Asian Journal of Information Technology 16 (2-5): 282-286, 2017
ISSN: 1682-3915

A Comprehensive Review of e-Government Security

Tri Kuntoro Priyambodo, Uzayisenga Venant, Tatang Irawan and Devi Valentino Waas
Department of Computer Science and Electronics, Gadjah Mada University,
Yogyakarta, Indonesia

Abstract: The e-Government (eGov) has become an increasingly important program of governments that has been implemented in almost all countries: developed countries as well as underdevelopment countries. E-Government programs ought to be the use of online services by citizens for obtaining information and also for interacting and transacting with the government services. Many problems from various sectors have been successfully solved using the e-Government and its variants. This study carries out a comprehensive review of e-Government security issues, analysis of information security, Information security threat, e-Government threat management for success to enhance the security of information and it also introduces to an ICN approach as an alternative solution to traditional security management of e-Government. Aim of this study is to make an assessment of e-Government security issue, a lot of work has been done but more is needed to secure e-Government applications. To provide e-Government services with the different levels of confidentiality, integrity and availability which are the main targets. The results of this literature review are to give a suggestion or a recommendation in an effort to establish and maintain security systems in a network of e-Government.

Key words: Information security, e-Government security threats management, ICN for e-Government, traditional, confidentiality, network

INTRODUCTION

The term Electronic government (e-Government) can be defined as the use of Information and Communications Technology (ICT) tools and applications to provide services to the public (OECDPMS, 2001). The benefits of ICTs to enhance governance are perhaps most strongly felt at the local level. ICT and the internet in particular, provide an opportunity for improving local government services and a new way for ordinary citizens to participate more directly in the decisions that affect their environment. Various public sector organizations and government's services have focused their efforts towards digitalizing their services to their customers or citizens through the internet, so that users can easily use the available services from any place, any time.

Owing to their potential to integrate data in a more structured and comprehensive form, they contribute to a better knowledge management, improved information sharing and help to create conditions for an open and transparent society based on trust and accountability. Implementation of e-Government enhances the transparency, accountability and reduces the level of corruption by providing online services (Singh and Karaulia, 2011) in order to encourage citizen to use the e-Government services, it is essential to make the people trust in government services and make sure their information and its privacy are protected. A major concern over trust, protection and safety of such information demands a high level of security within e-Government systems (Upadhyaya *et al*., 2012).

In the case of Nepal country, government adopted e-Services with some prelimnary security measures, the research findings from the three institutions revealed that Nepal has e-Government implementation strategy within Inland Revenue Department (IRD), Supreme Court of Nepal (SCN), Nepal Investment Bank Limited. Then, later it has been propagated to the ministries, departments and agencies. However, they are still lagging behind from a security management perspective. In short, security issues have been neglected and may create various types of hazards (Upadhyaya *et al*., 2012).

According to Priyambodo and Suprihanto (2016) information security is a major factor in the service of government. The using of host to host in previous services of government is considered as lacking in security. Thus, they proposed Information Centric

Corresponding Author: Tri Kuntoro Priyambodo, Department of Computer Science and Electronics, Gadjah Mada University,Yogyakarta, Indonesia

Networking (ICN) as an alternative approach that can be used to secure the content on e-Government rather than conventional approach on e-Government that uses host-to-host principles (Priyambodo and Suprihanto, 2016).

This study will only present the general overview of e-Government security issues, analysis of information security: the challenges and key mechanism in securing the information, information security threat as well as e-Government threat management for success to enhance the security of information.

MATERIALS AND METHODS

Security information analysis: As mentioned in an introduction, security is focal point in determining the success or failure of an e-Government use. From literature review, e-Government is a critical requirement. Joshi *et al.* (2001) and Arcieri *et al.* (2004) identified a set of security requirements that should be respected in e-Government. We have listed a set of the most important requirements: authentication; authorization; confidentiality; traceability; integrity and nonrepudiation. Various goal of information security also includes secrecy, availability, accountability and information assurance (Joshi *et al.*, 2001).

