Optimizing Security and Flexibility by Designing a High Security System for E-Government Servers

Y.Y Abdul Talib[1], B.B Zaidan[2], A.A Zaidan[2], A.W.Naji [3]
yurita@uum.edu.my ; bilal@perdana.um.edu.my ; awsalaa@perdana.um.edu.my; ahmed@iiu.edu.my ;
[1]College of Business
University Utara Malaysia
Sintok Kedah, Malaysia
[2]Department of Computer Science and Information Technology
University Of Malaya
Kuala Lumpur, Malaysia

I. INTRODUCTION

Web sites are now a major vehicle through which government agencies deliver information to the public, also known as E-Government. Through Information Technology (IT), particularly the Internet, Government can deliver public services in a much convenient, cost-effective and altogether different and better way. Realizing the potential benefits of IT, The government agencies worldwide began actively posting information on the Web.

In ensuring the success of e-government initiative, a level of trust is required from all transaction parties - within agencies, between agencies, across governments, and with businesses and ultimately the citizens. The issue of trust involves two special concerns to any online service, these are privacy and security. Privacy is refers as a protecting personal information the government collects about individuals whereas security is refers as protecting e-government sites from attack and misuse. While e-government is working in an open environment (internet), the issue of privacy and security is of a great concern especially to decision makers and designers of e-government systems.

Government around the world has invested a huge amount of money and time to ensure the security of electronic transactions by constantly enhancing the information security infrastructure. But, unfortunately many security breaches over government website still exist [1]and the continuing emergence of attack and misuse can affect users' trust and confidence towards the e-government services and hinder them from using e-government services [2][3]. Though it is about time to develop a security system than can truly effective in protecting the e-government sites and efficient in protecting individuals personal information.

Therefore, this paper introduces a security model that is designed especially for e-government systems. The proposed model not only uses various security tools and techniques such as biometric, password, intrusion detection and other security approaches such as fiber optic, but also increases its flexibility by introducing four types of server to cater different type of users with different function and authority.

***Abstract* - E-government is one of the most popular applications in the Web base applications. It helps people to do those work online, access the government sites, apply for online jobs, access to importent data from the government database, and on top of that it also helps the government employees to access cameras and sensors over the country. However there are many challenges to keep the government data safe and secure in an open environment (network). Therefore, this paper is proposed to discuss two issues. In the first stage how to keep the data in safe, where this paper introduces many applications that guarantee a very high security for accessing and editing of data. The paper also carries a new design for E-government servers in which the authors try to distribute the security service on each line to avoid any attack from out or inside. The second issue is to ensure the flexibilty of the data flow from the servers to the user which is the second challenge in the design. The experiment shows a good expected result, with the new approach have a high security and at the same time flexible E-government access. This paper provides a different view and uses a mixture of technologies to achieve a high security rate that will not affect different user's access. E-Government environment is subject to multiple security challenges, thus this paper proposed a model on how to secure the servers and how to ensure the flexibility of the system, in a simple way balance between a lot of security tools and the appreciate protecting vs. granting the flexible data flow up and download to the user.**

(keyword): E-Government, IDS, Biometric, Quantum Mechanism, Fiber Optic's

difficult string of password. User behavior can actually circumvent password security by failing to choose password wisely, to remember the password, to change the password frequently and to the extreme, to keep the password at secure place.

In order to overcome the situation, instead of entering the password alone to gain access to the system, the admit need to prove physical characteristics too. Biometric is capable in differentiating between the authorized user and fraudulent imposter because each and every individuals has unique features that are difficult to be copied. Even though the criminal successfully crack the password, he will not pass the security procedure when the fingerprints check failed. So, the proposed model is a combination of both password and biometrics technologies to increase e-government security level.

