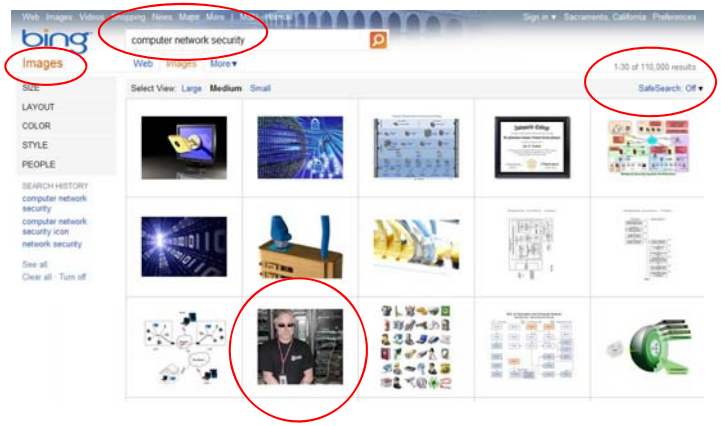
Instructor



Overview 2

Martin Maxwell - Visiting Professor

Contact Information

- Office: Anderson 214
- Hours: Tuesday & Thursday ~ 11:30-12:00
  - Generally in lab or office after class
- E-mail: mmaxwell@pacific.edu
- E-mail: mmaxwell@treacle.com
- Class Content:
  - Sakai
  - www1.pacific.edu/~mmaxwel2
- Syllabus
- Schedule
- Grading Policy
- Updates – class changes

Overview 3

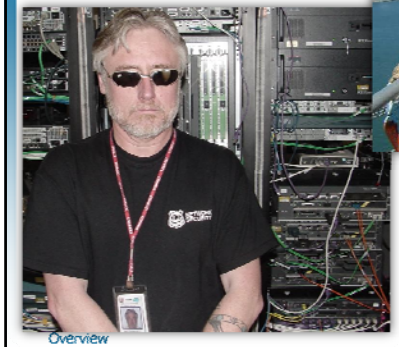
.com - Consultancy

- TREACLE.COM domain since 1995
- /29 Internet address space
- SMTP, DNS, DHCP, HTTP, NTP
- NetBot, PDU
- Firewall
- 3620 router, 2950 switch

.gov - Retired - 2012

Enterprise Network Security – Chief, Lead

Test Lab racks



Installing a wireless network bridge

Overview 5

We put the dot *in* .ca.gov.

- Team designed, implemented, and administer a statewide network infrastructure with MPLS core, GigabitEthernet and ATM switches and routers, GigaMAN, OC3 (155mbs) and DS3 (45mbs) circuits, Frame-Relay distribution network connecting over 550 sites supporting 22,000 users. Three gigabit Internet connections.
- Team manages all security devices: firewalls, IDS/IPS, web filtering, sniffers.
- Services provided include DNS, DHCP, NTP, etc. Statewide traffic cameras, webcasting, and videoconferencing.

Overview 6

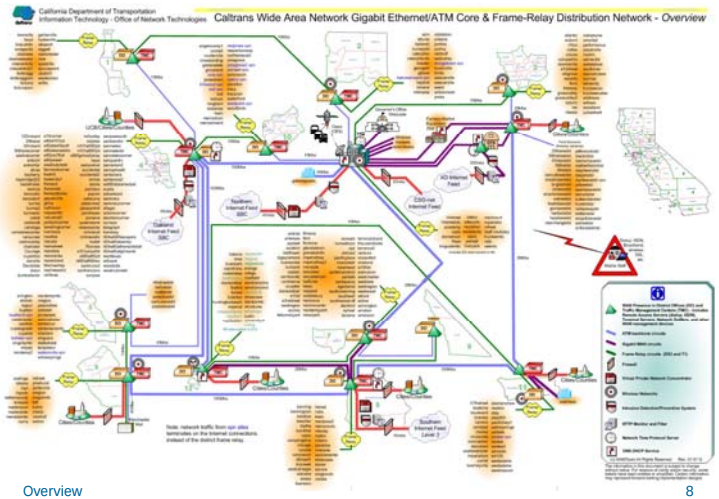
We keep the dot *in* .ca.gov.

