CS-5323-001 Principles of Information Security

Design Project

To

Dr. Shouhuai Xu

By,

Venkat Rahul Dantuluri (fpj626)

Submitted on

9th December, 2015

CS-5323-001 Principles of Information Security, fall '15 Design Project

Venkat Rahul Dantuluri (@01518869/fpj626)

Design Objectives:

University of Texas at San Antonio is a public university which has many IT resources. These IT resources are spread across the vast and beautiful campus. As a Chief Security Officer of UTSA I am responsible for securing and protecting these valuable resources. And when I say resources I mean IT resources. The term IT resources is broad term and it encompasses multitude of subtle resources. In this first section I would like to highlight these subtleties and set achievable objectives in an attempt to secure them. This will also include identification of the type of threats each resource might be vulnerable to, although this is the major accomplishment of threat modelling which will be discussed in the next section. UTSA's IT resources include:

a) Physical VDI clients: These are thin client hardware peripherals which run VMWare Horizon Client software on them. These are innumerable in number and are present in classrooms, Library, Labs. An authenticated UTSA student is allocated a VM account in the UTSA Cloud and he/she can access his/her VM using any of these physical VDI machines from anywhere across the campus. It is extremely important to secure these VDI machines as they are potential attack vectors. UTSA students log into the VDIs using their UTSA ID which is unique for a student. He also need to type in his passphrase along with. Once the UTSA student logs into these VDIs he is given a platform to create applications and is also connected to UTSA network. He can run his custom application on the virtual cloud platform provided to him. Here the protection objectives are twofold. Firstly we need to make sure that authentic UTSA students alone log in and no other outsider can log in. Secondly we need to limit the resources provided to him on the VM.
b) Central Library Servers: These are restricted servers that hold the details of all the books available in the library and details of their current rent state. It also contains scholarly articles such as research papers written by the esteemed faculty of the university and other universities, details of scholarly articles published by the same. These servers are twofold. One set of servers act as data servers and other set run a secure application that is used to retrieve necessary information from the data servers. It is extremely important that only authorized University personnel can log into the application and store information in the data servers. Rest of the university stakeholders only retrieve and read information from the data servers. This library application is only available within the university network as it is designed to cater only to the university students, faculty and other university concerned body of interest. As a CSO of UTSA it is my primary objective to protect and preserve the Confidentiality of these Library Data. UTSA scholarly contribution to various fields of study is electronically preserved in these servers and it's my objective to protect them from any possible attacks.
c) Student Record Servers: These UTSA servers are meant to store Student records from the beginning of his admission until his graduation. These include his/hers' outstanding tuition balance, payment history, student's profile, his/hers' registered courses, grades obtained etc. Certain data needs to be more secure and confidential like payment history and grades. Write access to these data should only be permitted to a secluded subset of UTSA employees. All data

have read access to any UTSA stakeholders. Like in Central Library Servers, as a CSO, it is my responsibility to secure these student sensitive information from attacks. Such data are more vulnerable to insider attacks and my security architecture should be able to prevent such attacks. Also, student information is subject to be accessible only within the UTSA network.

d) Employee Servers: These store the employee details of all the employees of the UTSA system. This information is very sensitive to employee of UTSA. For example it contains authentic identity of each employee and occasionally may contains employee's income and bank details. It is my responsibility to secure this sensitive information and come up with a technique for safely dealing with these information. It is extremely important to limit the number of accesses to each account in these systems as these are confidential information pertaining to each employee. Usually each employee wants his information to be secured. The sensitive data present in these servers can be like employees SSN number, employee ID, his investment details, his bank account details, and his billing rate assigned, his monthly income, and so on. In is customary that such information is updated by the employee himself. Only employee has write access to his information. Other authorized units of organization can read such data and act upon. And it is my duty to see to that this is preserved.
e) Employee Machines: These are systems or workstations provided to the employees of UTSA to perform their daily duties and chores. These systems are immovable and are always within the UTSA network and campus. Hence these systems are assumed to be authorized. It is very important that these systems are safeguarded from falling into wrong hands. Any unauthorized subject, if got access to these systems inside UTSA offices can disrupt everything.

