Portal Security Issues

Prepared for the Electronic Government Task Force: Strategic Issues Subcommittee
By the Department of Information Resources

August 2000
Austin, Texas

INTRODUCTION **3**

BACKGROUND 3
PURPOSE AND ORGANIZATION OF THIS REPORT 4

INFORMATION SECURITY BACKGROUND **4**

WEB SITE CONSIDERATIONS 5
POTENTIAL THREATS AGAINST WEB SITES 6

ISSUES AND CONCERNS **7**

ACCOUNTABILITY 7
SECURITY STANDARDS 8
SECURITY REPORTING PROCEDURES 8
STATEWIDE PUBLIC KEY INFRASTRUCTURE 8
DATA COLLECTION 8

CONCLUSIONS AND RECOMMENDATIONS **8**

END NOTES **10**

Introduction

Reduced transaction time, round-the-clock availability, and convenience are all reasons for the public to access government services over the Internet. As discovered in the Task Force business and public surveys, security and privacy concerns rank as the biggest concerns about the use of the Internet. In fact, the public's main concern about state and local government providing services over the Internet was the security of transactions. The state business portal, TexasOnline, must gain and sustain the public trust by conducting secure and private transactions.

> "*No computer or networked system can be one-hundred percent attack proof and the job of securing a system against an illegal intrusion will never be complete. But using best practices and recommended security measures can move us forward to a more secure environment for securing the nation's infrastructures.*"
>
> National Infrastructure Protection Center (NIPC), October 1998

The goal of this paper is not to establish a security policy; rather it is to identify security issues related to the maintenance and development of a state portal, created through a public-private partnership.

Background

Recognizing the importance of electronic commerce to the state and its potential to help increase the effectiveness of state government, the Texas State Legislature mandated a demonstration of electronic government through Senate Bill 974 (Section 2054.062). The 1999 legislation charges the Department of Information Resources (DIR) with "establishing a task force to assess the current and future feasibility of establishing a common electronic system using the Internet through which state agencies and local governments can accomplish the following types of functions electronically:

1. Send documents to members of the public and persons who are regulated by a state agency or local government;
2. Receive applications for licenses and permits and receive documents for filing from members of the public and persons who are regulated by a state agency or local government that, when a signature is necessary, can be electronically signed by the member of the public or regulated person; and
3. Receive required payments from members of the public and persons who are regulated by a state agency or local government."

The Task Force is composed of a representative of each of the following state officers or agencies:

- the Office of the Secretary of State;
- the Office of the Comptroller of Public Accounts;
- the Texas Department of Economic Development;
- the General Services Commission;
- the Texas Natural Resource Conservation Commission;
- the Texas Department of Insurance;

- the Public Utility Commission of Texas; and
- representatives of local governments appointed by the governor in the number determined by the governor;
- three representatives of businesses that are regulated by a state agency or local government, appointed by the governor; and
- three public members appointed by the governor.

To accomplish its mission, the Task Force elected to issue a statewide contract for development of a "common business portal" as a framework through which members of the public and persons who are regulated by a state agency or local government can do the following:

- send documents to members of the public and persons who are regulated by a state agency or local government;
- receive applications for licenses and permits;
- receive documents for filing; and
- receive required payments.

The contract awarded was for a pilot that included six agencies and fourteen applications.

Purpose and Organization of this Report

Texas is among several states that are exploring the public-private partnership business model. This public-private partnership has created the framework for conducting electronic government services via a self-supporting model. The private partner will operate and manage the Texas business portal and the payment processing system for the state, and thus must provide appropriate security and services (including support for digital signatures). While state agencies are already required to follow state security standards specified in the Texas Administrative Code, the relationship between the public and private partners still requires definition regarding the establishment and enforcement of a portal security policy. This report highlights the main security issues surrounding the operation of state portal, as well as some additional concerns that arise as a result of the partnership.

