

Cyber Security Spring '08 Final Project Scenarios

Second Draft

1. Common Requirements

There are four final project scenarios. Each scenario has 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 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 tradeoffs and the motivations for choosing one technology or technique over another. The design should include an overview diagram which can be hand drawn.
- 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

March 13 – tentatively form groups and narrow set of projects down to four.

March 27 - : group members and scenario assignments finalized

March 31 – April 4: 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 24 and April 29: In class presentation of design.

May 5: Final design and lab due

2. Collaborative Information Sharing Scenario

In this scenario, a number of different organizations are collaborating to address an urgent problem. 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 Mikel Matthews, mikel@argus-systems.com.

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 enable 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
 - Certificate-based
- Strong, flexible cross-organization data sharing.
- Automated, safe data-sharing

3. Web Service Provider Scenario

The target company is a mid-level Internet service provider. It wants to move into the web hosting space. It wants to offer a range of web hosting options from basic web sites to content management systems (CMS) to completely customer managed sites.

In giving more power to the customer, the ISP must worry about attacks generating from the customer (either intentional or externally exploited). A poorly implemented javascript may open the customer up for a variety of attacks. Such attacks may steal resources from that customer or other customers, and the attack traffic may cause the ISP's addresses to get black listed which will cause unhappiness from their other customers.

It wants to differentiate itself from the myriad of ISP's as the more secure option by offering security services such as customer configurable firewall filtering, spam protection, and IPSec gateways. It is also open to other ideas about services to provide.

Major goals for the new architecture are:

- Service availability and quality
- Web hosting safety
- Differentiating services

The virtual customer is Parisa Tabriz, parisa.tabriz@gmail.com

3.1 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.

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 may no longer be possible.

As the service provider offers more services, there are more options for the customer to configure. The design needs to consider the possibility of allowing the customer to configure some options himself (e.g. firewalling management) versus the security implications of customer errors in his configuration.

3.2 Infrastructure Requirements

- Range of web hosting options.
- Framework for detecting/protecting exploitable flaws or directly malicious code on customer sites.
- Some additional security services such as configurable firewalling, spam protection

4. 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 still being finalized.

4.1 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 out of 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.

4.2 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).

5. Research Organization Scenario

In this scenario, you are responsible for designing the next generation security architecture for the *Information Trust Institute*, a large research organization that collaborates with many other organizations.

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 still being finalized.

5.1 The Research 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. 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.

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.

Recently students also raise legal concerns from the music and entertainment industry. Department 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 university community. There is a university-wide infrastructure for authentication, storage, and computation. It may or may not make sense to leverage this infrastructure, but your design must at least co-exist with the university infrastructure. Your organization’s infrastructure must also be able to support visitors from other departments. Many researchers are collaborating across disciplines and such cross department people must be able to work in any of their home departments.

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.