For the Year 2012

## **10 Major Security Threats**

∼ Changing and Growing Threats! ∼



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

March 2012

### Contents

INTRODUCTION
CHAPTER 1. CHANGES IN ENVIRONMENT SURROUNDING INFORMATION SECURITY
1.1. Changes in Attack Techniques5
1.2. Changes in System Environment7
1.3. Changes in the Whole Figure Surrounding Information Security
1.4. Changes in Impact When Attacked10
1.5. Current Situation of Security and Future Challenges
CHAPTER 2. 10 MAJOR SECURITY THREATS FOR THE YEAR 2012
1 st APT Attacks [Countermeasure Priority: 1st]14
2 nd Unpredictable Disasters [Countermeasure Priority: 6th] 17
3 rd Hacktivist Attacks [Countermeasure Priority: 8th]20
4 th Attacks Targeting Unpatched Client Software [Countermeasure Priority: 2nd]
5 th Website Attacks [Countermeasure Priority: 3rd]25
6 th Attacks Targeting Smartphones and Tablets [Countermeasure Priority 5th]27
7 th Danger in Digital Certificates [Countermeasure Priority: 14th]
8 th Internal Threats [Countermeasure Priority: 7th]
9 th Reuse of the Same Credentials [Countermeasure Priority: 4th]
10 th Privacy Invasion [Countermeasure Priority 12th]
Threats Preferentially Dealt With40
CHAPTER 3. THREATS AGAINST WHICH TAKING ACTION IS CRITICAL IN THE FUTURE
3.1. Attacks Targeting Social Infrastructure (Critical Infrastructure)
3.2. Threats in Using Cloud Computing42
3.3. Management of Smartphones by the Businesses43
[APPENDIX] UNSELECTED 10 MAJOR SECURITY THREATS CANDIDATES

#### Introduction

This report summarized 10 major security threats in 2011. The report was produced by the 10 Major Security Threats Committee, which consists of those involved in the Information Security Early Warning Partnership, information security researchers and IT staff. IPA hopes this report will help the readers to understand the current circumstance surrounding information security and improve security measures.

#### **Organization of this Report**

This repost consists of three chapters.

Chapter 1 looks at and explains the changes in the environment and threats surrounding information systems in recent years, focusing on the following four aspects: attack techniques, system environment, attack/defense model, and impact when attacked.

countermeasures for the 10 most socially influential threats in 2011 selected via voting by the 10 Major Security Threats Committee members. The 10 major security threats for the year 2012 ranked by the Committee are listed in Table 1.

Chapter 3 explains the overview and trend of the threats that have caused little damage so far but may become notable in the future.

Chapter 2 explains the impact of and

Table 1. To Major Security Threats for the fear 2012					
Rank	Title				
1st	Advance Persistent Threat (APT) Attacks				
2nd	Unpredictable Disasters				
3rd	Hacktivist Attacks				
4th	Attacks Targeting Unpatched Client Software				
5th	Website Attacks				
6th	Attacks Targeting Smartphones and Tablets				
7th	Danger in Digital Certificates				
8th	Internal Threats				
9th	Reuse of the Same Credential				
10th	Privacy Invasion				

 Table 1. 10 Major Security Threats for the Year 2012

#### 10 Major Security Threats Classification Map

In 2011, we witnessed that some threats, which had caused little harm previously in Japan and only the possibility of attack had been suggested, began to show that they are capable of causing a real harm.

Adding such aspects, 10 Major Security Threats for the Year 2012 classified the threats into two categories: "continuous old threats" and "growing new threats". The outcome is shown in Figure 1.

"Continuous old threats" have caused harm since well before 2011 and they are the types of threats we need to keep dealing with.

"Growing new threats" is those that have caused actual harm in 2011 for the first time and the need for countermeasures was recognized.



Figure 1 10 Major Security Threat Classification

## Chapter 1. Changes in Environment Surrounding Information Security



Figure above shows the changes in the ranks of the threats selected for the "10 Major Security Threats" in last six years. As you can see, the threats related to the new devices or the attacks that produced lots of victims ranked high. On the other hand, it cannot be ignored that classic threats, such as targeted attacks, website attacks, attacks that target client software and information leak, as well. It implies that although they have been recognized as threats for a long time, not much progress has been made in solving them or it is very difficult to solve. As for those old threats that have existed for some time, it is important to secure budget on the ground that they will come every year, just like typhoons, and be prepared to respond promptly when vulnerability is found.

On the other hand, what a certain threat means to the organization changes depending on its business/work model, changes in the system environment or attacker's intention and objectives. In 2011, things like what information security means, changes in system and service environment, seemed to have become clear. For example. changes and diversification in attack techniques. changes in the system environment as

represented by the spread of smart devices and cloud computing, and the impact on an organization caused by security incidents.

In Chapter 1, changes in the system environment will be explained focusing on

the four aspects: Changes in Attack Techniques, Changes in System Environment", Changes in the Whole Figure Surrounding Information Security, and Changes in Impact When Attacked.



#### **1.1.Changes in Attack Techniques**

In the past, attackers performed web page tampering and unauthorized access to show off their skills or just to make fun of it. In recent years, however, attacks that employ the techniques to deceive people psychologically or strategically to thwart security measures have been emerged. Four characteristics of recent attacks are listed below:

#### Diverse, multi-phased attacks

In the past, a vulnerability is exploited by a certain same attack in most cases. In recent years, however, attacks have become multi-phased, like accessing the system, bypassing authentication, obtaining root privileges and installing malware. System administrators are required to implement not only a single countermeasure but a comprehensive set of measures including vulnerability management and system configuration review to solve configuration error.

 Attacks exploiting legitimate websites
 Attacks against websites are still a big threat for website operators. Until a few years ago, IT users were lured to fake websites, such as phishing websites, and fell into a victim in most cases. In these days, however, attacks where IT users get infected with virus via legitimate websites, are on the rise, using legitimate website as a stepping stone to spread infection. For IT users, it is a legitimate website after all and they access it without knowing that the trap is waiting for them since there is no reason to doubt. As a result, it looks as if the legitimate website is attacking its visitors, which makes the operator a victimizer and shakes up the operation of the website operation as well.

#### Abuse of social engineering

As represented by targeted email attacks, attacks that target very specific people and use social engineering techniques to manipulate people psychologically are on the rise. By being tricked by the attacker to open an attachment file or click URLs in email, IT users get infected with virus or data is stolen. Since these attacks target specific organizations or individuals, attack information is often not shared with others. Thus, they are not known and detected by antivirus software. For the organization, in addition to the traditional security measures, behavioral control measures such as user education is getting more important. Under the circumstances, there seems to be a change in the user education program provided by the organizations. Some train their employees not to be tricked by the attacker, such as prohibiting to open suspicious emails.

• Emergence of strategic attack techniques

Since 2010, a new type of attack called advanced persistent threat (APT) has been emerged mainly abroad. An APT attack targets specific organizations, tactically combines social engineering and existing techniques, and changes its attacking techniques depending on the situations. The characteristic of this attack is that it is a tactical attack where a virus that has breached and lives inside the system changes its attacking techniques as communicating with the attacker outside the network depending on the situations. For that. the implemented security measures can be bypassed and sensitive information is stolen from the victim organizations.



#### **1.2. Changes in System Environment**

In last few years, the system environments have gone under major changes. New devices emerge, control systems become more and more open, and as seen with cloud computing, the service structure is also changing - which led to changes in aspects of the existing threats and emergence of new threats.

#### • Emergence of new device

Smartphones become prevalent and Internet-connected home appliances are increasing. By connecting to the Internet, the devices are exposed to the threats of being attacked remotely. Thus they are required to implement security measures just like information system devices. Especially, it can be said that smartphones are suspicious to attacks compared to the traditional cell phones due to their open specifications. In addition, they handle personal information that is possible to identify individuals, such as, address book and emails, making the damage severer.

 Increased openness of control systems

A control system, such as one at a factory, and an information system used to be considered two different things, and they were often built completely separately from each other as a system as well. In addition, OS and communication protocols used by control systems were specialized ones and different from those used by information systems. In recent years, however, due to the advantages in operability and cost, OS and communication protocols used by information systems have begun to be adopted by control systems, and their access to the external networks has been partially enabled. As control systems become more open like this, the environment surrounding control systems has become similar to information systems

and it is changed into something much easier for attackers to exploit.

Prevalence of cloud computing

A cloud service, which provides an information system environment to organizations as a service instead they prepare and maintain it by their own, is becoming popular. Of course a cloud service needs to implement adequate security measures. Cloud service users also should be aware that not all data are always under their control. That is to say, the users need to understand that the incident response procedures are different from those for traditional information systems.

