that it is difficult to tell the authenticity of received email and cannot detect the attacks as a result.

In addition, since targeted attacks target very specific persons and organizations, information about the virus used in the attacks tends not to circulate publicly. That delays the provision of the pattern file for the virus, making the antivirus software unable to detect the virus sooner.

<Impact>

In targeted attacks, the targets change depending on the attacker's aim. Thus, their impact

also change depending on the types of information stolen or systems destroyed.

In the case of an oil company, the information about oil drill sites was stolen by the targeted attack. Since the information that was kept secret within the company was stolen and it would affect the company's future business.

In the last year's popular cyber attack against Google, the targeted attack was also used. According to Google, the attack's aim was to gain access to the Gmail accounts of Chinese civil-rights activists. Needless to say, if a third party obtains the access to the email account, the contents of email exchanges are free to see for the third party, which is an incident of information leakage.

〈Statistics for the Year 2010〉

Because the targeted attacks that target the central government functions are more likely featured in the news media, companies may feel they are out of the target scope. According to a report from an antivirus vendor, however, the vendor observed that one out of 22.6 companies have received targeted attack emails. Whether the actual damage was done or not is unknown, but there is a chance that the companies could not detect the attacks or their damage.

In 2010, many targeted attacks were reported both in Japan and other countries. A targeted attack that was widely covered in the news media in 2010 would be the one against the Ministry of Economy, Trade and Industry. According to news media, the targeted attack email was sent to the ministry personnel and about 20 of them opened it. The email was about the discussions made in a meeting and the source IP address was closely imitated that of the personnel who took care of the meeting. This fact suggests that the targeted attack is tactful, making a trapping email so believable that the targets do not suspect by using the information shared between the sender and receiver.

In other countries, besides oil company and Google, targeted attacks have been used in the attacks against the U.S. military contractors, and are becoming a common practice to breach information systems.

The organizations should be aware that the attackers' target will change depending on their aim and make sure to apply security patch to the software applications in use, update the pattern file for the antivirus software and block unnecessary ports used in communication from within the organization to the outside.

References

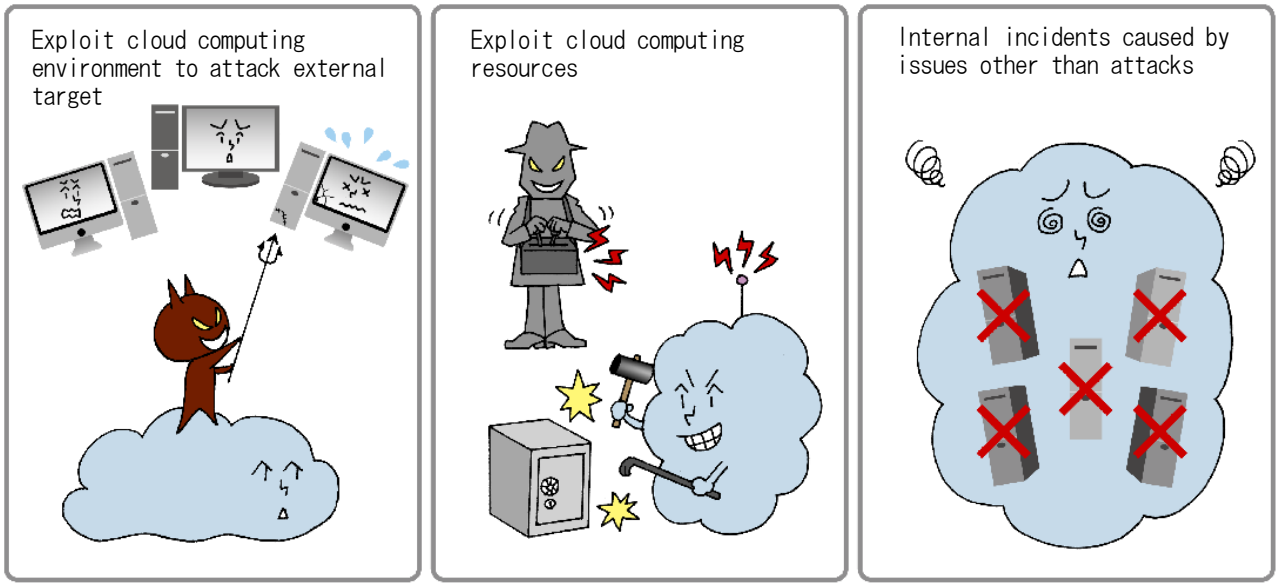
CSMonitor.com: US oil industry hit by cyberattacks: Was China involved?

http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved

Itmedia: http://www.itmedia.co.jp/enterprise/articles/1001/14/news085.html (in Japanese)

PCOnline: http://pc.nikkeibp.co.jp/article/news/20101101/1028271/ (in Japanese)

[9th] Security issues in cloud computing



The IT services using cloud computing (hereafter called the “cloud”) have become popular as a new business model in the last couple of years and are spreading among the companies. On the other hand, the cloud’s security issues have become slowly apparent as well and the incidents and new threats in the cloud environment have been reported.