Fiber Optic with Quantum Mechanism

The emergence of high-speed interconnected with all these security requirements, the speed of data transmission is of pivotal consideration in making information exchange across the servers in our module. The use of fiber optic allows for transmission of information as light impulses. Fiber optic is a technology that uses glass (or plastic) threads (fibers) to transmit data with much greater bandwidth than metal cables and less susceptible than metal cables to interference [9]. However, recent technology advances have resulted in the ability to easily and inexpensively tap a fiber optic cable.

Access to E-Government Services

Traditional security model of having a hard perimeter to one's organization does not work when one is trying to deliver complex shared services across boundaries [10]. As an alternative, an architecture that mirrors the organizations' mode of interaction is desirable. This model therefore, is more flexible where it will be able to accommodate four different types of users from the same database under different levels of security clearance, without compromising the security of other sensitive information.

III. System Overview

FOUR Different servers required for the infrastructure

- Main Server which includes the Database of the sensitive data connected to four servers, each one has its own work, explained below.
- Server for checking authentication and authorization for each request. This server will check all the requests for accessing the database.

II. Related Work

Access Control Systems

Authentication is important concept in security to control over user accessing the system. The most general authentication controls are password and biometric. Password is a common type of first layer defends strategy to determine that a computer user requesting access to a computer system, in fact, the person he claims to be. While password is effective control and the cornerstone of an effective access control system, password is very vulnerable to interception especially when transmitted over a network to authentication machine. Once the password is compromised, the intruders can cause a great harm and significant financial losses [4].

Biometric systems are now becoming widely used by many organizations to provide greatest level of security because it more reliable than then password and it represent the user. Many biometric research publications are already done especially related to pattern recognition and digital signal processing issues [5] [6] [7]. Biometrics refers to the measurement of specific attributes or features of the human body, such as the fingerprints, the retinas and irises and even the voice, with the purpose to distinguish that person from others. These characteristics are unique to each individual thus it become an access password to the user. Therefore biometrics is a powerful technology to defend the e-government systems from unauthorized access.

An intrusion detection system (IDS) inspects network activities and identifies suspicious patterns and alerts the system or network administrator [8]. IDS may indicate a network attack from someone trying to break into or compromise the system. The proposed model will use two type of IDS, signature based and anomaly based to protect e-government network from malicious and anomalies.

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. Whereas the anomaly based will monitor the network traffic and compare it against 'normal' function, such as the bandwidth, the protocol, the ports and the connected devices of the system. Any significant different from the baseline will be alerted to the network administrator.

Password – Biometric

The password system suffers from many drawbacks and unable to positively identify the user [iii]. Simplistic passwords are easily anticipated by computer hacker using tools such as password cracker and login spoofing. Once the intruder can obtain the password, the system cannot recognize the true identity of the user and the he has a total access to associated resource. Making the password more complicated sounds good but end users tend to forget

IV. CONCLUSION

This paper discussed many approaches on how to keep data in safe and also to improve the flexibility of exchange the data between the client and the servers. Many of security issues could be improved by offering a design that involve many security tools such as encryption, biometric and IDS. In this system we didn't depend on bring many tools only but how to distribute the security tools in the network, in other word "security tools distribution", the main using of this schema to avoid many of the popular attackers. This paper also highlight on how to distribute the data base on the users so that we will reach the less number of hanging on network and ensure the right access has been request from the current user. Actually this design will handle many great issues, such as, high level of security, fast response, flexible data flow, data base distribution, access distribution, which all is considering as a requirement for implementing E-government .

