Cyber Security Spring ’10 Final Project Scenarios

First Draft

1. Common Requirements

There are several possible final project scenario options. Each scenario will have a customer assigned. You can ask that customer or Prof. Hinrichs for clarification of the requirements. The class will divide into four groups of five or six people.

In all scenarios, your group will be responsible for creating:

- A security policy and a threat model. What are the goals of the architecture? What are the threats that the design is concerned with?
- A security architecture design. This design should identify what technologies are used and where. It should discuss the implementation and maintenance issues (e.g. key management and access changes in the in face of a changing population). Where appropriate, the design should discuss the trade-offs and the motivations for choosing one technology or technique over another. The design should include an overview diagram.
- A laboratory implementation for a subset of the design. Depending on what is implemented, you should submit an implementation design, configuration files, and supporting log data. In most cases you should also arrange a demonstration of the implementation.
- A final presentation and writeup. The presentation and writeup will review the problem and your solution. It should be targeted at your customer. You will have 30 minutes allocated for the presentation.

1.1 Important Dates

April 1 – form groups and select project scenarios.

Week of April 5 - groups meet with Prof. Hinrichs for initial design review and identification of lab implementation subset. An initial security policy is due at this time.

April 27, 29, and May 4: In class presentation of design.

May 6: Final design and lab due

2. First Responder Scenario

In this scenario, a number of different organizations are collaborating to address a time critical urgent problem, e.g. St. Loius destroyed by an event on the New Madrid fault. Each organization has strong information labeling and information flow constraints. Each organization has a separate user authentication space.

The primary goals for this architecture are:

- Flexible but high assurance entity authentication
- Flexible but high assurance information sharing.

The virtual customer is still TBA.

2.1 Collaborative Environment

In response to an emergency, we need a scheme to quickly map how the labeling schemes relate and have an automated means to share information between the different organizations. The emergency may be a natural disaster like Katrina, a terrorist act like 9-11, or a regional war like in Iraq or Sudan. In all cases, people from a variety of organizations will need to share information starting very quickly for the period of weeks to years. This can be very sensitive information, so the design must also be careful to not drop security so much that the malicious entity can take advantage of the chaos of the event to gain access to restricted information.

Several approaches have been taken to share data between organizations. One approach is to have each member of the coalition maintain their own portion of the data and use access control or a guard approach to automatically enables a process of upgrading/downgrading data between different labels.

Alternatively, the coalition could create a joint data repository or community of interest that is accessed by all organizations. The joint authority can either be hosted by a "lead" organization (this is reasonable in a military setup), by a trusted third party (not easy to find), or maintained with a consensus based policy approach. Some recent work on the joint repository approach is described in the following papers:

- Laura Pearlman, Von Welch, Ian Foster, Carl Kesselman, and Steven Tuecke. A Community Authorization Service for group collaboration. In *Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks*, 2002.

- Rakesh Bobba, Serban Gavrila, Virgil Gligor, Himanshu Khurana, and Radostina Koleva. Administering Access Control in Dynamic Coalitions. In Proceedings of the 19th USENIX Large Installation System Administration Conference (LISA), Tucson, AZ, December 2005.

In addition to enabling information sharing, your design will also need to address how people are authenticated into the system. Since these collaborations are dynamic and not pre-planned a basic password scheme is not going to be sufficient. Most technologies that attempt scalable authentication use some form of certificates plus strong multi-factor authentication. Safely deploying and maintaining long-lived certificates is a major concern.

In practice only limited forms of multi-factor authentication may be viable for coalition environments. This is because each organization is likely to retain its own identity certification process that is trusted by other domains in the coalition. Therefore, trusting multiple factors for the authentication gets complicated. There are protocols such as OpenID and SAML for delegating authentication to trusted parties.

2.2 Collaborative Infrastructure Requirements

- High-assurance environment.

- Strong, flexible cross-organization authentication
- Strong, flexible cross-organization data sharing.
- Automated, safe data-sharing

3. Financial Organization Scenario

Customer is Ken Rowe (kenrowe@uillinois.edu).

In this scenario, you are hired to create a security architecture for a local bank paying special attention to the ensuring that your security implementation meets the requirements of Gramm-Leach-Bliley (GLB). In particular, your design must allow for auditors to verify that security has been enforced according to the GLB requirements.

In this scenario, a financial institution is contracting your group to design their next generation security architecture. The primary goals for this architecture are:

- Customer perception of a highly trustworthy system
- Regulatory compliance

3.1 The financial environment

The perception of trust is key for companies in the financial industry. Customers choose one bank/broker over another on a number of attributes, but in the end if one bank is perceived as more trustworthy than the other, this will be the primary decision factor. This trust perception includes availability in addition to the more expected security issues of data confidentiality and integrity.

Because of the importance of trust, financial companies tend to be very conservative with respect to deploying technology. They are less likely to use wireless communication. They can enforce a small set of supported hardware, OS, and software. They restrict employee mobility.

