Introduction

CS642: Computer Security

Professor Ristenpart

http://www.cs.wisc.edu/~rist/

rist at cs dot wisc dot edu

Computer security:
understanding and improving the behavior of computing technologies in the presence of adversaries

Target/victim computing systems

Attackers

Security engineers

Computer systems:

- Operating systems
- Networks / Internet
- Web (2.0)
- Software applications
- iPhones
- Embedded systems
- …

We will not even attempt to be exhaustive

Security goals

- Confidentiality
  - data not leaked
  - encryption, access controls
- Integrity
  - data not modified
  - message integrity checks, access controls
- Authenticity
  - data comes from who we think it does
  - digital signatures, passwords
- Availability
  - services operating when needed
  - redundancy

2010: “Highly sophisticated and targeted attack”

2011:
“Advanced persistent threat”

2011:
Bad crypto = cracked PS3
PSN is down

Adversaries:

- “31337” script kiddies
- Criminals
- “hacktivists”
- Dissidents (if you are an oppressive regime)
- Nation states
- …

John “Captain Crunch” Draper and Joe “joybubbles” Englessia

Phreaking

Targets:
AT&T phone system

Escapades:
> Written up in Esquire
> 2600Hz Cap’n Crunch whistle
> Blue box

Read more:
http://en.wikipedia.org/wiki/John_Draper

Steve Jobs and Steve Wozniak

Phreaking

Targets:
AT&T phone system

Escapades:
> Built blue boxes before Apple
> Great sales pitch to Berkeley college students

Read more:
http://en.wikipedia.org/wiki/Phreaking

Kevin “Condor” Mitnik

Free LA bus rides, breaking into corporate systems

Made off with:

> 1 year prison, 3 years supervision
> Consulting career
> Book deal

Read more:

http://en.wikipedia.org/wiki/Kevin_Mitnick

Julian “Mendax” Assange

Hacker in early 90’s

Targets:
> Nortel
> USAF 7th Command
> Wikileaks

Made off with:
> Free stay at Ecuadorian embassy

Read more:
http://en.wikipedia.org/wiki/Julian_Paul_Assange

Albert “soupnazi” Gonzalez

Committed various electronic crimes while also a FBI/USSS informant

Targets:
Heartland Payment Systems, TJX, others

Made off with:
> 130,000,000 credit card numbers
> $2mil in cash
> 15-20 years in jail

