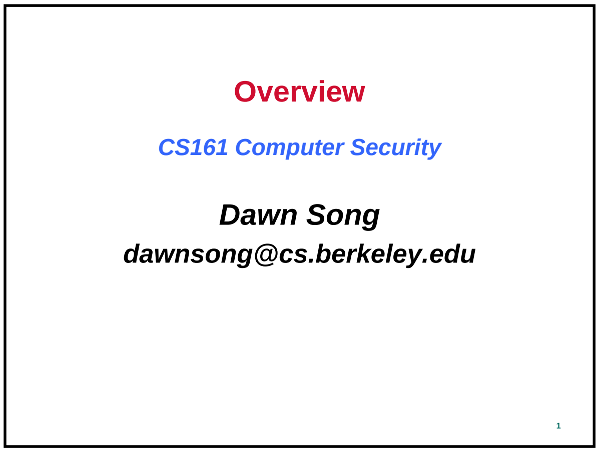
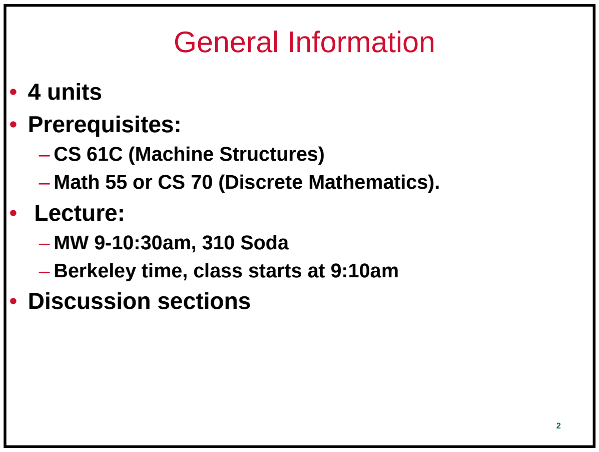


Overview

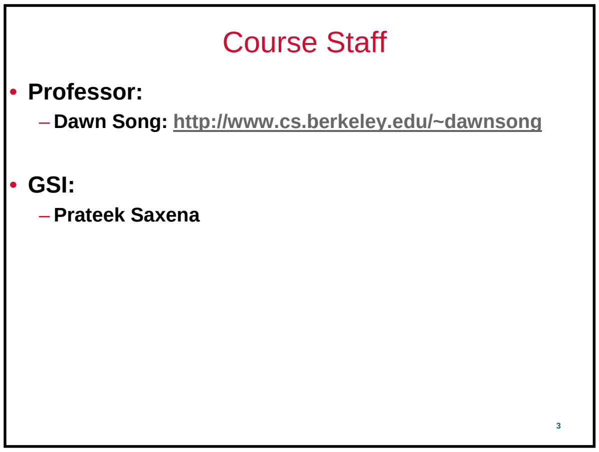
CS161 Computer Security

Dawn Song
dawnsong@cs.berkeley.edu



General Information

- **4 units**
- **Prerequisites:**
  - **CS 61C (Machine Structures)**
  - **Math 55 or CS 70 (Discrete Mathematics).**
- **Lecture:**
  - **MW 9-10:30am, 310 Soda**
  - **Berkeley time, class starts at 9:10am**
- **Discussion sections**

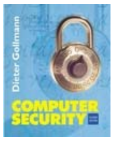


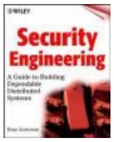
Course Staff

- **Professor:**
  - **Dawn Song: http://www.cs.berkeley.edu/~dawnsong**
- **GSI:**
  - **Prateek Saxena**

Textbooks

- Required: Computer Security, 2nd ed.(Gollmann)
  - 1st ed. is insufficient
  - Assigned readings will be posted
- Security in Computing, 4th ed. (Pfleeger & Pfleeger)
  - *Optional*
- Security Engineering (Anderson)
  - *Optional*
  - Available in online form





