Principles of Computer and Information Security

Design Project

Submitted by: Viswanath Nuggu

Submitted to: Dr. Shouhuai Xu

1. Introduction

The purpose of this document is to design a security architecture to protect UTSA's electronic assets and digital information. It is written from the perspective that I am the CIO/CSO of UTSA.

In this proposed design, I tried to addresses the security of the entire UTSA IT infrastructure which includes computers in classroom, library, labs, electronic library documents, etc., by demonstrating the importance of integrating security with each component, including networking devices, databases, web and email, so that they can collectively strengthen the overall UTSA IT infrastructure.

2. Description of the Design Objectives

The objectives of the security involves guarding data and information technology (IT) networks against many types of threats. Here we need to assure that particular system resources of UTSA, from the level of the individual computer that contains data and programs, to the entire network, is available only to authorized users but unavailable to unauthorized users. The basic security design objectives here is to provide confidentiality, integrity and availability.

This design provides confidentiality to users, integrity of data and availability of resources for the authorized users only. To ensure better security, our emphasis must not be on the mechanisms that we implement but it should be on the policies we enforce on the mechanisms. Here we keep the design as simple as possible , deny access by default, give least privileges to users and rely less on security through obscurity.

There are various kinds of sensitive information like employee data, student data (including grades) in UTSA databases that contain all the information of the students, employees, library books, research data etc., this data is stored in more than one database like in each department database and in centralized database. Our defense mechanisms must provide a way to secure these data fields that are more often targeted. The most targeted data in an university includes grades, courses curriculum , Social Security Numbers, salary information of employees, etc.. So here our main design objectives includes preventing attackers from obtaining sensitive user data like grades, including passwords and profile information.

Our design will also establish proper policies and mechanisms to be implemented to make UTSA IT infrastructure more secure. Our security policies should define clearly what is, and what is not, allowed whereas security mechanism is a method, tool, or procedure for enforcing a security policy.These mechanisms include individual user profiles that identify users and their access privileges, and mechanisms that differentiate between different resource environments. These

mechanisms guard against threats such as intruders who try to gain access to data in order to manipulate or steal it.

3. Design and Security Analysis

Software design depends on the quality of the analysis we perform in different perspectives based on our requirements, from this analysis process itself we need to integrate security in every component of the application for better security. So to design better secure product we need to construct a proper design by analysing possible threats to our data and IT infrastructure.

We need to identify the data and applications which are sensitive and predict the attacker's activities, so that we can design our defense mechanisms more effectively. For example an attacker may want to disrupt the records by changing the student records like grades, which is sensitive data. For staff and faculty, it is information like salary, bank account details is the most sensitive information that an attacker will be looking for. The attacker might attempt to modify these numbers for some economic benefits in particular.

Apart from the data attacker may try to attack application itself by hijacking the web server and he may revoke access for legitimate users, so that legitimate users can not access applications like blackboard, e-books from library, asap portal etc.. This kind of analysis helps us in developing a proper threat model.

3.1 Threat Model

Threat modeling focuses on identifying and addressing vulnerabilities. Threat modeling is a structured activity for identifying and evaluating application threats and vulnerabilities. Threat modeling can also help us to identify security design problems early in the application design process. We can do the analysis at network level and application level to identify more vulnerabilities and create our threat model, I used this strategy in designing my threat model in this project.

I have designed threat model based on the possible security attacks
Following table is the identified threat model:

Possible Threat	**Possible Attacks**	**Violating security objective**
Theft of sensitive data and information (loss of confidential information)	Eavesdropping Port Scanning Packet Analyzing APT attacks Man-in-the-middle attack	Confidentiality
Unauthorized Access	Password Cracking Dictionary Attacks Key Logging Password Guessing Elevated Privileges	Confidentiality Integrity
Modifying data or unauthorized access of data from database	SQL Injection Privilege Escalation. Exploiting unused database services. Brute-force for cracking of weak or default usernames/passwords.	Integrity
Resource unavailable for authorized users	DOS DDOS	Availability
Modifying / deleting logs	Root kit attack	Non-Repudiation
Executing Malicious scripts	XSS Buffer overflows Memory Leakage Malware ROP	Integrity
Packet Modifications or eavesdropping	Packet analyzing Eavesdropping Port Scanning	Confidentiality Integrity
Network related threats	Hijacking Phishing spoofing DDOS botnets	Availability Integrity Confidentiality

Transaction Modification	Man in the Browser	Integrity

Table 1: Threat model

Based on the above threat model, we can now prepare our defense mechanisms and design a better secure IT infrastructure for UTSA.