Read more:
http://en.wikipedia.org/wiki/Albert_Gonzalez

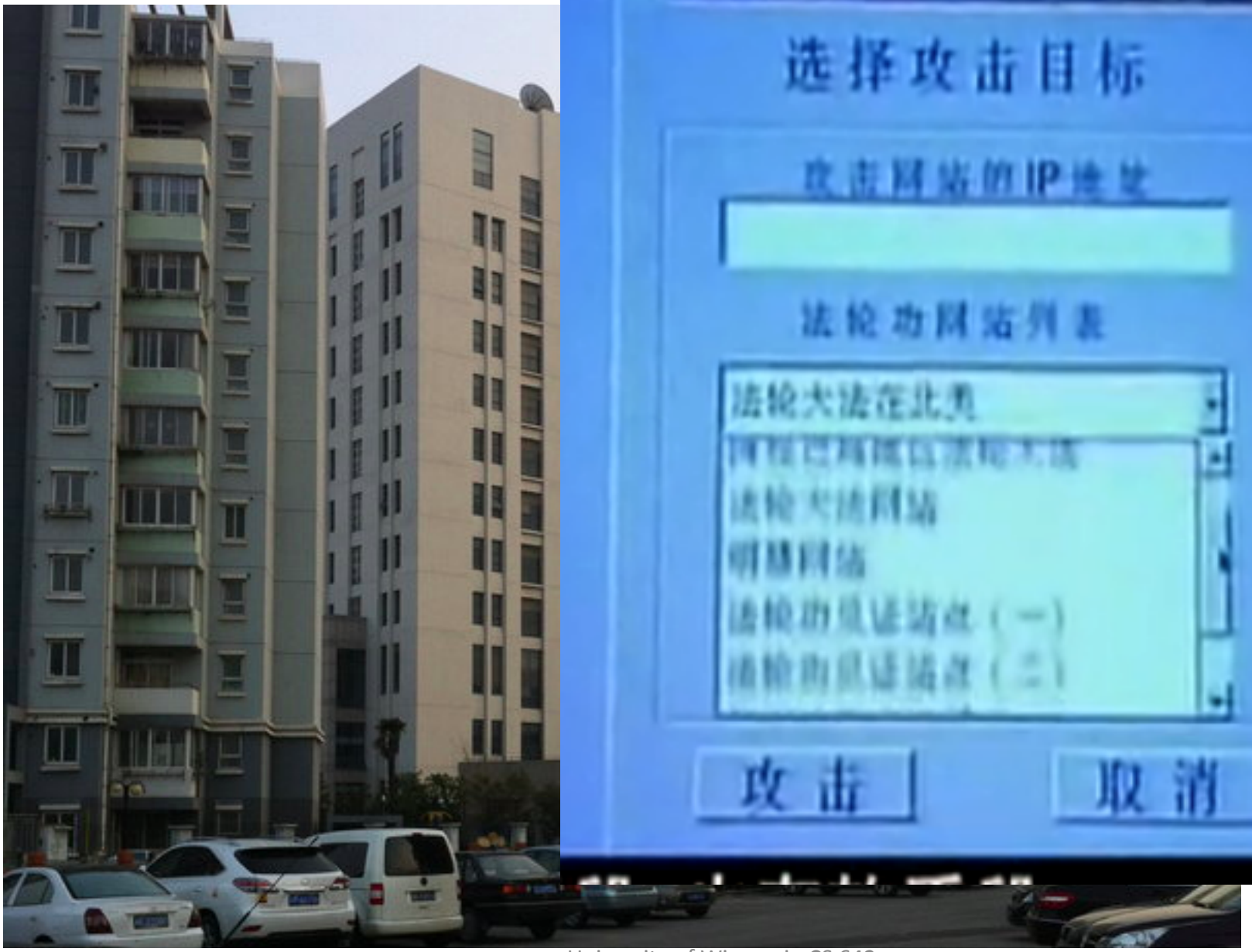
Russian Business Network

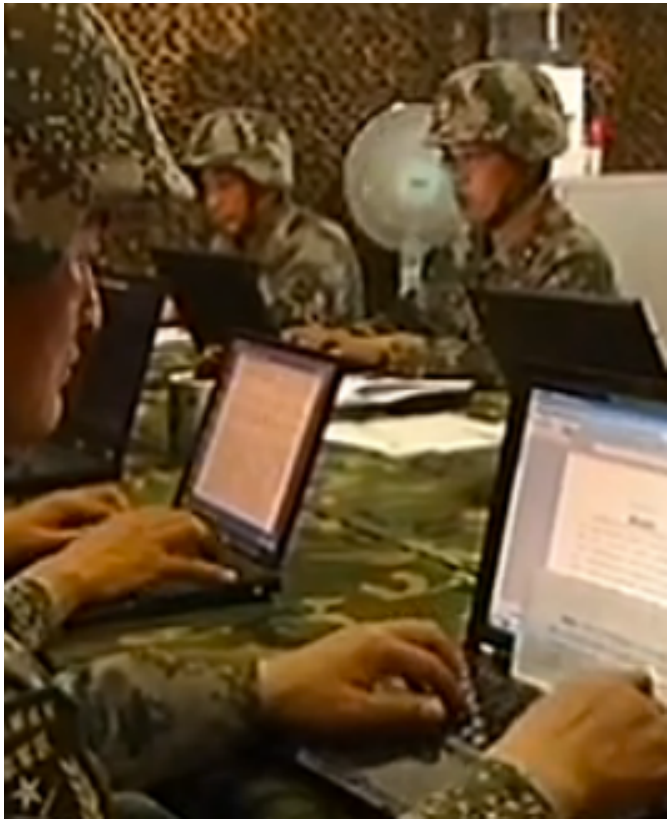
St. Petersburg Internet hosting company involved in numerous criminal activities

Started as legitimate ISP (2006)
Hosts malware, spammers, phishing sites
Alleged operator of Storm botnet
Accused of involvement in DoS on Estonia

