CSE 484 / CSE M 584 (Winter 2010)

Introduction (Continued)

Tadayoshi Kohno

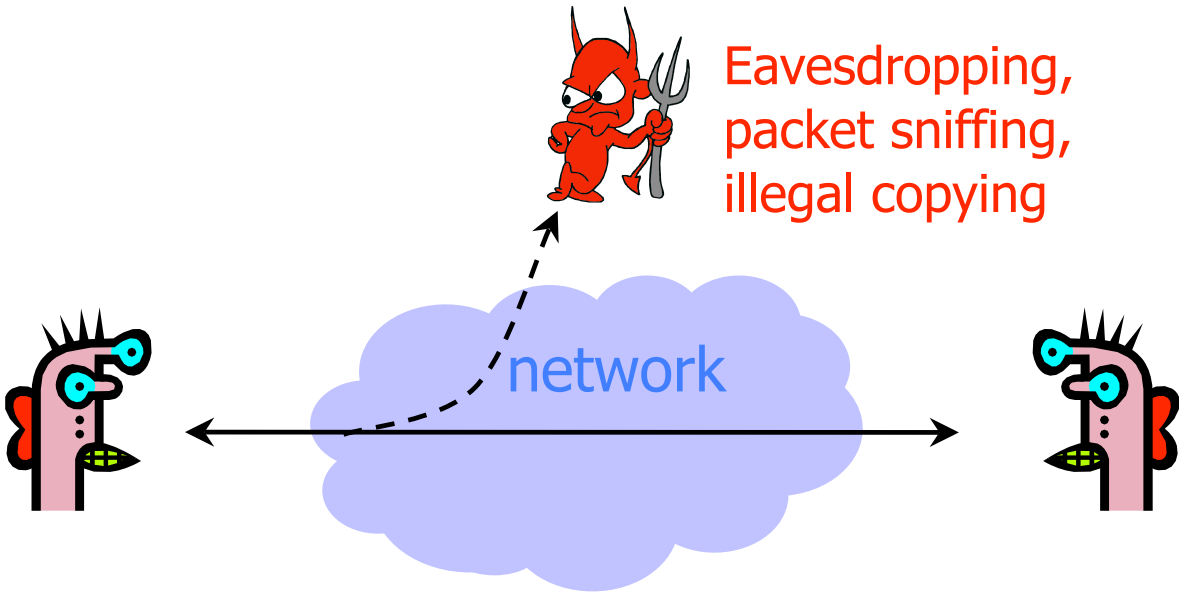
Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Goals for Today

- Principle goals of computer security
- Steps for analyzing a system (assets, threats, risk management)
- Effects of modularity and complexity
- Practice

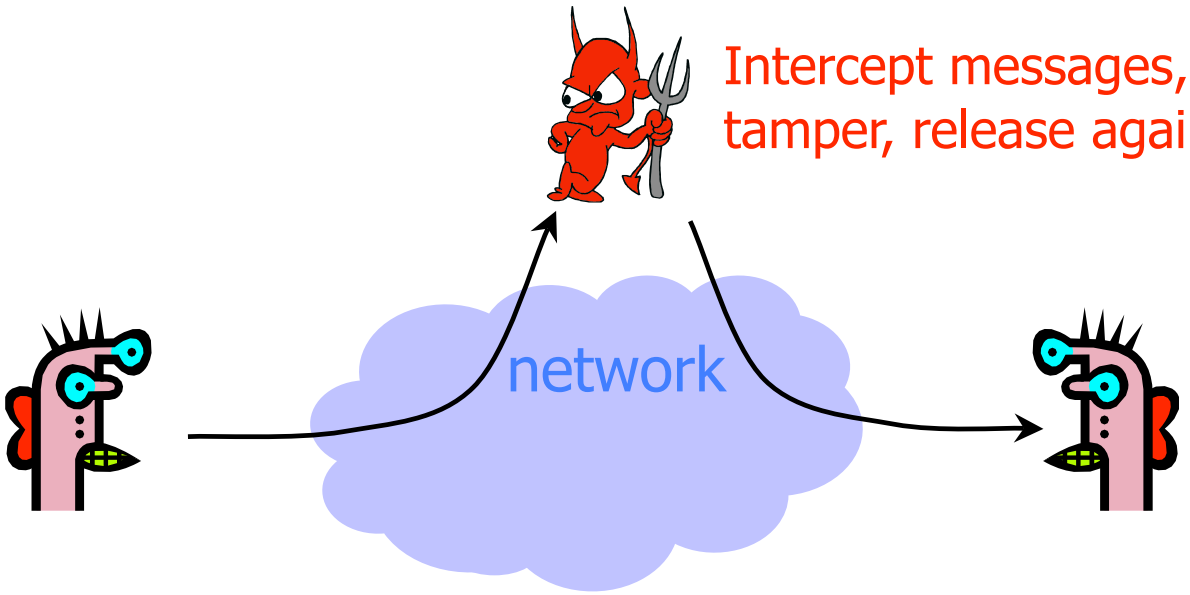
Confidentiality (Privacy)

