ICHIGAN Security – A Security Architecture that Enables Situation-Based Policy Switching

Hiroshi Maruyama*, Kiyoshi Watanabe†, Sachiko Yoshihama‡,
Naohiko Uramoto‡, Yoichiro Takehora§, Kazuhiro Minami*
*The Institute of Statistical Mathematics
The Research Organization of Information and Systems
Tokyo, Japan
Email: hm2@ism.ac.jp, minami.at.uiuc@gmail.com
†Microsoft Services
Tokyo, Japan
Email: kiwatana@microsoft.com
‡IBM Research – Tokyo
Tokyo, Japan
Email: sachikoy@jp.ibm.com, uramoto@jp.ibm.com
§Keynote Systems, Inc.
Tokyo, Japan
Email: Yoichiro.Takehora@keynote.com

***Abstract*—Project ICHIGAN is a voluntary-based attempt to build a reference IT architecture for local governments that can withstand large-scale natural disasters. This architecture is unique in that 1) it has the concept of *phases* of the situation for which different priorities on non-functional requirements are applied, and 2) the functionalities and services provided by the IT systems in the suffered area will be taken over by those of the "coupled" local government. These features pose specific challenges on the information security policy, especially because different policies need to be applied for the different modes. This paper describes two key elements to enable the policy; policy templates and deferred authentication.**

I. Introduction

At the 3.11 earthquake in 2009 in Japan, many local governments lost their functions and they took long time to recover. At the City of Rikuzen-Takata, the tsunami reached to the fourth floor of the city office building, and their data servers located on the first floor were completely submerged under the sea water. It took them four months to recover the data from the damaged hard drives and magnetic tapes and to resume the pre-disaster level of the public service[1]. The loss of the data of the local governments prevented effective relieve activities to the suffered areas. Resilient IT systems would have greatly improved their effectiveness and could even have saved many lives.

On May 25th, 2011, a number of well-known IT architects in Japan got together and launched a voluntary activity called *Project ICHIGAN*. The goal is to build a reference IT architecture for local governments that can withstand large-scale and wide-area disasters. The basic ideas behind the architecture are that 1) it has the concept of *modes* depending on the phases of the situation, and 2) the functionalities and services provided by the IT systems in the suffered local government will be take over by the "coupled" local government. These features pose specific challenges on the information security policy, which the authors of this paper were responsible for.

[1]See the report "Research on the local governments' responses to the Great East Japan Earthquake and their future plans," available at https://www.lasdec.or.jp/cms/9,26859,24.html (in Japanese).

A. Motivating Scenario

Consider the following scenario:

> In the year 202X, a combined Tonankai-Nankai earthquake (magnitude 9+) hits south-west of Japan. Town of Minami-Ise (population 16,000) was hit by the tsunami that took place short after, and the function of the local government is severely damaged. Three hours later, an officer of Japan Ground Self-Defence Force phoned Mr. Ota, a local government employee, asking for the list of all the residents in the town for their rescue operations. The backup IT system is already active by the coupled local government, but Mr. Ota has no access privilege to the database. He has no access to his superiors to obtain an approval, either. What has Mr. Ota to do?

The ICHIGAN reference architecture (hereafter ICHIGAN RA) defines the phases, such as *EarlyWarning*, *Emergency-1*, *Emergency-2*, etc. that are to be declared by the local government according to the situation of the disaster. These phases imply different priorities on the requirements on the business processes and IT systems, some of which (such as confidentiality, availability, and integrity) fall into the category of the information security policy. For example, Mr. Ota in the above scenario should be allowed to access the system although he has no authorization to do so in a normal situation.

Thus, the information security policy should also be switched according to the phase.

Many security policies have explicit "exception" provisions to deal with emergency situations. For example, the Japanese Personal Information Protection Law[2] allows the use of privacy information in an emergency situation in which people's lives and/or properties are in danger. However, it is not clear in which situations these exceptions apply. It is too much burden for the field personnel to make such decisions. Instead, we institute organization-wide temporary change of policy that is declared top-down.