The above description of the design objectives may be very clear but to a security person these descriptions are still too ambiguous to do anything about. We define a set of security policies that encompass all the above objectives and are comprehendible within security profession. In these policies we state what security property should be preserved.

Policy 1: We need to preserve the Availability property of VDI clients.

Policy 2: We need to preserve the Confidentiality, Integrity and Availability of the student information present Student Records server.

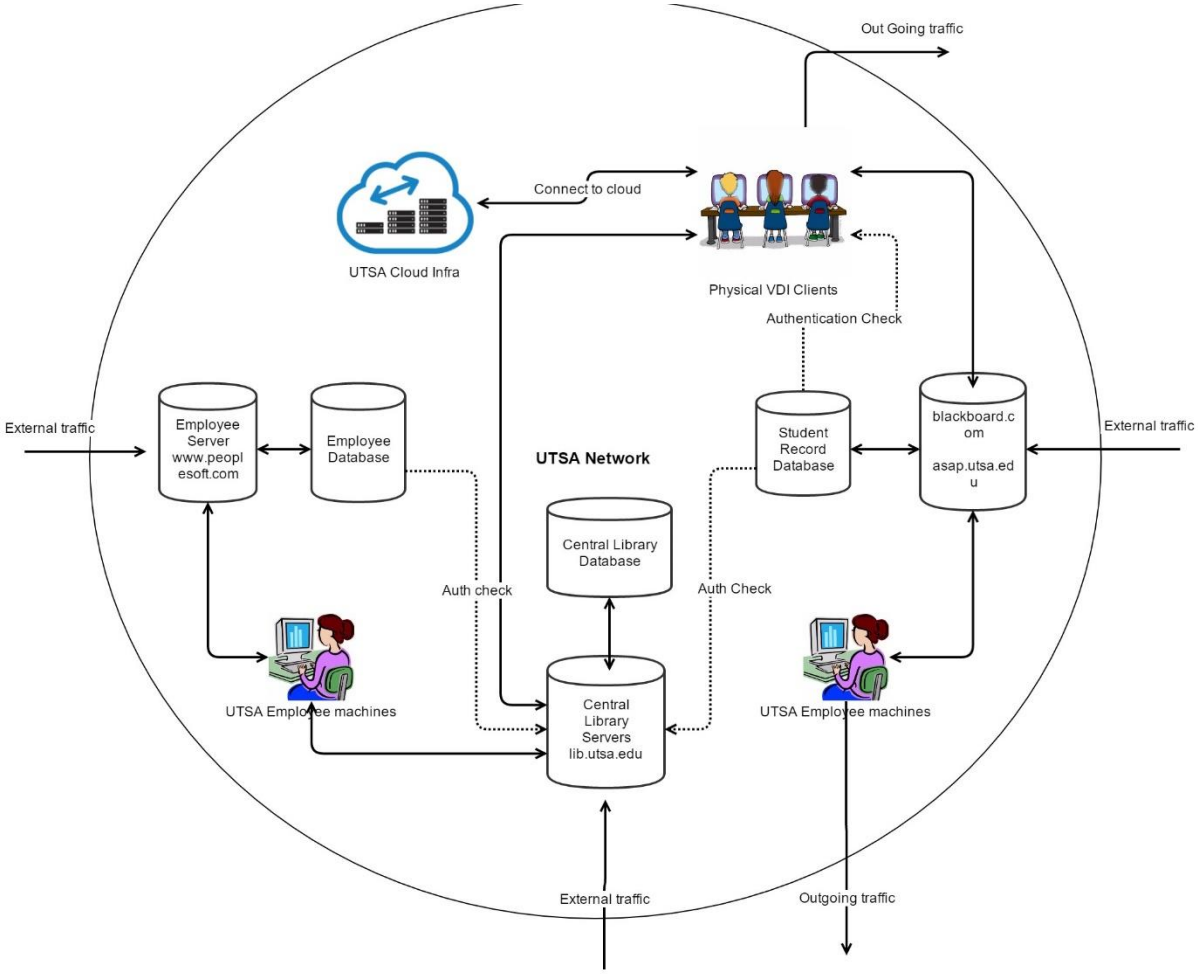
Policy 3: We need to preserve the Confidentiality, Integrity and Availability of the employee information present Employees server.