- Confidentiality is concealment of information



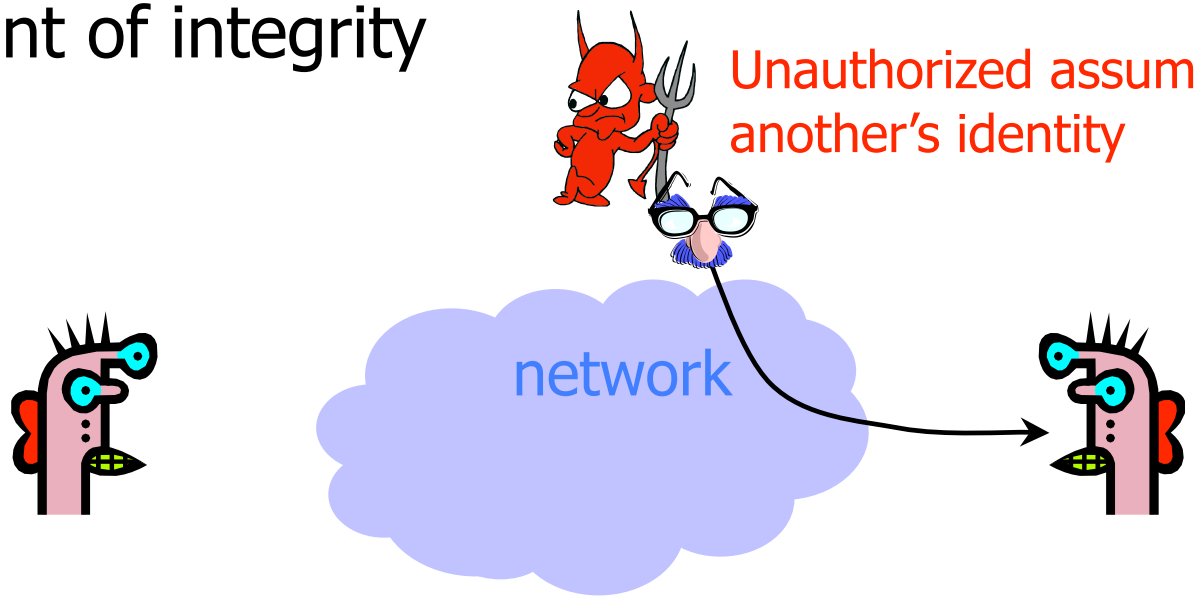
Integrity

- Integrity is prevention of unauthorized changes



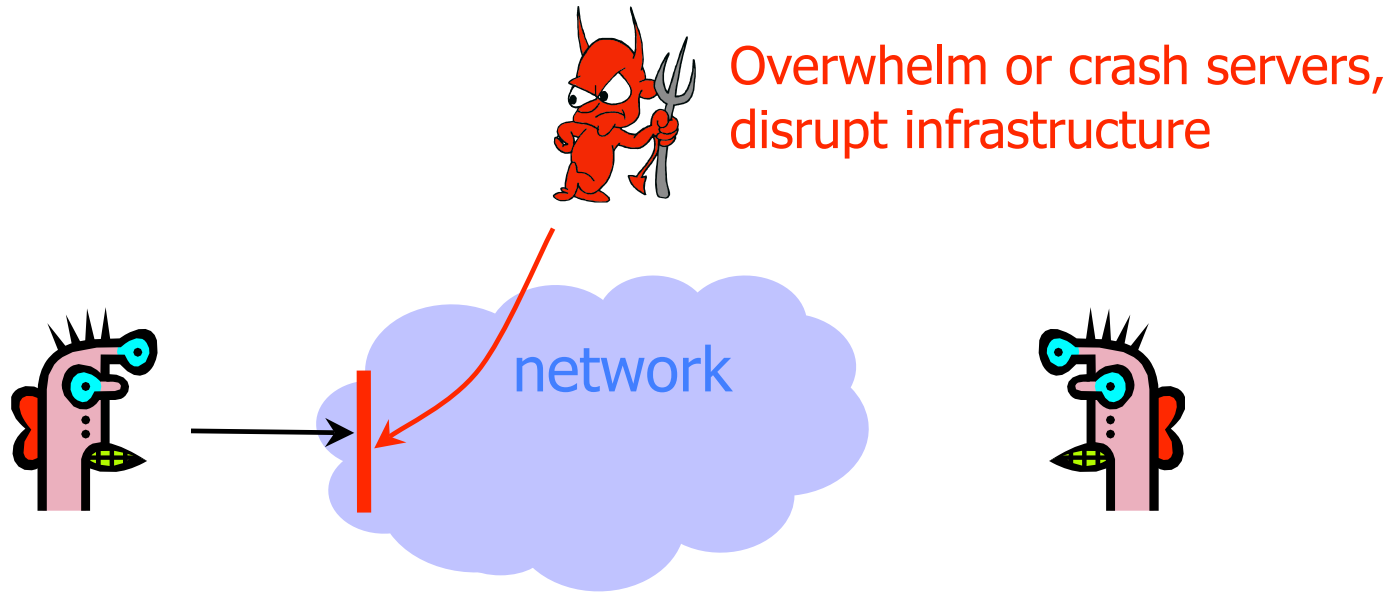
Authenticity

- Authenticity is identification and assurance of origin of information
- Variant of integrity



Availability

- Availability is ability to use information or resources desired



Whole-System is Critical

- Securing a system involves a whole-system view
  - Cryptography
  - Implementation
  - People
  - Physical security
  - Everything in between
- This is because "security is only as strong as the weakest link," and security can fail in many places
  - No reason to attack the strongest part of a system if you can walk right around it.
  - (Still important to strengthen more than the weakest link)

Analyzing the Security of a System

- First thing: Summarize the system as clearly and concisely as possible
  - Critical step. If you can't summarize the system clearly and concisely, how can you analyze it's security?
- Next steps:
  - Identify the assets: What do you wish to protect?
  - Identify the adversaries and threats
  - Identify vulnerabilities: Weaknesses in the system
  - Calculate the risks

Assets

- Need to know what you are protecting!
  - Hardware: Laptops, servers, routers, PDAs, phones, ...
  - Software: Applications, operating systems, database systems, source code, object code, ...
  - Data and information: Data for running and planning your business, design documents, data about your customers, data about your identity
  - Reputation, brand name
  - Responsiveness