II. Scope

When a disaster occurs a local government needs to perform disaster-time specific tasks such as providing assistance to suffered citizens. ICHIGAN RA introduces the following concepts into the processes and IT systems of a local government.

Disaster-time Tasks:
: Tasks to be performed by a local government in case of a disaster. These tasks include creating and maintaining the master record of the suffered citizens, confirming the safety status of the citizens, providing shelter, food, healthcare, and other assistance to the suffered people. Also there are tasks that cannot be pre-planned before a disaster, such as radioactivity measurement after the Fukushima nuclear power plant disaster.

Disaster-time IT Systems:
: IT systems that are used for disaster-time tasks. Some systems are pre-developed and become online when a disaster occurs. Other systems are developed after the disaster.

Coupling:
: Transfer of business processes and/or IT systems from a suffered local government to the assisting local government. We assume that a local government is paired with a remote local government and has a mutual agreement so that in case of disaster in one local government, the other can back up the processes and the IT systems of the suffered local government.

In defining ICHIGAN security policy, we assume that the local government already has implemented a sound security policy based on the best practices such as ISO27001[4] or the security guidelines defined by the Ministry of Internal Affairs[3]. Our security architecture then considers the protection of the processes and IT systems newly introduced by ICHIGAN RA, as shown in Fig. 1.

In order to make the idea of *coupling* work, there are two preconditions:

1) Coupled local governments have ability to interoperate their IT systems and to migrate their systems from one location to another if necessary. Many cloud computing services provide this capability. Also Global Inter-Cloud Technology Forum[3] defines such technical specifications explicitly.
2) Coupled local governments have compatible business processes defined in a common language. For example, The Association for Promotion of Public Local Information and Communication (APPLIC)[4] defines such business processes.

[2]http://www.caa.go.jp/seikatsu/kojin/houritsu/index.html

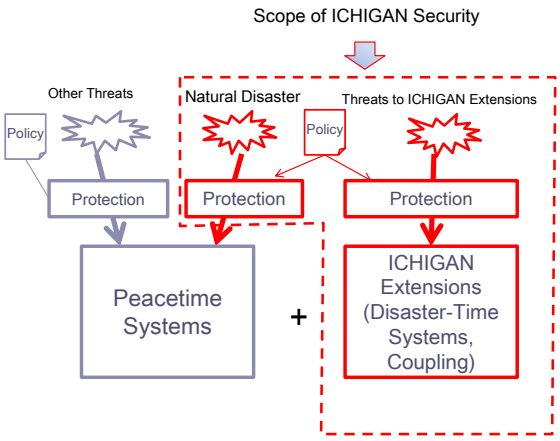

Fig. 1. Scope of the ICHIGAN Security Architecture

Our security architecture is designed so that the coupled local governments can compare their security policies and make necessary adjustments to make them compatible should the necessity arises.

III. Phases

ICHIGAN RA defines the following six phases.

Normal:
: Ordinary time. The local government performs normal operations. Also emergency drills are performed in this phase.

EarlyWarning:
: When a large disaster is imminent, the chief of the local government declares the *EarlyWarning* phase. The disaster countermeasures office is set up. The local government prepares for launching the disaster-time systems and transferring the processes to the coupled local government.

Emergency-1:
: On the event of a large disaster, the chief of the local government declares *Emergency-1*. Emergency response units such as the police department, fire department, and Japanese Self-Defence Force are mobilized for rescue operations. Temporary shelters are set up. The disaster-time systems become online.

Emergency-2:
: The local government starts providing basic public services to the suffered people in temporary

[3]http://www.gictf.jp/index_e.html
[4]http://www.applic.or.jp/

shelters or people staying at home but without power/water/etc. Safety confirmation, healthcare services, food/water/living necessity supplies are provided. Many public services are performed in less ideal environments (e.g., no regular power supply, no landline communication, etc.) Disaster-time systems may rely on offline devices such as tablets.

