CS526 Fall 2004 Final Solutions, December 13, 2004
Prof. Chris Clifton

Time will be tight (it took me 60 minutes, but I already knew the questions.) If you spend more than the recommended time on any question, **go on to the next one**. If you can't answer it in the recommended time, you are either going in to too much detail or the question is on material you don't know well. You can skip one or two parts and still demonstrate what I believe to be an A-level understanding of the material.

The space given is roughly what it took me to (hand)write the solution set answer. Feel free to use more space if you desire and have time. It is okay to use abbreviations in your answers, as long as they are unambiguous and reasonably obvious.

While some of the questions may seem to be general knowledge / essay, for full credit you should make use of formalisms covered in the class where appropriate. A long essay may answer the question, but using the models and terminology learned in class will give a shorter and more precise answer, giving you time to answer all the questions.

Solutions given in italics, followed by scoring.

Expectations: Out of 73 possible points, I expect around 61 to be the bottom of the A range, 53 to be the bottom of the B range. I would put passing around 30.

1 Malicious Code & Authentication (15 minutes, 9 points)

There have recently been several viruses / trojan horses that propagate via email. The messages in question carry forged "From" addresses, to improve the likelihood that the recipient will activate the attachment.

1.1 Risks (6 minutes, 3 points)

In addition to convincing people to open an attachment containing a trojan horse / virus, name one other risk posed by forged-source e-mail.

Integrity: a malicious party may send data purporting to be from a trusted (high integrity) source. The receiving party will trust it because of the (forged) From address.

Scoring: 1 point for risk, 1 for description, 1 for it being a result of forged From address.

1.2 Authentication (8 minutes, 6 points)

What authentication methods have we covered that might help reduce the losses due to e-mail viruses? Identify two and describe how they would help reduce the losses.

Authenticate source machine, e.g., digital certificates at each link. This would ensure that a message came from the purported host, otherwise the message would be suspect.

Digital signature of sender. Would ensure that the From address matches the real sender.

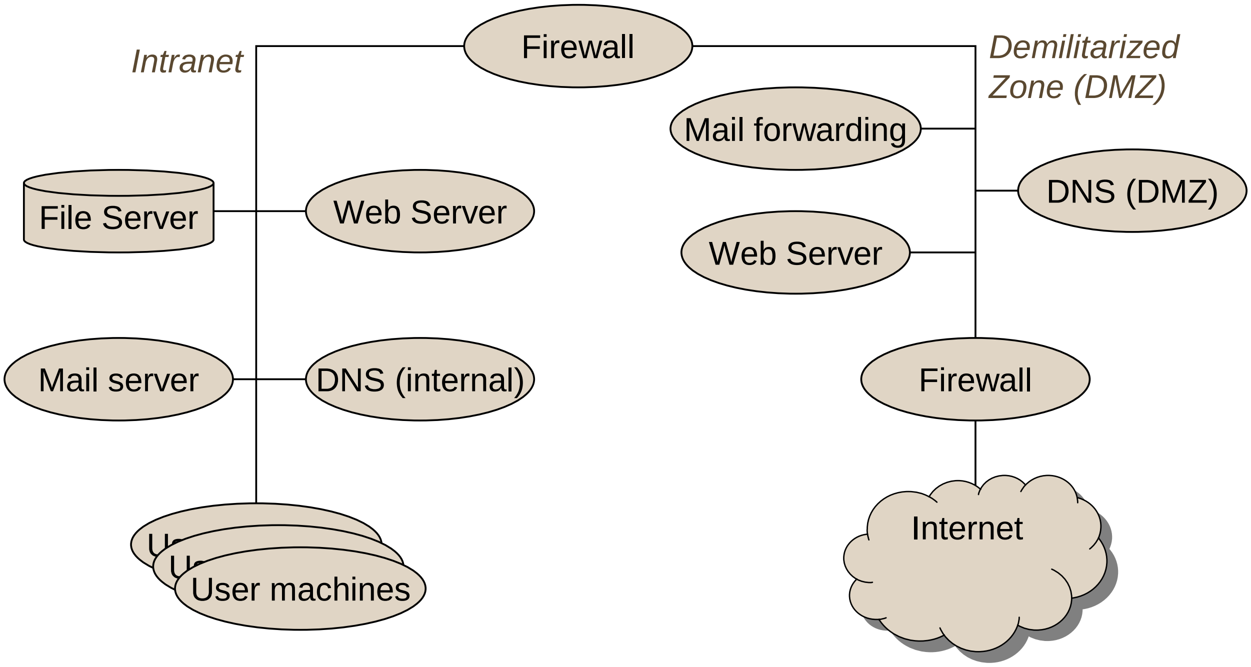
Scoring: 1 point each for method, 1 for how it helps, 1 for clearly dealing with forged From addresses.

2 Design Principles (10 minutes, 8 points)

We discussed eight design principles:

1. Least Privilege
2. Fail-Safe Defaults
3. Economy of Mechanism
4. Complete Mediation
5. Open Design
6. Separation of Privilege
7. Least Common Mechanism
8. Psychological Acceptability

For four of the principles, describe how a “typical” network architecture (as in the diagram) either follows or violates the design principle. Assume that the “company” is Purdue University; the Intranet is all on-campus machines.