Resources

- Website:
  - http://inst.eecs.berkeley.edu/~cs161/fa08/
- Mailing list:
  - cs161-fall08@lists.eecs.berkeley.edu
    https://lists.eecs.berkeley.edu/sympa/info/cs161-spring08
  - Used for announcements, especially urgent notices
  - If you haven't subscribed, pls do asap!
- Newsgroup:
  - Newsgroup: ucb.class.cs161
    Server: news.berkeley.edu (from campus), authnews.berkeley.edu (off campus)
    See http://www.net.berkeley.edu/usenet/.
  - For general class related questions, pls post on newsgroup instead of emailing the staff, so other students can benefit too

Course Load

- 2 Exams: closed book
  - Midterm exam: covers the first half of the course
  - Final exam: covers the second half of the course
- 5 Homeworks
  - Three homeworks for first half of semester
  - Two homeworks for second half of semester
- 3 Projects
  - In groups of two

Grading

- 20% Homeworks (4% each)
- 40% Project (5% Proj 1, 15% Proj 2, 20% Proj 3)
- 20% Midterm exam
- 20% Final exam

Class Participation

- Showing up (on time) is the first step
- Asking/answering questions is encouraged
- Turn off your cell phone ring in class
- Treat students and staff with respect

Collaborative Work

- Projects will be in groups of two
- Homeworks are done individually
- You may use the following resources:
  - Instructors, TAs, assigned texts, posted notes
- No “Googling for answers”
  - Consult with TAs over problem cases
  - Always cite references – plagiarism is not permitted

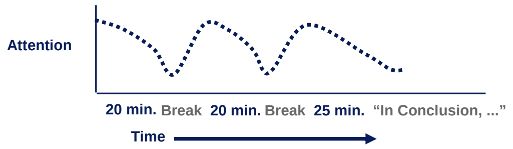
Academic Dishonesty Policy

- **Copying all or part of another person's work, or using reference material not specifically allowed, are forms of cheating and will not be tolerated.**
- **http://www.eecs.berkeley.edu/Policies/acad.dis.shtml**

Note on Security Vulnerabilities

- **From time to time, we may discuss vulnerabilities in widely-deployed computer systems. This is *not* intended as an invitation to go exploit those vulnerabilities. It is important that we be able to discuss real-world experience candidly; students are expected to behave responsibly.**
- **Berkeley policy is very clear: you may not break into machines that are not your own; you may not attempt to attack or subvert system security. Breaking into other people's systems is inappropriate, and the existence of a security hole is no excuse.**

Typical Lecture Format



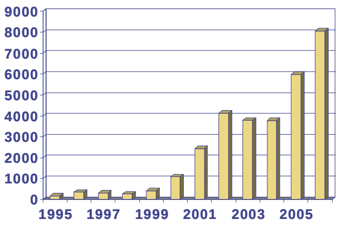
- **2-Minute Review**
- **20-Minute Lecture**
- **5- Minute Administrative Matters**
- **3-Minute Break (stretch)**
- **20-Minute Lecture**
- **5-Minute Break (water, stretch)**
- **25-Minute Lecture**
- **Instructors will come to class early & stay after to answer questions**

Computer Security is Important

- Unpatched PC survives less than 16 min [SANS04]
- $10billion annual financial loss [ComputerEconomics05]
  - Worms
    - CodeRed: Infected 500,000 servers, $2.6billion in damage [CNET03]
    - SQL Slammer: Internet lost connectivity, affected 911, ATM, etc.
  - Botnets
    - Over 6 million bot-infected computers in 3 months [Symantec06]
  - 61% U.S. computers infected with spyware [National Cyber Security Alliance06]

Trends

- Attacks are increasing in scale, sophistication, & severity
  - Real financial incentives

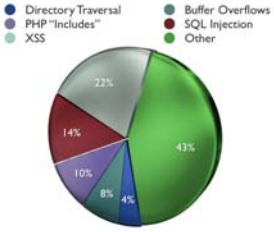


CERT Vulnerabilities reported

Most-common attacks on systems

- 2006 MITRE CVE stats:
  - 21.5 % of CVEs were XSS
  - 14 % SQL injection
  - 9.5 % php "includes"
  - 7.9 % buffer overflow.