Information Security Background

In April 2000, DIR published Practices for Protecting Information Resources Assets as a general security overview and guide for agencies and universities to use in establishing information security policies. These guidelines were based on Texas Administrative Code, Chapter 1, Section 201.13b, Information Security Standards (T.A.C. 201.13b). The guidelines detail security safeguards, including access control, authentication, confidentiality, data integrity, encryption, and non-repudiation.

> *Access Controls* are the procedures and controls that limit or detect access to critical information resource assets (people, systems, applications, data and/or facilities) to guard against loss of integrity, confidentiality, accountability, and/or availability. Access control is accomplished by specifying which services users may access and who may use them.

Authentication is used to positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. Authentication is accomplished using passwords, challenge-and-response methods, biometrics, and/or smart keys.

Confidentiality is the assurance that information is not disclosed to unauthorized persons, processes, or devices. Confidentiality is accomplished through access controls, and protection of transmitted data through encryption techniques.

Encryption is the process of cryptographically converting plain text electronic data into a form unintelligible to anyone except the intended recipient. This is the key in protecting information on the Internet. The type of encryption used will depend on what and how the information is being exchanged.

Data Integrity refers to a condition when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. Data integrity is accomplished through access controls and the protection of transmitted data through encryption techniques. Data integrity also uses a "time-stamp" to prevent data from being copied, altered, and replayed at a later time.

Non-repudiation is a method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data. This method requires strong authentication and data integrity, as well as verifying that the sender's identity is connected to the data that is being submitted.

Additionally, the guidelines provide a general overview of a wide array of information security features, from transactional security and Web site security. This understanding of basic security features is beneficial to comprehend the larger security issues that follow.

Web Site Considerations

Web sites can be broken down into three categories based on the level of interaction they provide. Basically, sites are categorized as:

Information only, where a Web site is more static in nature, displays information only, and there is no interaction via a Web page. For example, a site may contain a list indicating the point of contact for renewing a particular license.

Information exchange sites allow a constituent to send or receive information through a Web page. However, while information can be sent via a Web page, the payment functionally is not available. For example, someone could send an application renewal via the Web page; however, they would have to mail their payment in.

Fully transactional sites allow a constituent to complete business transactions (e.g., credit card payments) via a Web page. For example, a person can renew a license and pay for it online.

The state portal is intended to be a fully transactional Web site. A fully transactional Web site has a higher security risk than a purely informational Web site, and therefore requires a greater number of controls to achieve a high level of security. Although Texas has a rule (T.A.C 201.12) that addresses minimum security safeguards for Web sites, greater security controls are needed to conduct secure transactions. The portal security policies should, at a minimum, adhere to the state Web site security standards. The DIR standards also include information regarding conducting a transaction risk assessment. Every transaction an organization plans on including on the portal should be assessed for risks, and the appropriate privacy and security measures should be implemented. The key in protecting information on the Internet is encryption. The type of encryption used will depend on what and how the information is being exchanged. Any government site that requires users to enter sensitive information must provide a secure environment. The greater the security risk, the greater the security controls needed to fend off malicious attacks.

Potential Threats against Web Sites

When the world is connected to your computer, there is no such thing as "quiet time". The Internet never sleeps. All Web sites are susceptible to attacks. Attacks, like viruses, are constantly being dreamed up by hackers. The following is a list of examples of recent attacks.

Distributed Denial of Service (DDoS) is an attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. A recent example is the attack on Yahoo.com and eBay. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks.[1]

Web Graffiti and Defacement is an attack where a site is vandalized, and the physical look and feel of the site is compromised. A recent example of this is the attack on the Apache Software Foundation site. In this instance, a hacker replaced Apache's logo with a Microsoft logo.[2]

Credit Card Fraud happens when a hacker is able to steal credit card numbers that are stored electronically. Recently, crackers broke into Western Union's Web site servers and grabbed the credit and debit card numbers of 15,700 customers. It was noted that the attackers hadn't actually "use" the stolen numbers.[3]