V. ACKNOWLEDGEMENT (ACKNOW)

This work was supported in part by the Universiti Utara Malaysia, Kedah Malaysia

VI. REFERENCES

Matthew Stibbe (2005).E-government security. Infosecurity Today. [i] Volume 2, Issue 3, May-June 2005, Pages 8-10

Hoffman, D., Novak, T.P., Peralta, M. (1999), "Building consumer[ii] .trust online", *Communications of the ACM*, Vol. 42 No.4, pp.80-5

Adams B., Berner, E.S., Wyatt, J.R. (2004), "Applying strategies to[iii] overcome user resistance in a group of clinical managers to a business software application: a case study", *Journal of .Organizational and End User Computing*, Vol. 16 No.4, pp.55-64

Hall J.A. and Singleton T. (2005). Information Technology Auditing[iv] and Assurance 2nd Edition. Thompson South-Western. USA

Nalini K. Ratha, J.Connell, R.Bolle 1999. A Biometrics-based[v] Secure Authentication System. Proceeding 1999 IEEE Workshop on Automatic Identification Advanced Technologies (WAIAT-99), .Morristown NJ, October 1999

Jain A., L.Hong, S. Pankanti, and R.Bolle. 1997. An Identity[vi] Authentication System Using Fingerprints. Proceedings of the IEEE, .Vol.85, No.9, pp. 1365-1388, 1997

A.M. Awadelkarim and M.G.M Johar 2005. A Cryptographic-[vii] Biometric Mechanism for Enhancing SET Authentication. Proceedings of International Conference on E-Commerce 2005. .pp109 – 114, 2005

http://netsecurity.about.com/cs/hackertools/a/aa030504.htm access[viii] on 2 January 2009. Introduction to Intrusion Detection Systems (IDS), Tony Bradley

http://webopedia.internet.com/TERM/f/fiber_optics.html Accessed[ix] on 4 January 2008

Bill Goodwin, Government buys in to deperimeterised security.[x] Computer Weekly; 4/25/2006, p4-4, 1/4p

VII. Author Information

Yurita Yakimin Abdul Talib Lecturer College of Business / Universiti Utara Malaysia/Kedah/Malaysia

This server responsible in permitting the request for access from different type of users. The server works by checking the digital signatures that come from the fingerprint and the password gathering. In case some one in between has a copy of the buckets that include this signature, the server will check the expired date of the signatures with the original one.

- Server for adding or editing the database also known as Admin Server. This server will be connected to fingerprint reader. The reader can differentiate between the human finger and the glue copy of the fingerprint by sensing the human heart pulse or human temperature. Using this method, it ensures that no one can use the copy of the fingerprint. On top of this, we also add password to the module, with a purpose to make it looks more complicated by anyone who tries to access the database. The main server will not accept any adding or editing process unless there are two password and two fingerprint checks by this Admin Servers.

Server for internal user; this server connected to the main server, to allows the internal users (government officers) to (Sensors, CCTV'S, etc) or normal people use accessing sites for the government business, ministries sites, etc)

Fiber Optic's

Two significant from use fiber optic, the 1st one to apply the Quantum Mechanism which is the faster and the more secure algorithm that known until now for key distribution and data encryption using PKI (Public Key Infrastructure), and the 2nd one to insure a high speed data transmutation with all these security requirement's, this also to be sure there are no physical layer attacking

Intrusion Detections

Here we will use two type of Intrusion Detection Systems (IDS), the 1st one is (anomaly detection systems) (learning from the users normal use), and the 2nd one is (misuse detection systems) (signature base) both will help to minimizing the problems or the attacked from outside, it will distribute as followed