Recovery-1:
: The chief of the local government declares the dissolution of the disaster countermeasure office. People start returning to their homes. Subsidies to rebuild houses, offices, and other infrastructures are provided.

Recovery-2:
: All the shelters are closed. Long-term rebuilding plan starts. All the peacetime systems are in full service. Most (if not all) of the disaster-time systems are shutdown.

A typical phase transition is shown in Fig. 2. This diagram shows typical transitions only. Depending on the situation, some phases can be skipped. For example, if there is no advance warning, the phase can go directly into *Emergency-1* from *Normal*. The *Normal* and *Recovery-2* phases are called *Peace-Time*. The other four phases are called *Disaster-Time*.

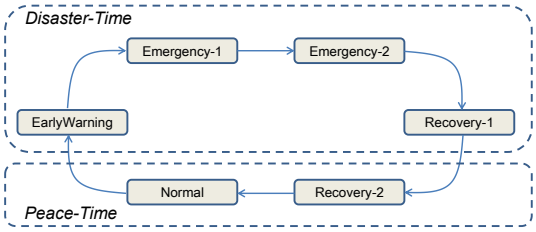

Fig. 2. Phase Transitions

IV. Switching Policy

Security policy of an organization is usually defined by a set of documents, such as *security policy*, *security guidelines and standards*, and *security procedures*. We call a particular combination of these documents a *policy set*. At a given time, we assume that only one policy set is active across for the local government. Each phase must be associated with a policy set. In the following subsections we describe the *policy templates* for *Normal*, *Emergency-1*, and *Emergency-2* only. The policy templates for the other phases are omitted due to the limitation of space. See [2] for full descriptions. Each local government is expected to modify their security policy based on these templates.

A. Information Asset Classification

Disaster-time systems such as the master record of suffered citizens would have higher priority on availability than confidentiality and integrity. Even in these emergency situations, however, the peace-time security levels of the local government need to be maintained as much as possible. To achieve this goal, we recommend to implement an additional classification of the information assets as follows:

Confidentiality-Sensitive:
: Information assets that require high confidentiality and have less needs to be used in an emergency. For example, privacy-sensitive information such as income information and tax status are not critical in emergency, and thus classified as *Confidentiality-Sensitive*. On the other hand, information such as name, address, healthcare needs is not categorized as *confidentiality-sensitive* because this information has to be available for rescue and aid operations.

Integrity-Sensitive:
: Information entered via disaster-time systems may contain errors due to the confusion of the field operations or lowered security levels. Therefore, this information should not be mixed with the information with high integrity of the normal operations. Especially, the low-integrity information must not be written-back to the high-integrity databases of the peacetime systems. To prevent this, we define some information as *integrity-sensitive*. Examples include audit trails and the basic (and stable) attributes of residents, such as names and date of birth.

B. Normal *Policy Set*

The *Normal* policy set is the base policy of the peace-time. In addition, the *Normal* policy set should define a procedure for transition to the *EarlyWarning* phase or the *Emergency-1* phase. This is done by the declaration of the chief of the local government. In case that the chief is not available (for example, she or he is incapacitated immediately after the disaster), the policy set should clearly define the condition of automatic transition to *Emergency-1*.

Also in the *Normal* policy set, you should define a set of procedures to perform emergency drills. These drills should not present a window of vulnerability even if the drill involves tests on the switching procedures of the policy sets.

C. Emergency-1 *Policy Set*

In the *Emergency-1* phase, citizens's lives are in danger. The availability of information may determine the life-or-death situation. Since the survival rate of suffered people drastically declines after 72 hours of the suffering[1], this phase should be at most 72 hours long.

This policy set only applies to the disaster-time systems. The peacetime systems that may be operational during the *Emergency-1* phase should follow the peacetime policy set. However, the office of disaster countermeasure may temporarily apply this policy set to the peacetime systems if absolutely necessary.