Basically, authentication is the capability to identify who is using the services (person or software program), processes of verifying that you are who you say you are. Authorization is the capability to give rights access to resources or process to verify someone having the rights to do what they are trying to do. While confidentiality or secrecy is the capability to prevent unauthorized access to information. Traceability the capability to chronologically interrelate any transaction to a person or system that performed the action in a way that is verifiable. Non-repudiation is the capability to prevent the intervening person or system in an event or action to denying or challenging their participation on the event.

Information integrity guarantees that information is protected from intentional or accidental modifications. Information availability implies access to information uninterrupted by malicious denials of service or unauthorized deletions. Accountability ensures that an entity's every action is uniquely traceable to that entity. Information assurance implies that a specific implementation provides some degree of confidence about pre-established security goals.

Security key mechanisms: Joshi *et al.* (2001) has identified three key mechanisms that provide the foundations for an information security are authentication, access control and audit. Authentication establishes the identity of an entity and is a prerequisite for access control. Access control limits the actions or operations that a legitimate entity performs. While the audit process collects data about the system's activity and detects possible security breaches. Once, it establishes user authentication, the system should enforce access control using an established technique such as a reference monitor that mediates each access by a user to an object.

Several access control models have been proposed to address the security needs of information system. Traditional access control approaches fall into two board categories: Discretionary (DAC) and Mandatory (MAC). DAC approach lets users grant their privileges to others users whereas MAC approach uses a classification scheme for subject and objects.

User classification leads to several clearance levels for access control whereas classification of objects can be established according to their sensitivity. To avoid the unauthorized flow of sensitive information, the MAC model also referred to as the multilevel model can enforce no read up and no write down rules at a given level (Ravi Sandhu).

Several security technologies that are becoming indispensable for large distributed and networked heterogeneous system, like Digital Government (DG), including firewall, Intrusion Detection systems, encryption techniques, PKI (Public Key Infrastructure) technologies. Privacy concern over the internet foreshadows the critical citizen information it will have in its databases. For DG infrastructure, designing and implementing these mechanism and technologies in an integrated manner poses a daunting challenge.

Security challenge: The study on "digital government security infrastructure challenges" (Joshi *et al.*, 2001) literally says: "Among all government functions, maintaining collective security remains the most crucial element, requiring that security concerns be addressed at each level of the government's information infrastructure". One of the key challenges there identified is "ensuring secure interoperability among systems from several agencies".

One of online government services is e-Voting that supports the conduction of several types of election procedures like polls, internal elections, decision-making, etc., through the internet, all eligible voters can thus participate in the election irrespective of their geographical location. The authentication of voter and election organizer credentials is a prior necessity to any kind of interaction of the user with the system so that no one can vote twice.

According to Alshehri and Drew (2010), there are nine main challenges and constraints of implementing e-Government such as: ICT infrastructure, policy and regulation issues, security, privacy, lack of qualified personnel and training, lack of partnership and collaboration, digital divide, culture, leaders and management support. While the research done by the European Union has grouped extent of information security into areas such as: trust in e-Government, information quality, Cyber infrastructures for e-Government. Data privacy and personal identity. For more details (Priyambodo and Suprihanto, 2016; Wimmer *et al*., 2008).

Information security threats: The networks providing data to the end users of the e-Government remain vulnerable to variety of threats. A typical attack pattern consists of gaining access to a user's account, gaining privileged access and using the victim's system as a launch platform for attacks on other sites an intruder maybe an individual, software tools looking for a personal gain or a paid "spy" seeking information for the economic advantage of a corporation or Foreign country. Singh and Karaulia (2011) listed possible threats on e-Government such as packet sniffer, probe, malware, internet infrastructure attacks, Denial of Service (DOS) attack, Remote to Local (R2L) attack, User to Root (U2R) attack.

Packet sniffer: A sniffer program that targets packets of data transmitted over the internet.

Probe: Trying to discover information that other people do not want you to know.