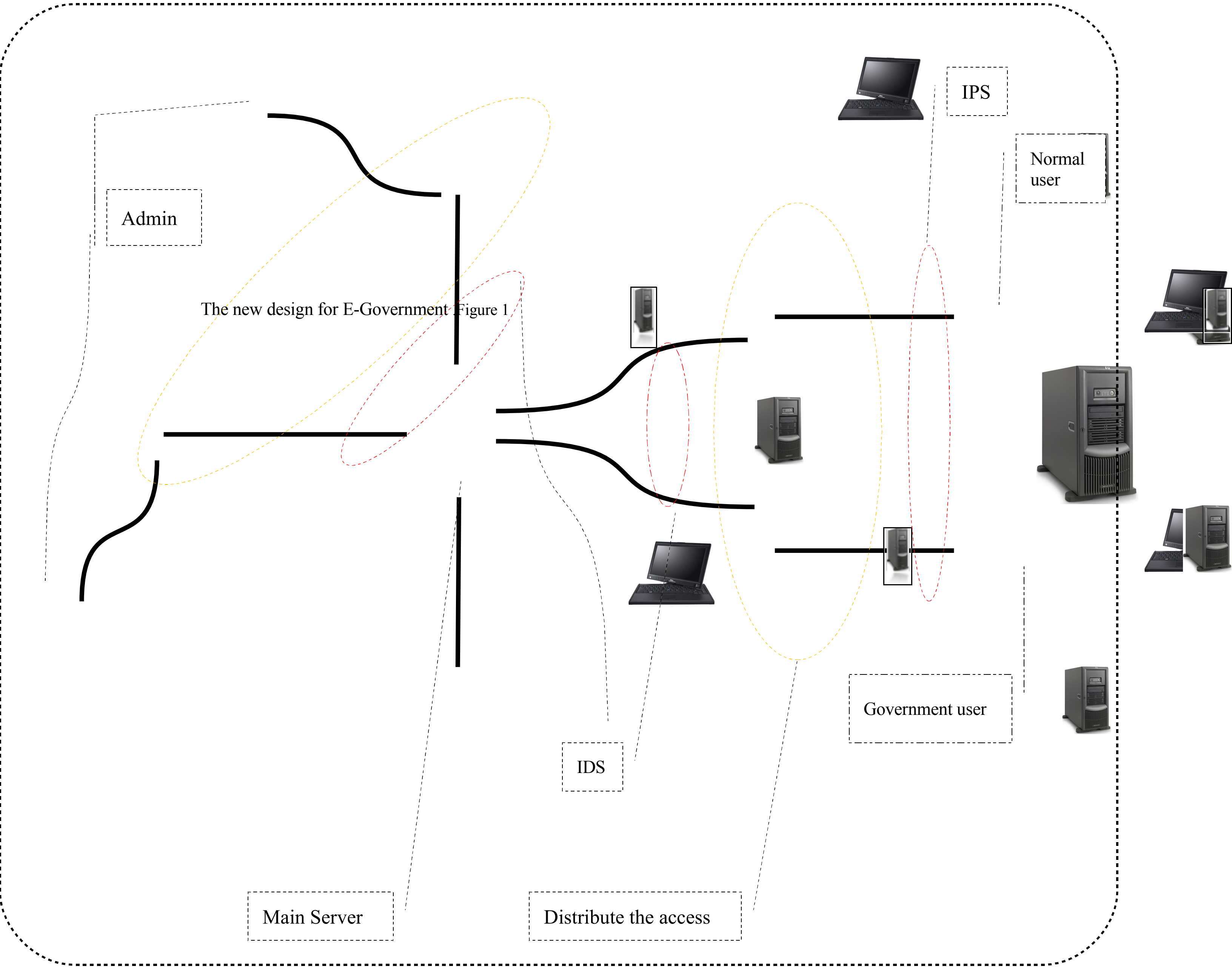
- Two Intrusion Detections system (anomaly detection system) the use of this type is to know
- what is normal use and what is abnormal use from the admin, in other word if one of the trusted people try to do anything abnormal

The servers that connect the user each one connect in to two intrusion detection one (anomaly detection) and the other one (signature base), different IDS may help to check the traffics in and out these servers

Bilal Bahaa Zaidan Master of Computer System & Technology Department /University of Malaya /Kuala Lumpur/Malaysia

Aws Alaa Zaidan Master of Computer System & Technology Department /University of Malaya /Kuala Lumpur/Malaysia

Ahmed Wathik Naji Senior Asst Professor / Faculty of Electronic Engineering/ International Islamic University of Malaya / Kuala Lumpur/ Malaysia



The new design for E-Government Figure 1

1

2

3

4

5

6

7

8

9

10