<Threats>

According to IPA’s Study Group Report on Infrastructure for Cloud Computing Society, 5 attack patterns are addressed as threats in the cloud.

(1) Attack from the outside to the cloud environment
(2) Attack from within the cloud environment to other users
(3) Attack that uses the cloud as a stepping stone
(4) Abuse of the cloud’s computing power (such as password and cryptography decoding)
(5) Incidents caused by issues other than attack (such as power outage, system failure)

Also, Top Threats to Cloud Computing V1.0 by CSA (Cloud Security Alliance) addresses the following 7 points as the cloud’s security issues.

(1) Abuse and Nefarious Use of Cloud Computing
(2) Insecure Interfaces and APIs
(3) Malicious Insiders
(4) Shared Technology Issues
(5) Data Loss or Leakage
(6) Account or Service Hijacking
(7) Unknown Risk Profile

Various threats and security issues for the cloud environment have been pointed out and some have caused the actual incidents. When using the cloud, consider to what extent the organization will entrust its information processing and data management to the cloud in advance.

<Impact>

If threats for the cloud become real, both the cloud service providers and users are affected.

For the cloud service providers, they need to stop the services. They may also suffer damage to customer confidence due to the fact that their cloud has been compromised.

For the cloud service users, they may suffer leakage of information entrusted to the cloud, violation of laws such as the Act concerning Protection of Personal Information, and impact on the business continuity. The users also need to understand that they do not have full control over the cloud services. For example, when an information leakage occurs through the cloud service, depending on the services, they may not be able to obtain information necessary to investigate the incident such as logs and firewall policies. When using the cloud services, it is important to clarify the SLA (Service Level Agreement) and OLA (Operation Level Agreement) between the user and the service provider.

<Statistics for the Year 2010>

In 2010, several incidents concerning the cloud were reported.

In April 2010, the password brute force attack that targeted the SIP (Session Initiation Protocol) servers and clients used in the Internet telephone service of the Amazon EC2 operated by Amazon was confirmed as an example of the cloud abuse (or used as a stepping stone). Besides that, the observation suggests that the cloud environments were also exploited as the source address of the spam mails.

The failures due to power outage have happened for various cloud services such as Amazon, Microsoft and Apple's. Some cloud service providers have diversified the risks by diversifying the operation sites to mitigate the impact on the users.

Other than the failures, there was a case where email data were leaked for about 2 hours at Microsoft's BPOS (Business Productivity Online Suite) service.

References

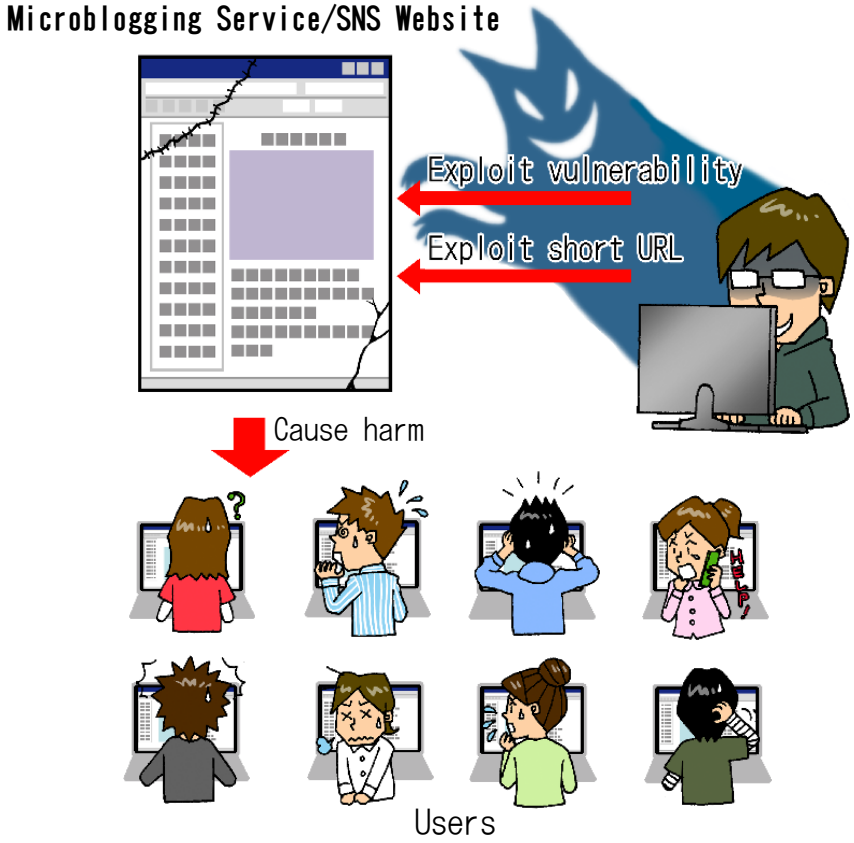
VoIP Tech Chat: Amazon EC2 SIP Brute Force Attacks on Rise

http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/

internet.com K.K. (Japan): http://japan.internet.com/webtech/20110113/11.html (in Japanese)