Policy 4: We need to preserve the Confidentiality, Integrity and Availability of the university knowledge base present Central Library Servers.

Policy 5: We need to preserve the Confidentiality, Integrity and Availability of the UTSA employee workstations.

As a Chief Security Officer of UTSA it is my primary objective to implement a Security Architecture that enforces these states policies. Before starting off with the architecture it is beneficiary to understand all the different types of threat that our system is vulnerable to. We realize those by Threat Modelling.

To build an efficient threat model it very necessary to observe the existing network model of the UTSA systems:



This schematic will give you a clear picture of the network structure of UTSA network. It also showcases the various resources I need to safeguard and the various communications that happen among them within the network and between external to it.

Design and Security Analysis:

Threat Model:

To identify the various types of attacks that are possible we use Threat Modelling. It is extremely important to define the scope of Threat model. As per the scope of threat model is concerned I will be sticking to threat modelling only the above mentioned IT Resources. I won't be threat modelling the OS each system in UTSA uses. I will be threat modelling the various web app services like blackboard.com,

peoplesoft.com, asap.utsa.edu but will not go into detail like modelling their architecture and design. Will only model their requirements. It is extremely important to specify the scope because otherwise threat modelling will never end. I will continue for ages and I will not be able to achieve anything worthwhile from it.

Threat Model VDI Clients:

Threat 1	VDIs Clients can be detached and stolen.
Threat 2	An unauthorized subject may try to illegally access into an account.
Threat 3	Valid UTSA student credentials may be stolen and the perpetrator may try to log in to the target's account using VDI.
Threat 4	Authorized student may use the resources of cloud to create malicious code to infect other systems on the cloud.
Threat 5	Authorized student may accidently download malware when connecting to external networks.

Threat Model Central Library Server, Employee Server, and Student Record server:

Threat 6	Bypassing the web application and directly connecting to the Central Library database, Employee database or Student Record database from external network to access the files and corrupt them.
Threat 7	SQL and XSS injection attacks.
Threat 8	Man in middle attack while authenticated and authorized UTSA stakeholders are writing or editing data into the databases.
Threat 9	Authenticated and Authorized UTSA stakeholder's (authorized to write into the Database) credentials are lost and the perpetrator launches an attack to bring down the database.
Threat 10	A non UTSA subject may try to illegally access UTSA data by attempting dictionary attacks on the Applications.
Threat 11	Valid UTSA student credentials may be stolen and the perpetrator may use target's credentials to access UTSA's content.
Threat 12	Server may come down due to Natural Hazard or any other reason.
Threat 13	An insider with valid credentials to DB may directly log into the DB box and change connection settings or corrupt the data.
Threat 14	An insider with valid credentials to Web servers may directly log into the server box and access the password file in attempt to gain credentials.

Threat Model Employee Machine

Threat 15	A non-authorized personal can gain access to these machines and access to all the severs. A connection from these machines is assumed to be authentic.
Threat 16	Authorized employee may accidently download malware when connecting to external networks.

Threats are due to the presence of one or more vulnerabilities in the existing system. Currently our system comprises of the UTSA network and the IT resources it contains. Through threat modelling I hypothesized

all possible attacks to our systems. Now I would like to list the vulnerabilities in our system that the attacker could possibly take advantage of to realize the above stated threats. Together I will also put forward a possible design and implementation that helps us to detect the threat or help patch the vulnerability. Patching the vulnerability is sometimes hard and if it tends to go beyond the scope of the discussion it is better we rely on the detection techniques.