For full credit, choose at least one principle that you feel is followed, and one that you feel is violated. Remember, you only need to answer four of the eight. You will be scored on showing 1) that you know the meaning of the principle, and 2) that you nderstand networking security issues as related to the principle.

2.1 Least Privilege

Violates: All on-campus users have equivalent access to the intranet, not just to needed servers.

2.2 Fail-Safe Defaults

Followed: External users default to no access to intranet.

2.3 Economy of Mechanism

Violated. Given insecurity of internal network, and considerable need for outside access, the double firewall is unlikely to add value beyond a single firewall, and it does add complexity.

2.4 Complete Mediation

Followed: All external connections checked.

Open Design

Followed: Since final is published at my web site, the web / security structure is visible and can be openly vetted.

Separation of Privilege

Followed: Distinguishes administration/privilege for internal, external communications.

Least Common Mechanism

Violated: Network security for all applications based on a single mechanism, the firewall.

Psychological Acceptability

Violated: In a University, people expect a wide-open environment, not differences between internal and external. As such, they are likely to use alternative means to access the Internet, possibly leading to unofficial "gateways".

Scoring: 1 point for showing understanding of principle, 1 for how it relates to the network environment. Note that there isn't necessarily a right/wrong answer.

3 Authentication (26 minutes, 18 points)

The following have been proposed or used as authentication mechanisms for secure areas. Formally model each in terms of the **A**uthentication information, **C**omplementary information, authentication function (**L**), etc.

3.1 Picture ID card (6 minutes, 4 points)

Each person has an Identification card with a picture, a guard checks to make sure anyone entering has their ID.

A: Face, ID card
C: Picture on ID card, guard's knowledge of ID card
f: Take picture and produce card, train guard
L: Does the face match the ID card, does the ID card appear valid?
s: Design non-forgeable card

3.2 Location- and time-specific code (6 minutes, 4 points)

Doors have an electronic lock with a code that must be entered, the code consists of a 4 digit randomly-chosen prefix (changed every three months), followed by the 3 digit telephone area code where the door is located. People with access to all locations are told the above algorithm, people with access to only a single location are told only the seven-digit number for their location.

A: 7 digit code or 4 digit code & local area code & algorithm
C: 7 digit code for the particular location
f: Take 4 digit code and append local area code
L: Does the code entered match the appropriate code for the lock?
s: Randomly select 4 digit code

3.3 Card-swipe and ID (6 minutes, 4 points)

Each person has an ID card with their Social Security number encoded on the card (using a one-way hash, e.g. MD5). To enter, they must swipe their card and correctly enter their social security number. The lock/card reader checks to make sure the number matches the card.

A: Card, Social Security Number (SSN)
C: Hashed SSN
f: Hash SSN and write to card
L: Hash entered code and compare with value on card
s: Apply for new SSN

Scoring: 1 point per reasonable answer for each of the five criteria, up to 4 points per question.

3.4 Problems (8 minutes, 6 points)

For ONE of the above,

1. describe a problem/attack that would allow an unauthorized person to successfully authenticate and gain access to the secure area,

   3.3: Attacker could make their own card by hashing their own SSN.

   Scoring: 1 to 2 points for good attack.

2. give a modification of the method that would prevent the described attack, and

   Rather than hash, use encryption with a key known only to the card-reader and card-generator.

   Scoring: 1 point for reasonable solution, 1 point if it actually prevents attack.

3. describe a drawback of your modification (a situation where the original method would have an advantage of your method.)

   Card-reader must resit tampering to get key. Also key-exchange challenges.

   Scoring: 1 point for drawback, 1 point if it is something that didn't exist with the original approach.

4 Intrusion Detection (15 minutes, 9 points)

The SecureExpresso Corporation has been working with the Purdue University computer security class members for several years now to assess the cryptographic protocols they purchase. The executives of the company have now decided to invest in an Intrusion Detection System (IDS) and they want your advice. The purpose of the IDS is to determine whether a competitor, the FreeExpresso Corp, is reading their internal corporate documents containing secret recipes for mocha-brewing.

The SecureExpresso internal network, which is an Ethernet-connected network of Linux computers, is housed in a single building. The mocha-brewing documents are stored on individual host computers within the SecureExpresso network. Computers on this network are primarily accessed by employees who work in the building housing them, although a few employees occasionally log on from the many SecureExpresso kiosks located throughout the nation from time to time. Individual computers run mail, ftp, telnet/login, and similar network services.

The SecureExpresso executives have devised a preliminary list of questions based on the concerns raised by their internal IT department but they want your input before they speak with the various IDS vendors. Give a short answer for each question, describing what about their environment makes your answer the most appropriate solution.

The key is to show you understand the types of Intrusion Detection Systems and their advantages/disadvantages - there isn't necessarily a right or wrong answer for each.

4.1 Do you recommend an anomaly-based IDS or a misuse-based IDS? (4 minutes, 3 points)

Misuse-based. FreeExpresso could succeed with a very short intrusion into the system. This may be insignificant statistically, and not show up as an intrusion in an anomaly-based approach.