2005 was the first year that XSS jumped ahead of buffer overflows …



A Thriving Underground Economy

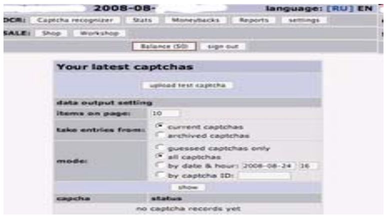
- **Average bot costs**
  - **$0.04**
- **Zero-day vulnerability for**
  - **$75K [SecurityFocus07]**
- <A> Sell Cvv US(1$ each),Uk(2$ each)Cvv with SSN & DL(10$ each)and ePassporte Account with 560$ in acc(50$),Hacked Host(7$),Tut Scam CC Full in VP-ASP Shop(10$).shopadmin with 4100 order(200$), Tool Calculate Drive Licsence Number(10$).... I'm sleeping. MSG me and I will reply U as soon as I can !

- **With one IRC channel, 24-hr period, just a few samples**
  - **Accounts worth $1,599,335.80 have been stolen**
- **"*The Underground Economy: Priceless*" [;login Dec06]**

Automatic Tools for Attacks (I)

- **anti-captcha.com**

"We work with tens of thousands of people from all over the world who are ready to work for a small payment to convert text pictures sent by you. You give the CAPTCHAs to our server, which hands it to the workers. In a few seconds, our server will receive the converted CAPTCHA as text and relay it back to you. As a rule, this time does not exceed 20 seconds and [that's] quite fast enough for a successful registration everywhere there is CAPTCHA in use."



Your latest captchas

data output setting

items on page: 10

take entries from: ● current captchas ○ archived captchas

mode: ○ guessed captchas only ● all captchas ○ by date & hour: 2008-08-24 16 ○ by captcha ID:

capcha	status
no captcha records yet	

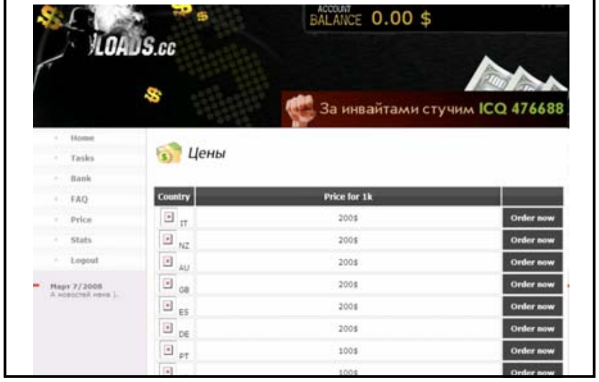
Automatic Tools for Attacks (II)

- **Tools to automatically build your malware**
  - **Select from menu: anti-AV feature, spam, ddos, anti-VM feature, etc.**

- **Tools to automatically distribute your malware:**

"Currently, loads.cc claims to have 264,552 hacked systems in more than a dozen countries that it can use as hosts for any malicious software that clients want to install. The latest details from the "statistics" page displayed for members says the service has gained some 1,679 new infectable nodes in the last two hours, and more than 33,000 over the past 24 hours."

Load.cc

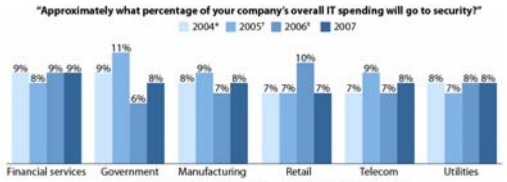


Цены

Country	Price for 1k	
IT	200$	Order now
NZ	200$	Order now
AU	200$	Order now
GB	200$	Order now
ES	200$	Order now
DE	200$	Order now
PT	100$	Order now
	100$	Order now

January 2007, Trends **"2007 Security Budgets Increase: The Transition To Information Risk Management Begins"**

Security Spending Variance By Industry



*Base: 604 executives at North American and European enterprises
†Base: 840 executives at North American and European enterprises
‡Base: 616 executives at North American and European enterprises
Base: 447 executives at North American and European enterprises