3.2 Main Design

Considering the above threat model and following KIS(keep it simple) design principle, I have designed network security design and web application security design along with database security . Both the designs are simple to implement and maintain, when design is simple there is less to go wrong and also easy to detect design faults and change.

3.2.1 Network Security Design

In network security, we have to protect UTSA workstations, servers, email server and other devices like Kiosks in library, vending machines, etc.

Below is the recommended design for network which contains Firewalls, IDS as security

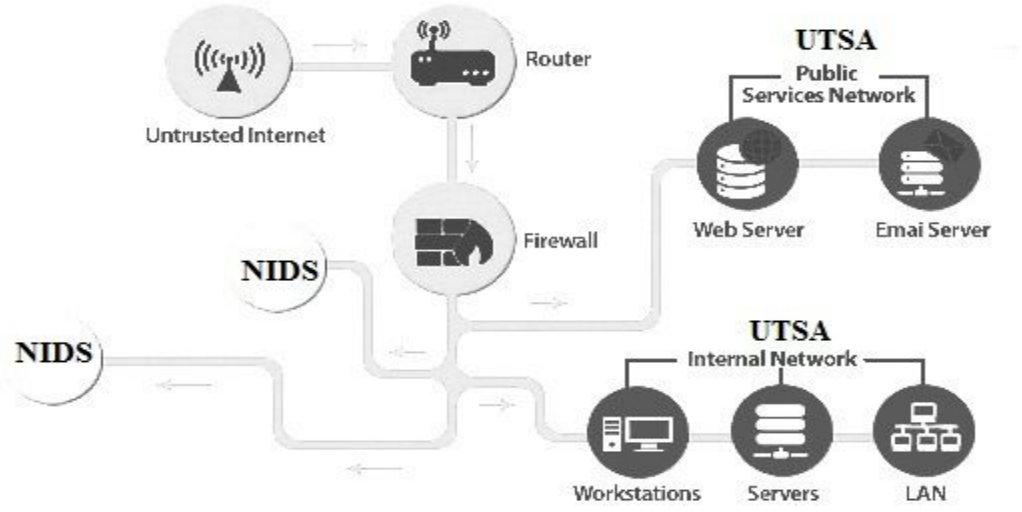

Fig 1: Network Security Design

Network for UTSA is designed by keeping in the mind that security budget will be limited for UTSA and to meet our objectives stated, the above network design protect workstations, servers, email server. By using this network design Students/Employees can access the UTSA resources like ebooks, email, blackboard, asap, etc from outside of university campus also securely. I have used network intrusion detection systems and Firewalls at the entry point of the network, so as to

protect all the network resources. IDS is used to detect malicious activities and protect UTSA resources, firewall is used to block based on the rules we configure.

In the above design there will be public network and the internal network. Public network will hold public services such as web servers, email servers and this will be used to serve students/ employees who are trying to access resources of UTSA externally. Internal server is used to serve department wise computers and computers which are related to UTSA administration.

3.2.1.1 Securing Wireless Network:

Wireless security is to be given high priority, if an attacker can attack UTSA wireless network he can do lot of malicious activities by introducing botnets in the network. This is because,In wireless networks though the user is safe from outside threats , we may face a threat from the internal users using the UTSA network. UTSA provides a wireless network in its campuses for people to connect to the internet on their devices. UTSA provides three types of wireless networks namely: student, faculty, guest. Faculty. Guest network is more insecure as it is public network and no credentials is required. We will be keenly observing users activities by logging to identify malicious activities and suspend the connections to that particular users and devices. Firewall should be configured and below are the recommended configuration policies for firewall:

Firewall Policies:

Default Deny

Here we use our design principle fail safe defaults and implement this. Every connectivity path and service that is not specified or permitted by this document issued by the CIO must be blocked by the firewall.