Identity Theft is when a hacker assumes someone's identity in order to commit fraud. When someone uses stolen credit card numbers to purchase items, they are committing identity theft. Recently two people were accused of stealing more than $700,000 from the online stock-trading accounts of eight U.S.-based employees of Ericsson. The names of employees were used to obtain new card accounts, which were in turn used to open online stock-trading accounts. Both suspects were charged with bank fraud, mail fraud, wire fraud, and identity theft.[4]

A recent FBI survey reported that $1,000,000 is the average amount it costs per intrusion to investigate, repair, and secure corporate/governmental systems once they have been hacked. In 1999 the FBI reported that verifiable losses due to poor security totaled over $265,000,000. They discovered that prosecution after the fact is costly and has practically no effect. Intellectual property is impossible to recover. Furthermore, it is difficult to restore trust in a failed system.[5] Therefore, The goal of information security is to be able to provide the best security possible to prevent attacks, as well as having processes in place to detect and deal with the unavoidable ones.

Issues and Concerns

Security and trust in conducting transactions over the Internet is critical in ensuring the success of the state portal, as it will deal with citizens' financial and personal information. This is a challenge even without the added complexities that arise as a result of the public-private partnership. Securing a portal necessitates an enterprise approach. The security risks must be analyzed from the top down, collectively examining the different levels that make up the portal: the network, the applications or services, the storage, and the transactions. Security needs vary depending upon the level and application. For example, hacker attacks, such as Web site graffiti and denial of service, can occur at the network level; unauthorized access attacks can occur at the application level; and session stealing - where an unauthorized user takes over a live session - can occur at the transaction level. To combat such attacks, security mechanisms such as software packages, firewalls, and intrusion detection systems are put in place.

The portal must be able to provide an adequate level of security for a wide array of services - from online database searches to online license purchasing using a credit card. Since agencies can use some or all of the framework, appropriate security measures need to be in place to protect the various applications that are on the portal, and as well as those that will come on in the future. The portal needs to provide the appropriate level of security for the initial pilot agency applications, as well as being flexible to accommodate those that will come on in the future. While this flexibility is essential in dealing with multiple state agencies, with multiple application and transaction needs, this creates a situation where the security needs are difficult to assess, and difficult to control. The following questions flush out the main security issues and concerns.

- Who is responsible for overseeing the security of the portal?
- What are the minimum security requirements?
- When is the security of the portal assessed?
- Where is the public key infrastructure for the encryption of transmitted data?
- How much personal data is collected, and how long is it stored?

Accountability

Accountability is critical to establish the relationship between the contractor, the contract management, and the participating agencies so that it is clear where the security responsibilities lie. Since security problems occur at various levels, it is important to define the responsibilities for each level. Aspects such as ownership, whether the responsibility resides with the state agency or the private vendor, need to be clearly

detailed and explicitly stated. The lack of accountability for a particular security risk could allow a security breach to go undetected.

Security Standards

Security standards for the pilot agencies, as well as future agencies that want to utilize any or all pieces of the portal, are crucial to ensuring the security of the portal. Security requirements are necessary to protect all applications operating on the portal. The Task Force should also set the minimum standards for future applications. Allowing an agency to come aboard without the appropriate security measures would cause a weak link that could lead to a crippling security breach. The addition of applications should not jeopardize the security of the other applications. In an instance where an agency lacks the technical expertise and staffing to provide an adequate amount of security, the agency can utilize the security features provide by the portal. Furthermore, establishing secure connections to transfer agency data and/or payment information requires a combination of agency and contractor expertise, and also requires several options for securing communications.

Security Reporting Procedures

Established security reporting procedures attempt to detect intrusions and attacks. Formalized procedures should include updates to the Task Force and other agencies involved in incident tracking. These security monitoring reports are valuable for analyzing whether existing security tools are working or if additional tools are required to provide security for the portal.