Malware: Malicious software or computer programs designed to infiltrate and damage computers without the users consent.

Internet infrastructure attacks: It is a kind of wide spread automated attacks that Infrastructure oflarge portion of the Internet and can seriously hinder the day-to-day operation of many sites.

Denial of Service (DOS) attack: A user or organization is deprived of the services of a resource they would normally expect to have.

Remote to Local (R2L) attack: Leads to vulnerability issues to access secured information from the machine, accessing unauthorized information and it affects security issues more effectively.

User to Root (U2R) attack: Leads to several vulnerability such as sniffing password, a dictionary attack and social engineering attacks.

According to Singh and Karaulia (2011), all those listed above cyber security attack can attack all services provided by e-Government via. internet as well as mobile connections.

e-Government security threats management: According to Zhou and Hu (2008) in the journal entitled "Study on the e-Government security risk management, they identified the procedures of security risk management of government through 3 aspects: risk identification, risk analysis, risk control and its countermeasures (Zhou and Hu, 2008). Risk identification is based on the collecting of various relevant threats bugs and corresponding counter measures and then recognizes any possible risks or potential threats to the e-Government system. The goal of risk identification is to recognize risks existing in network environment, in data or data exchange.

For risk analysis, you must first identify the possible threats that you face (risk identification) and then estimate the likelihood that these threats will be arisen. The possible threats can be dived into 2 categories (intentional and natural threats (Zhou and Hu, 2008). Meanwhile risk control is the method by which organizations evaluate potential losses and tak action to reduce or eliminate such threats. The goal of e-Government security risk controlling is to reduce the risk degree which e-Government projects suffering.

According to Zhou and Hu (2008), among the e-Government risk management counter measures, it is popular to use defense-in-depth strategy at present. Defense-in-depth strategy is consisted of depth security and multi-level security. The main goal of disposing the countermeasures is to reduce the potential risks and security bugs, so that we can reduce the risk which the government system environment facing.

RESULTS AND DISCUSSION

Improving security in e-Government: In order to improve security of e-Government, it is recommended to determine in advance the state of security at that site. The article of "the information society and privacy, media and culture in the information age" discusses the methods for making that determination; the policies, procedure and technology methods provide more detail are documented.

Security policy: Are a set of policies issued by an organization to ensure that all information technology

users within the domain of the organization or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network. It addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.

Security practices: Are employed for the purpose of verifying that an electronic signature, record or performance is that of a specific device or a user or for detecting changes or errors in the information in an electronic record. For example procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling using encryption, authentication for issuing accounts, configuration and monitoring.

Security procedures: It is employed for the purpose of verifying that an electronic signature, record or performance is that of a specific device or a user or for detecting changes or errors in the information in an electronic record. For example procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration and monitoring.

Security technology measures: A variety of security measure (Joshi *et al*., 2001) has been established to help government to secure e-Government against intruders. These measure or technologies help protect systems and information against attacks, detect unusual or suspicious activities and respond to events that affect security.

Operational Technology (OT): The hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices performance.

One-time passwords: Typically, a one-time password is a series of meaningless numbers or characters or it might be a half dozen or so short, random words which is valid only once and changes every time you sign-in your system. By using one-time passwords in e-Government services, the probability of an attack relying on the interception and replay of network traffic is lessened because a previously valid password will not be accepted on a second or following round. As it is used in security-critical environments in which clear-text passwords continue to be re-used.

Cryptography: Encryption is the process of translating information from its original form (called plain text) into an encoded, incomprehensible form (called cipher text). Decryption refers to the process of taking cipher text and translating it back into plaintext. For e-Government technology, any type of data may be encrypted including digitized images and sounds. The authenticity of data can be protected in a similar way too.

Firewalls: Firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A simple firewall may consist of a filtering router, configured to discard packets that arrive from unauthorized addresses or that represent attempts to connect to unauthorized service ports.