Main Design and Security Analysis:

1) Secure against Threat 1: It is extremely important to secure the Physical VDIs. To ensure this we need to ensure the access to the classrooms to only the Students of UTSA. To implement this it is important to install card readers at the entrance to any UTSA building and provide entry access to only those UTSA authorized personnel who has valid credentials. In this way we can limit the access to UTSA stakeholders only. Further, constant surveillance using mountable cameras is important to detect threat against any insider trying to steal any VDI clients. A more secure implementation is to use sensors that detect individual VDI connections. The moment a sensor goes down we may need to be vigilant in our monitoring until we detect the cause.

2) Secure against Threat 2 and Threat 3: It is also possible that one of the UTSA students may try to log into another students account to access the sensitive information of the victim. Here we need to protect the confidentiality of the victim's cloud account. UTSA implements traditional password protection technique where in the students will type in their UTSA ID as username and their private password to be authenticated. Although authentication through passwords have proven to be helpful we cannot really know that the person who is entering the password is really the same person the password belongs. Passwords are meant to be kept secret, but humans are bad at choosing good passwords. A good password is the one that makes the attacker take a really long time to decrypt. So we mandate that each UTSA user to use a really long and complicated password that incorporates special characters, lower case and uppercase alphabet and numerals. This will prohibit an attacker from performing dictionary attacks. But what if the password of victim is compromised. To deal with these cases I recommend we also use biometric based detection at each VDI client. Biometric based authentication has become very cheap and companies like DELL are installing such authentication mechanisms in common Personal computers. Complementing biometric based authentication with password protection system with strong password policy is the security design I suggest to secure VDIs from threat2 and threat3.

3) Secure against Threat 4: It is possible for an authenticated student to launch an attack by logging into the UTSA cloud and connecting to the UTSA network. The student can develop malicious code and run it to compromise other cloud accounts and VMs. Or he can also deploy this malware he developed to other systems connected to same UTSA network. Since this attack is launched and targeted towards systems within UTSA networked, Firewalls may not help us to detect such attacks as firewalls are like "eskimo pie" (Hard exterior but smooth and soft interior). I suggest we go for a more preventive approach that incapacitates any student from performing such malicious activity. The cloud accounts given to the individual students should not give them any admin privileges. By default any activity that needs admin privileges like installing a software, should be

denied. Every activity performed by the student should be thoroughly logged so that we can preserve the non-repudiation property in case of any malicious activity is detected.

4) Secure against Threat 5 and Threat 16: Accidently or intentionally, now and then, we land up browsing a malicious site that downloads malware and compromises our system. For systems in UTSA this is one of the biggest hurdles. Static approaches like keeping track of all the URLs that thousands of UTSA students frequently browse from many of the UTSA systems and comparing it with blacklisted set of URLs is very hard and laborious. Instead I suggest to use a newly researched technique of Cross layer detection. Cross Layer detection is as fast as static approaches and as accurate as dynamic techniques. It includes observing not just the application layer but also the network layer for malware detection. This is a very robust and latest technique of malicious website detection. Empirical analysis have proved it to be effective and fast.