#### 1.3. Changes in the Whole Figure Surrounding Information Security



The whole figure surrounding information security is also changing. Especially in cyber space, not only attacks with financial motives but also cyber espionage to steal sensitive information, such as intellectual property (know-how), have been observed. To respond to these attacks, the business sectors and government agencies that had not been so keen on information security are left with no choice but to do something.

(1) Changes in the offensive side

• Attacks against social infrastructures and cyber espionage

Until a few years ago, the objectives of cyber attacks were mainly financial gain or theft of personal information. However, in addition to financial motive, a new movement has emerged and attacks that aimed to steal proprietary information from defense contractors and energy companies have begun to be reported. These attacks are more like spy operations in the real world. Also, as represented by Stuxnet that targeted Iran's nuclear facilities in 2010, manufacturing and control lines have been added to the list of targets.

These attacks are so elaborated and sophisticated that the offenders behind the attacks are said to be a large organization who has ample supply of funds and skills.

• Attacks by groups of people who share common ideology

In 2011, a word "hacktivist" swept the news media. Hacktivist is a portmanteau word of hacker and activist. Hacktivists are a group of people who execute cyber attacks against nations and firms politically opposed to them as a means of protest to promote their political ideology. Some of the characteristics of their attack are to give notice about the attack in advance or post the result of the attack on the Internet. By making their activities public, they make a point.

(2) Changes in the defensive side

• Attacks expanded to control systems and embedded systems as cyber attacks began to target a wider range of systems, changes are shown in the defensive side. One of the factors for these changes was that the target of attack is expanded to those systems which previously seemed to be safe from attacks, such as control systems, infrastructures, manufacturing plants and embedded systems. For that, the concept of security specialized for information systems spread to control and embedded systems, and the engineers in those fields are required to implement security.

• Response as a threat to national security

The U.S. Department of Defense (DoD) has declared cyberspace as a new, fifth battlefield for DoD activities as other domains of land, sea, air and space in the DoD Strategy for Operating in Cyberspace released in July 2011. Information security that aims to protect information assets within the organization from various threats now has a significant military meaning. Some media report that preparation to establish a unit in the Self-Defense Forces for defending cyberspace is in progress as well in Japan, making information security part of the national security agenda and a framework that involves government agencies and defense industry.



#### **1.4. Changes in Impact When Attacked**

The impact a security incident has on the organization has getting bigger than before. Until a few years ago, the worst impact a security incident could impose was a scandal for a mere organization. In recent years, however, it has expanded to social infrastructures to national security, and even the impact on social life is discussed.

#### • Theft of sensitive information

The cyber attacks against a heavy industry giant and government agencies in 2011 where military and political information were leaked and hotly covered by news media show that the kind of information the attackers aim to get their hands on is changing. Also, the cases have been reported overseas where the businesses' intellectual properties and information that could influence corporate strategies have been stolen. Let's consider a case where someone steals the national secrets unrightfully. By losing sensitive information that way, the victim nation could lose diplomatic advantage. As for the theft of intellectual property of businesses, it could harm its competitive edge due to the counterfeit goods that may be put in the market.

#### Megaleak of information

Economic loss caused by major information disclosure is also non-negligible problem. In the case of a major video game maker, the services had been halted for a month and the business activity was restricted during that time. The game maker announced in May 2011 that the incident might impact its business profit for FY2012 about 14 billion yen. In addition to losses due to missed opportunities, damage to the brand image and cost for recovery will be incalculable.

 Attack targeting social infrastructures No case has been reported yet in Japan, but in other nations, there were some reports that the control systems at a manufacturing plant and for railway system were disrupted by cyber attacks. Control systems have been used in social life. If attacks disrupt the operation of infrastructures, out life will be affected.

#### **1.5.Current Situation of Security and Future Challenges**

The environment surrounding information security has changed in various aspects. Along with that, threats surrounding information security have also been changing. These changes lead to the cost increase for applying security patches and technical challenges in responding to emerging attack techniques that are difficult to prevent, and make implementation of security more cumbersome and complicated. Below, three future challenges in security are listed.

#### (1) Total system security approach

When things were much simpler and attacks were straightforward, security was much easier and just buying a security product that would fix one particular However, APT attack was enough. attacks exploit a wide variety of weaknesses from system misconfigurations to software vulnerabilities to the user's psychological aspects. Now, it is critical to implement security measures heuristically from a broad range of viewpoints, for example, deploying security products at the adequate locations with adequate settings, managing information assets, designing the networks to prevent the damages from attacks should they occur, raising awareness of the users. To do so, it is required for not only the system

administration department and users, but also the planning department and executives, to collaborate and consider total system security.

#### (2) Information Sharing Scheme

As represented by targeted email attacks, recent cyber attacks tend to be stealthy and make it difficult to notice the damage. Also, attack information tends not to be shared openly because attacks are done to very specific targets. Since little information about those attacks is available, it is difficult for the defenders to come up with effective measures. That suggests there is so few things one organization or agency can do and a scheme to share information is much needed.

Currently, an establishment of a public-private cyber attack information

sharing scheme is in progress and discussions about effective measures by experts from the various fields have been done.

(3) Examining threats for each organization

In 2011, many large scale attacks and high-impact security incidents occurred and we recognized afresh that the importance of cyber security efforts taken in each organization. In some cases, however, it may not be appropriate to implement security measures by just taking up the problems and threats experienced by other organizations into one's own organization. The impact a threat may impose on an organization depends on the security measures the organization is taking and the purposes of the attacker. Also, there are many cases where a threat for the company A is not a threat for the company B at all.

It is important for each company to examine the damage an attack could impose on its business and then discuss how to defend accordingly to its business, system operation and the current security measures.

# Chapter 2. 10 Major Security Threats for the Year 2012

The 10 most socially influential threats in 2011 selected via voting by the 10 Major Security Threats Committee members were presented in Table 2. This chapter explains each of the top 10 threats.

Rank	Title				
1.04	APT Attacks				
1st	$\sim$ Targeted, advanced persistent threat (APT) attacks to steal valuable information $\sim$				
2nd	Unpredictable Disasters				
Znu	$\sim$ Failure of IT systems, loss of business data due to natural or man-made disasters $\sim$				
3rd	Hacktivist Attacks				
JIU	~ Information disclosure and/or interference of business by hacktivists ~				
4th	Attacks Targeting Unpatched Client Software				
401	$\sim$ Vulnerabilities in client software often exploited by targeted attacks $\sim$				
5th	Website Attacks				
500	~ Vulnerabilities in websites continue to be targeted ~				
6th	Attacks Targeting Smartphones and Tablets				
oun	~ Smart "mini PC" devices locked-on as targets ~				
7th	Danger in Digital Certificates				
7 01	~ Problems caused by bad management of digital certificates ~				
046	Internal Threats				
8th	$\sim$ information disclosure and/or interference of business by insiders or associates $\sim$				
046	Reuse of the Same Credential				
9th	~ ID spoofing caused by sloppy management of IDs and passwords ~				
10th	Privacy Invasion				
	$\sim$ Issues in handling information strongly associated with the user $\sim$				

#### Table 2 : Top 10 Major Security Threats for the Year 2012

#### 1 st APT Attacks [Countermeasure Priority: 1st]



~ Targeted, advanced persistent threat (APT) attacks ~

In 2011, targeted, APT attacks that aimed to tactically steal sensitive internal information targeting a heavy industry giant and congress have been observed in Japan. The characteristics of these attacks are that it is difficult to notice attacks and damages, and that virus which has compromised the system executes attacks while communicating with the attacker on the different network.

#### <Threats & Impacts>

In 2011, organizations like a local heavy industry giant and congress were hit by APT attacks and received public attention. With these APT attacks, a virus sent through targeted emails breached the system, conducted espionage activities and stole the internal information. In other words, industrial spies and secret agents are in action in cyberspace just like in the real world. In overseas, it is also called APT attacks or cyber espionage.

An APT attack is done through the following steps. Let's see an example.

1 Preparation for Attack

Collect information needed to attack a target organization.

2 Initial Infiltration

Send targeted attack emails to the target and infects PC.

- ③ Building the attack Infrastructure. Set up a backdoor in the infected PC, communicates with the external server, and, downloads the new malware.
- 4 Probing the System

Probe the system and specify where the target information is. The attacker keeps attacking based on the information obtained through the attacks.

(5) Pursuing the final goal of attackObtain the target information.

What special here is that by using a virus to compromise the system, setting up a

backdoor and communicating the C&C servers, all internal information is handed out on the silver platter to the attacker. It is as if the attacker has his or her clone inside the system and is executing hacking. The current network design concept assumes that it is secure inside the perimeter and focuses on blocking the threats from the Internet. For that reason, the systems that do not expect the hacking from the inside are vulnerable and easy for an insider to compromise.

#### <Case Studies & Statistics in 2011>

 Attack against House of Representatives

By remote attacks, the IDs and passwords of all 480 members were stolen, and their email exchanges could have been leaked up to for 15 days. One member opened the virus-infected file sent via targeted emails and infected his computer. From there, it infected the rest of the house network. As a result, 32 PCs were infected.