- Assets should have an associated value (e.g., cost to replace hardware, cost to reputation, how important to business operation)

Adversaries

- National governments
- Terrorists
- Thieves
- Business competitors
- Your supplier
- Your consumer
- The New York Times
- Your family members (parents, children)
- Your friends
- Your ex-friends
- …

Threats

- Threats are actions by adversaries who try to exploit vulnerabilities to damage assets
  - Spoofing identities: Attacker pretends to be someone else
  - Tampering with data: Change outcome of election
  - Crash machines: Attacker makes voting machines unavailable on election day
  - Elevation of privilege: Regular voter becomes admin
- Specific threats depend on environmental conditions, enforcement mechanisms, etc
  - You must have a clear, simple, accurate understanding of how the system works!

Threats

- Several ways to classify threats
  - By damage done to the assets
    - Confidentiality, Integrity, Availability
  - By the source of attacks
    - (Type of) insider
    - (Type of) outsider
    - Local attacker
    - Remote attacker
    - Attacker resources
  - By the actions
    - Interception
    - Interruption
    - Modification
    - Fabrication

Vulnerabilities

- Weaknesses of a system that could be exploited to cause damage
  - Accounts with system privileges where the default password has not been changed (Diebold: 1111)
  - Programs with unnecessary privileges
  - Programs with known flaws
  - Known problems with cryptography
  - Weak firewall configurations that allow access to vulnerable services
  - ...
- Sources for vulnerability updates: CERT, SANS, Bugtraq, the news(?)

