08.26.12

CS261 Scribe Notes

Administration
40% Project
30% Homework
15% Scribe Notes
15% Summaries + class discussion

Other Classes
CS261N – Network Security
CS294 – Internet Freedom
CS276 – Cryptographic Theory

Discussion: Is online banking secure?

Better question: Is online banking secure enough?

- We need to weigh the benefits and costs
- Depends on which bank system and who we are looking at

Answer: It is definitely secure enough for the average customer in the U.S.

- *Terms and Conditions:* Unauthorized transactions will be covered for personal accounts
- Average customer is safe and fraud is not really a risk for them
- It is secure enough. But the original question is, is it secure?

Technical Security vs. Personal Account Safety

- Personal Accounts: The bank will take responsibility and they are safe
- Business Accounts: The bank has no accountability or responsibility to protect them from fraud.
- There are costs, so it's necessary to look at the technical security of the system

Attacks
Man-in-the-middle

- Compromise my password (and more) through wifi connection
- *Question:* Is it possible for the bank to secure against connection security?
- *Example:* ***SSL Strip***
  - Attacker positions self as man-in-the-middle and presents an HTTP connection
  - No browser certificate warning, no green bar at the top
  - attacker -- bank = SSL Connection
  - attacker -- user = unencrypted
  - *Description:* Attacker presents a login page to the user, who then gives their username and password. The attacker feeds this into the bank system through an https connection. The attacker can control whatever the user sees and has access to their entire account on the other side.
  - Spent a lot of time focusing on this attack

    - Successful for everyday people, but we should be looking at the more popular attacks!

Phishing and/or Malware

- Infect the victim's computer/machine
- Information is encrypted over the network, but the attacker has direct access to the machine where the info is unencrypted
- This attack is more prevalent
- We were focusing on one specific attack the entire time

Key Takeaways:

What do we mean by Security?

- not black and white
- dependent on context and environment
- end-user behavior
- risk-management

How do we measure the security of a system?

1. Start with a security analysis of the system
   ex: no unauthorized transactions or no irreversible unauthorized transactions
2. Analyze the specific threats, risks, attacks or vulnerabilities
   Note: Important to focus on the correct attacks
   ex: man-in-the-middle
3. What potential or existing defenses are there?

Discussion: Which is more secure: Mac or PC?

Mac:

- relatively newer and less popular which means less attacks
- users are more complacent, which might prove to be an issue later

PC:

- have developed defenses for many attacks and have been doing it for years
- the number of attacks is far greater!

What is a good measurement of Security?

- Number of attacks
- Severity of attacks (weighted)
- Ratio of successful attacks to actual targeted attacks
- Assess vulnerabilities and the severity of them
- Develop attacks of equal caliber for both
- Number of distinct exploits/methods
- Measure the time taken to fix the machine after the attack

User studies! – They are ideal, but extremely expensive. So we have to make tradeoffs in research. Unfortunately, there are not many user studies in security research due to the high costs.

Research: consists of a hypothesis and the best evaluation with a limited amount of resources.

Game Theory Analysis

90 PCs and 10 Macs

Simple Model:

Assumptions

1. There is no cost if an attacker fails by attacking a defended machine
2. Defenses are 100% effective: if a machine has a defense, it will always stop the attack
3. Attacks are 100% effective: if a machine does not have a defense, the attack will be successful

Defender

		PC	MAC
Attacker	PC	0	90
	MAC	10	0

Optimal Strategy

Attacker: PC 90%
Reasoning: mixed attacks, otherwise both stalemate at 0

Tweak #1: Attacks aren't perfect

Assumptions

1. Attacks are 50% effective: if an attacker targets an undefended machine, it will be successful half the time

Defender

		PC	MAC
Attacker	PC	0	45
	MAC	5	0

Optimal Strategy

Attacker: PC 90%
Reasoning: Payoff is scaled by a factor, so strategy is the same

Tweak #2: Attacks aren't equally effective

Assumptions

1. Attacks on Macs are 50% effective, attacks on PCs are 100% effective (undefended machines only)
   Note: Macs are more secure out-of-the-box

		Defender	
		PC	MAC
Attacker	PC	0	90
	MAC	5	0

Optimal Strategy

Attacker: PC 95%

Reasoning: Payoff for successfully attacking a Mac is halved

<u>Tweak #3:</u> Attacks aren't equally effective

Assumptions

1. Attacks on PCs are 50% effective, attacks on Macs are 100% effective (undefended machines only)
   Note: PCs are more secure out-of-the-box

		Defender	
		PC	MAC
Attacker	PC	0	45
	MAC	10	0

Optimal Strategy

Attacker: PC 80%

Reasoning: Payoff for successfully attacking a PC is halved

Note: Huge difference in "out-of-the-box" security required in order to have an effect large enough to matter. Market share has a significant effect

<u>Tweak #4:</u> Defense are not perfect

Assumptions

1. Defending a machine is only 50% effective

		Defender	
		PC	MAC
Attacker	PC	45	90
	MAC	10	5

Optimal Strategy

Attacker: PC 100%

Reasoning: Payoff for attacking a PC (defended or not) is higher than for Mac

Key Takeaways:

- hard to measure security
- figuring out which experiments accurately measure is difficult
- Security analysis
  - What's the threat model?
  - What attacks are there? Think like an attacker
  - What defenses are there?