Technical lead over CT Enterprise Network Security
Despite bad guys, lusers, management

- Dec 29, 2011 *firewall* log:
  3,482,586 entries - 575MB
- Webfiltering log ~ 6GB/day
- Firehose of events
- Misconfigured devices
- Weather
- Vendors
- Politics
- Technology (lifecycle, complexity)

Overview 7

Caltrans WAN

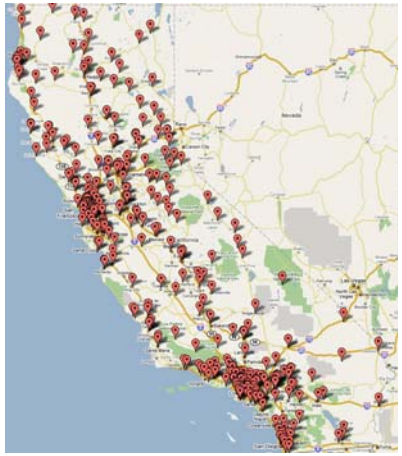


Overview 8

Operational Security

- Mgmt network
- Configuration control
- Access control
  - Physical
  - Network
- Event management

- Appliances
- Embedded



Defacements Happen

...and happen again

Unintended Results

You can't stop stupid

What Is Computer Security

Computer security is a branch of computer technology known as information security as applied to computers and networks.

The objective of computer security includes protection of information and property from theft, corruption, or natural disaster*, while allowing the information and property to remain accessible and productive to its intended users.

* cluelessness, stupidity, lusers, etc.

Overview 13

Course Description

ECPE/COMP 178. Computer Network Security (3)

An introduction to security of computer systems and security of communication on networks of computers. Topics include TCP/IP protocols, Internet cryptography, Internet authentication, malware, and social engineering. Emphasis is on network and computer attack methods and tools, and how to defend against those attacks. Includes lab.

Students should be familiar with Internet architecture, TCP/IP, packets structure, IP addresses, and port numbers.

Students must be completely comfortable navigating a directory structure and moving and copying files within DOS and Linux command line environments.

Overview 14

Revised

- Course Description: Computer Network Security (3). An examination of the pervasive security threats related to the Internet, data communications and networking. Topics include TCP/IP protocols, authentication, encryption, malware, cybercrime, and social engineering. Emphasis is on computer and network attack methods, their detection, prevention and analysis, and the integration of the tools and techniques employed in this effort. Includes lab.

Overview 15

Course Outcome Assessment

- Homework/Labs: 25%
- Quizzes: 25%
- Mid-Term Exam: 25%
- Final Exam: 25%
- GRADING POLICY:
  - A: 90 - 100%
  - B: 80 - 90%
  - C: 70 - 80%
  - D: 60 - 70%
  - F: 0 - 60%
  - Grades within 2% of a border assigned a ± accordingly.

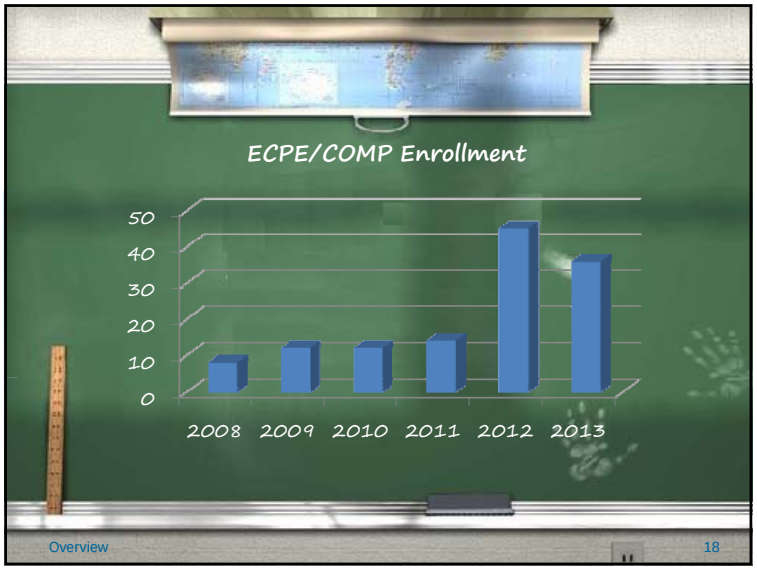
Required Textbook: ? *Assigned readings*

