6.857 Computer and Network Security September 05, 2002

Lecture Notes 1 : Introduction

Lecturer: Ron Rivest *Scribe: Fu/Shelat*

[These notes were originally written in Fall 2001.]

Change your password!

1 Administrivia

There are one and a half (1.5) teaching assistants for this course. As a result, you might consider flipping a two-thirds/one-thirds biased coin when choosing which teaching assistant to direct your question. You might also just use the `6.857-staff@mit.edu` email list.

2 Overview

In security, theory and practice come together very nicely. Theoretical algorithms are often incorporated into real-world applications quickly, and conversely, theoretical attacks against a system are quickly implemented (e.g., WEP).

As a result, one good quality of this course is that you can pickup a newspaper and find no dearth of important, unsolved security problems. In today's news, there are half a dozen term paper projects. Here are some of the articles appearing recently:

2.1 Payment systems

1. Paypal allows one to use the Internet to transfer money. In this article, Paypal describes one of their largest problems. They handle approximately 20,000 new sign-ups per day. The customer service requirements to process that many new accounts and verify that each credit card account is legitimate are overwhelming their model.
2. The US Government is launching a tax payment service over the Internet. This schemes requires prior account setup in order to tap into a bank account. What are the security issues and how does this scheme compare with Paypal in terms of user confidence?

2.2 Basic security, confidentiality, privacy

3. Echelon is a global spy network that monitors phone calls, faxes, IP traffic and countless other communication mediums. Europe has concluded that this system exists and claims that it is

[0] May be freely reproduced for educational or personal use.

led by USA. “Europe should setup encryption system to guard against this.” The former CIA director admits to the existence of Echelon and claims that it is used to intercept commercial communication only when fraud and bribery is being investigated.

4. Cookies. Sample Earthlink ads appeared on the front page of today’s New York Times. A photo showed a bag of free chocolate chip cookies labeled, “Do you know where your cookies came from?” Cookies can enable detailed tracking of Internet users. How do we build in encryption to protect privacy? ZeroKnowledge markets the Freedom system for this. [`http://www.freedom.net/`]

5. Law or privacy. Are there technological solutions to privacy problems or can law serve as a better alternative? Laws can stifle technology. Maybe you will develop an opinion after this course.

2.3 Sale of information goods on the Internet

6. Yahoo E-Books. Four publishers agreed to sell e-books on Yahoo. Selling digital content to users poses an interesting problem. How should a publisher conduct the transaction? In particular, the adversary in this case is not a third party, but rather the purchaser herself. Can one redistribute the e-book for free after buying it? Security is usually much easier when a third party is the adversary.

7. Disney/NewsCorp will sell video on demand over cable and the Internet. Their service will allow playback on televisions or computers that are equipped with special hardware. Napster shook the music industry; could the same thing happen to the video industry?

2.4 Controlled distributions

8. French court vs. Yahoo. Yahoo had auctions of Nazi memorabilia. A French count ruled that Yahoo cannot make available any of the Nazi memorabilia to French citizens since that would violate a French law prohibiting the sale of Nazi merchandise. How can Yahoo abide this ruling without completely censoring the entire service for all users? Which court has jurisdiction over Yahoo. If you worry about privacy, you might want to hide your identity, but if Yahoo abides by French law, it would need to identify each user to determine if that user is from France.
   Q: What if someone from France orders Nazi goods and sends them to Spain?
   A: There are services that attempt to identify where in the world you are coming from. Such services can do a decent job if one does not purposefully hide oneself. However, these things don’t always work. For instance, the citizenship of a client remains unknown.

9. Kermit the frog is trying to boost awareness of the V-Chip, targeted for parents to censor what their kids can watch. That is, if parents can figure out how to use the V-Chip without the kids’ help....

10. Microsoft XP wants to thwart piracy. The software tries to make bootleg copies self-destruct in 30 days. Microsoft’s hope is to use “product activation” to keep that freshly installed version running. One must activate the software within 30 days or the software ceases to function. This controversial registration process only works once and only on one machine. Alternatively, one can use the phone to activate the software. The phone process is time-consuming and tedious (entering long numbers by hand).

What is the news? An XP crack appeared 7 weeks before the XP's public debut.

Someone posted a corporate version to a newsgroup. Apparently Microsoft has locked the front door and left the backdoor open. Microsoft claims that the cracking program does not work and might be filled with viruses. In addition, they state that they are not trying to solve piracy, but rather hope to reduce it. Coincidentally the release build number for XP is 2600, which is also the name of a group that was recently prosecuted for linking to the deCSS software.
Q: What will happen when someone cracks that security?
A: They have. Some people will get a pirated product for free. It's a tradeoff. Security is always a tradeoff. It gets in the way of both the good and bad guys.

Prof. Rivest asked who in the lecture has taken 6.046. Rivest himself encountered a piracy problem when an electronic version of the CLR Algorithms book appeared online in Switzerland. It was soon removed. "You all should go buy my book." :-)

11. Images/Web. Search engines cache content. The copyright holders of these images are not getting paid for their work and are therefore complaining about the caching by search engines.

2.5 Classic hacking

Hacking used to refer to the good old hacker. Nowadays the popular press has vilified the term.

12. Hacking is cracking. A man was jailed for hacking massive computers. A 21-year-old man was sentenced for breaking into two NASA computers. In his plea bargain, he admitted to stealing long distance and using computers to alter the effects of the MTV movie awards[1]. He installed a sniffer at NASA to collect passwords from universities. Authorities found 76,000 passwords on his computer. He used John the ripper, a popular password cracking tool.

13. Setting out snares for hackers. Honeypots are little machines that attract maundering intruders. In a non-profit honeypot project, Windows 98 was found to be compromised 5 times in 4 days. One computer was port scanned 17 times a day. The default installation of a Redhat 6.2 server was compromised within 72 hours. Sixty to eighty percent of crackers break in for bragging rights, 20 percent for financial gain.