In case of emergency, proper authentication may not be possible or practical. For example, a legitimate personnel may have lost his/her ID credential. Even so, the availability of the information asset may be critical to save lives and

properties. Therefore, we introduce a new concept called *deferred authentication* in this policy set.

1) Deferred Authentication: In the phase of *Emergency-1*, we allow access to the critical information without proper verification of identity. However, we *do* require *claim* of the authentication recorded that can be later verified. To do this, we collect the *claim* of the identity when an access is attempted. For example, a local government employee enters the userid and password to the system but the directory of the system is not available and the identity can not be confirmed at the time of access. Nevertheless, the identity claims will be recorded and later verified.

The identity claim could be gathered in many different ways. For example, a hand-written memo on a piece of paper saying that "Hiroshi Maruyama logged in to the system on the request of JSDF officer Mr. XX, witnessed by Sachiko Yoshihama on March 11th, pm 1:20" could be a recorded claim. Or the biometrics of the user (e.g., the picture of the user) can be recorded by a surveillance camera that is automatically turned on when the *Emergency-1* phase begins.

When a deferred authentication is performed, its verification must be done without delay after the verification systems become available. If an illegal access is found in this process, it must be handled as a security incident. Also all the updates that were done under the false identity must be able to be undone when necessary. More rigorous discussions on retrospective security enforcement are done by Dean Povey in 2000 [6].

Deferred authentication is not a proper authentication. The system's confidentiality and integrity may be compromised due to the introduction of deferred authentication. Still, in case of an emergency the availability of information may have higher priority to confidentiality and integrity. We have to balance among these security requirements.

D. Emergency-2 *Policy Set*

After 72 hours of the disaster, the focus of the local government shifts to the assistance to the citizens who suffered. Particularly important in the view of IT systems is makeshift applications that are essential to support the victims.

1) Acquisition of Disaster-Time Systems: Some disaster-time systems are pre-planned. For example, we can anticipate that the master records of suffered is something that is needed in any large-scale disasters. However, some systems are not anticipated and thus must be developed on the spot. The radioactive measurement and mapping application in the face of the Fukushima nuclear power plant failure is one example. These applications must be deployed without delay. Some applications may be developed by a group of volunteers who have no idea about the acquisition process of the local government.

The normal testing and acquisition procedures may be too conservative for these applications to be deployed in a timely fashion. Therefore, we recommend to relax the conditions of acquisition in the *Emergency-2* phase. We anticipate many makeshift applications developed for supporting the people staying in the temporary shelters.

2) Infrastructure Requirements: In temporary shelters there would be severe restrictions on the infrastructure, such as the loss of power supply and network connections. Also some IT equipment that are retrieved from reserved resources may not be up to the latest standards (e.g., running older versions of operating system). These machines may not be allowed according to the normal set of policies, but nevertheless must be used to help the people in a greater need. We allow a temporary degrade of security requirements on infrastructure, provided that this would not compromise the confidentiality and integrity of the confidentiality-sensitive and integrity-sensitive information assets as defined in the policy. For example, the disaster-time systems need to be separated from the peacetime systems via a firewall.

3) Federated Authentication: In the phase of *Emergency-2*, we expect that relief personnel from other organizations (such as those from other local governments, national governments, and volunteers) will use the disaster-time systems. It would be too much burden to resister all of their accounts one-by-one into the system. To reduce this complexity, we recommend to use a federated authentication system introduced into the disaster-time systems. For example, you can allow anybody who has a proper authentication of the federated organization (such as those in another local government, the national government, or any other government affiliate organizations such as national universities) can have an access to some systems. This will greatly reduce the complexity of account management of the disaster-time systems.

V. IT Platform Requirements

The above security policy requires unique features on the supporting IT. These features include switchable authentication mechanism, audit trails, and cross-system global variable for holding the phase information, which we will describe in the following subsections. These features will be included in the other parts of ICHIGAN RA (especially in the Application Architecture and Data Architecture).

