Introduction to Computer Security

- Why do we need computer security?
- What are our goals and what threatens them?

Why Is Security Necessary?

- Because people aren't always nice
- Because a lot of money is handled by computers
- Because a lot of important information is handled by computers
- Because our society is increasingly dependent on correct operation of computers

History of the Security Problem

- In the beginning, there was no computer security problem
- Later, there was a problem, but nobody cared
- Now, there's a big problem and people care
  - Only a matter of time before a real disaster
  - At least one company went out of business due to a DDoS attack
  - Identity theft and phishing claim vast number of victims
  - Stuxnet seriously damaged Iran's nuclear capability
  - Video showed cyberattack causing an electric transformer to fail
  - There's an underground business in cyber thievery
  - Increased industry spending on cybersecurity

Some Examples of Large Scale Security Problems

- Modern malicious code attacks
- Distributed denial of service attacks
- Vulnerabilities in commonly used systems

Malicious Code Attacks

- Multiple new viruses, worms, botnets, and Trojan horses appear every week
- Recent estimate of $10 billion annual damages from botnets
- Stuxnet worm targeted at nuclear facilities
  - Unspecified amounts of damage done to Iran's nuclear program
- IM and smartphone attacks are popular

Distributed Denial of Service Attacks

- Use large number of compromised machines to attack one target
  - By exploiting vulnerabilities
  - Or just generating lots of traffic
- Very common today
- A favored tool for hacktivists
  - Recent large DDoS attacks on Ello and others
- In general form, an extremely hard problem

Vulnerabilities in Commonly Used Systems

- 802.11 WEP is fatally flawed
- Recently, critical vulnerabilities in iOS, Windows, Linux kernel, glibc, Oracle Java implementation
- Many popular applications have vulnerabilities
  - Recent vulnerabilities in Adobe Acrobat, Android OS, Internet Explorer, Microsoft Office, VMWare vCenter Server, Adobe Flash, Oracle Database, etc.
- Many security systems have vulnerabilities
  - OpenSSL and Comodo Internet Security recently

Electronic Commerce Attacks

- As Willie Sutton said when asked why he robbed banks,
  - "Because that's where the money is"
- Increasingly, the money is on the Internet
- Criminals have followed
- Common problems:
  - Credit card number theft (often via phishing)
  - Identity theft (phishing, again, is a common method)
  - Loss of valuable data from laptop theft
  - Manipulation of e-commerce sites
  - Extortion via DDoS attacks or threatened release of confidential data
- 2010's Sony data breach estimated to cost the company $170 million

Another Form of Cyberattack

- Click fraud
- Based on popular pay-per-click model of Internet advertising
- Two common forms:
  - Rivals make you pay for "false clicks"
  - Profit sharers "steal" or generator bogus clicks to drive up profits

Some Recent Statistics

- 2015 Verizon report found over 2000 data breaches from just 70 organizations
  - In 60% of cases, attackers broke in within minutes
  - And only 20% of the organizations found the breach within a few days
- FBI Cybercrime report for 2014 showed 260,000 reports
  - And losses of over $800,000,000

Cyberwarfare

- Nation states have developed capabilities to use computer networks for such purposes
- DDoS attacks on Estonia and Georgia
  - Probably just hackers
- Some regard Stuxnet as real cyberwarfare
  - Pretty clear it was done by US
- Attacks on Ukrainian power grid
- Continuous cyberspying by many nations
- Vulnerabilities of critical infrastructure
  - The smart grid will only increase the danger

Something Else to Worry About

- Are some of the attempts to deal with cybersecurity damaging liberty?
- Does data mining for terrorists and criminals pose a threat to ordinary people?
  - The NSA is looking at a lot of stuff . . .
  - And they aren't the only ones
- Can I trust Facebook/Google/MySpace/Twitter/ whoever with my private information?
- Are we in danger of losing all privacy?

Why Aren't All Computer Systems Secure?