Risks Analyses: Lots of Options

Risk Exposure Risk Impact Probability

- Quantitative risk analysis
  - Example: Risk = Asset × Threat × Vulnerability
  - Monetary value to assets
  - Threats and vulnerabilities are probabilities
  - (Yes: Difficult to assign these costs and probabilities)
- Qualitative risk analysis
  - Assets: Critical, very important, important, not important
  - Vulnerabilities: Has to be fixed soon, should be fixed, fix if convenient
  - Threats: Very likely, likely, unlikely, very unlikely

Helpful Tables

Asset	Confidentiality	Integrity	Availability
Hardware			
Software			
Data			
People			
…			

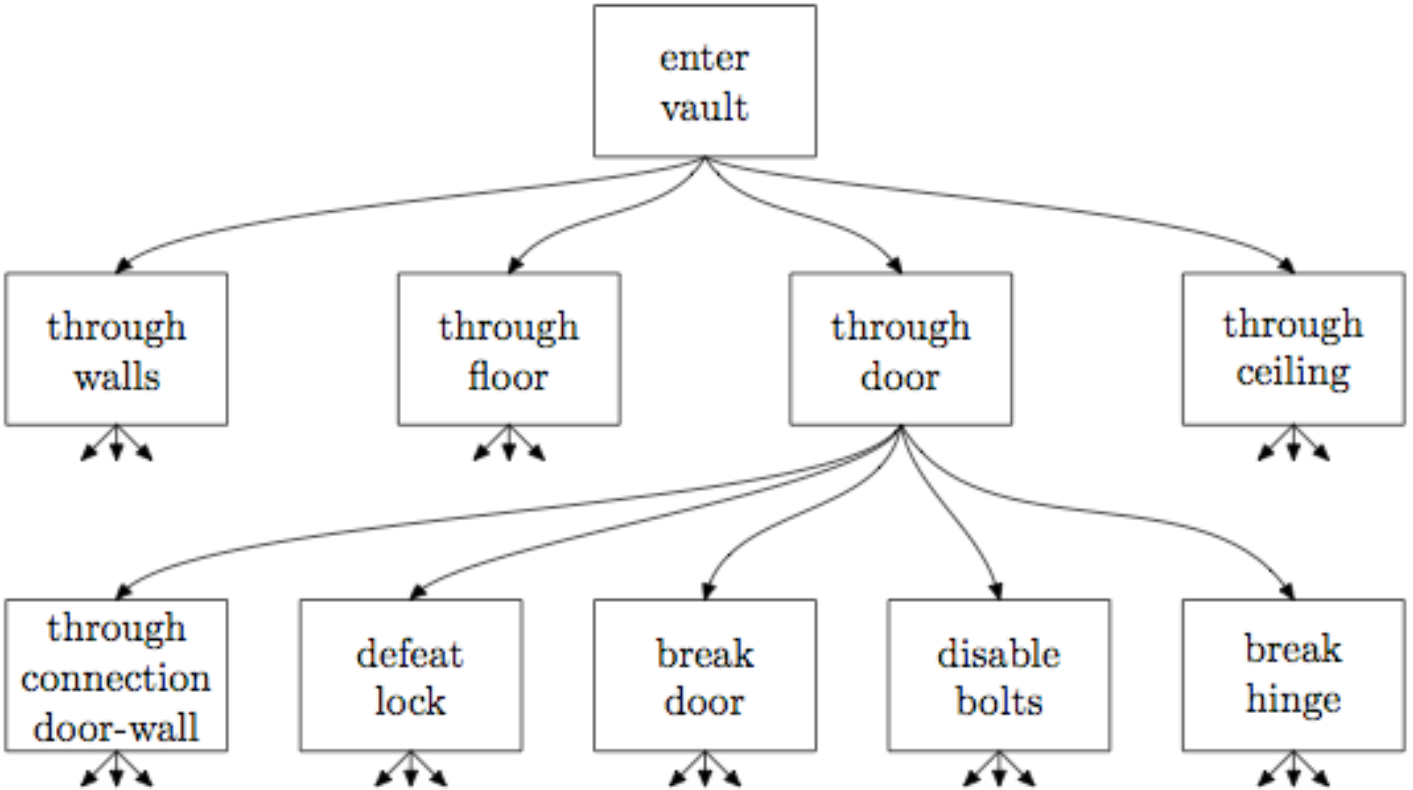
Helpful Tables

	Voter	Election official	...
Privacy of vote			
Integrity of vote			
Availability of voting system			
Confidence in election			
...			

Helpful Tables

	Create New Voter Cards	Decrypt voting record	...
Privacy of vote			
Integrity of vote			
Availability of voting system			
Confidence in election			
...			