4.2 Do you think we should place our IDS sensors using a central or a distributed strategy? (4 minutes, 3 points)

Central. The key documents are in the internal network. This could have a single gateway, and it would be sufficient to place the IDS at that gateway.

4.3 Should we be concerned about false positives or false negatives or both? (4 minutes, 3 points)

Both - but primarily false positives. If the system has too many false positives, they will be ignored. If FreeExpresso makes several attempts, catching only one will be sufficient to take legal or public relations action against FreeExpresso, thus deterring future attempts.

Scoring: 1 point for showing understanding of difference, 1 point for showing how it relates to the system in question, 1 point for reasonable justification of your choice.

5 Audit (15 minutes, 9 points)

Logging mechanisms, just like everything else in a computer system, are subject to failure. The Common Criteria recognizes this, one of the functional components dealing with audit states:

> FAU_STG.3.1 The TSF shall take [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].

Give three examples of possible "actions to be taken in case of possible audit storage failure", i.e., what you might want done when the audit trail exceeds the size limitation. For each, describe the action, and other characteristics of the system (assumptions you might make) that would make the action appropriate (i.e., the action would be unlikely to cause a security violation to go undetected.)

Discard old log values. Acceptable if old values already audited, and a new audit can proceed without using old values.

Selectively discard old values. Need automated audit mechanism that can perform analysis to determine which values are no longer needed for audit, or which have lowest value.

Stop operation until an audit shows no violations and old data is not needed to detect future violations. Only works if integrity/confidentiality MUCH more important than availability.

Scoring: 1 each for showing understanding of what is important about auditing, 1 for a reasonable action, 1 for what you need to know about system to ensure action doesn't violate something important.

6 Risk Analysis (40 minutes, 20 points)

You have been asked to provide advise on how a company can manage security on their customer information database. The database maintains information on customer sales contacts, orders, and pricing options. Their goal is a database that will be available to their (traveling) sales people via the internet, to customers for reviewing orders and payment, and within the company for financial reporting, order forecasting, etc. As such, the system contains confidential information, information where integrity is critical, and other security issues.

Your task is to identify threats, and to choose approaches to reduce the risk of vulnerabilities to those threats.

Sample threats/mitigation techniques:

Threat

Insider obtaining confidential data
Malicious insider modifying data
Network-based theft of information
Customers obtaining elevated authority to modify payment information
Competitors stealing pricing data

Mitigation technique

Red-team testing
Firewalls and Intrusion detection
Access control modeling (e.g., access control matrix, schematic protection model)
Formal security evaluation

As an example, one threat might be a salesperson putting confidential customer information into the database, and another salesperson working with a competing customer obtaining that information and providing it to the customer. A techniques to address this threat would be to evaluate access control using the Chinese Wall model.

6.1 Identify threats and techniques to mitigate them (15 minutes, 8 points)

Write down four such threat / mitigation technique pairs. You must use two threats and two mitigation techniques from the lists above, and come up with two of each that aren't on the lists. Note that the mitigation techniques given above are not necessarily appropriate for the threats in the lists – this is part of the reason you have flexibility to come up with your own.

You are not required to explain why the techniques addresses the threat, or why the threat matters to the particular application, but if it isn't obvious to me an explanation may help.

Insider obtaining confidential data—Access control modeling

Competitors stealing pricing data—Authentication mechanisms

Customers learning data used to set prices—Mandatory access control

Network-based Denial of Service—Firewalls and Intrusion Detection

Scoring: 1 point for each threat / techniques you come up with (up to 4), -1 each for failing to use the provided ones, 1 point for each reasonable pairing.

6.2 Explain one of the above (22 minutes, 12 points)

You need to describe your recommendations to the Chief Information Officer of the company. For one of your answers to part 6.1, or for my "salesperson disclosing confidential customer / Chinese Wall model" example, provide a short writeup for the CIO. This should cover:

1. What the threat is,
2. A brief description of the mitigation techniques,
3. How you would apply the technique, and
4. How the techniques would protect against vulnerabilities to the threat.

CIOs are busy people, so you will be graded both on your ability to answer these questions and on the brevity/conciseness of your answer.

To get the best possible solutions to their problems, some of your customers are willing to share trade secrets with your sales force under non-disclosure agreements. There is a threat that an unethical salesperson may provide such data from one customer to a competing customer, either to help make a sale or with promise of other reward such as a job offer from the customer.

The Chinese Wall security model supports access control that would prevent a salesperson from accessing data of a company that competes with their customer. Customers would be grouped as "competitors", a salesperson who writes to one customer record in a group would lose access to other customers in that group. Financial analysis would not write to customer records (since they don't record visits/sales), so the would be able to read all data.

While it would still be possible for a salesperson to see competitors' data before working with a customer, incentives for unethical behavior are unlikely to arise before contact has been established. Once a relationship with a customer is formed, access to competitors' data would be denied.

Scoring: Up to 2 points for identifying threat, 3 for description of the mitigation technique, 2 for how you would apply the techniques, 3 for how it prevents vulnerabilities to the threat, 2 for conciseness/brevity/clarity of writeup.