*Source: Forrester's Business Technographics® June 2004 North American And European Benchmark Study
†Source: Forrester's Business Technographics November 2004 North American And European Benchmark Study
‡Source: Business Technographics November 2005 North American And European Enterprise IT Budgets And Spending Survey
Source: Business Technographics November 2006 North American And European Enterprise IT Budgets And Spending Survey

This Class

- **How to build secure systems?**
- **How to evaluate security of systems?**
- **Topics in this class**
  - **Crypto, software security, OS security, Web security, Network security, other advanced topics**

Steal cars with a laptop

- In April ‘07, high-tech criminals made international headlines when they used a laptop and transmitter to open the locks and start the ignition of an armor-plated BMW X5 belonging to soccer player David Beckham, the second X5 stolen from him using this technology within six months.
- … Beckham's BMW X5s were stolen by thieves who hacked into the codes for the vehicles' RFID chips …

Class Topics (I)

- Part I: Introduction to Cryptography
  - Secret-key encryption
  - Public-key encryption
  - Hash functions, MACs, Digital signatures
  - Authentication, key exchange protocols
  - Secret sharing, random number generator
  - Timing attacks, fault attacks, etc.

IPhone Security Flaw

- Jul 2007: “researchers at Independent Security Evaluators, said that they could take control of iPhones through a WiFi connection or by tricking users into going to a Web site that contains malicious code. The hack, the first reported, allowed them to tap the wealth of personal information the phones contain.”

Charles Miller, shown on his iPhone,
said that after finding a hole in security, “you were in complete control.”

iPhone attack

- iPhone Safari downloads malicious web page
  - – Arbitrary code is run with administrative privileges
  - – Can read SMS log, address book, call history, other data
  - – Can perform physical actions on the phone.
    - » system sound and vibrate the phone for a second
    - » could dial phone numbers, send text messages, or record audio (as a bugging device)
  - – Can transmit any collected data over network to attacker

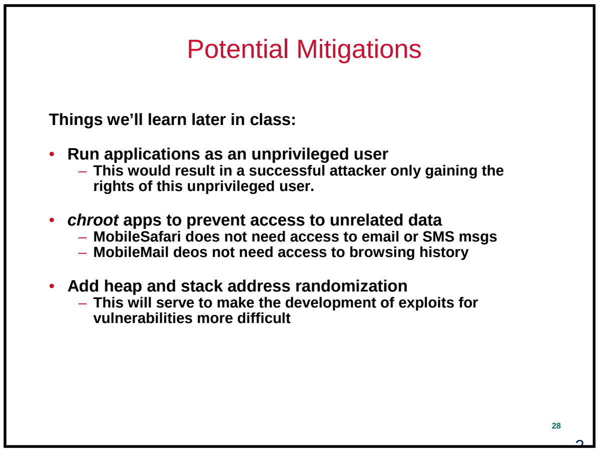
See http://www.securityevaluators.com/iphone/

iPhone security design

- "Reduced attack surface"
  - – Stripped down and customized version of Mac OS X
    - » does not have common binaries such as bash, ssh, or even ls.
  - – MobileSafari - many features of Safari have been removed
    - » No Flash plug-in, many file types cannot be downloaded
- Some internal protection
  - – If USB syncing with iTunes, file system cannot be mounted
  - – File system accessible to iTunes is chroot'ed
- Weak security architecture
  - – All processes of interest run with administrative privileges
  - – iPhone does not utilize some widely accepted practices
    - » Address randomization
      - Each time a process runs, the stack, heap, and executable code located at precisely the same spot in memory
    - » Non-executable heaps
      - Buffer overflow on heap can write executable instructions

