The Usefulness of Audit to Guarantee the Security on the Electronic Systems

Rie Shigetomi Yamaguchi
Research Institute for Secure Systems (RISEC),
National Institute of Advanced Industrial Science and Technology (AIST)
1-1-1 Umezono, Tsukuba, Ibaraki, 305-8568
JAPAN
e-mail: rie-shigetomi@aist.go.jp

Hajime Watanabe
Research Institute for Secure Systems (RISEC),
National Institute of Advanced Industrial Science and Technology (AIST)
1-1-1 Umezono, Tsukuba, Ibaraki, 305-8568
JAPAN
e-mail: h-watanabe@aist.go.jp

***Abstract*—In a conventional system, people have created a mechanism to take advantage of collateral security by using audits without being checked by users. However, in recent electronic systems, the users need to do many things to guarantee the security. In this paper, we discuss how to use audit systems to archive security in digital communications.**

Keywords-Audit; Security; Usability.

I. INTRODUCTION

Recently, in terms of ensuring convenience and cost effectiveness, a lot of paper-based services have been replaced by network services, for example, postal mail by email. The more people use digital information and network communications, the more people surface information security issues. For example, the number of the exploitation of information and money has been increasing in the Internet.

Although there are several things that a user must do in order to improve security, a user cannot be told to do something. It is difficult for a user not only to show the state of security, but also whether a user can select the state of the security on the setup mode of the computer. One example to show security to the users is a trial that show warning to the users in the Internet browsers, such as Internet Explorer [6] and Firefox [7].

If a user cannot verify a web server in SSL/TLS [1], the user can see warning sign on the screen such as the Figure 1 and Figure 2 [3]. The site certificate for SSL/TLS is installed in Browsers.

If a user tries to connect to a server via SSL/TLS and the server's site certificate is valid, then an SSL/TLS connection is established between the user and the server. On the other hand, if a server's site certificate is invalid, that is, the server's certificate is not in the certificate chain, the user must see warning that she should not connect the server.

A service shows instructions that the user should push the button to ignore. Even browsers show the warning, the service encourage users ignore warning, select to push "red" button, and connect the server which is not confirmed. That is because servers do not buy right server certificate for SSL/TLS and install the certificate correctly. That means that the user cannot understand the read sign meaning, that it is unable to verify the certificate and the user might connect fake serer. After the user sees that the server recommends pushing "red" button, the user misunderstand it is right way to push "red" button. The user cannot recognize the server has got the risk and avoid the dangerous server.

In recent years, this problem is solved because most web sites have got right certifications. We need to discuss that the user has misunderstood such that the server recommends ignoring the warning. The way to ignore the warning is wrong way to lad to the user misunderstanding for security.

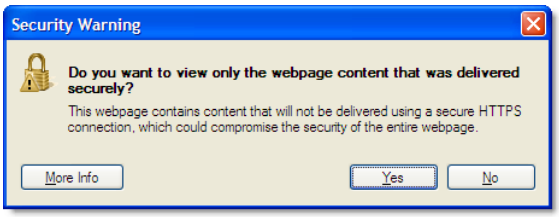

Figure 1. IE8 Security warning.

Users do not have to do anything to archive security in the non-digitized system. One example is the voting system. People do not have to see all processes, but know all processes proceed correctly. This is because users know there is a strict law and the system uses audit system.

In digital communications, a lot of kinds of process are designed simplify and straightforward. In the conventional systems, people have created a mechanism to take advantage of collateral security by using audits without having checked by users. In the current social system, taking advantage of even such as audit and evaluation and certification, and has incorporated confirmation by third-party organization. This is because you cannot verify that their users to understand how everything on the market, if they are realized as how it works.

In this paper, we discuss how to use audit system to archive security in digital communication.

We take two examples for the conventional system: voting system and board of audit in the government. In addition, as they are digitized system, we discuss how to show security in two situations key issue by using card or SSL/TLS in browsers.

 ISBN: 978-1-61208-249-3

Figure 2. IE8 Security warning (in Japanese), they say "There is a problem that security certificate for this Web site."IE8 Security warning.

A. Outline

The paper is organized as follows. Section 2 introduces the relationship of the current audit and security. Section 3 shows and discusses two example of audit for electronic communication. Section 4 discuses another topic for audit. Section 5 concludes the paper.

II. RELATIONSHIP OF THE CURRENT AUDIT AND SECURITY

A. Conventional Voting

We explain how to archive security in the current voting system. We describe how to prohibit unauthorized acts such as double voting and how to protect privacy [4].