Regulatory compliance is also a huge operational issue for financial institutions. They must undergo periodic third party audits to satisfy a variety of regulations including Sarbanne-Oxley, GLB, Federal Reserve, and international regulators. The audits include verification that the security implementation matches the higher level security policy, but they also include looking at operations logs to prove that the security devices were operating as expected (e.g., customer initiated transactions were completed as expected). Some regulations place restrictions on what data can be visible to protect the privacy of the end user.

Most company employees are associated with a given branch/location, but there is a small set of employees that travel between multiple locations and must operate in a set of locations with relative ease. These employees use laptops which may contain customer critical information. The security architecture must be concerned with laptops lost in transit. Due to regulations, such loss of customer information would require the financial company to notify all customers of the possibility of information loss in such a situation. The financial company might also be concerned with desktop theft, and associated loss of information, so the security architecture should consider the possibility of strong protection of data on all machines from theft.

One of the trickiest security aspects of the financial scenarios is securely providing web access to customers. Many customers are not technically savvy. The design must resilient against direct attacks by malicious users and indirect attacks via co-opted users.

The company also needs to communicate between branches. Currently they are using dedicated frame relay networks, but they are interested in the possibilities of using the Internet assuming the risk exposure is not too high.

3.2 Infrastructure requirements

- Third party security verification
- Web banking
- Remote branch communication over public networks

4. Service Provider Scenario

Mr. Lee's Greater Hong Kong includes a mid-level Internet service provider. This company sells networking services to burbclaves who in turn resell the service to the burbclave citizens.

To date security has taken a back seat to performance and ease of use (reducing costs by limiting customer support), but in an effort to comply with legal requirements and expand their market Greater Hong Kong ISP needs to reconsider some design issues with respect to security.

Greater Hong Kong ISP only provides a limited number of routable addresses to each property, so address translation is required. For more money a citizen could acquire one or more routeable addresses.

Major goals for the new architecture are:

- Ease of use and low customer support requirements.
- Ability to comply with law enforcement requests (via CALEA or recording industry complaints)
- Limiting the generation of “bad traffic” from customer sites to the Internet.
- Identification of new security services which could be sold to the tennants.

The virtual customer TBA

4.1 Service provider environment

High uptime and good quality are critical for the service provider to keep their customer base. Anything that denies or degrades service such as lowered bandwidth or bounced emails must be avoided. This implies that avoiding Denial of Service attacks is important.

It also means that the service provider avoids gaining a reputation of being a source of spam or other attacks. The service provider must prevent customers from using their service for bad purposes, e.g., botnet, phishing, domain squatting. If the service provider gains a reputation as a source of bad traffic, other service providers will drop packets and email from its space resulting in bad service for other paying customers.

The service provider provides different levels of service for the burbclave depending on the contract they negotiated with the burbclave organization or directly with Greater Hong Kong

ISP. The infrastructure needs to be able to enforce the service level agreements or detect when the tenant is running outside his portion of the agreement. Some aspects of the agreements include bandwidth usage, providing services to the outside world, volume of traffic, and not using the service for illegal means.

Another unique aspect of the service provider environment is limited trust between customers and between the customer and the service provider, which requires segmenting customers from each other and from the service provider. This segmentation takes several forms:

- Protecting customers from other infected customers (virus, spam).
- Preserving confidentiality of information between customers and between customers and the service provider itself.

The customer would like to trust that the service provider does not look into or change his data. The service provider needs to claim ignorance of a customer's data stream to avoid legal liability for the customer's data (e.g., bootlegged music or unsavory photos). Although with recent changes to CALEA this enforced ignorance is no longer possible.

4.2 Infrastructure Requirements

- Ability for new devices of already registered users to join the network with limited Greater Hong Kong ISP involvement.
- Minimize customer premise equipment. There will be one to a handful of devices per property. There will not be equipment per tenant.
- Ability to track traffic is required to avoid legal problems.

5. Educational Organization Scenario

In this scenario, you are responsible for reviewing and upgrading the security architecture for the Information Trust Institute (ITI), a large teaching and research school. The ITI is mostly a traditional "brick and mortar" University, but it has a growing group of remote students who access lectures and research from the Internet.

The major goals for this design are:

- Protect core organization assets
- Prevent organization assets from being subverted and used as launch points for broader attacks
- Enable flexibility setting up trusted members of the environment. Visitors should be quickly and easily given access to the network.
- Enable security research with direct access to the Internet or with known malicious software, but constrain the spread of such experiments

Virtual customer TBA.

5.1 The Educational Environment

The academic environment is inherently very dynamic both in terms of people and technology. People range from very technically savvy to rather technically naïve.

Unlike the commercial environments you cannot dictate the hardware platforms and OS images or versions deployed. A somewhat standard windows environment is used by the administrative staff. Research labs will introduce a wide variety of somewhat esoteric hardware and software. Student labs are more standardized, but there will be differences between labs based on class requirements. Some of these labs can be isolated from the outside world, but in the age of the Internet, some labs must be connected to the greater world. In the case of student labs, remote students must be able to access any student lab in all cases.