 Attack against Mitsubishi Heavy Industries.

In September 2011, Mitsubishi Heavy Industries announced that their system was infected with virus. Infection of 45 servers and 38 PCs used by the employee were confirmed and they spread over 11 locations including the headquarter, factories and research centers in Japan. It is said that the system was compromised remotely through the targeted emails.

#### <Measures & How to Respond>

One of the characteristics of APT attacks

is that using a virus that has compromised the system to communicate with external servers, it can update the virus and steal the internal information. As an approach to countermeasure development, it is important to have the "inbound protection measures" which prevent the threats from getting into the network and "outbound protection measures" which prevent the remote attacker from transmitting information to outside the network even if the system is breached. The "inbound "outbound protection measures" and protection measures" are explained below.

Inbound protection measures

It is important to build a threat-free system environment as much as possible by implementing security measures like antivirus software, vulnerability countermeasures and IDS/IPS. Because most attacks aim to exploit vulnerabilities in client software, it is critical to update client software timely.

Outbound protection measures

In a guide provided by IPA, "Design and Operational Guide to Protect against "Advanced Persistent Threats", **IPA** recommends 8 network design controls as outbound protection measures. What is important is a network design and configurations that will block the communication with the external devices and prevent infection within the internal network.

#### References

I. YOMIURI ONLINE: http://www.yomiuri.co.jp/net/news/20111115-OYT8T00237.htmIPA: Design and Operational Guide to Protect against 'Advanced Persistent Threats' http://www.ipa.go.jp/security/vuln/documents/eg\_newattack.pdf [Last visited on Mar. 15, 2012]

#### **Related Documents**

• IPA: <u>http://www.ipa.go.jp/about/technicalwatch/pdf/111003report.pdf</u> (Japanese) [Last visited on Mar. 15, 2012]

#### 2 nd Unpredictable Disasters [Countermeasure Priority: 6th]

~ Failure of IT systems, loss of business data due to natural and man-made disasters ~



The 2011 Tohoku Earthquake had an enormous impact on our social life. Both natural and man-made disasters cannot predict. It has reminded us afresh that it s necessary to develop a disaster response plan and prepare for emergencies to mitigate the damage and impact on the employees and business property.

#### <Threats & Impacts>

Natural disasters, such as earthquakes, storms and floods, or man-made disasters like business interference and accidents may affect the business continuity.

Many businesses depend on IT. If the IT systems that support the foundation of the business are disrupted or data are lost or destroyed, the business will be halted.

The cause of IT system disruption can be hardware failure, software bug, data loss, electric power outage and so on, and how to recover or what resources are needed depends on the cause. If an organization does not have a disaster response plan and put it into practice in advance, the possibility where the response may not work will increase because of the troubles, for example, backups fails and cannot restore the system and cannot ensure the necessary resources. As a result, the business may be forced to stop for a long period of time. A long disruption could cause the following problems.

- No revenue
- Affect the affiliates and their business
- Lose user confidence

If a business that would stop is his or her core business, the impact will be even higher.

Remember that by prioritizing the availability of an IT system in the time of emergency, the confidentiality and integrity may not be fully protected. Thus, when considering the priority for the system continuity, in addition to the risk of system disruption, discuss what level of confidentiality and integrity should be satisfied.

#### <Case Studies & Statistics in 2011>

In 2011, the Tohoku Earthquake, the biggest earthquake in Japanese history, hit the northern area of Japan and the massive tsunamis, caused a major disaster. Part of the damage includes the destruction of servers caused by the earthquake and loss of the family register data due to tsunami.

The disaster imposed the planned outages (rolling blackouts) in some regions. According to the survey conducted by a private company, 38 percent of the businesses answered that the rolling blackouts affected their business one way or another<sup>1</sup>. Also, a flood of donation transfers triggered the crash of a banking system that lasted for 10 days. The multiple causes were pointed out but the bank reported that one of the reasons stemmed from the flaw in preparation for emergency recovery planning<sup>II</sup>.

In another case, a man-made disaster where a contractor cut through the cable at the data center disrupted the company's core business for a period of time<sup>III</sup>.

#### <Countermeasures & How to Respond>

To prepare for emergencies, it is effective to develop a disaster response plan and/or business continuity plan (BCP) to continue the business or recover the capability as early as possible and put the plans in practice.

A BCP is not limited to IT systems but should include every process, methods and procedures that are needed to continue the business. It is desired to develop a BCP that takes into account the following points, and have a mechanism to practice or review the plan continuously not to make it a mere documentation practice.

Prioritize the business lineups

• Identify the resource essential for the businesses

• Examine the possible alternative resources

• Decide the acceptable system downtime

• Sort out the kind of disasters the businesses will be affected

• Develop a disaster recovery plan

• Consider the preliminary measures before activating the BCP

After the Tohoku Earthquake, a BCP that is written not only from the perspective of IT service continuity, but also including the cooperation with the local communities and other organizations is getting attention.

As for a guideline for developing and maintain a BCP, the Small and Medium

Enterprise Agency provides the "BCP Guide for Small and Medium Enterprises<sup>IV</sup>. Also, the Ministry of Economy, Trade and Industry provides the "IT Service Continuity

Guideline" which lists up concrete measures focus on IT-related issues in BCP<sup>V</sup>.

#### References

- I. TechTarget: <u>http://techtarget.itmedia.co.jp/tt/news/1106/27/news05.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- II. Mizuho Bank Ltd.: <u>http://www.mizuhobank.co.jp/company/release/2011/pdf/news110520\_4.pdf</u> (Japanese) [Last visited on Mar. 15, 2012]
- III. NS Solutions Corporation: <u>http://www.ns-sol.co.jp/press/2011/20110825\_000000.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- IV. Small and Medium Enterprise Agency, Japan: <u>http://www.chusho.meti.go.jp/keiei/antei/index.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- V. Ministry of Economy, Trade and Industry, Japan: <u>http://www.meti.go.jp/policy/netsecurity/docs/secgov/2011\_loformationSecurityServiceManagementGuidelineKaite</u> <u>iban.pdf</u> (Japanese) [Last visited on Aug. 28, 2012]

#### **Related Documents**

Japan Users Association of Information Systems: <u>http://www.juas.or.jp/servey/it12/it12\_bcp.pdf</u> (Japanese) [Last visited on Mar. 15, 2012]

#### 3 rd Hacktivist Attacks [Countermeasure Priority: 8th]

## 

~ Information disclosure and/or interference of business by hacktivists ~

Until 2010, cyber attacks were mainly some organized acts aiming for financial gain. In 2011, however, hacktivist attacks that aimed to make their political claim became very active. For example, there were the attacks that targeted government agencies and companies, and disclosed the sensitive information or caused a denial of service condition with very clear purposes.

#### <Threats & Impacts>

Most of cyber attacks in 2010 were executed by cybergangs aiming for financial gain or organized acts by people living in some specific region.

In 2011, however, attacks by hacktivists, which is a group of people who share common ideology, oppose some business or organization's claim or action and use cyber attacks as a mean to make their point, became very active. In most cases, each hacktivist group does not have a particular leader. It is said that attacks by hacktivist groups are not executed by people living in some specific region but those who have sympathized with each group's ideology through the Internet participate in the attacks planned and announced by each group on an attack-by-attack basis.

Attacks by these bound-by-ideology groups are not particularly novel. Although the objective and scale are different, the distributed denial of service (DDoS) attacks or boycott campaigns organized by the users of a certain domestic mega-message board would be categorized as cases of hacktivist attacks.

One of the background factors that influenced the activization of hacktivist attacks in recent years would be the widespread use of social media. By effectively using the growing social media, hacktivists recruit members widely, announce their attacks to make a point and demand that their target rethink its claim or action. If their target does not accept their demand, hacktivists will execute the attacks like below:

- DDoS
- Disclosure of sensitive information
- Tampering of website

#### <Case Studies & Statics in 2011>

(1) DDoS attacks against Sony<sup>I</sup>

In April 2011, some members of a hacktivist group called Anonymous executed the DDoS attacks on Sony's multiple websites. Due to the attacks, multiple websites have being shut down and became unable to provide the services.

(2) Disclosure of sensitive information at Nintendo<sup>II</sup>

In June 2011, a hacktivist group called LulzSec executed unauthorized access to the Nintendo's server(s) in the U.S. As a result, the web server configurations were disclosed online. Although LulzSec's purpose was for Nintendo to fix the vulnerabilities in its server(s), this can be a case where a hacktivist group has attacked and disclosed sensitive information.

#### <Measures & How to Respond>

Among the attacks likely performed by hacktivists, DDoS attacks can be mitigated, but are difficult to thwart completely. As for the disclosure of sensitive information, there is no special countermeasure but do what we can do in general - review and make sure its personal information handling policy is secure or web servers do not have vulnerabilities. It is necessary to keep security awareness high while working hard on security on a daily basis.