1) Prohibition double voting fraud

In order to prevent double voting fraud, it has to check to pass the ballot correctly and to vote properly. The Board of Elections manages this process by using the poll book.

According to the poll book, the Board sends the information by mail to a person, who has the election franchise, before the Election Day. This information is a kind of a certificate or a ticket for voting, include where and when the person can vote, and organize number. A person brings the mail to the polls and shows the mail to vote officers who checks whether he or she has the right to vote in this election.

To prevent double voting fraud is made sure that vote officers are able to check whether the voter has the right mail.

2) The correctness of elections

In conventional voting, it is difficult for most people to check whether their ballot is counted correctly because users do not see all process of voting after the elections.

To solve this problem, in conventional voting scrutinizer, there is a person called a scrutinizer who has selected from the electoral roll and checks voting correctly. In other words, there is audit system to verify all procedure correctly by neutral observers.

The scrutinizer selected by the Board of Elections see every process of vote counting such that this procedure is third party verification. The poll watcher checks whether the people vote correctly, and sends ballot box to ballot-counting station. After checking all process, ballot-counting officers count the votes under checking by scrutinizer.

3) Privacy

In election, nobody is able to link between ballots which is written by voter and the poll book, so nobody knows anyone who vote for.

To achieve this privacy requirement, the current system selects the following system:

- Voting paper does not include voter's name
- People use the same ballot paper; so, it is very difficult to select which paper is whose.

The voter knows, by third party such as scrutinizer, that this procedure is correct and the privacy is protected.

In the current systems, people do not have to check that an election is correct by them, because of checking by third party audit.

B. Board of Audit

In this section, we explain who check the government uses our taxes legally by Board of Audit.

1) Tax Obligation

People living are obligated to pay taxes. It is necessary to gain taxpayer acceptance for the use of taxes. That means that people need to check the way tax money is used because tax is by people.

2) Board of Audit

Because taxpayers want to check the use of tax, for this checking, there is Board of Audit. The Board of Audit is a constitutional organization that is independent of the Cabinet and belongs neither to the Diet nor to the Courts. The Board of Audit audits the national accounts as well as those of public organizations and other bodies as provided by laws, and also supervises of public accounting to ensure its adequacy.

Because there is this kind of system, taxpayers do not have to check national account by themselves.

III. CONVINCING USERS ON SECURITY

It is important to convince users that the system is secure. In this section, we explain how to show to archive security and discuss how to reduce user's burden in two recent systems: the process of key issue to card and warning of SSL/TLS at the browser.

A. Key Issue to IC Card

In a PKI system, the issuer of root certificate issues user's key, who asks to be provided the service. We explain how to get secret key to user by the issuer to service.

1) Security Requirements

In this process, the most important thing is a user's secret key issued by a rigorous process. The user signs a document

 ISBN: 978-1-61208-249-3

with the key. A verifier verifies the signature of the document by the public key of the user.

The secret keys are known only by the user. The difficulties of this situation are difficulties how to explain to create key by the user. After creating the key correctly, to manage the key, which not reveal the key to anyone, is important but difficult for the user. If the computer might be contaminated such as a virus, the key might leak to adversaries.

The solution is to keep the key in the card of tamper-proof.

2) How to protect secret keys

If the system adopts the card process, still there are some difficulties for the user.

When the user creates the key by herself to be provided the service, she must use her personal computer or electronic computing equipment. However, when the card system adopts is the user's equipment, the process of key issue might be under adversaries' attacks.

To solve these problems, Japanese government adopts the dedicated system to create the user's key. To use this system, when the user needs the keys for the service, the user do not have to get the special system before getting the card but the user needs to go to the municipal office [5].

The user's process of key issue is as follows:

1. When a user wants to get certificate for electronic application by the government, she goes to the municipal office.
2. The user asks the municipal officer to create it; the municipal officer and users do the paperwork. By the paperwork, the officer is able to check the user identities.
3. The municipal officer asks to the user to go to the dedicated system in the office. The dedicated system is able to create public and secret keys of PKI and save these keys to the user card. Even the municipal officer, nobody is able to know keys information without the user.
4. The user creates public and secret keys of PKI and saves the keys to her card by using the dedicated system by her.

In this process, there is only the user in front of the dedicated system. That means this keys are known by only the user. Even officers to help users are not able to know it.

Officers have to wait near the user during the user creates the keys. This process is very complicated.