Finding the Flaw

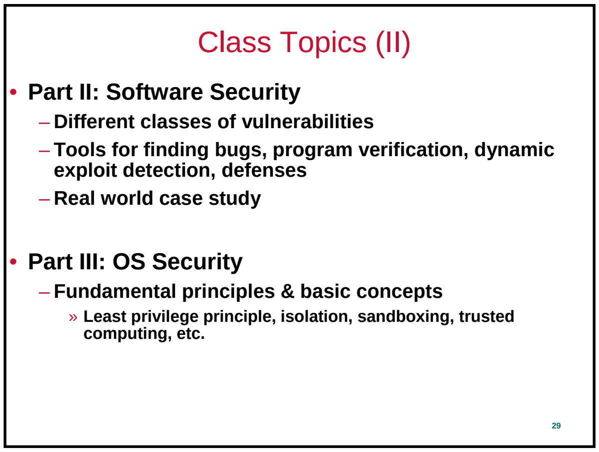
- Extract and statically analyze binaries
  - – Using jailbreak and iPhoneInterface,
- Audit related open-source code
  - – MobileSafari and MobileMail applications are based on the open source WebKit project
- Dynamic analysis, or "fuzzing"
  - – Sending malformed data to cause a fault or crash
  - – Look at error messages, memory dump, etc.
  - – MobileSafari attack discovered using fuzzing



Potential Mitigations

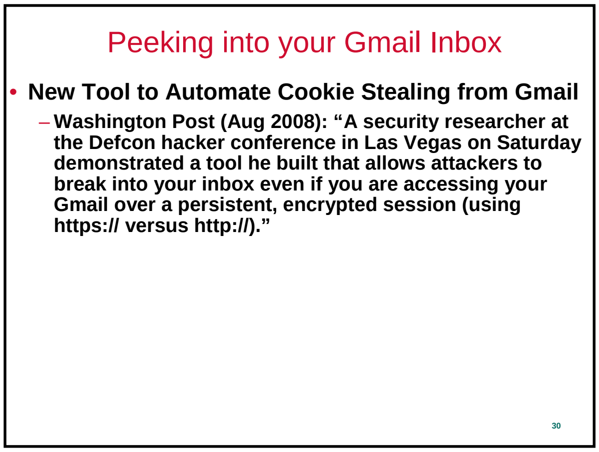
Things we'll learn later in class:

- **Run applications as an unprivileged user**
  - **This would result in a successful attacker only gaining the rights of this unprivileged user.**
- ***chroot* apps to prevent access to unrelated data**
  - **MobileSafari does not need access to email or SMS msgs**
  - **MobileMail deos not need access to browsing history**
- **Add heap and stack address randomization**
  - **This will serve to make the development of exploits for vulnerabilities more difficult**



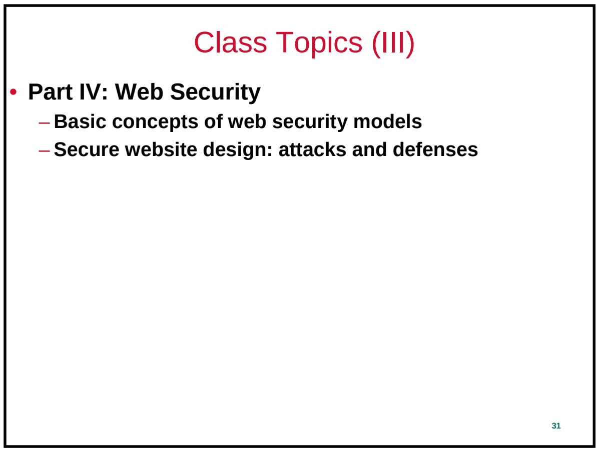
Class Topics (II)

- **Part II: Software Security**
  - **Different classes of vulnerabilities**
  - **Tools for finding bugs, program verification, dynamic exploit detection, defenses**
  - **Real world case study**
- **Part III: OS Security**
  - **Fundamental principles & basic concepts**
    - **Least privilege principle, isolation, sandboxing, trusted computing, etc.**