Impress: http://internet.watch.impress.co.jp/docs/news/20101104_404541.html (in Japanese)

[10th] Attacks Targeting Users of Microblogging Service and SNS



The users of the microblogging service and SNS (Social Networking Service) are exponentially increasing. The attacks targeting them are also increasing commensurately.

<Threats>

There are the microblogginh services like Twitter and AmebaNow, and SNS like mixi and Facebook. The characteristics of the services on these websites are that the users can easily send out their current doings and ideas to the Internet and that they can interact with those who have the same interests and ideas. Some of the services have tens of millions of users. It is an information environment with a massive number of users where people can easily exchange information and communicate with friends and strangers alike.

At the same time, the attacks that exploit these characteristics of the microblogging services and SNS to rip off their users and infect their PC with viruses have emerged.

For example, an attacker tweets something that attracts the interest of the Twitter users and leads them to an external website to infect their PC. Sometimes, the “short URL” service, which allows to shorten a long URL string, is used. It takes advantage of a nature of the short URL that the users do not know to what website they are redirected until they actually crick it.

The attacker also sends out false information or makes the users do things they do not intend to exploiting vulnerability in websites. Cross-site scripting and cross-site request forgery are often-used vulnerabilities in real attacks. Besides

them, common web application vulnerabilities like SQL injection and directory traversal can be used as well.

The website operators must implement vulnerability countermeasures for web applications.

<Impact>

The direct harm comes to the users of the microblogging services and SNS. The users may leak information due to virus infection or notice that slandering comments are posted to some websites under their name without their knowledge. To prevent these from happening, the users should keep their operating systems and software applications up to date, and use a tool or service that displays a short URL in its original form to ensure the URL's authenticity. However, there are little things for the users to do about the problems that exploit vulnerability in websites. The website operators need to implement security measures to protect the users from harm.

The website operators should try hard to keep their website vulnerability-free from its design phase and establish an operation framework to respond in case vulnerability is found.

〈Statistics for the Year 2010〉

In 2010, there were an incident at pixiv that exploited cross-site request forgery and another at Twitter that exploited cross-site scripting.

In February 2010, a cross-site request forgery vulnerability on pixiv, an SNS service that specialized in posting and viewing illustrations, was exploited. As a result, some users found that slandering comments were posted to other user's work under their name without their knowledge.

In September 2010, a cross-site scripting vulnerability on Twitter, a microblogging service, was exploited. In this incident, some users found that tweets were made or done under their name without their knowledge or the display on their screen was corrupted.

In December 201, there was an attack that exploited the short URL and led the Twitter users to the external websites to infect their PC with viruses.

References

IPA: http://www.ipa.go.jp/security/txt/2010/05outline.html (in Japanese)

Twitter Blog: All about the "onMouseOver" incident

http://blog.twitter.com/2010/09/all-about-onmouseover-incident.html

pixiv Developer's Blog: http://dev.pixiv.net/archives/1026973.html (in Japanese)

CNET Japan: http://japan.cnet.com/news/sec/20423830/ (in Japanese)

Chapter 3 Countermeasures

As mentioned in Chapter 1, once a security incident happens, it will have a huge impact not only on the information systems but also on the organization's brand image and business. Since lack of security may result in unintentionally participating in the attacks against others, ensuring security can be a part of the organization's social responsibility. This chapter explains the points and approaches towards information security based on 10 major security threats addressed in Chapter 2.

3.1 Classification of Threats

When implementing security measures, the organization needs to understand the business impact of the possible security incidents and decide the countermeasures to implement in the light of the current security controls. This year's 10 major security threats can be divided into 3 categories.

The following sections explain the point of view and approach towards each of 3 categories: threats of information leakage, threats of external attacks and threats caused by design, implementation or operation of information system.