Attack Trees



Security is Subtle

- Security attacks can be subtle
- Can't provably and accurately identify / quantify all risks, vulnerabilities, threats.
- So need to think careful!
  - And keep the whole system in mind
- Phishing one example
  - If attacker can trick user into entering private information, then no protection mechanism will help
  - (So research tries to focus on helping users not be tricked)

Many Desirable Security Properties

- Core
  - Confidentiality
  - Integrity / Authenticity
  - Availability
- Variants
  - Accountability and non-repudiation
  - Freshness
  - Access control
  - Privacy of collected information
  - ...

On Modularity and Complexity

- Modular design may increase vulnerability
  - Abstraction is difficult to achieve in security: what if the adversary operates below your level of abstraction?
- Modular design may increase security: small TCB
- Complexity may increase vulnerability

Bad News

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems may be poorly understood
  - Higher-level protocols make mistaken assumptions
- Implementations are buggy
  - Buffer overflows, XSS vulnerabilities, ...
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks
- No matter what technical mechanisms you have, people may circumvent them
  - Phishing, impersonation, write down passwords, ...
- Attackers may be very powerful
  - ISPs, governments, ...
    - –

Better News

- There are a lot of defense mechanisms
  - We'll study some, but by no means all, in this course
- It's important to understand their limitations
  - "If you think cryptography will solve your problem, then you don't understand cryptography… and you don't understand your problem" -- Bruce Schneier
  - Security is not a binary property
  - Many security holes are based on misunderstanding
- Security awareness and user "buy-in" help

Syllabus

- Thinking about security; the "big picture"
  - The hardest part: Getting the "security mindset"
- Software security (including buffer overflow attacks)
- Web security (including XSS attacks)
- Cryptography
- Network security
- Botnets and malware
- The users (including usability)
- Anonymity

Field broad. All parts interconnected, so we will "bounce" around in a methodical way

Forum

- Help you develop the "security mindset"
- Best way to learn a foreign language: move to that country and immerse yourself in the language.
- Same thing applies to "security thinking"
- Forum: opportunity to think about security on a regular basis -- outside of class
  - Current events
  - New product announcements
  - While doing regular, day-to-day activities?
    - When you pass a bank, do you start thinking about how you might break in?

Current Events

- Important for computer security practitioners (and all computer scientists) to be able to
  - Reflect on the broader context of technology
  - Guide future development of technology
  - Guide future policy
- For the course blog
  - Summarize current event
  - Discuss why event arose
  - Reflect on what could have been done prior to the event arising (to prevent, deter, or change consequences)
  - Describe broader issues surrounding current event (ethical, societal)
  - How should people respond to the event (policy makers, the public, companes, etc.)

Current Events

Your Rights Online: **Google Sets Censorship Precedent In India**

Posted b
from the

caeos wr

"New
Zeala
to mo
large
and r
shop
New
SIS)

December 17, 2009 6:48 AM PST

Predator drones hacked in Iraq operations

by Declan McCullagh

Font size | Print | E-mail | Share | 72 comments

141 retweet | Share 87

Iraqi insurgents have reportedly intercepted live video feeds from the U.S. military's **Predator drones** using a $25.95 Windows application that allows them to track the pilotless aircraft undetected.

Hackers working with Iraqi militants were able to determine which areas of the country were under surveillance by the U.S. military, **The Wall Street Journal reported** Thursday, adding that video feeds from drones in Afghanistan also appear to have been compromised.

Meanwhile, a senior Air Force officer said Wednesday that a wave of new surveillance aircraft, both manned and unmanned, were being deployed to Afghanistan to **bolster "eyes in the sky" protection** for the influx of American troops

The MQ-1 Predator.
(Credit: U.S. Air Force)

are weighing the harm of free speech against violence in their streets.'"

Security Reviews

- Summary of system
- Assets
- Adversaries and threats
- Potential weaknesses (OK to speculate, but make it clear that you are speculating)
- Potential defenses.
- Risks
- Conclusions.

Let's try thinking about security

- Integrated networks on 787s (let's assume that they are indeed integrated).
- Wireless Picture Frames: http://seattlewireless.net/~casey/?p=13.
- Smart phones
- Recall steps:
  - First thing: Summarize the system as clearly and concisely as possible
  - Identify the assets: What do you wish to protect?
  - Identify the adversaries and threats
  - Identify vulnerabilities: Weaknesses in the system
  - Calculate the risks (we'll do informally)