3) Discussion

After this process, the user might be convinced PKI better that the secret key is known by only user. However, this approach is very time consuming; the user needs to go to municipal office, and the officer needs to help during creating keys by users but does not see the user's operation.

This system have been under the assumption that the government officer is not able to be trusted. It is time-consuming that the user needs to go the municipal office and go to two places in the office. If there is a mechanism to audit system and users are able to trust the system, then there is an easier way to issue generate a key pair; generating the card of the key pair is in the trusted factory audited to third-party organization, and the card is delivered by trusted mail process.

There might increase the risk of leakage of the secret key because more people involved in this process; but this problem should be resolved in an operational process. This process makes people be better time-consuming that a user does not have to go to the municipal office and operate the system by herself.

All what a user has to do is to receive the card by mail.

B. SSL/TLS in Browsers

Over the Internet communication, such as web surfing, it is important for a user to protect from attacks that the user is able to verify the person whether a user wants to communicate. One solution is to use SSL/TLS communication.

1) SSL/TLS

SSL/TLS is based on PKI. In the beginning of the connection to a server via SSL/TLS, the browser asks the server to send the public key certificate.

The company to manage the root certificate checks the web's legitimacy; create a secret key, the public key, and the certificate for the keys, and sends them to the web site. After the web server receives the certificate, the server installs them to their web server software. If the server installs correctly, the user can connect SSL communication to the server.

2) Discussion

In issuing the certificate of public key site by CA, there is a kind of audit process to manage a web site. By using this process, a user does not have to install certificates of all public keys of web sites. This is to reduce the trouble of the user without one problem.

If a user wants to connect a server which has not installed the web certificate correctly, the browser shows the waning sign in the Figure 1. That means the browser recommend to the user to keep securely. However, the user is able to ignore warning [2]. That is because there is a description written by the web server that the user ignore the warning sign, up on the shelf the server cannot be installed properly.

The registration process is correct way but the user can be avoided from correct process. This means the audit is able to be eliminated by pressing the red button even having correct audit.

IV. SOFTWARE AUDIT

In this section, we discuss other items for resolution for audit in information technology system.

It is difficult to make sure that the security features are implemented correctly in the software. If a software is open-sourced and this is a kind of third party evaluation, the software is confirmed but has a problem of maintenance and integrity. Because a conventional IT system is simple, it is difficult to mix unjustness function. As the complexity of the

recent IT systems increased, it is difficult understand all of the software details.

Therefore, there is a need for a mechanism of verification for the implementation of the software audit.

V. CONCLUSION AND FUTURE WORK

In the recent systems, security measures are required; but, it must have a way that can be used without difficulty by the user. For non-electronic security measures, the burden of the user is reduced; so, goes with the audit of the election.

In this paper, we discussed that audit process is necessary for IT system. Not only the audit, but the process should be realized in a right operational process. To ensure that all, security should be ensured.

When developers create security systems, they have to discuss the balance between security and usability. Because nowadays developers have high skills for IT and especially security, and they tend to make the system which made full use of advanced technology. However users do not have such high advanced technology skills; so, the users cannot master such systems. On the other hand, users who have not IT skills fall to the hole of security easily. Before creating a system, there should have a discussion about the usability and security between developers and users since the system engineer has to do ad hoc security patch after the system starts.

[1] IETF Internet Society, "The TLS Protocol Version 1.0", http://www.ietf.org/rfc/rfc2246.txt, Jan 1999

[2] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Cranor, "Crying wolf: An empirical study of SSL warning effectiveness,", in Proceedings of Usenix Security 2009, pp. 399-416, Monreal Canada, Aug 2009

[3] Microsoft, "There is a problem with this website's security certificate when you try to visit a secured website in Internet Explorer", http://support.microsoft.com/kb/931850, [retrieved 20 Nov 2012]

[4] Ministry of Internal Affairs and Communications, "Japanese Election", (in Japanese) http://www.soumu.go.jp/senkyo/senkyo_s/naruhodo/index.html, [retrived 20 Nov 2012]

[5] Ministry of Internal Affairs and Communications, "Juuki-card Issue", (in Japanese) http://juki-card.com/syutoku/index.html [retrived 20 Nov 2012.]

[6] Microsoft, "Internet Explorer", http://windows.microsoft.com/en-IE/windows/home [retrived 20 Nov 2012].

[7] Moxilla, "Firefox", http://www.mozilla.jp/firefox/, [retrived 20 Nov 2012].

 ISBN: 978-1-61208-249-3