14. Worm sequel plays only in Europe. A more destructive version of the Magister virus hit Europe. This virus, spread as an email attachment named "readme.exe." Email-infested viruses are growing in popularity in part due to the relative ease with which one may modify a previously released virus. The Magister virus overwrites hard drives and system files, rendering a computer useless. It also disables the zonealarm personal firewall.

Two years ago, 6.857 allocated 6–7 lectures on classic computer security and dove into crypto oriented stuff, electronic payments, key establishment, voting, and quantum crypto.

Q: What about Dmitry Sklyarov?
A: Sklyarov broke a copy protection scheme used in Adobe e-books. Elmsoft in Russia wrote a program to do this which was perfectly legal in Russia. When Sklyarov came to the US to present a paper at DEFCON, the FBI arrested him for violating the Digital Millennium Copyright Act.

[1] Does anyone else remember the "Hank the Angry Drunken Dwarf" episode from People Magazine? :-)

Maybe you'll get a homework assignment that you will not be able to turn in because of the DMCA. You will all gets A's on this assignment as a result.
It is now illegal not to just circumvent, but to provide a tool that could circumvent copy protection.

3 Principles of Security

There are a number of quintessential security principles to keep in mind this semester.

1. Do not aim for perfection. It is usually impossible to design a perfect system. Instead, security is like building fences. We must determine how high we can build them, but it is impossible to make them infinitely high. In particular, crypto works when it is no longer the weakest link. As Adi Shamir states, "There are no secure systems, only degrees of insecurity."
2. Secure systems can be expensive. Careful code reviews are costly, as are hand-held tokens for logins, and shields around CRTs to prevent Tempest attacks. "To halve the insecurity, double the cost" – Adi Shamir.
3. Principle of least privilege. Do not give someone more power than they need for their job. In certain extreme cases, it is prudent to make two users cooperate in order to complete a certain task (e.g., two keys are required to launch a missile).
4. Minimize the number of trusted components. Identify which components of a system require assumptions. For example, we might assume that no one can highjack my telephone line.
5. Keep it simple. This is probably the most important principle. Security is hard, and complexity leads to more things that can go wrong.
6. Be skeptical. Force people to justify their security declarations.
7. Be paranoid. Identify all adversaries and determine their motives. This is street smarts for computers. Robert Morris Sr., a former National Security Agency scientist, says "Never underestimate the amount of time and effort that someone will put into breaking your system."
8. User awareness. People are often the weakest link because they do not understand their role in the security of a system. Therefore, educating users is important.
9. Personnel policies. Insiders are a large threat.
10. Defense in depth. Belt and Suspenders.
11. Do not rely entirely on security through obscurity. Keeping code secret is not a good idea, because eventually, the mechanism will become public. We should evaluate the system assuming the system details are available, except perhaps a small secret key.
12. Crypto allows interesting and useful applications. Adi Shamir quips that "crypto is bypassed, not broken."
13. Ease of use is important when people are involved.
14. Privacy is important. What level of identification is really needed for an application.

4 Voting

Florida has raised the issue of how voting works. Prof Rivest participated in a joint Caltech and MIT initiative on evaluating the voting problem. They are in the middle of studying it, and produced a report.

Consider voting from home or Internet voting. This is a hot topic that makes many people nervous about possible security problems. Rivest has supervised a few master's theses on the subject.

Lets brainstorm about the requirements of voting.

1. Ease of use. The voting system needs to be available and accessible. A student from Broward county in Florida made a comment about how the average voting age in his county was 66. This particular demographic has special requirements in terms of ballot design and accessibility. If you are blind, you might be able to find ballots printed in braille. Language is another issue.
2. The voting system should be understandable. Not only what they need to do to vote, but also what happens to the vote in order to establish voter trust. The system obviously must be trustworthy.
3. A vote cast is a vote counted.
4. No votes fraudulently added or deleted.
5. The privacy of votes must be sacred in order to protect against coercion and vote buying. Note, however, that both in England and in Arkansas, votes are not private. It is possible for law enforcement to discover how an individual voted. This property is both the most important one, and also the most difficult to deal with. In particular, this property distinguishes a voting system from a credit card system which is allowed to maintain detailed auditing. This implies that at some point in the process, the name of the votes must be removed from the vote itself. Maintaining legitimacy after this point is difficult.
6. Only registered voters are permitted to vote and they may vote at most once. Note, some states like North Dakota do not require registration beforehand.
7. Low cost. Since local governments are responsible for the cost of their own voting system, it is important that the total cost of the system be minimal.

Question: user authentication. Some poll stations do not check who you are. Prof. Rivest's son did not have to show identification in order to vote.

Michael Shamos is an attorney and adjunct faculty member in the School of Computer Science at Carnegie-Mellon University. He has been a statutory examiner of electronic voting systems for Pennsylvania since 1980 and serves as the designee of the Attorney General of Texas at electronic voting examinations in that state. Shamos outlines six commandments for voting in his survey paper entitled "Electronic Voting - Evaluating the Threat." The six commandments are summarized below. The full paper is accessible at `http://www.cpsr.org/conferences/cfp93/shamos.html`.

1. Thou shalt keep each voter's choices an inviolable secret.

2. Thou shalt allow each eligible voter to vote only once, and only for those offices for which she is authorized to cast a vote [2].
3. Thou shalt not permit tampering with thy voting system, nor the exchange of gold for votes.
4. Thou shalt report all votes accurately.
5. Thy voting system shall remain operable throughout each election.
6. Thou shalt keep an audit trail to detect sins against Commandments II-IV, but thy audit trail shall not violate Commandment I.