On the other hand, how to respond to this kind of difference of views with hacktivists is important. By listening to the users' opinion carefully and act adequately instead of advertising its claim and action one-sidedly, the businesses and organizations may be able to prevent an event from erupting into a problem.

In the case of Domino's Pizza boycott campaigns in the U.S<sup>III</sup>, even though Domino's Pizza lost customers trust due to two employees' improper action, it admitted its fault and made a public apology through the video message on the Internet. Through these actions, it gradually succeeded to regain customers trust.

Such case study may give us a hint for how to respond to hacktivist attacks.

## References I. Infosec Island, LLC: Sony Becomes Latest Operation Payback Attack Target http://www.infosecisland.com/blogview/12780-Sony-Becomes-Latest-Operation-Payback-Attack-Target.html [Last visited on Mar. 15, 2012] II. INTERNET Watch: http://internet.watch.impress.co.jp/docs/news/20110606\_450990.html (Japanese) III. ITmedia: http://blogs.itmedia.co.jp/itoman/2011/10/post-2baf.html (Japanese) [Last visited on Mar. 15, 2012]

#### 4 th Attacks Targeting Unpatched Client Software [Countermeasure Priority: 2nd]

~ Vulnerabilities in client software often exploited



In these days, attacks that target client software used by general IT users see no end. By exploiting vulnerabilities in client software, the attackers can infect PCs with virus and steal information.

#### <Threats & Impacts>

In the last few years, vulnerabilities in client software, such as Java (JRE) and Adobe Reader, are more exploited in cyber attacks than those in the operating systems like Windows. One of the techniques the attackers use to infect a target PC is to exploit vulnerability in software. An attacker tries to infect the target PC with virus by inducing the user of the target PC to visit a malicious website or open an email attachment that contains malicious code. One of the background factors that promoted attackers to target client software could be that the importance of keeping the client software up-to-date to ensure

security is still not understood by general IT users. According to an awareness survey conducted by IPA, the importance of OS update is beginning to be recognized, but there are lots of general IT users who do not recognize the necessity of updating client software.

The attacks that exploit vulnerabilities in client software are often used as a mean to breach the system in targeted attacks, and can infect PCs with virus and/or the steal information in the PCs or internal systems.

#### <Case Studies & Statistics in 2011>

 Trend in attacks targeting client vulnerabilities<sup>1</sup>

According to the report on the

vulnerabilities that were most exploited to download malware published by a U.S. computer software vendor, the attacks that targeted Java accounted for more than half of all, 58 percent to be precise. The vendor reports and warns that it was top among all software vulnerabilities found so far in the first half of 2011.

Situation in Security Patch/Software
 Update Practice of IT Users<sup>II</sup>

According to the Survey for Awareness of Information Security Threats for 2012 conducted by IPA, those who said they "apply security patches using Windows Update or some other means" was 70 percents and those who said they "update Adobe Reader" was 55.8 percent. The rest said they do not update. The result shows that they do not understand why it is necessary to update the software regularly.

#### Attacks against Mitsubishi Heavy Industries

As introduced as a case study for the 1st threat earlier (1st: APT Attacks), it was reported that 83 PCs were infected with virus in the series of attacks against Mitsubishi Heavy Industries. In those attacks, the attackers sent out emails attached with a malicious PDF file and set up backdoors exploiting the vulnerabilities in Adobe Flash and Adobe Reader.

#### <Measures & How to Respond>

Vulnerabilities in client software are discovered daily and the emergence of attacks that exploit those new vulnerabilities are also confirmed each day. Product vendors develop security patches to fix the vulnerabilities and make them available to the public. By applying those security patches, the vulnerable software is updated and fixed.

In some cases, the vulnerabilities for which security patch has not yet been available are exploited, but in most cases, the exploited vulnerabilities are already known ones and security patches are readily available. Thus, if client software is up-to-date, most of the attacks that try to exploit the vulnerabilities in client software can be prevented.

It is critical for IT users to pay close attention to the security patch information released by the vendors and update the software as soon as possible.

IPA provides MyJVN Version Checker<sup>III</sup>. The tool can check if the version of the software applications installed in a client PC is up-to-date.

#### References

- I. ITPro: http://itpro.nikkeibp.co.jp/article/COLUMN/20110904/368103/ (Japanese) [Last visited on Mar. 15, 2012]
- II. IPA: http://www.ipa.go.jp/security/fy23/reports/ishiki/index.html (Japanese) [Last visited on Mar. 15, 2012]
- III. IPA: http://jvndb.jvn.jp/en/apis/myjvn/index.html (Last visited on Mar. 15, 2012)

#### **Related Documents**

- IBM, Tokyo SOC Report : <u>http://www-935.ibm.com/services/jp/its/pdf/tokyo\_soc\_report2011\_h2.pdf</u> (Japanese) (Last visited on Mar. 15, 2012)
- Microsoft Security Intelligence Report: <u>http://www.microsoft.com/security/sir/default.aspx</u> [Last visited on Aug. 10, 2012]

#### 5 th Website Attacks [Countermeasure Priority: 3rd]



#### ~ Vulnerabilities in websites continue to be targeted ~

Malicious acts aimed to interfere the web services or steal sensitive information seem to never stop. Attacks exploiting the vulnerabilities in websites, such as disclosure of sensitive information, virus infection from visiting a website and denial of service, are still often observed.

#### <Threats & Impacts>

Attacks that target websites have been around for a long period of time, yet they still cause a lot of troubles.

A website is composed of the following three components:

- (1) Web applications
- (2) Middleware
- (3) OS

Many of the attacks that targeted websites in 2011 exploited the vulnerabilities in web applications and middleware. Most cases fall under (1) and to be specific, two types in them: custom-developed applications and open source software.

By writing codes riddled with

vulnerabilities, custom-developed applications can be exposed to attacks. Also, as for using open source software, the old versions are used in many cases. The tools that exploit the vulnerabilities in open source software are readily available on the Internet. Attackers can execute attacks easily using those tools.

As a result, for example, a hacked website may be altered to redirect the visitors to a malicious website, and they would be forced to download fake security software full of viruses there.

On the other hand, the attacks that exploited vulnerabilities in (2) were also observed in 2011. For that, many DoS attacks and unauthorized accesses

#### occurred.

#### <Case Studies & Statistics in 2011>

SQL injection attack "LizaMoon"

A U.S. security vendor has discovered and reported that a large-scale website-tampering SQL injection attack code was embedded in more than 226 thousands URLs. The attack embeds the code that points to malicious websites into the URL and redirects the visitors to the fake antivirus software distribution websites. The attack is named "LizaMoon" after its domain name.

Attack targeting OSS "osCommerce"

The U.S. Microsoft warned in its blog that a large-scale attack against online shopping websites which use open source software "osCommerce". It is confirmed that more than 90 thousands domains, including Japanese ones, have been already infected.

 "ApacheKiller"<sup>III</sup> attack code that exploits vulnerability in web server software Apache

In August 2011, a vulnerability that would enable denial of service attacks was discovered in the web server software Apache. The Apache developers immediately got to fix the vulnerability, but attack code had been already published before the security patch became available. The attack code was called "ApacheKiller". The attacks that exploited this vulnerability could have affected any website that used "Apache". In fact, it is said that a major Japanese bulletin board was attacked using this attack code.

#### <Measures & How to Respond>

It is important for web application developers not to build vulnerabilities into web applications. By using the IPA guidelines such as "How to Secure Your Website"<sup>IV</sup> and "Secure Programming Course"<sup>V</sup>, the developers need to improve the website security.

Also, it is important for website operators to perform vulnerability assessment regularly and update the software applications in use to keep their website safe.

Moreover, middleware needs to be kept up-to-date as well. An IPA tool "MyJVN Version Checker"<sup>VI</sup> enables to check if the software installed in PC is up-to-date and can be used effectively for that.

#### References

I. –	SecureBrain: http://www.securebrain.co.jp/about/news/2011/04/lizamoon.html	(Japanese)	[Last visited on Mar.
	15, 2012〕		

- III.
   IPA: <a href="http://www.ipa.go.jp/security/ciadr/vul/20110831-apache.html">http://www.ipa.go.jp/security/ciadr/vul/20110831-apache.html</a> (Japanese) (Last visited on Mar. 15, 2012)

   IV.
   IPA: How to Secure Website
- http://www.ipa.go.jp/security/vuln/documents/website\_security\_en.pdf [Last visited on Aug. 17, 2012]
- V. IPA: <u>http://www.ipa.go.jp/security/awareness/vendor/programming/</u> (Japanese) [Last visited on Mar. 15, 2012]
- VI. IPA: http://jvndb.jvn.jp/en/apis/myjvn/index.html [Last visited on Mar. 15, 2012]

II. IID Inc.: http://scan.netsecurity.ne.jp/archives/51999672.html (Japanese) [Last visited on Mar. 15, 2012]

#### 6 th Attacks Targeting Smartphones and Tablets [Countermeasure Priority 5th]



#### ~ Smart "mini PC" devices locked-on as targets ~

Because smart devices, such as smartphones and tablets, are communication devices that are highly functional and portable, they are inevitably prone to aggregate users' private information. The number of people using smartphones is keep increasing every year and attacks that target those people/smartphones are also on the rise.