Makes off with:
> Supposedly ~$150mil per year
> Seems to have been shut down ~2007

Read more:
http://en.wikipedia.org/wiki/Russian_Business_Network


选择攻击目标
攻击网站的IP地址
法轮功网站列表
攻击
取消



People's Liberation Army Unit 61398

Widely accused of participating in attacks against Falung Gong websites, US companies

Google said China originated attacks in Operation Aurora

Great Firewall of China

Read more:
http://en.wikipedia.org/wiki/Operation_Aurora
http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China

Makes off with:
> Allegedly, lots of intellectual property
> Strict control over Internet usage

Olympic Games

US (and Israeli) governments

Widely accused of developing Stuxnet worm that attacked and temporarily disabled Iranian nuclear reactors

Makes off with:

> Slowed down nuclear reactors

> First use of "cyberweapons" targeting physical damage

Read more:

http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all

Edward Snowden

Former NSA contractor. Whistleblower on USA mass surveillance and cyber espionage

Makes off with:

> 10s of 1000s of NSA documents
> Criminal charges in USA
> Several prizes
> Life in Russia

Read more:
http://en.wikipedia.org/wiki/Edward_Snowden

Anatomy of an example attack in 2011

http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/1

Anonymous vs HBGary

rootkit.com

Ran by Greg Hoglund,
owner of HBGary / HBGary Federal

hbgaryfederal.com

Aaron Barr is CEO
Was set to “unmask” some anonymous members

Anonymous vs HBGary

http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27

usernames, password hashes

hbgaryfederal.com

SQL injection attack

Runs a CMS

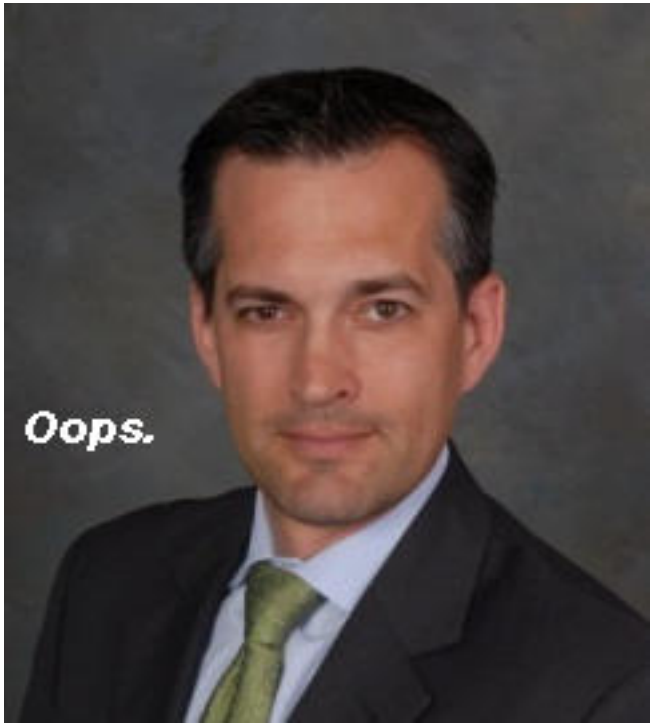
h = Hash(pw)

Given h, recover pw by brute force attack
if pw is “simple” enough

Aaron Barr's (CEO of HBGary) and Ted Vera (COO) had passwords only 6 digits, lower case letters and numbers

JohntheRipper easily inverts hashes of such passwords

http://www.openwall.com/john/



Anonymous vs HBGary

login: ted
password: tedv12

hbgaryfederal.com

This gave user level account

Exploit a privilege escalation vulnerability
in the glibc linker on Linux

Runs a CMS

http://seclists.org/fulldisclosure/2010/Oct/257

Now have root access on hbgaryfederal.com (and more?)
Delete gigabytes of data, grab emails, take down phone system

Anonymous vs HBGary

login: aaron
password: aaro34

google apps

This gave access to Aaron's gmail account, since he used same password here

Aaron was administrator for companies' email on google apps

Runs a CMS

Read Greg Hoglund's emails

Anonymous vs HBGary

From: Greg
To: Jussi
Subject: need to ssh into rootkit
im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?
thanks