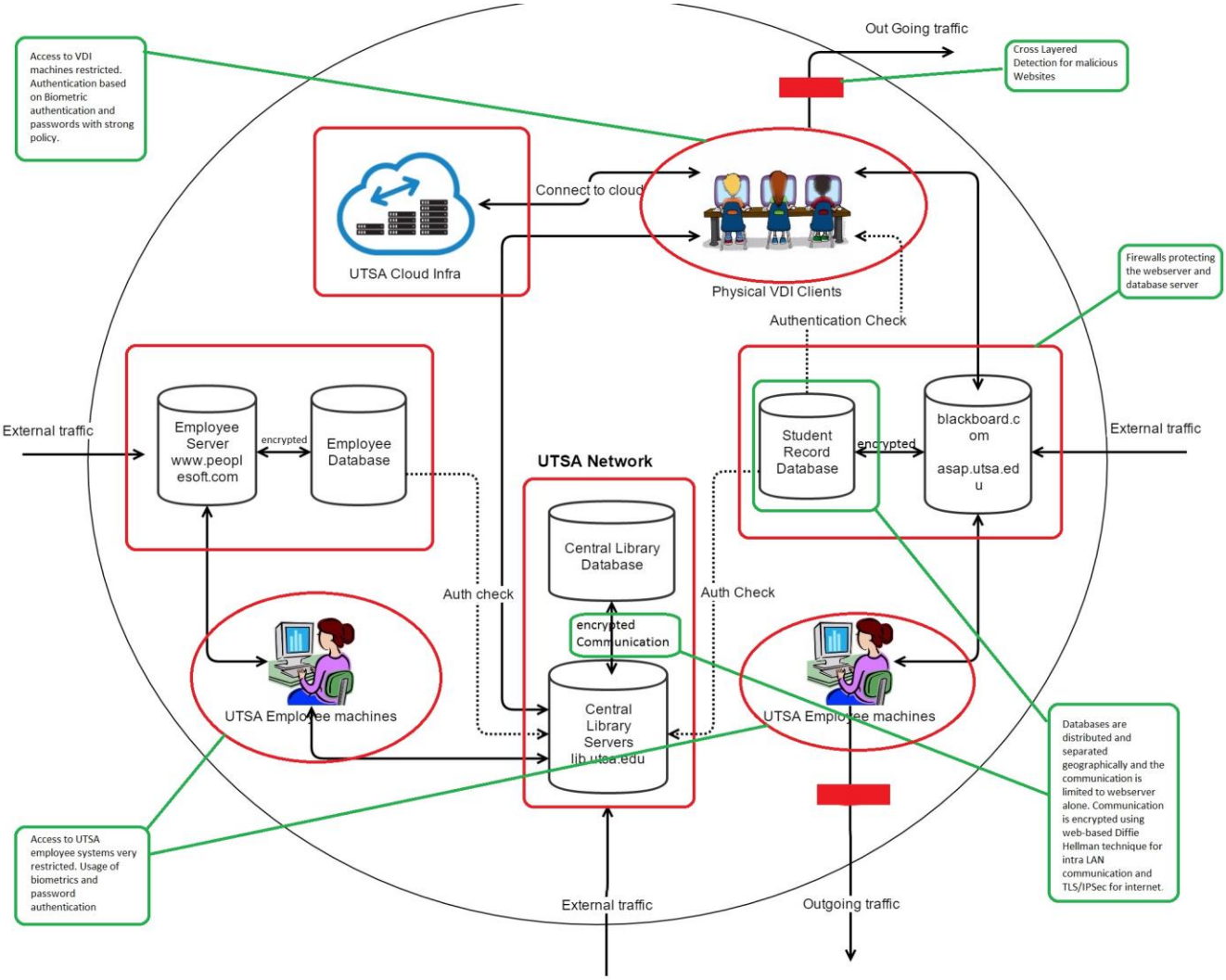
5) Secure against Threat 6, Threat 8, Threat 9 and Threat 13: Databases are the heart of UTSA. Securing them is extremely important. Because of their importance it is my pivotal responsibility to enforce Confidentiality, Integrity and Availability of these systems. Firstly and foremost I suggest to disconnect any external to internal connections onto the hosts that contain the database on them. We use state-full firewalls and set strong rules to disallow any direct connection from outside UTSA network to inside database host. Secondly we also disallow all internal connections to database hosts except those from corresponding web servers. The above diagram highlights the webserver and data server connections. These limited connections should also be cryptographically encrypted using password-based Diffie-Hellman technique or TLS and IPsec protocols depending whether the webserver and database are located in one place or geographically separated and use internet to communicate. This will help prohibit man-in-middle attacks as specified by Threat 8. Further database connections should be logged and audited more regularly. Very few UTSA organization trusted authorities have privilege to access the database and their privilege is also separated. The privilege required to log into the Database box should be distributed among the Database Administrator, top business executive of UTSA like the Chancellor and the Chief Technology Officer of UTSA. This separation of privileges will mitigate Threat9.