#### <Threats & Impacts>

A smartphone is a portable device that allows a user to browse the same websites that are available for PC, add favorite applications and expand functions and so on.

The number of smartphone users has been increasing yearly, and it is said that the volume of shipments was 23 millions in 2011I. As the user demographic expands, the possibility of being attacked is increasing just like PCs.

Since smartphones are highly functional and portable, the data related to their owner, such as personal information, address book data, photos and movies are likely stored on them. These devices face the threats like theft and lost, virus, unauthorized applications and phishing. In and after 2011, especially the threats of virus and unauthorized applications became bigger.

For example, an attacker may try to install a malware by fooling the smartphone user. If installed, the user information may be stolen or scammed.

Also, if infected with the virus that exploits the vulnerability, the following things may occur:

- Shutdown of smartpones
- Tampering and disclosure of data stored in smartphones
- Remote, unauthorized manipulation of smartphones

The necessity for the smartphone users to recognize the threats for smartphones, such as virus and malicious applications, and to take security actions is getting higher. Tablets are affected just like the same way and require the same necessity. **Case Studies & Statistics in 2011>** 

In 2011, various attacks targeting smartphones have began to be observed even though there were not many incidents reported yet.

According to the report published by a security vendor, the number of viruses that exploit vulnerabilities in Android-based smartphones is especially increasing<sup>II</sup>. The causes behind this increase seem that with Android, anyone can distribute applications without introducing through the Android Market operated by Google (the name changed and integrated to Google Play in March 2012), and that there is no strict evaluation for the applications to be distributed at Android Market (as of 2011).

Also, just like the same for PCs, the existence of one-click fraud websites targeting smartphones have been confirmed where all user does is just one click and he or she is charged for the services. In January 2012, a case that used a malicious application was reported. If a user is fooled and installs a fake application, the charge screens are displayed frequently and/or the telephone numbers

and email addresses can be stolen<sup>III</sup>.

#### <Measures & How to Respond>

IPA presents the six rules to use smartphones safely countering the attacks that exploit viruses and vulnerabilities<sup>IV</sup>. IPA hopes they will help the users when using a smartphone.

- (1) Update smartphone applications
- (2) Do not tamper smartphones (jailbreak or such)
- (3) Install applications only from trustable providers
- (4) For an Android-based cell phone, check access control before installing applications
- (5) Implement security software
- (6) Regard a smartphone a small PC and maintain like a PC

In addition, the smartphone security efforts by the industrial organizations were active as well. JSSEC (Japan Smartphone Security Forum) has published the "Security Guideline for the Business Use of Smartphones Tablets and (the first edition)"V and JNSA (Japan Network Security Association) has released the "Smartphone Security Guidelines ß Edition<sup>VI</sup>.

#### References

I. MM Research Institute Ltd.: <u>http://www.m2ri.jp/newsreleases/main.php?id=010120120313500</u> (Japanese) [Last visited on Mar. 15, 2012]
 II. McAfee: <u>http://www.mcafee.com/japan/security/threatreport11q2.asp</u> (Japanese) [Last visited on Mar. 15, 2012]
 III. IPA: <u>http://www.ipa.go.jp/security/txt/2012/02outline.html#5</u> (Japanese) [Last visited on Mar. 15, 2012]

IV. IPA: http://www.ipa.go.jp/security/txt/2011/08outline.html#5 (Japanese) [Last visited on Mar. 15, 2012]

V. JSSEC: Security Guideline for the Business Use of Smartphones and Tablets

http://www.jssec.org/dl/guidelines2012Enew\_v1.0.pdf [Last visited on Aug. 28, 2012]

VI. JNSA: http://www.jnsa.org/result/2010/smap\_guideline\_Beta.pdf (Japanese) [Last visited on Mar. 15, 2012]



#### 7 th Danger in Digital Certificates [Countermeasure Priority: 14th]

~ Problems caused by bad management of digital certificates ~

Digital certificates (hereinafter referred to as "certificates") are used to check the credibility of websites and/or software. In 2011, some CAs (certificate authorities) and government agencies were cyber attacked and their digital certificates have been stolen and/or falsified. As a result, we found ourselves in a situation where we could not confirm the credibility of websites and/or software that used the certificates issued by the compromised CAs or government agencies.

#### <Threats & Impact>

Certificates that use the PKI (public key infrastructure) technology are used to verify a website operator or software developer (for code signing). In a certificate, data about a website operator or software developer are written and the validity of the certificate contents is assured by a third-party CA (certificate authority). The system works out based on the mutual relationship of trust. By using the certificates, general Internet users can check if a website they are visiting is indeed the real one run by the legitimate operator or if software they are going to use is indeed the authentic one released by the

#### developer.

If a third-party CA which assures and issues certificates is compromised by a malicious attacker, it is possible that the validity of the certificates is compromised as well (compromised certificates are hereinafter referred to as "fraudulent certificates"). Should it happen, the established certification infrastructure is compromised and it will affect the safety of the whole Internet including the IT users.

Unlike unsigned certificates (so-called self-signed certificates), fraudulent certificates are nothing different from legitimately issued certificates for the general Internet users. Thus, if they access

a website that uses a fraudulent certificate, the browser does not display warnings. Because of that, even though they are accessing a phishing website, they mistakenly believe that they are accessing the authentic website. As a result, their personal information such as credit card number may be stolen.

On the other hand, there is a possibility that software is maliciously code-signed using a fraudulent certificate. When installing unsigned or unverified software, popularly-used operating systems like Windows OS (XP and later version) display warnings. However, if code-signing is properly done by using a fraudulent certificate, the warnings are not displayed when installed. Thus, even though it is malicious software, the general Internet users mistakenly believe that it is a legitimate software and may proceed to install the malware.

#### <Case Studies & Statistics in 2011>

In 2011, several cases were reported where the websites of some third-party CAs were compromised by cyber attacks and fraudulent certificates were issuedl<sup>,II</sup>. According to the media reports, the causes of these incidents were mainly vulnerabilities in the CA websites.

On the other hand, there was another report that a malware which was code-signed by the certificate stolen from a Malaysian government agency<sup>III</sup>. In Malaysia's case, the certificate was not issued fraudulently but the issuer of the certificate used to sign the malware was indeed a Malaysian government agency.

#### <Measures & How to Respond>

It is necessary for the organizations that provide the certificate services, such as CAs and those who use the certificates, to recognize the risks in case the certificates are compromised, and manage the certification infrastructure strictly by improving the security measures to prevent unauthorized access. Also, when the issue of fraudulent certificates is confirmed, take actions to revoke those certificates immediately and ask related organizations to take necessary actions.

On the other hand, as for general Internet users, in addition to confirming the validity of the certificates when browsing websites or installing software, if they notice that they are fooled by the fraudulent certificates, apply security patch based on the vendor information and take actions to disable the certificate immediately.

#### References

- I. Symantec Connect Community: <u>http://www.symantec.com/connect/blogs/comodo</u> (Japanese) (Last visited on Mar. 15, 2012)
- II. @IT: <u>http://www.atmarkit.co.jp/news/201109/08/diginotar.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- III. ITmedia: <u>http://www.itmedia.co.jp/enterprise/articles/1111/15/news022.html</u> (Japanese) [Last visited on Mar. 15, 2012]

#### **Related Documents**

• IPA: http://www.ipa.go.jp/security/pki/ (Japanese) [Last visited on Mar. 15, 2012] (Japanese)

#### 8 th Internal Threats [Countermeasure Priority: 7th]



~ Information disclosure and/or interference of business by insiders and associates ~

The internal threats of system tampering and information disclosure by disgruntled employees or former employees seem unstoppable. Because the internal threats are caused intentionally by those who know well about the organization, the extent of the impact is bigger.

#### <Threats & Impacts>

One of the factors behind these seemingly never-stoppable internal threats by disgruntled employees or former employees that non-management is employees are granted to access sensitive information and it is easy for them to steal information in most cases. Moreover, in many cases, access control is not properly implemented. For example, the accounts of persons like the former employees have not been deleted as they should be.

When an attack is done by an insider or someone associated to the organization, the extent of the impact is big because those people know where to find important information. In addition, once they gain access to the information, they can access a large amount of data simultaneously. Thus, the extent of the impact tends to become bigger.