"social engineering"

rootkit.com

Recap:

- SQL injection
- Password cracking
- Privilege escalation via setuid program
- Social engineering

Themes in this course

- Understanding threats
- Security evaluations (thinking like an attacker)
- Defensive technologies
- Advancing our technical skills
  - x86 assembly, low-level programming
  - networking
  - cryptography
  - web security

Topic areas

- Low-level software security
- Network security
- Web
- Cryptography
- Misc: E-crime, cloud/virtualization, hardware, ethics/law

We will learn how systems break

Security currently is an arms race between attack and defense

Security engineers must understand attack vectors in order to improve systems' security

“The price of greatness is responsibility”
Winston Churchill

Black hat:

cracker, a criminal

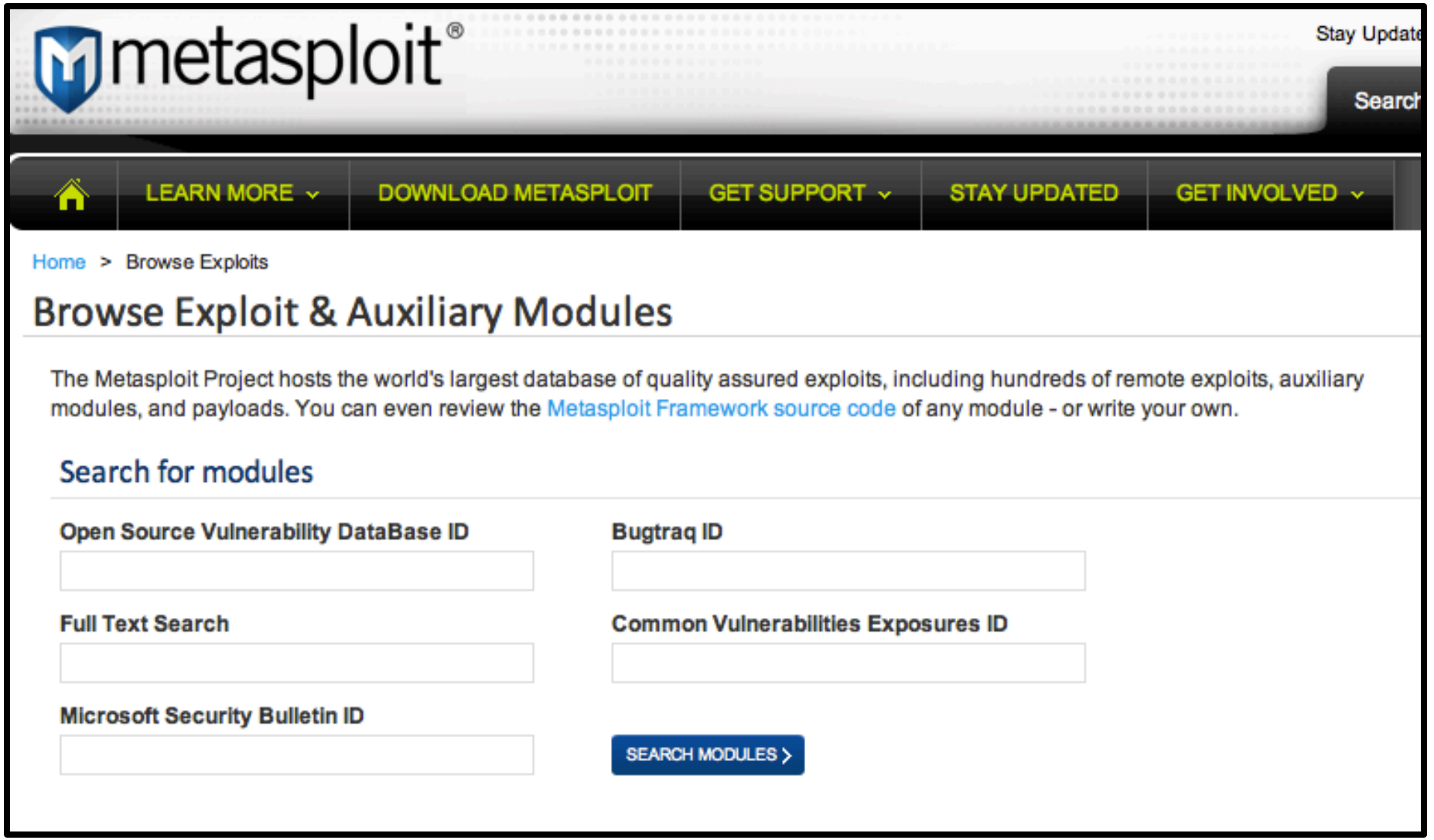
Grey hat:

sometimes criminal, or at least “bending the law”

White hat:

ethical hacker, working within legal framework to perform security evaluations

Being a malicious script kiddie is easy … and stupid



iCloud

Apple ID
password

Backed up pictures, texts, etc.

Apple ID
password

Backed up pictures, texts, etc.

Forensics tool advertised to law enforcement/intelligence
If you know Apple ID, password it
Performs rest of work for you to fetch from iCloud backups http://www.elcomsoft.com/eppb.html

Article linking elcomsoft to iCloud hacks:
http://www.wired.com/2014/09/eppb-icloud/

Reverse engineering and Zero days

Vulnerability/Exploit	Value	Source
"Some exploits"	$200,000 - $250,000	Gov't official referring to what "some people" pay [9]
Significant, reliable exploit	$125,000	Adriel Desautels, SNOSoft [11, 22, 13]
Internet Explorer	$60,000 - $120,000	H.D. Moore [22]
Vista exploit	$50,000	Raimund Genes, Trend Micro [24]
"Weaponized exploit"	$20,000-$30,000	David Maynor, SecureWorks [18]
ZDI, iDefense purchases	$2,000-$10,000	David Maynor, SecureWorks [18]
WMF exploit	$4000	Alexander Gostev, Kaspersky [26]
Microsoft Excel	$\geq$ $1200	Ebay auction site [21, 25]
Mozilla	$500	Mozilla bug bounty program [4]

Table 1: Estimates on exploit values.

The Legitimate Vulnerability Market. Inside the Secretive World of 0-day Exploit Sales by Charlie Miller

The law and ethics

- Abuse of security vulnerabilities
  - is against University of Wisconsin policies.

    I will report anyone who "crosses the line" to the relevant university authorities

    http://www.cio.wisc.edu/policies.aspx
  - runs afoul of various laws.
- Abuse of security vulnerabilities is unethical
  - Think about what you're doing and the price it has on yourself, the victims, and society in general

Rules of thumb

- When in doubt … don't.
  - Come ask me
- You must have explicit (written) permission from a system owner before performing any penetration testing
  - Homework assignments will generally be on your own system
  - We will give explicit permission to hand us exploits for us to test

Responsible disclosure

- **Full disclosure** means revealing everything about a vulnerability including an example exploit
- **Responsible disclosure** (generally) refers to ensuring potential victims are aware of vulnerabilities before going public

CERT/CC process (2000)

- Reporter notifies CERT
- CERT notifies vendor
- 45 days later, CERT makes vulnerability public
- CERT acts as (potentially anonymous) communications channel between reporter/ vendor

Security Update for Gray GoPayment Card Reader

We recently learned from the University of Wisconsin, Madison about a security vulnerability with the gray GoPayment credit card reader made by our partner ID TECH. As soon as we learned about this vulnerability, we immediately started working with the university and ID TECH to test it and ensure that our GoPayment customers were not at risk.

http://security.intuit.com/alert.php?a=51

- Notified companies when we had a draft of paper finished
- Worked with them to ensure they could fix vulnerabilities
- Full disclosure at presentation at workshop

Vulnerability Class	Channel	Implemented Capability	Visible to User	Scale	Full Control	Cost
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port	Yes	Small	Yes	Low
Indirect physical	CD	CD-based firmware update	Yes	Small	Yes	Medium
	CD	Special song (WMA)	Yes*	Medium	Yes	Medium-High
	PassThru	WiFi or wired control connection to advertised PassThru devices	No	Small	Yes	Low
	PassThru	WiFi or wired shell injection	No	Viral	Yes	Low
Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app	No	Large	Yes	Low-Medium
	Bluetooth	Sniff MAC address, brute force PIN, buffer overflow	No	Small	Yes	Low-Medium
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)	No	Large	Yes	Medium-High
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)	No	Large	Yes	Medium-High

Checkoway et al.