Analysis tools: It is essential to periodically assess the network's susceptibility to be compromised. A variety of vulnerability identification tools are available having garnered praise and criticism. Critics claim that such tools, especially those freely available to the Internet community, pose a threat if acquired and misused by intruders.

Monitoring tools: Network monitors may be installed at strategic locations to collect and examine information continuously that may indicate suspicious activity. Understanding of security issues and developing a security perception based on perceived threat profile is important to articulation of a security policy.

Icn technology approach: According to Priyambodo and Prayudi (2015), there are four key strategies that can be used as reference for egovernment information security which are aspects of data types and services, policy aspects, human aspect and aspects of infrastructure and technology strategies. Those strategies are supported by Priyambodo and Suprihanto (2016) based on the basic principles of Information Centric Networking (ICN), the issues on e-Government security can be solved by ICN approach with the proposed solution in securing the contents which are contained in e-Government by altering host to host security concepts into the concept of content security.

CONCLUSION

Currently development of e-Government is very necessary and has become a vital need for the community, in this case as a service to its citizens. Therefore, the development and maintenance including networking, security, data confidentiality, etc. is very important to note. Various forms of construction, development and security have a lot to offer. It can be used as a rationale to be able to build or develop a form of e-Government reliable systems. To protect e-Government systems,

current information security procedures of risk management shall be used (how to identify potential issues, risk analysis of that issue and set risk control of them), strategies of improving security like security polices, security practices and security procedures must be in place as well as utilization of security technology measures such operational technology, one-time passwords, cryptography, firewalls, analysis tools, monitoring tools which help to protect e-Government systems against attack.

According to Priyambodo and Suprihanto (2016), ICN technology approach can be an alternative solution to e-Government security issue which proposes the solution in securing the contents which are contained in e-Government rather than host to host security concepts into the concept of content security. ICN model approach provides better security due to the use of digital signatures and security of data packets. It is recommended to do deep research oh this approach compared to convention approach host to host principle.

REFERENCES

Alshehri, M. and S. Drew, 2010. E-Government fundamentals. Proceedings of the IADIS International Conference on ICT Society and Human Beings, July 29-31, 2010, Clayton State University, Morrow, Georgia, pp: 35-42.

Arcieri, F., F. Fioravanti, E. Nardelli and M. Talamo, 2004. A layered IT infrastructure for secure interoperability in personal data registry digital government services. Proceedings of the 14th International Workshop on Data Engineering: Web Services for E-Commerce and E-Government Applications, March 28-29, 2004, IEEE, Rome, Italy, ISBN:0-7695-2095-2, pp:.95-102.

Joshi, J., A. Ghafoor, W.G. Aref and E.H. Spafford, 2001. Digital government security infrastructure design challenges. Comput., 34: 66-72.

OECDPMS., 2001. E-Government: analysis framework and methodology. Organization for Economic Co-operation and Development, Public Management Service, Puma SE, Herzogenaurach, Germany. http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=PUMA(2001)16/ANN/REV1&docLanguage=En.

Priyambodo, T.K. and D. Suprihanto, 2016. Information security on eGovernment as information-centric networks. Intl. J. Comput. Eng. Res. Trends, 3: 360-365.

Singh, S. and D.S. Karaulia, 2011. E-governance: Information security issues. Proceedings of the International Conference on Computer Science and Information Technology, December 1, 2011, IEEE, Pattaya, Thailand, pp: 120-124.

Upadhyaya, P., S. Shakya and M. Pokharel, 2012. Information security framework for E-government implementation in Nepal. J. Emerging Trends Comput. Inf. Sci., 3: 1074-1078.

Wimmer, M., C. Codagnone and M. Janssen, 2008. Future E-government research: 13 research themes identified in the eGovRTD2020 project. Proceedings of the 41st Annual Hawaii International Conference on System Sciences, January 7-10, 2008, IEEE, New York, USA., pp: 223-223.

Zhou, Z. and C. Hu, 2008. Study on the E-government security risk management. Intl. J. Comput. Sci. Network Secur., 8: 208-213.