For example, if sensitive information is disclosed, the public confidence will be lost. Or, if intellectual properties are leaked, it is concerned that future competitive advantage will be diminished. If the data is about the joint development of multiple about consignment companies or а development, the leak will also cause damage on partners or customers.

Besides, in 2011, not only the thefts of sensitive information, but also data

tampering occurred as well.

Those are intentional attacks by the insiders who know well about the organization. For that, mitigating the risk is possible but completely preventing the attacks would be difficult.

#### <Case Studies & Statistics in 2011>

 Interference of business due to data tampering<sup>1</sup> at domestic telecom

In May 2011, a domestic telecom company experienced that a contractor's former employee tampered the ATM line configuration data between a base station and the network center.

By this incident, the cell phone service was degraded in the service area, affected 72,700 users.

 Domestic credit card company customer data disclosure<sup>II</sup>

In August 2011, at a domestic credit card company, a maximum of 160,000 customers' information was taken out and likely sold.

The perpetrator was a person involved with the insurance agent work the company had outsourced in the past and the contract was already terminated as of October 2009.

 Data tampering of 1.3 million users of social games

In May 2011, a former employee accessed a social game server of the former employer without authorization and interfered its business by tampering 1.3 million users' game data. This former contractor set up a program that could nullify the unauthorized access control when left the job with the termination of a term.

Unauthorized access lasted for 2 days and caused about 10 million yens.

#### <Measures & How to Respond>

To mitigate the insider thetas, it is necessary to implement physical security measures to control access to the places where sensitive information is stored and the terminals to access sensitive information are located, and cyber security measures to control access to sensitive information. It is also important to clarify the role and privileges of each employee. For example, when handling very important data, do it in a pair as one does the work and the other authorizes, and unless authorized, the work cannot proceed.

Such rules like separation of job functions and access control are one of the challenges for the organizational internal control. These rules and mechanisms tend to become a mere façade. Not to make the operation superficial, it is important to check and review the whole operation.

Incident response, should something happen, is also critical. If information disclosure occurs, various works, such as investigation of the cause, apology announcement, report to the supervisory agency, compensation to those affected, recovery of public confidence. Thus, how fast the organization can go back to the normal business is the key of the incident response. It is necessary to develop an incident response plan before information disclosure does happen.

#### References

- I. japan.internet.com: <u>http://japan.internet.com/allnet/20110711/1.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- II. Cedyna: <u>http://www.cedyna.co.jp/info/20110816.html</u> (Japanese) [Last visited on Mar. 15, 2012]

#### **Related Documents**

SECURITY NEXT: <u>http://www.security-next.com/cat\_cat25.html</u> (Japanese) [Last visited on Mar. 15, 2012]

## 9 th Reuse of the Same Credentials [Countermeasure Priority: 4th]

~ ID spoofing caused by Sloppy Management of



If using the same credential (ID/password) for the multiple web services and it is leaked from one of the services, the spoofing attack and resulting damage may spread in chain reaction to all services. In fact, there were some media reports that harm was done because of the reuse of the same credential for various services.

#### <Threats & Impact>

These days, many web services, such as Internet banking services, are offered. However, because of inadequate management of the account information, for example, no password is set or password is not managed properly, spoofing harm is spreading.

The users are required to register the account information, such as ID and password, per web service, but it is said that many users use the same ID and password for these multiple services.

Maintaining a credential per each service

may be a hassle, but using the same ID and password pair for the various web services may spread harm unexpectedly.

For example, let's assume a user is using the web service A and B. If the web service A has vulnerability, an attacker can exploit it and steal the user's personal information and account information.

If the user uses the same ID and password pair for the other web services, then the harm is not over. The attacker can use the same ID and password pair to log in to the web service B to spoof the user's identity. As result, even though the login credential for the web service B is not leaked, still the attacker can log in, steal the user information and user the service, spreading the harm.

#### <Case Studies & Statistics in 2011>

According to iPA's Report on the Survey for Awareness of Information Security Threats for 2012I, about 80 percent of users basically use the same ID and password pair for various Internet services. Upon such situation, because of inadequate management of the account information, for example, no password is set or password is not managed properly, spoofing harm is spreading and some cases have been reported in the news media.

For instance, there is an article that a major SNS service says spoofing is happening a lot daily<sup>II</sup>.

PlayStation®Network (PSN), Sony Entertainment Network (SEN) and Sony Online Entertainment LLC (SOE)<sup>III</sup> are the examples where examples where the credential disclosed by one service is used to try to login to other services because of the reuse of the same ID and password pair.

#### <Measures & How to Respond>

For the web service providers, it is necessary to make sure to implement basic security measures, such as keeping the software up-to-date. In preparation for being attacked and compromised, it is important to encrypt the sensitive information, such as credit card data, to minimize the damage.

Also, as for the "identifier" like the password, it is important to makes sure to store it using a one-way function. By taking such measures, even if the credential is stolen, it could prevent the information from being abused to access other web services.

For the users to counter spoofing, first they need to take basic security measures to prevent the theft of the account information. One example could be to install antivirus software, keep the pattern file up-to-date and patch vulnerabilities in OS and applications. This will prevent virus from stealing the account information.

Next, the users need to take actions against the reuse of the same credential for multiple web services. The users should not share the account information for the web services that could possibly result in financial fraud with other services. Make sure not to set an easy password or be sloppy like keeping the ID and password on a note at hand.

As for those countermeasures, refer to IPA's slogan for December 2011 "My Passwords are Mine and Mine Only"<sup>IV</sup>.
#### References

- I. IPA: <u>http://www.ipa.go.jp/security/fy23/reports/ishiki/index.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- II. ITmadia: <u>http://www.itmedia.co.jp/news/articles/1110/31/news014.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- III. Sony Corporation <u>http://www.sony.co.jp/SonyInfo/News/Press/201110/11-1012/index.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- IV. IPA:<u>http://www.ipa.go.jp/security/txt/2011/12outline.html#5</u> (Japanese) [Last visited on Mar. 15, 2012]

#### 10 th Privacy Invasion [Countermeasure Priority 12th]



~ Issues in handling information strongly associated

By utilizing the information like attributes, such as age and sex, current location and browsing history, the service providers can offer the user-customized services. However, such information that is strongly associated with the user may invade the privacy if wrongly handled.

#### <Threats & Impacts>

Data like the user's attributes, current location and browsing history are the information strongly associated with the user (hereinafter referred to as "user information").

There are various services that utilize the user information. These services are provided through smartphone applications or web browsers. By utilizing the user information, it becomes easier for the service providers to provide more user-customized information.

For example, by using the user's current location, the restaurant and foodservice information around the user can be

provided. Also, by using the user's service usage data as feedback, the service providers can improve the quality of service.

From the service provider's viewpoint, the user information is very attractive data. However, it is the privacy information partly extracted from the overall data. It is also personally identifiable information if various user data are aggregated.

Thus, if wrongly handled, for example, collecting information without the users' knowledge or proper explanation, or collecting unnecessary information to provide the services, and if such improper handling of user information is known to the public, it is possible that both the users and the service providers may suffer detriment.

For the users, it may invade the privacy if the information is used against their intentions. For the service providers, by collecting too much user information, it may lose public confidence and place the continuity of service at risk.

#### <Case Studies & Statistics in 2011>

There were some case studies in smartphone applications.

As an example for the smartphone applications, there was an advertisement distribution program embedded to applications.

This advertisement distribution program collected the information about the applications installed in the device and the usage information. It was accused that the program did not provide sufficient explanation and the way it requested permission of the user was inadequate. In the end, the provider terminated the service. It is assumed that one of the causes can be the lack of consideration about how to handle the user information at the design phase of the service.

In addition, there were the cases where a public wireless LAN service collected unnecessary user information<sup>1</sup> and the information such as game history collected from the game devices was published online without the players' consent<sup>II</sup>. The former stopped collecting unnecessary information and deleted unnecessary information already collected. The latter

clarified the information disclosure policy in the terms of service and told it would consider providing a way for the users to choose if he or she would permit the publication of data in the future.

#### <Measures & How to Respond>

The service providers should clarify what user information they need and what they do not at the service design phase, and do not collect unnecessary information. After that, they should carefully examine the purpose of collecting and using the information needed to provide the services and then collect it.

It is assumed that there are mainly two intended purposes for collecting user information:

- To provide the services
- To improve the quality of service

The former means that the information is mandatory to provide the services. The latter means that the information is helpful to improve the quality of service but not mandatory. In the case of a service provider that offers the restaurant and foodservice information around the user' current position, the user's location information falls under the former and the restaurant visiting history would fall under the latter.

For each intended purpose, it is desired for the service providers to use the user information in the proper way in consideration of the users like the following:

 For the information mandatory to provide the services, make it clear for the users how the information is handled

For the information required to improve the quality of service, collect the information only from the users who show their consent and also provides the way to stop collecting later should they change their mind. Currently, Ministry of Economy, Trade and Industry is working on establishing the Working Group on Handling User Information Collected through Smartphones<sup>III</sup>.