A. Authentication Mechanisms

Since this policy requires different authentication methods (differed authentication in *Emergency-1* and federated authentication in *Emergency-2*), it is desirable that the applications have a pluggable authentication mechanism.

B. Audit Trails

In the *Emergency-1* and *Emergency-2* phases the security level is temporarily decreased. This presents a window of potential attacks on the systems. ICHIGAN RA requires that even in emergency situations all accesses and updates are recorded in the audit trail so that any incidents can be analyzed and possibly corrected *after the fact*. These audit trails are treated as *integrity sensitive*, meaning that even administrators cannot erase or modify them.

ICHIGAN RA defines the items and the format of the information recorded in the audit trail. Especially important is the operations on the databases – who accessed what information.

To do this, all the end-user identity must be propagated to the backend databases. ICHIGAN RA recommends to use middleware that provides this capability without too much effort on the programmer's side.

C. Maintaining and Propagating the Phase Information

When operating this security architecture, it is paramountly important that every stakeholder has unambiguous understanding of the current phase in effective. If somebody thinks that it is *Emergency-1* and others do not, there is a significant security risk. Therefore, the local government must provide a mechanism to communicate the current phase to everybody in the organization. One way to do this is to have a global variable that is shared by the all applications and to always display the current phase on the screen of any applications. Also the local government must to have a countermeasure against illegal modification of the phase information.

VI. Deploying ICHIGAN Architecture

ICHIGAN RA assumes that the non-functional requirements (including security) may change depending on the current phase. This introduces new threats to the system, such as an adversary illegally changes the current phase from *Normal* to *Emergency-1* and take advantage of the deferred authentication to steal confidential information. The local government has to recognize these additional risks and manage them.

We recommend the local government who intends to implement ICHIGAN RA to reexamine the existing security policy in the following steps:

1) Determine the scope
2) Define the threat model
3) Set the security goals
4) Define the policy set for each phase
5) Determine the requirements to the IT systems
6) Modify the operating guidelines

In particular, we believe that it is very important for all the stakeholders to understand the threat model and the security goals and implement appropriate risk management strategies.

VII. Concluding Remarks

Many security policies have "exception" provisions that can be used in the case of emergency. However, ambiguous interpretations of these provisions will lead to an uneven security level, especially for a large organizations such as a local government. In many cases, the field personnel do not want to take a risk to make their own decisions. ICHIGAN security will make sure that every stakeholder has the common understanding of the current policy set and let them perform their tasks even in the case of emergency. In this sense, ICHIGAN security tries to empower the field personnel, which is recommended in ISO22320 (Emergency Management - Requirements for incident response)[5].

ICHIGAN RA is still under development but we expect that some local governments will consider as the baseline for their more resilient IT systems. Once the architecture is in use in real systems, we will learn more and adjust the architecture accordingly.

References

[1] F Fiedrich, F Gehbauer, and U Rickers. Optimized resource allocation for emergency response after earthquake disasters. *Safety Science*, 35, 2000.

[2] H. Maruyama, K. Watanabe, S. Yoshihama, N. Uramoto, and Y. Takehora. Ichigan security architecture rev 0.3. 2012. http://hiroshimaruyama.org/about/publications/20120324IchiganSecurity-v0.3.pdf (in Japanese).

[3] Ministry of Internal Affairs. Guideline on information security policy of local governments. 2010. http://www.soumu.go.jp/denshijiti/jyouhou_policy/pdf/100712_1.pdf (in Japanese).

[4] Intenational Standard Organization. ISO/IEC 27001 – information security management system. 2005.

[5] Intenational Standard Organization. ISO/IEC 22320 – emergency management - requirements for incident response. 2011.

[6] Dean Povey. Optimistic security: a new access control paradigm. In *Proceedings of the 1999 workshop on New security paradigms*, NSPW '99, pages 40–45, New York, NY, USA, 2000. ACM.