Statewide Public Key Infrastructure

A public key infrastructure (PKI) is essential if agencies on the portal are to utilize digital signatures. PKI is used to send encrypted information between users. This allows the information to be sent confidentially (e.g., the information can not be viewed by outside parties.) Digital signatures are used to ensure the that the individual who sent to message actually was the sender. One of the tasks of the e-government framework was to find a way to begin using digital signatures. The pilot projects have discovered many complexities in trying to implement digital signatures.

Data Collection

Authentication is a viable piece of the security puzzle, but the amount of information should be limited to only what is needed. For example, many transactions do not need, nor should require, detailed information about the individual. Agencies should only request information from the user that is required for that particular application. Providing excessive personal information increases the security risk of the application. A thorough security policy needs to detail the transmission and storage requirements for sensitive information to mitigate this risk.

Conclusions and Recommendations

Security and trust in electronic communications is critical to the success and adoption of TexasOnline by government entities and the public. The pilot project has proven that a portal approach to online services requires additional security considerations. Multiple

agencies are using multiple applications, which creates some unique situations. Some additional recommendations to expand existing security measures are listed below.

Each of the recommendations are prefaced by a code that directs the reader to the specific government body the recommendation most concerns:

LEG – These are recommendations that require legislative action in order to be implemented.

STATE – These are recommendations that can be implemented by state agency action.

TF – Task Force initiatives may require setting portal policies and standards.

1. *(TF)* The governing body should establish a security policy relating to the use of the portal. The security policy should be an extension of the state's existing security policy, addressing the specific issues related to the specialized functions and environment of TexasOnline. The policy should contain:

- Extension of the DIR standards to include portal security at all levels.
- Detailed accountability roles explicitly outlining the security responsibilities at each level, thus ensuring that each entity involved in the partnership is aware of their particular security responsibilities. For instance, an agency should know where the state network (TEX-AN) security responsibility ends, and the agency security responsibility begins.
- Formalized procedures for coordinating with the Office of the Attorney General (OAG), the State Auditor Office (SAO), Department of Public Safety (DPS), and DIR on reporting intrusions and detecting fraud.

2. (STATE/TF) The new governing body should coordinate with the SAO and DIR to require periodic security audits of the portal operational facilities. This audit should incorporate the ongoing internal reviews conducted by the Portal Management Office and security reports generated during daily operation of the portal. The audits should examine the security monitoring reports and processes and recommend necessary actions. In the interim, monthly reports on intrusion detection should be provided to the new governing body, DIR, and SAO for internal monitoring.

3. *(STATE)* Participating state agencies should be very deliberate about every piece of data collected on individuals, and collect only that data for which there is a legitimate need. Especially when collecting information online, agencies should not collect more information from the user than is required for the application and/or transaction. As a prerequisite, the Portal governing body should require agencies to show proof of conducting an application review to ensure that they are collecting only the minimum amount of information for that application. Agencies should also review the key identification information collected and make sure that the information is kept for a finite period, as needed for completing the transaction.

4. *(LEG)* The pilot project showed the complexities involved in using digital signatures and establishing a statewide public key infrastructure (PKI). The state should coordinate with the Task Force to conduct a feasibility study of implementing a statewide PKI Plan.

End Notes

[1] McCullagh, Declan. "Was Yahoo Smurfed or Trinooed?" Wired.com. Retrieved 19 September, 2000 at www.wired.com/new/print/0,1294,34203,00.htm

[2] Finley, Michelle. "Apache Site Defaced" Wired.com. Retrieved 12 September, 2000 at www.wired.com/new/print/0,1294,36170,00.htm

[3] Dello, Michelle. "Cracker Hits Western Union Site" Wired.com. Retrieved 12 September, 2000 at www.wired.com/new/print/0,1294,38698,00.htm

[4] The Associated Press. "Suspects arrested in online stock fraud case" CNET News.com. Retrieved 12 September, 2000 at http://news.cnet.com/news/0-1007-200-2309062.html

[5] Craig H. Rowland. Chief Technology Officer. PSIONIC Software. Presentation to the Strategic Issues Subcommittee on 22 September, 2000.