It Begins... 16

Attendence

- Attendance at all classes is necessary
- Any student missing a class is responsible for studying the material discussed and for being aware of announcements made during the class
- Lecture material will be available online
- Additional reading material will be available online
- Quizzes will normally be announced in the schedule
- Low attendance on any given day will result in a pop quiz
- I do not create make-up quizzes. Therefore: Missed quizzes cannot be made up! Your ONE lowest quiz grade will be dropped. This allows you to miss one class meeting without penalty. The reason you missed class is irrelevant.

It Begins... 17



Overview 18

A Few Changes

- Different Classroom
- Lab Moved from Baun 212 to Baun 214
- Expanded Lab Hours - TBD
- Graduate Assistant for Labs- TBD
- Hacking Contest – TBD
- Evolution?

- 2013 - Due to popular demand
  - Added second section
  - Lab designed for 10h (+2 overflow buffers)

Overview 19

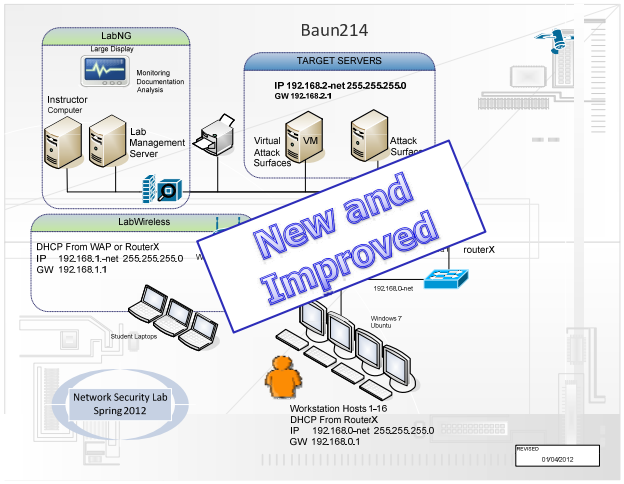
Here There Be Dragons

Security research takes time and experience

- Don't damage your computer/data/network
- Don't damage anyone else's either
- Don't damage your reputation (color of hat)
- Activity vs. Intent are fuzzy
- Use the test lab
- Set up you own test network
- AV tools vs. network tools = conflict
- Be paranoid – authorities & bad guys

Overview 20

Cisco Networking Lab - Baun 214



Labs

- Wireshark - Packet sniffing
- Google hacking
- Nmap - network scanning
- SQL injection
- Vulnerability assessment
- Windows OS internals

- Team project on log analysis

Rulez (aka Policy)

- Do not scan, hack, etc. outside of lab
- Be careful with the software tools

- White hat vs Black hat
- NDA
- Lab & Internet/campus
- RTFM
- Protect your computer
- Don't do dumb things