Comprehensive Experimental Analysis of Automobile Attack surfaces

Administrative stuff

- http://pages.cs.wisc.edu/~rist/642-fall-2014/
- Will use email list for announcements
  - compsci642-1-f14@list.wisc.edu

Homeworks

- Some problem sets will allow teams of up to 2
- Collaboration policy:
  - no collaboration with people outside team
  - using the web for general information is encouraged
  - Googling for answers to questions is not
  - Cheating will be reported to university authorities
- Need access to virtualization software

Exams

- Going to do a midterm this year
  - In-class, cover information up to that period
- Last year was a take-home final. Probably same this year

Project

- Grad students are probably going to be required to do a term project culminating in a short presentation last week of term
- Broad scope. Aim is to get introduced to security research:
  - Literature review on some topic of interest
  - In-depth analysis of some computing system
  - Be creative
  - I'll announce deadline for project proposals soon

Participation

- Please speak up in class
- No need to read all papers for a lecture in detail, but:
  - Be aware of topic areas
  - Read in depth selectively later

A warm up: security principles

Saltzer and Schroeder.
The protection of information in computer systems.
Proceedings of the IEEE, 1975

1) Economy of mechanism
2) Fail-safe defaults
3) Complete mediation
4) Open design
5) Separation of privilege
6) Least privilege
7) Least common mechanism
8) Psychological acceptability

Economy of mechanism

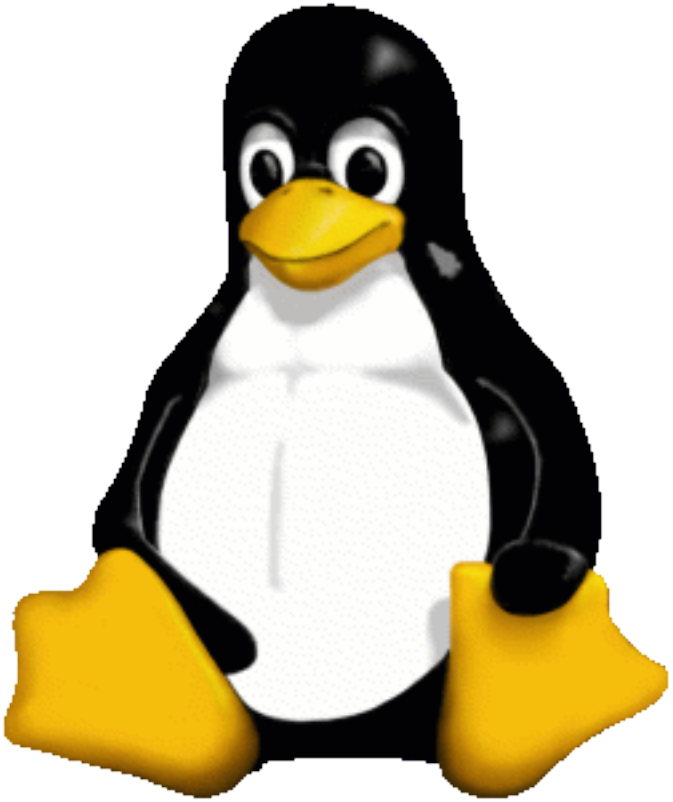
Fail-safe defaults

```
isAdmin = true;
try {
    codeWhichMayFail();
    isAdmin = isUserInRole( “Administrator” );
}
catch (Exception ex) {
    log.write( ex.toString() );
}
```

(Example from https://www.owasp.org/index.php/Secure_Coding_Principles)