Logs

All changes to the firewall policy must be logged. Any suspicious activity which may be an indication of breach attempt or unauthorized usage must be logged. The integrity of these logs must be protected with strong encryptions such as AES. The logs must be stored in a physically protected container and must be constantly reviewed to ensure the firewall is operating in a secure manner.

Intrusion Detection

The firewall must include a network based intrusion detection system approved by the OIT. The NIDS must be able to detect unauthorized firewall modifications and potential attacks, in particular, denial of service. Such IDS must also immediately alert the concerned staff by pager

about the attempt. The staff must be able to remotely access the systems to respond as soon as the alerts have been received.

Whitelisting

Instead of keeping track of all the malicious IP addresses, we keep a record of all the trusted ones. In this way, we can use the *default deny* principle for all the addresses that are not listed.

Firewall Access Privileges

Privileges to modify the functionality, connectivity and mechanisms of the firewall must be restricted to only a maximum of 2 individuals who are handpicked by the OIT and are full-time employees. Any other person will have a least privilege unless explicitly permitted by the CIO.

Firewall Changes - Any changes to the mechanisms of the firewall must go through the whole process again from the firewall policy.

Virus Screening - Virus Screening software approved by the OIT must be installed and enabled on the firewall. This software must be able to detect encrypted or compressed or other potentially

Monitoring Vulnerabilities - Any vulnerabilities in the system must be brought to the attention of the concerned officials and must be soon rectified.

3.2.2 Web Application Security Design

UTSA has web applications like blackboard, asap, webmail, library portal to reserve study rooms, access e-books, etc.. These applications has sensitive information and these needs to be accessed by authorized users only. So a layered security at each layer is a better approach for this kind of applications ie., securing web server, application server, database server. I would prefer to use Multiple firewalls at each layer as well as IDS also

Below is the design for web applications with multiple firewalls:

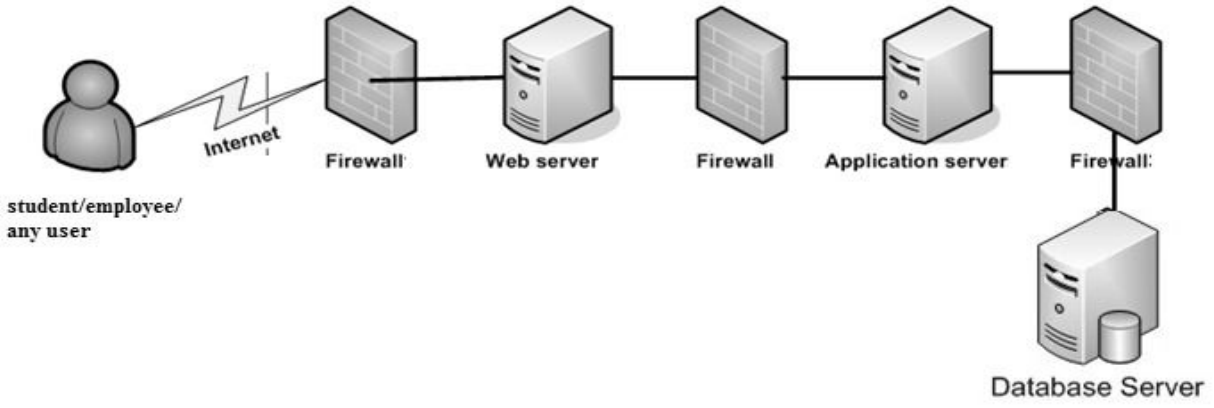

Fig 2: Web Application Security Design

In the above design first a user will be authenticated, we need to follow strict username and password policy and then request goes to a webserver via firewall which contains configured rules, and then request goes securely to application server via firewall which is another layer of protection, this will make sure webserver is not attacked and we are getting legitimate requests and similarly it goes to database server via another firewall. We can configure firewalls in a distributed fashion also especially at database layer which will tight bound security and protects our data. Along with firewalls we need to use HIDS and NIDS at each host and network layer.