Computer Network Security

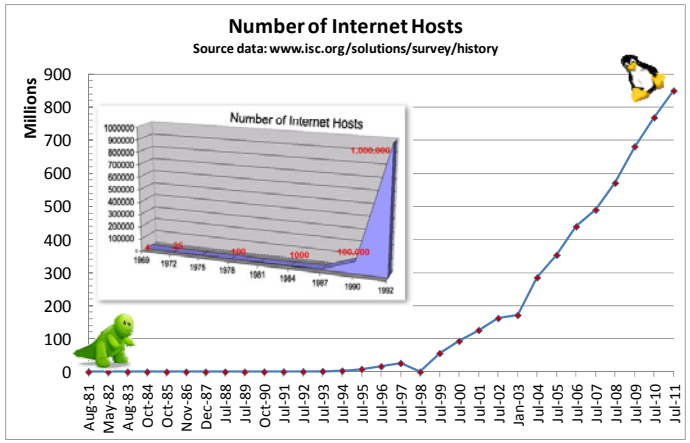
There is a *huge* gap between the "Defensive" and "Offensive" security fields. A gap so big that a 12 year old could outsmart a well seasoned security expert. Hopefully, if this separation between the "Defensive" and "Offensive" fields is clear enough, Network administrators and (defensive) security experts will start to realize that they are aware of only one half of the equation, and that there's a completely alien force they need to deal with - and that **in order to defend, they need to understand the attack(er).** ***- Offensive Security***

In the beginning…….

- Telephone switching network – *blue boxes!*
- ARPANET, MINITEL, CompuServe, AOL
- NSFNet Backbone (TCP/IP) 1986
- Morris Internet Worm – 1986
- Gopher – WideAreaInformationServer -1991
- CERN creates the WorldWideWeb -1991
- Mosaic 1.0 released - 1993
- Netscape founded, Comet Shoemaker-Levy - 1994
- Internet/WWW massive growth
- As of 6-30-10 1.966 B Internet users – 28.7% of pop.
- 2000-2010 growth 444.8% src.- internetworldstats.com

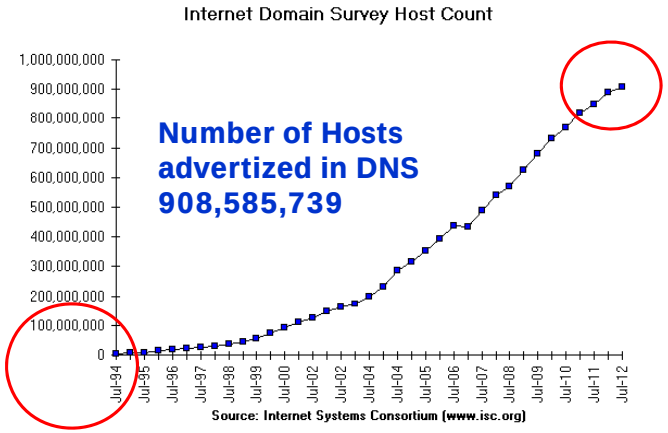
Overview 25

Hosts Growth



Overview 26

Latest revision



Overview 27

Ubiquitous Networking
Pervasive Computing

- Computers
- Digital Video Recorders
- Audio Systems, iPod's
- Cell Phones, VOIP
- Digital Cameras
- Home Appliances
- Cars
- Printers/Scanners
- Digital Picture Frames
- Smart utility meters

ALL OF THESE ARE HACKABLE

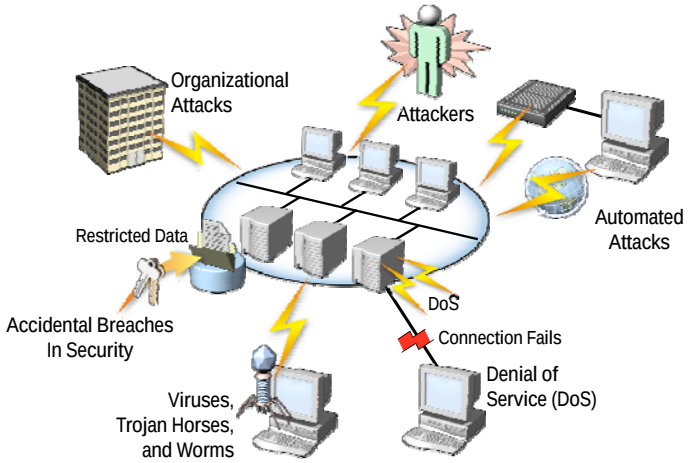
Overview 28

Perversity of Human Nature

- Activists/Hacktavists Anon
- Terrorists
- Unorganized/Organized Crime
- Corrupt/Repressive Governments
- Business Competition
- Unhappy - clueless employees
- Malcontents
- Students
- General monkey curiosity