#### References

- connectFree k.k.: <u>http://connectfree.jp/press/</u> (Japanese) [Last visited on Mar. 15, 2012]
   Sony Computer Entertainment Inc.: <u>http://www.jp.playstation.com/info/release/nr 20111117 psn pshome.html</u> (Japanese) [Last visited on Mar. 15, 2012]
   Ministry of Internal Affairs and Communications: <u>http://www.soumu.go.jp/menu\_sosiki/kenkyu/riyousya\_ict/02kiban08\_03000087.html</u> (Japanese)
  - [Last visited on Mar. 15, 2012]

### **Threats Preferentially Dealt With**

Chapter 2 has explained the security threats that were the most socially influential in 2011 as the 10 Major Security Threats for the Year 2012. When focusing on the countermeasures, some of them can be dealt by the system administrators and others may require the involvement of the service providers or should be dealt with as a society. Here, the 10 Major Security Threats Committee ranked the threats according to the priority with which threats should be mitigated by the businesses and organizations. The threats listed in Table 3 include those that can be avoided by applying security patch provided the vendor. It is important for the system administrator to make sure to have a maintenance contract to get security patch from the vendors as well as to prepare a budget for the expense required to examine and apply security patch as a necessary cost.

Rank	Title (the subtitle of those from the 10 Major Security Threats is omitted)	Impact/ Page
1st	APT Attacks	1st / P.14
2nd	Attacks Targeting Unpatched Client Software	4th / P.22
3rd	Website Attacks	5th / P.25
4th	Reuse of the Same Credentials	9th / P.34
5th	Attacks Targeting Smartphones and Tablets	6th / P.27
6th	Unpredictable Disasters	2nd / P.17
7th	Internal Threats	8th / P.31
8th	Hacktivist Attacks	3rd / P.20
9th	Phishing	11th / P.45
10th	Malware to Steal Money (Antivirus Software, Ransomware)	12th / P.45
11th	Attacks Targeting DNS	13th / P.45
12th	Attacks Targeting SNS Users (Short URL, Social Engineering)	15th / P.46
13th	Privacy Invasion	10th / P.37
14th	Danger in Digital Certificates	7th / P.29
15th	Malicious Code Injection to Software	17th / P.46
16th	DDoS Attacks	16th / P.46
17th	Loss of Public Confidence or Economic Damage due to Spread of Disinformation	14th / P.45
18th	Information Disclosure due to File Sharing software	18th / P.46
19th	Unauthorized Use of SIP	19th / P.46

#### Table 3 : Ranking of Threats Preferentially Dealt with

## Chapter 3. Threats against Which Taking Action Is Critical in the Future

In the environment surrounding information security, the innovation of information technology and emergence of new service models have improved the convenience. On the other hand, the new threats have come up to the surface. In Chapter 3, three threats that will be important to take action and mitigate are addressed as examples.

## 3.1. Attacks Targeting Social Infrastructure (Critical Infrastructure)

Critical infrastructure systems that support our social life, such as power, gas, water and transportation, also consist of multiple computers just like information systems. In these systems, the central computers manage and control industrial equipments and devices, and operate the systems. The computers that manage and control the other equipments and devices are called control systems. For instance, the control systems are used for manufacturing at the factory or industrial systems. Among the control systems, those that control and support the mandatory services for our social life, such as power, gas, water and transportation, are called critical infrastructure systems.

Because critical infrastructure systems in the past were not connected to the Internet and their system specifications were proprietary, it has been said that critical infrastructure systems are unlikely to be affected by cyber attacks. In recent years, however, from the perspectives of conveniences and cost advantage, remote monitoring using VPN (Virtual Private Network) has started and the shift from a proprietary system to an Windows or UNIX based control system have pushed the environment of control systems closer to that of information systems. As a result, the threats that threaten information systems have now begun to threaten control systems as well.

Critical infrastructure systems play an important role in supporting our social infrastructures. Thus, the attack will impact our life closely. For example, in the case of the transportation system, it is possible that transportation is suspended since the operation is stopped or time schedule is disrupted. In the case of the water supply and sewerage system, water supply may be stopped and could impact our survival. Since the attacks that target critical infrastructure systems aim to put the into chaos. the impact society is tremendous, should it happen. In overseas, cases that targeted some critical infrastructure systems have already been reported.

In 2003, a traffic signal control system of a railway company in the Eastern U.S. was infected with virus. Three lines around the region were forced to stop or time schedule was disrupted<sup>1</sup>. In another case, a virus infected an U.S. nuclear power plant control system via VPN and the system was shut down for 5 hours<sup>2</sup>. It is premature to think that oversea case studies would impose the same threats in Japan since the conditions such as the system environment and business model are different from those in the U.S. However, Japan should not regard these incidents as the misfortunes of others.

Under such circumstances and under the lead of Ministry of Economy, Trade and Industry, the Initiative for Cyber Security Information Sharing Partnership of Japan (J-CSIP)<sup>3</sup> has been launched in October 2011 with the focus on the manufacturers of the equipments and devices used in critical infrastructures, such as heavy industry vendors and heavy equipment vendors, to share information and take action promptly to prevent the spread of damage caused by cyber attacks. Unlike information systems, keeping the system operated, in other words, the availability of the system tends to be more important for control systems. Critical infrastructure systems are closely involved with our everyday life, thus 24/7 operations are required for their systems. For that reason, it is difficult to stop the

http://news.mynavi.jp/news/2003/08/21/20.html (Japanese) [Last visited on Mar. 15, 2012] systems to apply security patch unlike information systems. How to solve this problem and ensure security is a challenge.

## 3.2. Threats in Using Cloud Computing

According to IT research vendor IDC Japan, it is said that the market size of the domestic cloud computing service (hereinafter referred to as "cloud") as of November 2011 is 68.2 billion yen. Moreover, it is speculated that it will become 255 billion yen in 2015, which is 5.6 times more than that in 2010.

As the cloud service has become prevalent, the security threats for cloud computing have become obvious. IPA's Report by the Study Group for the Infrastructure of the Cloud Computing Society lists the following five patterns as the security threats in a cloud environment.

- (1) Remote attacks against the cloud environment
- (2) Attacks against other cloud users in the same cloud environment
- (3) Attacks that use the cloud as a stepping stone
- (4) Abuse of computing power (such as password cracking or cryptanalysis)
- (5) Other factors (such as power outage, system failure)

The cause of many of the media-covered cloud service incidents that have happened

Mynavi News:

<sup>&</sup>lt;sup>2</sup> Ministry of Economy, Trade and Industry, Japan: http://www.meti.go.jp/press/2011/08/20110805006/20110 805006-3.pdf (Japanese) [Last visited on Mar. 15, 2012]

<sup>&</sup>lt;sup>3</sup> IPA: <u>http://www.ipa.go.jp/security/J-CSIP/index.html</u> (Japanese) [Last visited on Mar. 15, 2012]

in Japan was something other than attacks (such as power outage and system failure, which fall under (5) above). For example, there was a case in 2011 where the file system of a cloud service located in Japan had a system failure and data were corrupted.

Other than five patterns listed above, there exist the security vulnerabilities that may affect the service users in Japan in the future. For example, an attack may exploit the vulnerability that allows an attacker to attack a host OS from a guest OS (i.e. CVE-2009-1244<sup>4</sup>), which falls under (2) above). This kind of attacks that exploit the vulnerabilities in cloud infrastructure software can be done without network (WAN connection nor LAN), and cloud-specific, meaning it is hard to prevent with the traditional security products such as firewalls.

The cloud service providers need to understand cloud-specific, potential threats such as five patterns addressed in IPA's Report by the Study Group for the Infrastructure of the Cloud Computing Society, and take action before the threat will realize. On the other hand, it is important for the service users to understand the cloud-specific threats and demerits and think about what to do. For example, if the user does not have a full control over the cloud service and an incident happens, the user should know that he or she may not be able to obtain the logs needed to investigate the incident, and do what should be done to prepare for that.

As for the things that the user should be careful about in terms of security when using a cloud service or the information that the user should obtain from the cloud service provider, the user can refer to a guideline called the "Security Management Guideline for Using Cloud services" published by Ministry of Economy, Trade<sup>5</sup>".