Securing a web server is very important as web servers are the common targets for the attackers because of the sensitive data they host. We need to use proxy servers for every web server since we want the identity to ensure anonymity. All the external connections will be handled by the proxy servers while the actual servers are connected to the database. Passwords are hashed along with salt in both the servers.In this way, even if our server is compromised, we can be ensure that the attacker will have to put lot of effort to break the password.

If a web server is compromised, attacker can perform malicious activities like modifying student grades, change bank accounts of employees and transfer money to his account, etc. To defend this our design follows "least privileges" design principle so that we will make sure we are not providing elevated privileges to users who are interacting with our application especially with webserver. For client-server communication we will be using SSL, HTTPS protocols and every IP packet needs to be encrypted.

In all the UTSA applications we will be using cryptography.Using a cryptographic system, we can establish the identity of a remote user (or system). A typical example is the SSL certificate of a web server providing proof to the user that he or she is connected to the correct server. So, here the identity is not of the user, but of the cryptographic key of the user. Having a less secure key

lowers the trust we can place on the identity. Cryptography provides confidentiality, Integrity, Authentication, Non-Repudiation services. In this design we will use RSA, a public-key encryption algorithm which is a standard for encrypting data sent over the internet and for hashing we will be using SHA-2, as they are not broken.

UTSA has to accept online payment through it's web interface, so there may be an attack while transactions being processed and we need to make sure we defend such attacks as well to preserve integrity of the transaction. Attacker may use "Man-in-the-Browser (MITB)" attack and add a new transaction or modify the transaction. So to defend this kind of attacks we need to implement "Out-of-band transaction verification", this overcomes the MitB trojan by verifying the transaction details, as received by the host (bank), to the user (customer) over a channel other than the browser. We will also place a honeypot which is used to detect, counteract attempts at unauthorized use of information systems.

3.2.3 Database Security

Most attacks are to steal the data residing in databases unauthorizedly. UTSA has sensitive information like student grades, employee salary details, faculty research information and results. All this sensitive data is being stored and maintain at department wise and some common data in central server too. So we need to take database security as high priority and secure UTSA databases.

Database Security has Access controls, Encryption, Auditing, Secure configuration concerns. So we need to make sure we address all of these in our design.

Access controls should be deployed based on the principle of least privilege. Access controls should be applied to two primary categories of users: administrators and standard end users. For administrators, each DBA should be limited to only the functionality they need to do their job. Many times default functionality, including default roles, provide many more privileges than are necessary because they are designed for ease of use. In such cases, default roles such as 'DBA' should not be used, and instead specific roles for administrative activities should be designed to grant only necessary privileges.

Database at UTSA must be encrypted using Symmetric Encryption, in particular, AES (Advanced Encryption Standard) Encryption. We use AES in particular because it offers the highest level of encryption till date.

Proper Auditing is to be implemented at a minimum, activities such as the following should be audited :

- Administrative activity

• Logon and logoff activity

• Failures

• Use of system privileges

• Alterations to the database structure

Databases also needs to be properly configured, to address this tools are required to automate the entire secure configuration life cycle. This includes database discovery, security scanning, configuration lockdown, automated remediation, and so on. Security consideration needs to be given to the database itself, as well as the surrounding environment, including the underlying operating system and applications.

3.2.4 E-mail Security

Malware is usually found in emails coming from external sources, but the main problem if an employee's machine gets infected, malicious emails can be sent via internal email. Employees are also more likely to click on an infected email attachment if it is from a co-worker. For this reason, it is important to ensure that your email security solution also scans internally sent emails.

Below are the security related email policies that will be used in this design for UTSA:

1. Stop Spam and Phishing Emails

Spam is one of the major security threats for email accounts. Spam can be monetized in many ways and phishing is also a type of monetizing spam. In many ways Phishing emails entice recipients to click on malicious links and provide credentials or confidential information, which can result in security breaches.

2. Use a Multi-Antivirus Scanner

Multiple antivirus engines will helps us in order to increase the rate of detection and reduce the window of vulnerability. Since email is one of the main sources of malware, we will use a fast performance multi-antivirus scanner to scan incoming email attachments for email-borne threats.

3. Check for Confidential Content

UTSA has vast amount of confidential information, which should not be shared to unauthorized persons, so in this design we are going to check the contents of email and see if there is any confidential information is being disclosed unauthorizedly.