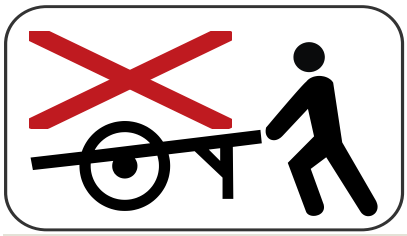
10 Major Security Threats		Classification		
		Information Leakage	External Attacks	System Issues
1st	Information leakage caused by "people"	○		
2nd	Unstoppable! Attacks via websites		○	
3rd	Attacks exploiting vulnerability in standard softwares		○	
4th	Attacks targeting smartphones on the rise		○	○
5th	Advanced Persistent Threats (APT) that combines multiple attacking methods		○	
6th	Troubles caused by inadequate security measures			○
7th	Security issues in mobile phone websites		○	○
8th	Hard-to-detect targeted attacks		○	
9th	Security issues in cloud computing	○	○	
10th	Attacks targeting users of microblogging service and SNS		○	

Threats of Information Leakage (Information Leakage)
Threats where information held by an organization (e.g. confidential Information, personal information) is exposed due to loss or theft.

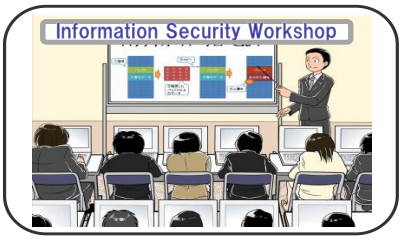
Threats of External Attacks (External Attacks)
Attacks that threaten the information system via network (mainly the Internet) or through electronic media.

Threats caused by design, implementation or operation of information system (System Issues)
Issues caused by inadequate security measures and handling of security problems for ordered/developed applications.

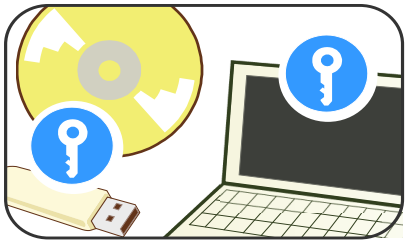
3.2 Countermeasure against Threats of Information Leakage



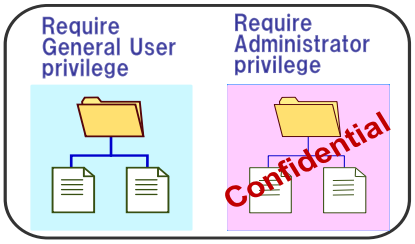
Forbid employee from taking information out of the premises



Enforce security training



Enforce encryption of data storage media



Implement proper access control

Since information leakage can occur through various channels, it is necessary to implement the countermeasures to the possible, probable risks.

<Points of Countermeasures>

Information leakage is caused by the insider's human error or intentional acts or external attacks. The basic points of the countermeasures are to identify information assets, manage their operation through establishment of rules and provision of security education, and implement well-planned countermeasures taking into account the risk mitigation and deterrent effect of the countermeasures.

Examples are listed below.

<Examples of Countermeasures>

(1) Security Operation Measures

1. Establish information handling rules/penalties
2. Implement account and privileges management
3. Provide security education
4. Establish an operation framework and procedures to respond to the possible incidents

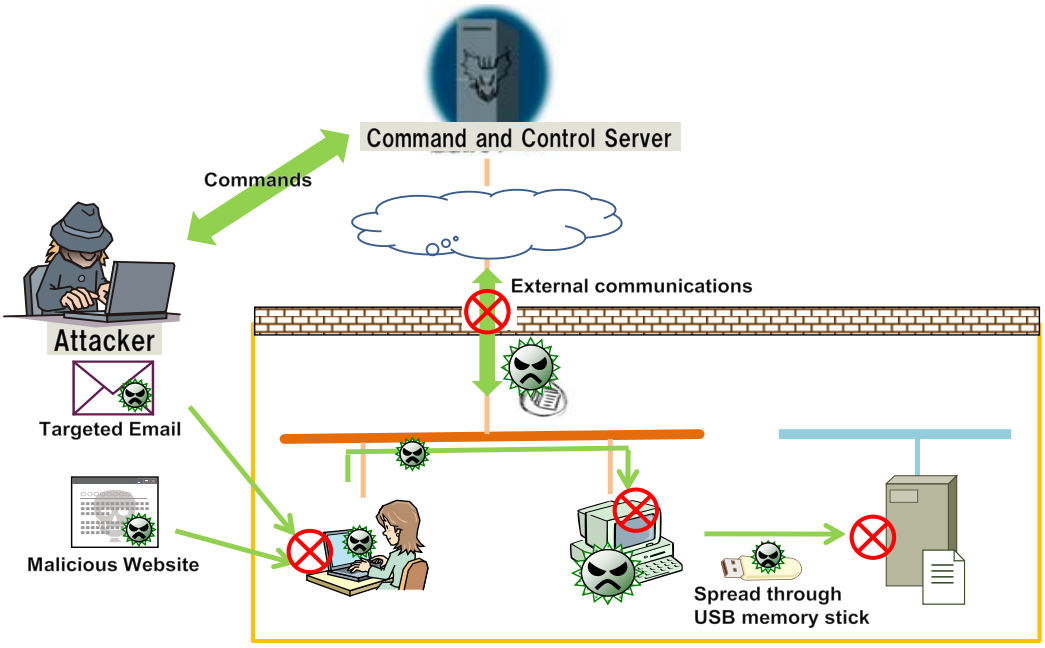
(2) Technical Measures

1. Fortify network design
2. Authenticate users and implement access control
3. Encrypt data being taken out from the premises and important data
4. Record access log