## 3.3. Management of Smartphones by the Businesses

Recently, adoption of smartphones and tablet PCs by the businesses is growing. According to the survey conducted by JFK Marketing Japan to people who hold an IT-related job in about 1,500 businesses located in Japan, those that have adopted smartphones as of November 2011 is 16 percent. Including those that were planning to adopt, about one-fourth of the businesses have answered they have or are planning to introduce smartphones. Compared to the survey conducted by the same company in September 2010, smartphones has increased by about 1.6 times and tablet PCs have increased by about 2.5 times. Considering such

<sup>&</sup>lt;sup>4</sup> MITRE : CVE-2009-1244

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-200 9-1244 (Last visited on Mar. 15, 2012)

 <sup>&</sup>lt;sup>5</sup> Ministry of Economy, Trade and Industry, Japan:, <u>http://www.meti.go.jp/press/2011/04/20110401001/20110</u>
 <u>401001.html</u> (Japanese) [Last visited on Mar. 15, 2012]

situation, it seems that the speed of the businesses' adopting smartphones will accelerate.

If the use of smartphones in the business proceeds, the business data will be stored more and more on the smart devices. However, because the smart devices have an excellent portability, the risk of loss when being outside or theft grows higher. If important information is stored, the impact that information disclosure will impose on the business will be big. Thus, when adopting smartphones, it is essential to have an adequate device management in place.

In addition, to improve the convenience and reduce cost, an approach called "BYOD (Bring Your Own Device)", a business policy of utilizing the employees' personally-owned device for work, is receiving a lot of attention mainly abroad these days. It may become popular as one form of the use cases of the smart devices in the future but it raises a challenge how far the business should or can monitor and manage personally-owned devices. Especially, the business should be cautious since there is a possibility that by allowing the employees to bring their smart devices into the work place, it may become possible for them to penetrate the existing security defense and take sensitive information out of the office.

As the "Six Principles to Use Smartphone Safely <sup>6</sup> ", IPA recommends and

disseminates the message that it is important to "see a smartphone as a mini PC and manage it like a PC". To be more specific, if a business uses smart devices, it is important to establish a policy about the issues such as the rules of using smart devices, extent of information accessible from them, extent of information that can be stored on them and what to do in case of loss or theft of them. Especially, it is an effective measure to introduce а mechanism like MDM (Mobile Device Management) that allows the company to mandatorily manage things like OS update and what applications can be installed onto smart devices.

As for the things the company should be careful about when using smart devices for business, the company can refer to the "Security Guideline for Using Smartphones Tablets <sup>7</sup> " and bv JSSEC (Japan Smartphone Security Forum) and "Smartphone Security Guideline 8<sup>8</sup>" by **JNSA** (Japan Network Security Association).

http://www.jnsa.org/result/2010/smap\_guideline\_Beta.pdf (Japanese) [Last visited on Mar. 15, 2012]

<sup>&</sup>lt;sup>6</sup> IPA: Computer Virus/Unauthorized Computer Access

Incident Report – July 2011

http://www.ipa.go.jp/security/english/virus/press/201107/ <u>E\_PR201107.html</u> (Last visited on Aug. 17, 2012)

<sup>&</sup>lt;sup>7</sup> JSSEC: Security Guideline for Using Smartphones and Tablets

http://www.jssec.org/dl/guidelines2012Enew\_v1.0.pdf [Last visited on Aug. 17, 2012]

JNSA:

## [Appendix] Unselected 10 Major Security Threats Candidates

This section introduces the candidates for the 10 Major Security Threats for the Year 2012 that have been left out of the final selection but had an impact on the society in 2011.

#### 11th. Phishing

The existence of phishing websites that looked like targeting Japanese users and spam emails that tried to lure the users to malicious websites were confirmed. The techniques to deceive people are getting cunning. For example, not only were these websites and emails written in Japanese but also they take advantage of the Tohoku Earthquake.

 Mynavi News: <u>http://news.mynavi.jp/news/2011/11/14/048/index.html</u> (Japanese) [Last visited on Mar. 15, 2012]

#### 12th. Malware to Steal Money (Antivirus Software, Ransomware)

Many fake antivirus software and ransomware (ransom-demanding malware) that prompted to enter the financial information, such as credit card numbers, were observed. Malware that supports Japanese have also been observed, making it difficult for the users to distinguish good ones from bad ones.

 CNET Japan: <u>http://japan.cnet.com/news/business/35000267/</u> (Japanese) [Last visited on Mar. 15, 2012]
 IPA: Computer Virus/Unauthorized Computer Access Incident Report – August 2011 <u>http://www.ipa.go.jp/security/english/virus/press/201108/E\_PR201108.html</u> [Last visited on Aug. 17, 2012]

#### 13th. Attacks Targeting DNS

Vulnerabilities in DNS and attacks against DNS were reported. For example, harm was done by a vulnerability which caused the abnormal ending of the DNS servers, and the DNS servers that were susceptible to cash poisoning were discovered. They were the eventd of great impact since DNS is part of the essential Internet infrastructuret.

- Securelist: Massive DNS poisoning attacks in Brazil Securelist
   <u>http://www.securelist.com/en/blog/208193214/Massive\_DNS\_poisoning\_attacks\_in\_Brazil</u> [Last visited on
   Mar. 15, 2012]
- JVN: http://jvn.jp/cert/JVNVU535830/ (Japanese) [Last visited on Mar. 15, 2012]
- @IT: <u>http://www.atmarkit.co.jp/news/201111/17/bind9.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- IPA: <u>http://www.ipa.go.jp/security/ciadr/vul/20110706-bind9.html</u> (Japanese) [Last visited on Mar. 15, 2012]

#### 14th. Loss of Public Confidence or Economic Damage due to Sread of Disinformation

There were the cases where disinformation was disseminated through some media such as Twitter and blogs, and that led to loss of public confidence and/or economic damage. While anyone can disseminate information easily and the amount of information we can refer to has increased, it has become difficult to judge the reliability of the information.

- ITmedia: <u>http://www.itmedia.co.jp/news/articles/1104/07/news077.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- ITmedia: <u>http://www.itmedia.co.jp/news/articles/1108/01/news091.html</u> (Japanese) [Last visited on Mar. 15, 2012]

#### 15th. Attacks Targeting SNS Users (Short URL, Social Engineering)

Attacks that infect the SNS users' PC with malware by using the SNS service as medium, exploiting short URLs and social engineering were observed. If infected, there is a possibility that sensitive information is stolen.

- TrendLabs Security Blog: <u>http://blog.trendmicro.co.jp/archives/4368</u> (Japanese) [Last visited on Mar. 15, 2012]
- SBI Serchina: <u>http://news.searchina.ne.jp/disp.cgi?y=2011&d=0824&f=it\_0824\_001.shtml</u> (Japanese)
   [Last visited on Mar. 15, 2012]

#### 16th. DDoS Attacks

DDoS attacks that target specific organizations or government agencies were observed. While being forced in a denial of service condition, the business cannot provide the services. The attacks caused not-so-small economic and social damages on the society, such as loss of business opportunity and shutdown of public services.

- INTERNET Watch: <u>http://internet.watch.impress.co.jp/docs/news/20110304\_431179.html</u> Japanese) [Last visited on Mar. 15, 2012]
- CNET Japan: http://japan.cnet.com/news/service/20426999/ (Javanese) [Last visited on Mar. 15, 2012]

#### 17th. Malicious Code Injection to Software

There were cases where malicious code was injected into source code of open source software released on the software's official website. By using the compromised source code, there is a possibility that the users' PC may be infected with malware without their knowing it

it.

- ITmedia: <u>http://www.itmedia.co.jp/enterprise/articles/1106/23/news019.html</u> (Japanese) (Last visited on Mar. 15, 2012)
- Security NEXT: <u>http://www.security-next.com/22158</u> (Japanese) [Last visited on Mar. 15, 2012]

#### 18th. Information Disclosure due to File Sharing Software

The cases where PCs are infected with virus though file sharing software and the information stored in PCs are disclosed are still happening. There is a possibility that the business information is stolen via file sharing software.

- Mynavi News: <u>http://news.mynavi.jp/news/2011/10/18/018/index.html</u> (Japanese) [Last visited on Mar. 15, 2012]
- ITmedia: <u>http://www.itmedia.co.jp/enterprise/articles/1108/04/news065.html</u> (Japanese) (Last visited on Mar. 15, 2012)

#### 19th. Unauthorized Use of SIP

Attacks that target SIP servers and SIP supporting devices used in growing IP phone services were observed. Some organizations were indeed charged for the communication they do not know.

• @IT: http://www.atmarkit.co.jp/news/201102/08/jpcertcc.html (Japanese) [Last visited on Mar. 15, 2012]

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

- [ Editor ] Hideaki Kobayashi Chisato Konno
- [ Advisor ] 10 Major Security Threats Committee
- [ Author ] Masashi Ohmori Isaso Kaine Shunsuke Taniguchi Noriko Tanamachi

# 2012 Edition 10 Major Security Threats ~ Changing and Growing Threats ~

March 22, 2012 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/index-e.html

## 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 computers have been infected by viruses, please report to IPA.

#### Software Vulnerability and Related Information

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

#### **Unauthorized Access**

When you detect unauthorized access to your computers via network (e.g. the Internet, 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 websites, please report to IPA.

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



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/