- Partly due to hard technical problems
- But also due to cost/benefit issues
- Security costs
- Security usually only pays off when there's trouble
- Many users perceive no personal threat to themselves
  - "I don't have anything valuable on my computer"
  - "I don't have any secrets and I don't care what the government/Google/my neighbor knows about me"
- Ignorance also plays a role
  - Increasing numbers of users are unsophisticated
  - Important that computer security professionals don't regard this ignorance as a character flaw
  - It's a fact of life we must deal with

Computer Security and History

- Much of our computer infrastructure is constrained by legacy issues
  - Core Internet design
  - Popular programming languages
  - Commercial operating systems
- All developed before security was a concern
  - Generally with little or no attention to security

Retrofitting Security

- Since security not built into these systems, we try to add it later
- Retrofitting security is known to be a bad idea
- Much easier to design in from beginning
- Patching security problems has a pretty dismal history

Problems With Patching

- Usually done under pressure
  - So generally quick and dirty
- Tends to deal with obvious and immediate problem
  - Not with underlying cause
- Hard (sometimes impossible) to get patch to everyone
- Since it's not organic security, patches sometimes introduce new security problems

Speed Is Increasingly Killing Us

- Attacks are developed more quickly
  - Often easier to adapt attack than defense
- Malware spreads faster
  - Slammer got 75,000 nodes in 30 minutes
- More attackers generating more attacks
  - US DoD computers targeted at least 43,000 times in first half of 2009
  - US military doctrine says cyber attack could be an act of war

Some Important Definitions

- Security
- Protection
- Vulnerabilities
- Exploits
- Trust

Security and Protection

- *Security* is a policy
  - E.g., “no unauthorized user may access this file”
- *Protection* is a mechanism
  - E.g., “the system checks user identity against access permissions”
- Protection mechanisms implement security policies

Vulnerabilities and Exploits

- A *vulnerability* is a weakness that can allow an attacker to cause problems
  - Not all vulnerabilities can cause all problems
  - Most vulnerabilities are never exploited
- An *exploit* is an actual incident of taking advantage of a vulnerability
  - Allowing attacker to do something bad on some particular machine
  - Term also refers to the code or methodology used to take advantage of a vulnerability

Trust

- An extremely important security concept
- You do certain things for those you trust
- You don’t do them for those you don’t
- Seems simple, but . . .

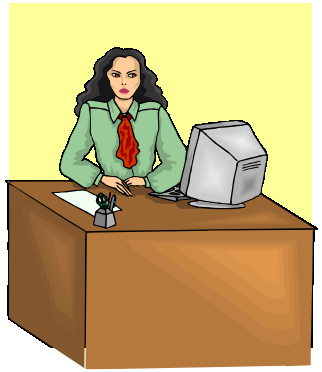
Problems With Trust

- How do you express trust?
- Why do you trust something?
- How can you be sure who you're dealing with?
- What if trust is situational?
- What if trust changes?

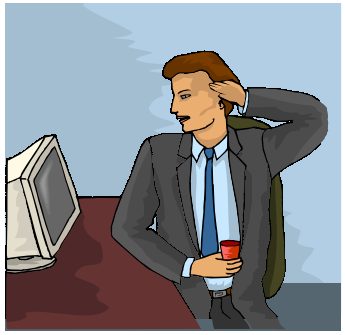
Trust Is Not a Theoretical Issue

- Most vulnerabilities that are actually exploited are based on trust problems
- Attackers exploit overly trusting elements of the computer
  - From the access control model to the actual human user
- Taking advantage of misplaced trust
- Such a ubiquitous problem that some aren't aware of its existence

Transitive Trust



I trust Alice

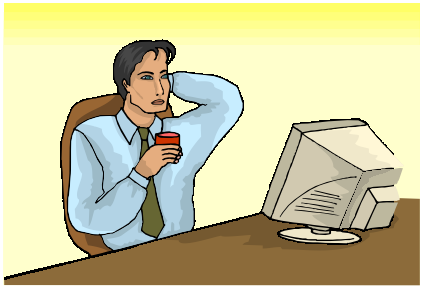


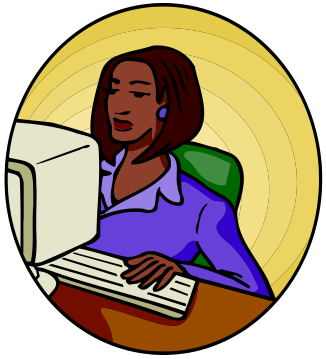
Alice trusts Bob

So do I trust Carol?

Should I?

Bob trusts David





David trusts Carol

Examples of Transitive Trust

- Trust systems in peer applications
- Chains of certificates
- But also less obvious things
  - Like a web server that calls a database
  - The database perhaps trusts the web server
  - But does the database necessarily trust the user who invoked the server?
  - Even if the web server trusts the user
- Programs that call programs that call programs are important cases of transitive trust