<In Case of the Cloud>

When entrusting data to the cloud environment, the data may be stored overseas depending on the cloud service providers. In that case, the legal issues and data insurance policy in case of data leakage or loss will be important from the aspect of business continuity. Thus, it is necessary to clarify the contract details with the cloud service provider in advance and select the data to entrust with the cloud service to mitigate the risks.

3.3 Countermeasures against Threats of External Attacks



A characteristic of the threats of external attacks is that a third party performs an attack against other's information system with clear malicious intent. To prevent the attacks, the countermeasures need to neutralize the attacks knowing what the attacker is planning. Here, the countermeasures against "5th :Advanced Persistent Threats (APT)" are explained.

<Points of Countermeasures>

The characteristics of the APT are that the PC is infected with virus through vulnerability exploitation or ingenious social engineering and the virus communicates with external command and control servers to grow and inflicts damage such as information theft and system destruction.

The most effective countermeasure against the second phase of the attack is to focus on the network design and implement the measures that block the unauthorized access from the outside and malicious communications between the viruses inside the network and the command and control servers on the outside.

Since the APT exploits vulnerability and uses masterly social engineering, making sure to fix vulnerabilities and educating the users not to open email attachments or click links lightly are also recommended.

<Examples of Countermeasures>

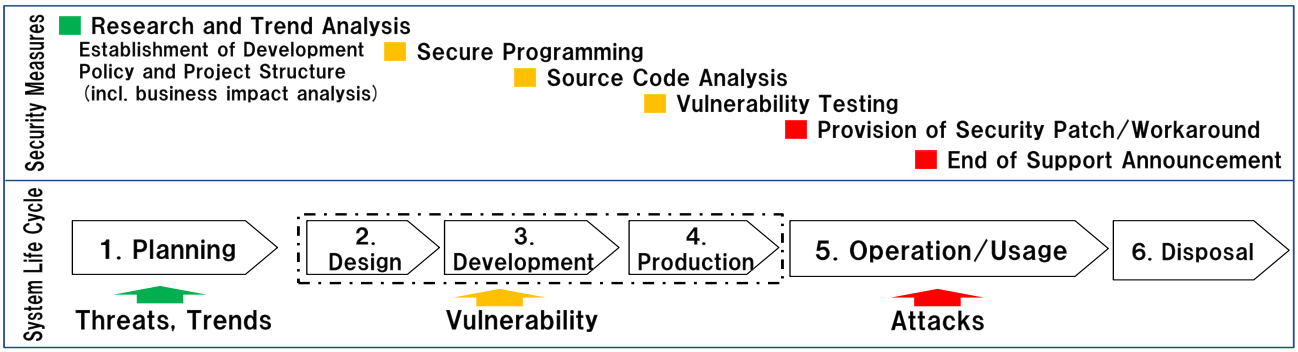
(1) Fortify System / Network Design

1. Network Design Measures
   - Separate the critical network segments from other segments
   - Separate the network segment with switches or other network devices
   - Employ authentication proxy server
   - Block P2P communications with the outside
2. Antivirus Software Deployment

(2) Security Operational Measures

1. Manage vulnerability in clients and servers
2. Provide security education
3. Monitor communications

3.4 Countermeasures against Threats Caused by Design, Implementation or Operation of Information system



Once developed and released, the information systems and software applications will be used for a long time. From the stand point of security, they are exposed to vulnerabilities and new threats all the time. Thus, throughout their lifecycle from the planning, design and development, and operational phase, it is necessary to make sure that no known vulnerabilities are left in the software in the development phase and establish an operation framework to respond, should something happen. Points and countermeasures at each phase are explained below.

<Points of Countermeasures>

・At planning, Design, Development and Production Phase

At the planning and design phase, expected threats for the software should be listed up and the security functions to counter them should be designed. At the development and production phase, it is necessary to put secure programming in practice and perform vulnerability testing to improve the security level of the software.

・At Operation Phase

Attacks targeting software applications are constantly advancing and if new vulnerabilities or attacking methods are discovered, the applications that were safe yesterday may become vulnerable tomorrow. For that, if a vulnerability is found after the release, the vendor should provide a security patch or work around and notify the users to prevent them from harm. If it is a publically available system, the vendor should fix it to prevent the damage from spreading to the users. If the system was developed by a third party (outsourcee), it is important to clarify to what extent the outsourcee is liable and responsible for vulnerable response in the contract.