6) Secure against Threat 7: Security against SQL and XSS are more often a requirement for the web applications that run on the webservers of UTSA. UTSA websites URLs that handle data are all encrypted with HTTPS. It is a mandatory requirement that the Web Application use stored procedures to avoid script injections. It also mandates filtering based on pattern matching. If any request URL body contains unwanted data like SQL or other scripts we should drop the connection. UTSA web applications should be equipped with these capabilities.

7) Secure against Threat 10, Threat 11 and Threat 14: UTSA webservers need to handle logins to webserver boxes as it is implemented for databases boxes. Only authorized personnel having access can log into the machine. But the implementation need not be so strict. The database connection credentials and credentials of authorized personnel should be protected. Usually OS will take care of that. I suggest using latest versions of OS with better security features. Such

Operating Systems usually stored passwords as a function and maintain the confidentiality of such functions. Salts are mandated to avoid any dictionary attacks. Access to any such sensitive information should trigger an alarm and alert the concerned security officer. Firewalls should be installed to intercept every communication. Firewalls should allow external TCP connections to internal webserver application only on the webserver box but not to any other application or port. All other applications have default deny access. This ensures that the system is more secure.

8) Secure against Threat 12: Database servers are so important that they need to be well protected against potential natural hazards like earthquake etc. Any unavoidable downtimes should be handled. This is the reason why we replicate databases, typically across geographies.



Conclusion and Discussion:

Threat modelling might have helped me a great deal in coming up with all the above listed threats, it does not mean that the system under study is devoid of all the threats and is completely secure. There are always 0-day attacks that are a nightmare for any Security person responsible for maintaining the security and integrity of the sensitive resources and information of his organization. A new way of detecting a 0-day attack involves heavy usage of Data Analytics. My current security design doesn't incorporate identification of possible zero-day attacks. Latest and more robust tools like WINE (Worldwide Intelligence Network Environment) detect a 0-day vulnerability only when the vulnerability is identified by the software developing company or organization. All the software that UTSA uses is developed by an IT organization and is not developed in-house by UTSA security department. Hence we have no clue of what vulnerabilities are present in the software. We can only mandate security and secure practices as requirement. Hence there is always a fear of a zero day attack that can compromise the integrity and confidentiality of UTSA systems.

Root kit attacks are always a well-known to be stealthy. Our system does not provide any detection or prevention mechanism for root-kit attacks. This is because detecting root kits is extremely difficult. They even tend to compromise the logs by forging them. One reason why we did not invest in preventing root kit attacks is because root kit attacks are too tough to execute. The attacker should be extremely crafty and very well knowledgeable to successfully mount a rootkit attack. It also consumes a lot of time. By launching a root kit attack on organizations like UTSA he may not get proper returns to his investment unless his interest in returns is knowledge.

I even haven't discussed about securing UTSA IT resources against bot net attack. Any prevention technique to disrupt a botnet attack is vague as the attacker can adapt his attack vector to launch the attack in a different way. The same argument sufficient for root kit attacks will also suffice for Bot Net attacks. Why would anyone launch a sophisticated botnet attack unless UTSA stores secure defense related information? But UTSA is all but a non-profit organization providing quality education. Hence Botnet prevention techniques are not so economical to implement. At the end economy and budget also matters in the security of system.

I conclude by stating that I have clearly chalked out the scope of Threat modelling before the start of threat modelling and have discussed each technique to counteract the threats. I have used my knowledge that I could acquire from Courses like Principles of Information Security and Secure Systems and Software. I purposefully exempted myself from borrowing any ideas or material from Internet so this is my own design.

References:

Lectures on Threat Modelling: https://www.youtube.com/watch?v=qBI8BOvP2l8

Cross layered Detection: http://business.utsa.edu/wps/MSS/0003MSS-432-2013.pdf

Drawing and Diagrams: https://www.gliffy.com/