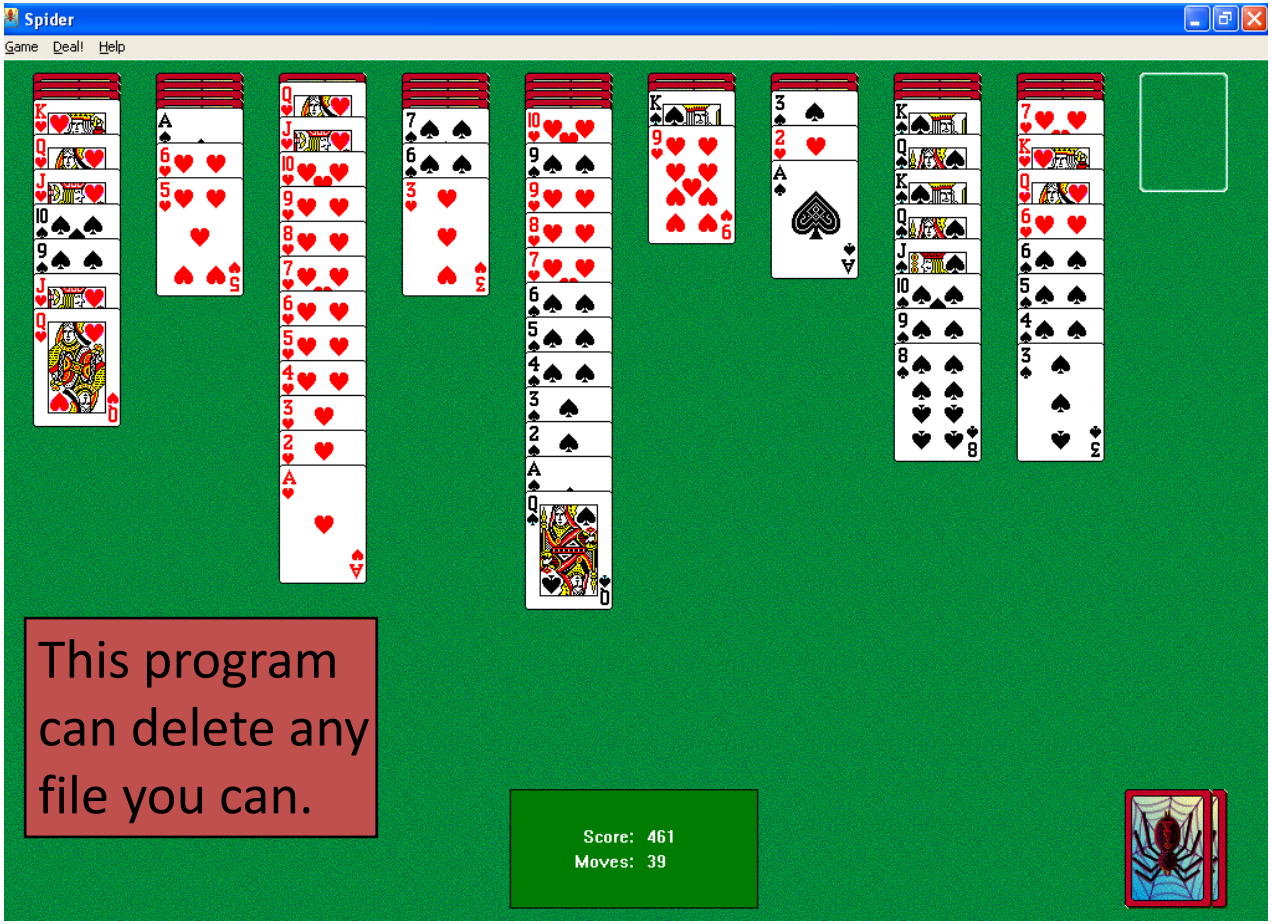
Complete mediation

Open design
(avoid “security by obscurity”)



Separation of privilege

Least privilege



(Courtesy of UCB CS161 slides)

Least common mechanism
(isolation)

Psychological acceptability
(consider human factors)