・At End of Support

When ending the support of a product, the vendor should release an end of support announcement in advance and make the users know that security patches will be no longer available after the date. If there are recommendations for those who continue to use the end of support product, it is desirable to announce them as well.

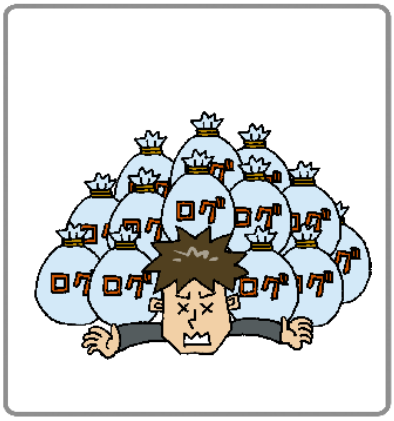
<Examples of Countermeasures>

1. Analyze threats and decide what measures to implement (at planning)
2. Put secure programming in practice
3. Perform source code review
4. Perform vulnerability testing
5. Provide security patch / work around
6. Announce end of support

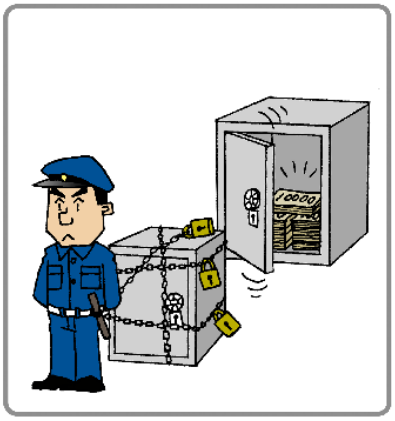
3.5 Points of Consideration

・Examples of Ineffective Security Measures

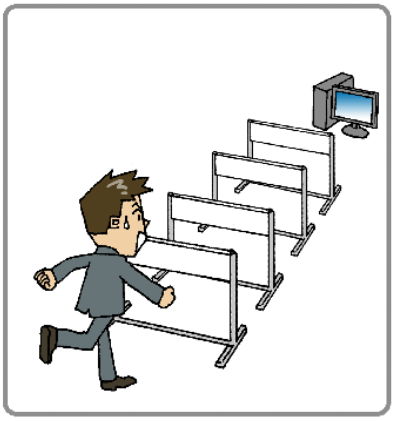
Lack of Staff



Incongruous Security Implementation and Operation



Impractical Security Rules

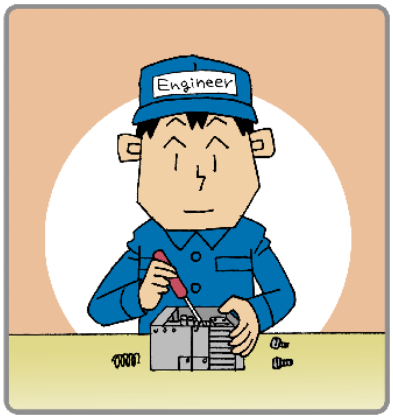


Pictures above are examples where the security measures are rendered ineffective.

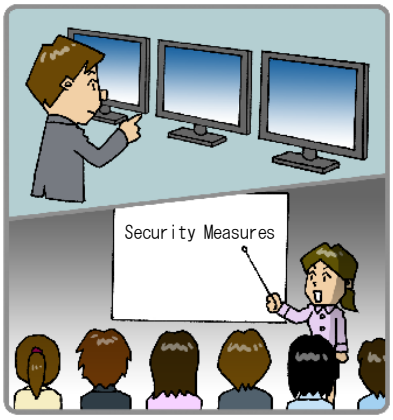
Even if the fancy rules are enforced and the best tools are employed but the human resource and an operation framework to operate the rules and tools are inadequate, the measures do not work effectively. When considering the security measures, it is necessary to come up with efficient and effective measures taking into account the organization's characteristics, operation framework and available resources.

Efficient Security Measures

Secure Design and Development



Continuous Operation



Security measures should be planned for throughout the information system's lifecycle from the planning phase. During the lifecycle from planning to operation, usually multiple venders are involved. In that case, the person in charge for the development and management and chain of command should be clarified when implementing security measures.

[Appendix 1] 10 Major Security Threats Relationships

Appendix Table 1 shows the target people who need to understand the 10 major security threats addressed in Chapter 2.

The business's dependency on information technology has increased ever continuously and an information system incident is now a risk that threatens even the continuity of the business. In fact, the loss caused by recent incidents of information leakage and website hacking is getting higher. To prevent those incidents from happening, it is critical to implement the adequate security measures.