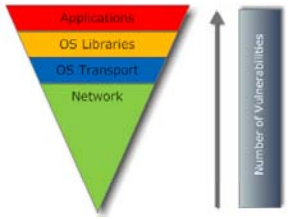
Mad, Bad, and Dangerous to Know
now has global connectivity and access!

Common Types of Attacks



Unpatched Software Flaws Put PCs at Risk

Computers are vulnerable to attack by hackers due to unpatched flaws in their software applications.



Its not just the OS!
Flash player - .swf files
Adobe reader - .pdf files
Word, Excel - .doc, .xls files
Pictures - .jpg files
Quicktime

Microsoft Update won't help with most of the above patching.

Partial Economic Cost

- Gartner's estimate for 2007 - phishing losses of $3.2B U.S.* * Gartner's estimates are self serving poop
- Loss per incident $886 (2007) $1,244 (2006)
- Individual victims 3.6 M (2007) 2.3 M (2006)
- RSA estimates phishing cost organizations $2.1B in 2011/Q1-2 2012
- Analysis of the economic impact of malware must also factor in wasted time, resources, and energies of the cyber-community, governments, companies and individuals, along with the lost economic cost of the misdirected effort.

Don't Quit Your Day Job.....

- Phishing is a classic example of tragedy of the commons (e.g. open access to a resource that has limited ability to regenerate)
- Since each phisher independently seeks to maximize return, the resource is over-grazed and yields far less than it is capable of
- There is little capital outlay or startup costs, no raw materials and no sophisticated equipment to rent or buy. The phisher merely harvests "free money" from the online population. But, the easier phishing gets, the worse the economic picture for the phisher – more phishers!

US Data Breaches In 2011/12

Fresh Data Commitment

- Report Date: 12/26/2012
- Pages: 86 5-6 events per page
- Reported Breaches: 414 (11) 447(12)
- Exposed: 22,945,773 (11) 17,317,184 (12)

Cause of breach

- 19.5% hacking
- 16.9% insider theft
- 27.5% human error (lost it)
- Majority of lost data neither encrypted nor password protected

- Source: Identity Theft Resource Center

2012 Exposed Records

Banking/Credit/Financial	17	470,048
Business	165	4,615,893
Educational Facilities	61	2,304,663
Government/Military	50	7,688,707
Medical/Healthcare	154	2,237,873
Total Incidents	447	17,317,184

U.S. Only – Report date 12/26/2012

Source – Identity Theft Resource Center

Fresh Data Commitment

Assigned Reading

For Thursday ~100 pages of tables

- ITRC Breach Stats Report 2012
  http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202012.pdf
- ITRC Breach Report 2012
  http://www.idtheftcenter.org/ITRC%20Breach%20Report%202012.pdf

What do you see?

Humor is Relative

Fake nuclear explosion

Czech art group to stand trial for hacking a TV channel watching a web cam monitoring weather at various resorts.

Network Security

Security is an ongoing process

- Policy development and adoption
- Computers patched and made secure
- Network Infrastructure protection layers
- User awareness
- Test
- Repeat the process

- www.sans.org/resources/policies/
- www.dir.state.tx.us/security/policies/

Insecurity Tools

Tools can show vulnerability, lead to better security

This class should enhance your overall security

But will not leave you feeling warm and fuzzy

Broad Field - Only One Class

- Cryptography
- Forensics
- Software
- Hardware
- Policy
- Auditing
- Programming

Goals

- Increased Vulnerability/Exploit Awareness
- Better security practices

Be paranoid – they <u>are</u> out to get you!