4. Block Large Email Attachments

Emails should not contain attachments that are larger than 20 MB. An email that's bigger than 20 MB will most probably not arrive, and the recipient might not even get an undeliverable message back. In the worst case, a large email attachment can bring a whole network to a halt. To prevent this from happening, set an email policy to block large emails and notify the sender, providing alternate methods for sending large files.

3.3 Security Analysis

In this design I mentioned my threat model and based on that I have provided my design in a way to defend the threats discussed in the threat model.In this design I tried to provide confidentiality, integrity and availability all these were ensured with our mechanisms and policies mentioned. Below is the security analysis for the design provided:

3.3.1 Security Analysis on Database

This design has provided encryption to the data in the databases at UTSA and also followed good database policies, which will provide high value of defenses on databases from attacks like SQL injections.

We are using encryption mechanisms, to store data in the databases which provides integrity to data. Passwords are being stored by adding salt and encrypting them which will provide confidentiality to users. MAny restrictions were mentioned on usage of databases like revoking default users and passwords these kind of policies were used to make sure database is not attacked by users by default credentials, which is a good implementation.

3.3.2 Security Analysis on UTSA Web Servers

Here we are using proxy servers to maintain anonymity on the internet and distributed firewall strategy too. For Intrusion detection we are using NIDS and HIDS at network layer and at server level which will provide an extra layer of protection to web servers and systems at UTSA.We designed a firewall with strict policies that are designed to prevent any kind of intrusion into our network. We are also following policy that all the web server resources are not accessed by single or some resources this can reduce the severity of DOS attacks by not letting any system use up all the bandwidth. This way we can be sure about the level of security provided to UTSA's servers.

3.3.3 Security Analysis on UTSA Wireless Network

We assign different levels of privileges to different kinds of users. Since the faculty and students need to log on using their own ID and passwords, their accounts will lead to a suspension if a

violation occurs. They will need to meet the CIO and only after his approval, they will be able to access again. If a violation occurs from the guest user, the IP address will be noted and blocked immediately. This can be resolved again only if the CIO approves.

3.3.4 Security Analysis on UTSA E-mail servers

Emails are the main sources for phishing and spam, so in this design it was addressed properly by blocking spam and phishing emails. Apart from this confidential data is being monitored ie., message content that is being sent from emails is being monitored, to protect confidential content of UTSA, this is a very good way of protecting data.

From my analysis on this design it has all the requirements needed for UTSA to protect its IT infrastructure and electronic data.

4. Conclusion and Discussion

Security design is very important for any IT product and its design involves lot of work and time. Here in this design I tried to put my knowledge from this course and from other courses such as "Secure Software Systems design" and "Security Incidence Response" to provide a better security architecture for all the UTSA computers and IT infrastructure. In designing a security design we must focus on many other aspects apart from network security such as data mining, software engineering, disaster management etc.

In this design our goal was to ensure CIA and I tried to address all the objectives and threats mentioned in the threat model. The design we proposed protects our assets and data in a way that it will be a harder task for attackers to attack on UTSA IT infrastructure and electronic data, even if compromised, we assure that the attackers cannot gain any useful information from the data because we are encrypting the data. This design is a simple, scalable, so that new features can be added to it when needed.

In conclusion, we can say that any architecture level design is complicated, as it gets bigger the complexity increases. The best principle to follow is to incorporate security as a part of application from initial stages itself but not like an add on feature. It is also better to follow cross layer network detection which will help us to identify more threats, so that we can defend accordingly with our proactive defense mechanisms. Although we can't achieve 100% security we can still create a better secure product by following good security design principles and policies. Security is a never ending battle between attackers and defenders, so defenders should be vigilant all the time to protect their resources.

References:

[1] https://msdn.microsoft.com/en-us/library/cc723497.aspx

[2]https://www.owasp.org/index.php/Guide_to_Cryptography

[3]https://www.sans.org/reading-room/whitepapers/analyst/making-database-security-security-priority-34835

[4]http://forums.techsoup.org/cs/community/b/tsblog/archive/2014/12/08/10-best-practices-for-email-security.aspx