The management executives need to show the organization's security policy and action plan to the inside and outside the organization, and the systems administrators need to manage the systems and accounts following the organization's security policy and action plan. Also, the system developers need to understand known vulnerabilities and prevent them from lurking in the software.

IPA hopes this report will help to understand the current circumstance surrounding information security and improve security threats.

Appendix Table 1: Those Who Need to Understand 10 Major Security Threats

10 Major Security Threats		Those Who Need to Understand the Threats		
		Management Executives	System Administrators	System Developers
1st	Information leakage caused by "people"	++	+	
2nd	Unstoppable! Attacks via websites		++	+
3rd	Attacks exploiting vulnerability in standard softwares		++	+
4th	Attacks targeting smartphones on the rise		+	++
5th	Advanced Persistent Threats (APT) that combines multiple attacking methods	++	+	
6th	Troubles caused by inadequate security measures	+		++
7th	Security issues in mobile phone websites		+	++
8th	Hard-to-detect targeted attacks	++	+	
9th	Security issues in cloud computing	++	+	+
10th	Attacks targeting users of microblogging service and SNS			++

++: Especially important to understand the threats　　+: Important to understand the threats

[Appendix 2] Change in 10 Major Security Threats

The Appendix Table 2 compares this year's top 10 threats addressed in Chapter 2 with past top 10 threats.

For the year 2011, 5 new threats that were not in top 10 in past years ranked in, such as attacks targeting smartphones and the SNS users. Information leakage and targeted attacks are making regular appearance on the top 10 list.

Appendix Table 2. Change in 10 Major Security Threats

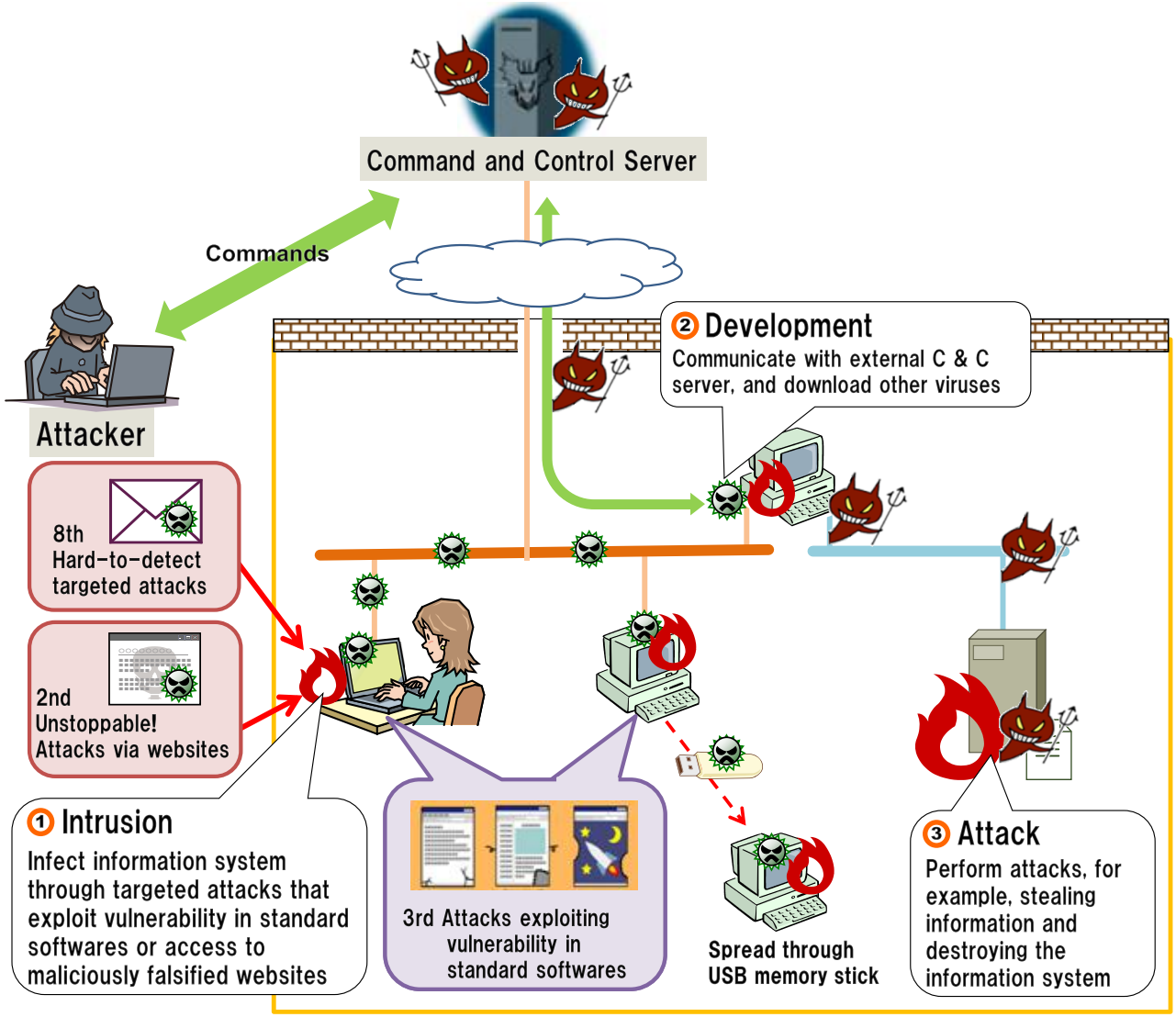
10 Major Security Threats in 2010		Ranking in 2009	Ranking in 2008	Ranking in 2007	Ranking in 2006
1st	Information leakage caused by "people"	5	5	3	7
2nd	Unstoppable! Attacks via websites	1	2	5	9
3rd	Attacks exploiting vulnerability in standard softwares	2	—	8	—
4th*	Attacks targeting smartphones on the rise	—	—	—	—
5th*	Advanced Persistent Threats (APT) that combines multiple attacking methods	—	—	—	—
6th*	Troubles caused by inadequate security measures	—	—	—	—
7th*	Security issues in mobile phone websites	—	—	—	—
8th	Hard-to-detect targeted attacks	6	3	4	2
9th	Security issues in cloud computing	9	—	—	—
10th*	Attacks targeting users of microblogging service and SNS	—	—	—	—