Principles from 1970's

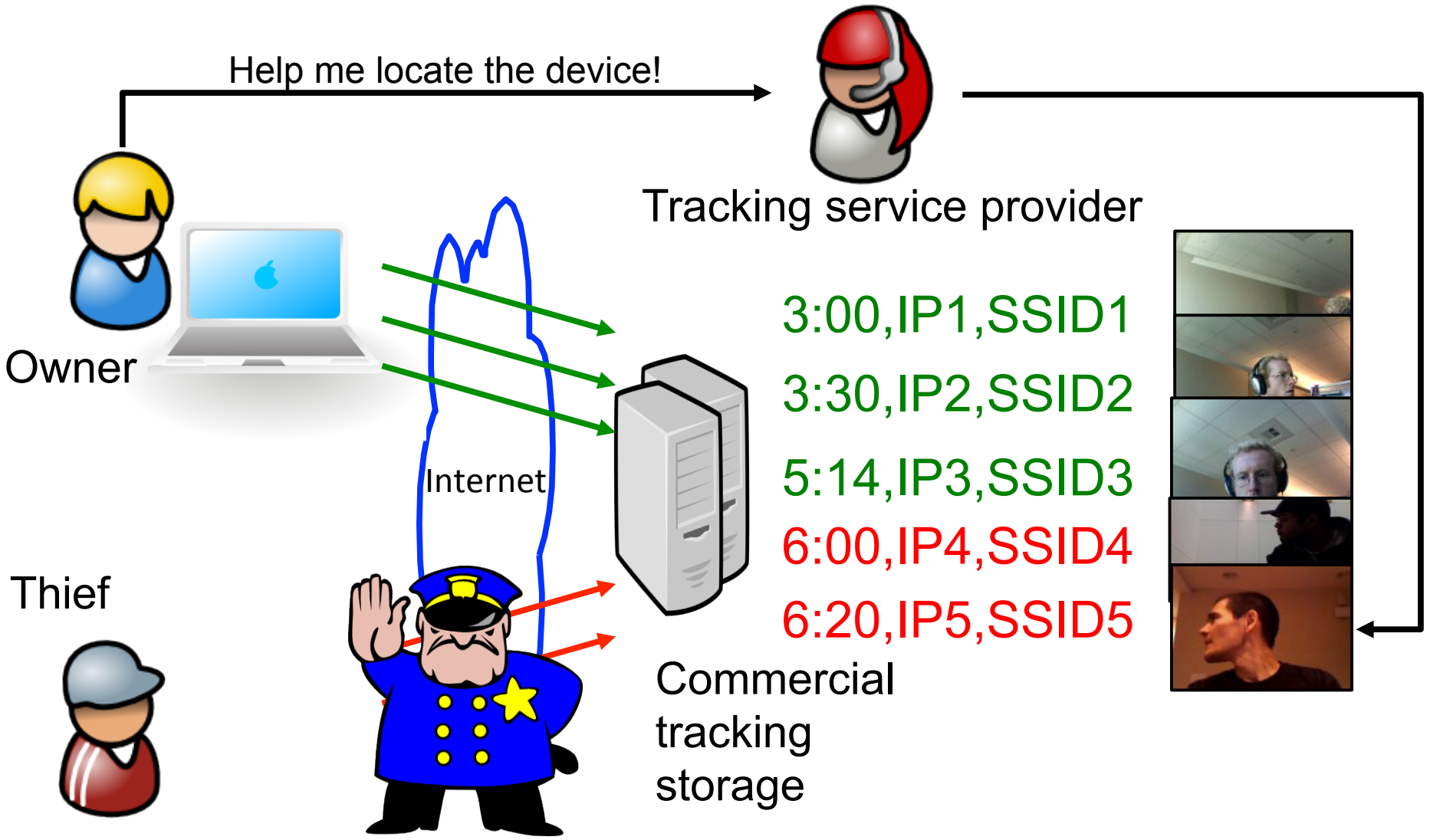
- Do you think they are relevant today?
- A bit… abstract
- Recur over and over again

US Cyber Command

USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.


UNITED STA
COM

Ethics, the law, and strange situations



http://thisguyhasmymacbook.tumblr.com/post/5821960131/guy-driving-away-with-my-macbook

Ethics, the law, and strange situations

"Couple Can Sue Laptop-Tracking Company for Spying on Sex Chats"
http://www.wired.com/threatlevel/2011/08/absolute-sued-for-spying/

Other courses at Wisconsin

- CS 435 (Prof. Jha, this term)
  - "Intro to cryptography"

- CS 838 (Prof. Ristenpart, last Spring 2011)
  - "Applied cryptography"