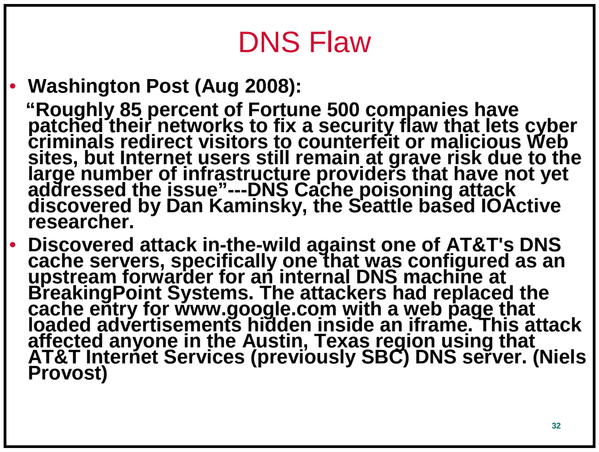
Peeking into your Gmail Inbox

- **New Tool to Automate Cookie Stealing from Gmail**
  - **Washington Post (Aug 2008): "A security researcher at the Defcon hacker conference in Las Vegas on Saturday demonstrated a tool he built that allows attackers to break into your inbox even if you are accessing your Gmail over a persistent, encrypted session (using https:// versus http://)."**



Class Topics (III)

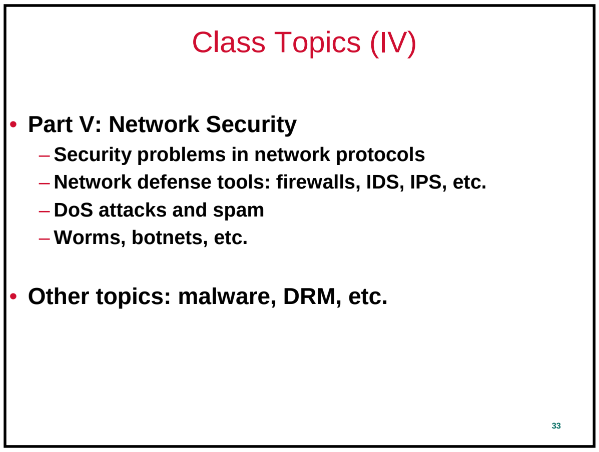
- **Part IV: Web Security**
  - **Basic concepts of web security models**
  - **Secure website design: attacks and defenses**



DNS Flaw

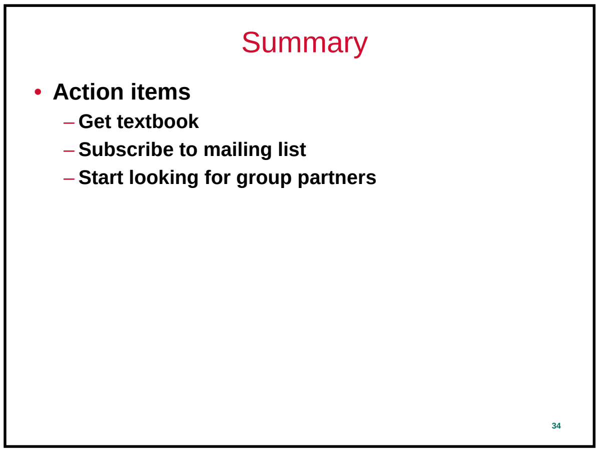
- **Washington Post (Aug 2008):**

  “Roughly 85 percent of Fortune 500 companies have patched their networks to fix a security flaw that lets cyber criminals redirect visitors to counterfeit or malicious Web sites, but Internet users still remain at grave risk due to the large number of infrastructure providers that have not yet addressed the issue”---DNS Cache poisoning attack discovered by Dan Kaminsky, the Seattle based IOActive researcher.
- **Discovered attack in-the-wild against one of AT&T's DNS cache servers, specifically one that was configured as an upstream forwarder for an internal DNS machine at BreakingPoint Systems. The attackers had replaced the cache entry for www.google.com with a web page that loaded advertisements hidden inside an iframe. This attack affected anyone in the Austin, Texas region using that AT&T Internet Services (previously SBC) DNS server. (Niels Provost)**



Class Topics (IV)

- **Part V: Network Security**
  - **Security problems in network protocols**
  - **Network defense tools: firewalls, IDS, IPS, etc.**
  - **DoS attacks and spam**
  - **Worms, botnets, etc.**
- **Other topics: malware, DRM, etc.**



Summary

- Action items
  - Get textbook
  - Subscribe to mailing list
  - Start looking for group partners