*：Threats that are newly ranked in IPA's 10 Major Security Threats

[Appendix 3] Association between 10 Major Threats and APT

The following figure shows the threats associated with the 5th threat in the 10 major security threats “Advanced Persistent Threats (APT) That Combines Multiple Attacking Methods” and complements its explanation in Chapter 2.

Here, a term “APT” is used as a collective name for attacks that aim to steal an organization’s sensitive information and destroy information systems. One of their characteristics is that they fit existing attacking methods together intricately and sophisticatedly, and use attacks like “the 2nd - Unstoppable! Attacks through Websites”, “the 3rd - Attacks Exploiting Vulnerability in Standard Softwares” and “the 8th - Hard-to-Detect Targeted Attacks”.



Appendix Figure 1.

Association among attacks in "5th: Advanced Persistent Threats (APT) that combine multiple attacks"

[Produced and Copyrighted by] Information-technology Promoting Agency, Japan (IPA)

[Editor] Hideaki Kobayashi
Chisato Konno

[Advisor] 10 Major Security Threats Committee

[Author] Shunsuke Taniguchi
Masashi Ohmori

2011 Edition

10 Major Security Threats
- Attacks are evolving... Is your security good enough? -

March 24, 2011 The First Edition

[Publication] Information-technology Promotion Agency

16F, Bunkyo Green Court Center Office,
2-28-8, Honkomagome, Bunkyo-ku,
Tokyo, 113-6591, Japan

http://www.ipa.go.jp/

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.

Unauthorized Access

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

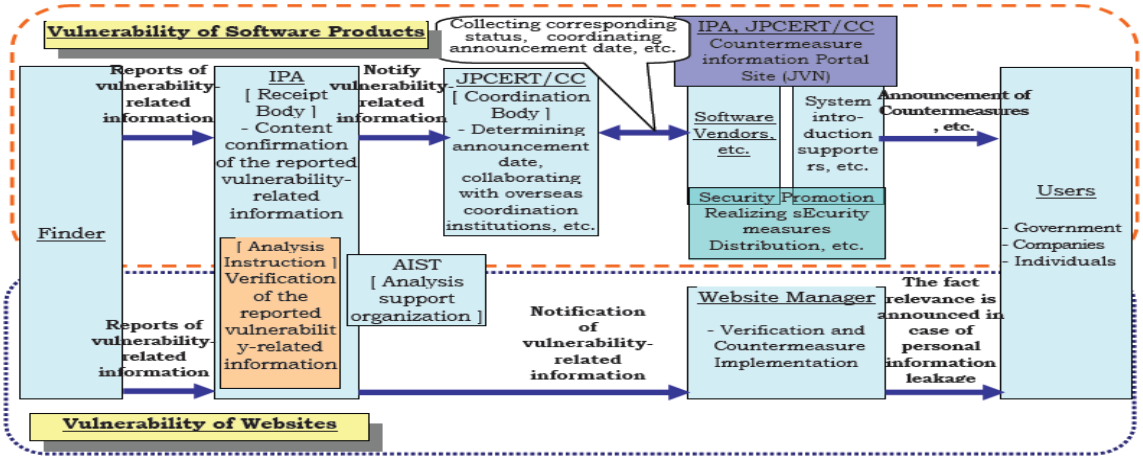
Software Vulnerability and Related Information

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.

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