Labs studying network and computer security place special constraints on the research organizations infrastructure. Some experiments must be performed on a “dirty” network, e.g., honey pots will not capture new viruses if they are on well protected networks. Other labs will involve experimenting with hazardous pieces of malware that must not be allowed to escape a constrained environment.

Visitors and students will bring in a wide variety of laptops running a wide variety of OS images and programs. Students tend to intentionally or accidentally try a wide variety of programs that can have unexpected consequences.

Students also raise legal concerns from the music and entertainment industry. University officials hope to ignore the whole issue, but they must protect themselves if a large entertainment company puts the university into its sights. Recent changes to the CALEA interpretation within a university environment also places additional constraints in the security environment. The infrastructure must be secure, but we must be able to tap into the network with required by law enforcement.

The research organization must interface with the broader research community. There are frequent visitors to the University, and they must be able to access the computer infrastructure to access the Internet and check their email back home.

5.2 Research Infrastructure Requirements

Specifically, the research organization must provide the following cyber infrastructures

- Wireless connectivity for all members of the community plus easy access for guests.
- Wired connectivity to offices and appropriate research labs. Enforced isolation for other labs.
- E-mail service for members of the community.
- Relatively small number of authentication mechanisms.

6. Distributed Office Security

You have been contracted to create a security architecture for an insurance company with huge numbers of remote offices covering a wide geographic area (international). Each office serves an agent and his/her support staff. The remote office team is not likely to be very technically savvy.

The major goals of this architecture are:

- Protection of key customer data to maintain customer trust and meet regulations.
- Timely communication in the field.

- Scalable deployment in both performance and resources (manpower and money).

Virtual customer TBA.

6.1 Insurance Company environment

Insurance agents operate over a wide geographic area. Ideally there are agents near all customers so they can offer personalized service. The agents must have access to information from the home office to provide accurate information to their customers. They must also update information as their customers change policies and file claims.

The number of offices can run into the 10,000's. The offices will be located in many states and countries with differing information security requirements. Some localities may have restrictions on encryption (e.g. requiring key escrow). Other localities may have stronger requirements on customer privacy.

Due to the scale, the central office needs to consider how to efficiently provide IT services to the remote offices. Can the offices be centrally managed? Will the company need to rely on outsourcing basic management to local IT firms? If critical IT functions are outsourced, how can correct operation be monitored and verified? What requirements would you suggest for setting the bar for IT contractors?

Most of the time the insurance agents will operate in their offices, but in times of major disasters (e.g., hurricanes or fires), additional employees may be sent to the area to help determine damages and get claims filed. These extra agents will need timely access to data and will not likely have access to a fully functioning office.

The following information is critical to the company

- Current customers, policies, and claim history.
- Outstanding claims.
- Actuarial data and algorithms.

6.2 Infrastructure Requirements

- Protecting key information that must leave the central office.
- Architecture for remote office communication with a very large number of offices.
- Plan for more dynamic communication in the field on an as needed basis (with a day or two of lead time).

7. Health Care Security

Mr. Lee's Greater Hong Kong also runs a network of health clinics and hospitals, HealthNow. Patient information is a huge issue for the health care industry. The patient's health history must be high integrity (random folks should not be able to add or delete to this history). The patient's health history must be highly available in the event of a medical emergency (when undergoing a stroke, extra minutes to access health information is critical). The patient's health history must be confidential (an employer should not be able to discriminate based on the patient's health conditions). HIPAA governs the privacy of a patient's health information.

You have been engaged to design the security framework for HealthNow's clinics and hospitals. HealthNow must provide health information to doctors and nurses so the can provide good service. The customer must be able to access his own health history, and his health history must be transferable to other treatment organizations. HealthNow must provide treatment information to the customer's insurance company to enable payment. Plus HealthNow must meet all governmental HIPPA requirements.

The major goals of this architecture are:

- Protection of customer health information to meet customer expectations and HIPAA regulations.
- Timely access to health information for treatment needs.
- Adequate communication of treatment information for responsible insurance payment.

Virtual customer TBA.

7.1 Health care environment

There are numerous health clinics in the HealthNow network. Customers should be able to visit any clinic and be ensured that the doctors and nurses have access to their health history. The clinics do not have a staff of dedicated IT professionals. There may be 100's of clinics within a single HealthNow network.

When customers visit clinics and hospitals outside the HealthNow network, the doctors and nurses should still be able to access the customer's health history. Ideally the customer is able to give a positive affirmation of the transfer, but depending on their illness they may not be in a position to give such affirmation. Within these bounds, HealthNow must minimize the possibility of leaking health history to unauthorized entities, e.g. tabloids looking for the latest medical procedures that Khloe Kardashian has undergone.

7.2 Infrastructure Requirements

- Protecting patient information.
- Finding the right trade-off of availability versus confidentiality.