Experiences with practice-focused undergraduate security education

Robert L. Fanelli and Terrence J. O'Connor
Department Electrical Engineering and Computer Science
United States Military Academy, West Point, NY, USA

Introduction

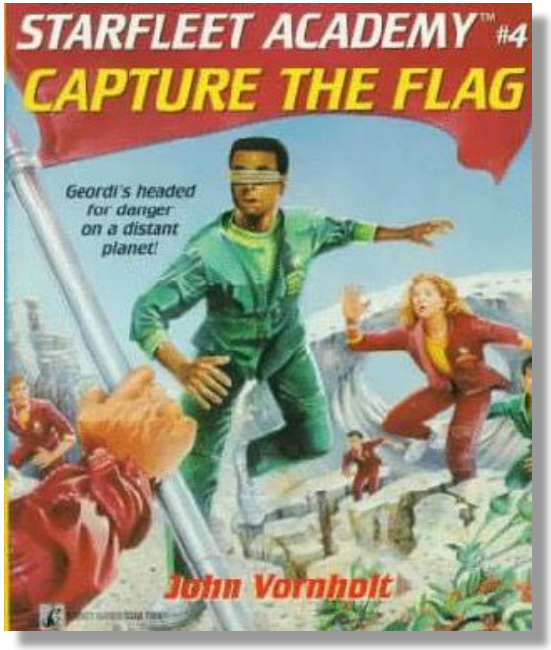
- Experiences from United States Military Academy's CS482 *Information Assurance*
  - Senior undergraduates in CS, IT and EE
- Imperatives
  - Provide graduates with knowledge of, and appreciation for, information system security
  - "What do I wish MY undergraduate program provided?"
- Theory and practice: classroom instruction and competitive security exercises

Classroom Instruction

- There is no substitute for hands-on learning, especially in security
- Alternating lectures and practical exercises, plus labs
- Active, self-guided learning
  - "STFW and RTFM"
  - "Google is your ~~fiend~~ friend"

Capture the Flag Scrimmage

- Head-to-head competition between groups
  - Objective: gather others' flags while protecting your own
  - Combination of offense and defense
  - Free form; loose rules of engagement
- Deliverables
  - Action plans
  - 'Flags found'
  - After action reviews
- Observations
  - Teamwork and a good plan carried the day
  - First contact with exercise conditions was an eye-opener
  - Several students showed a visible increase in enthusiasm

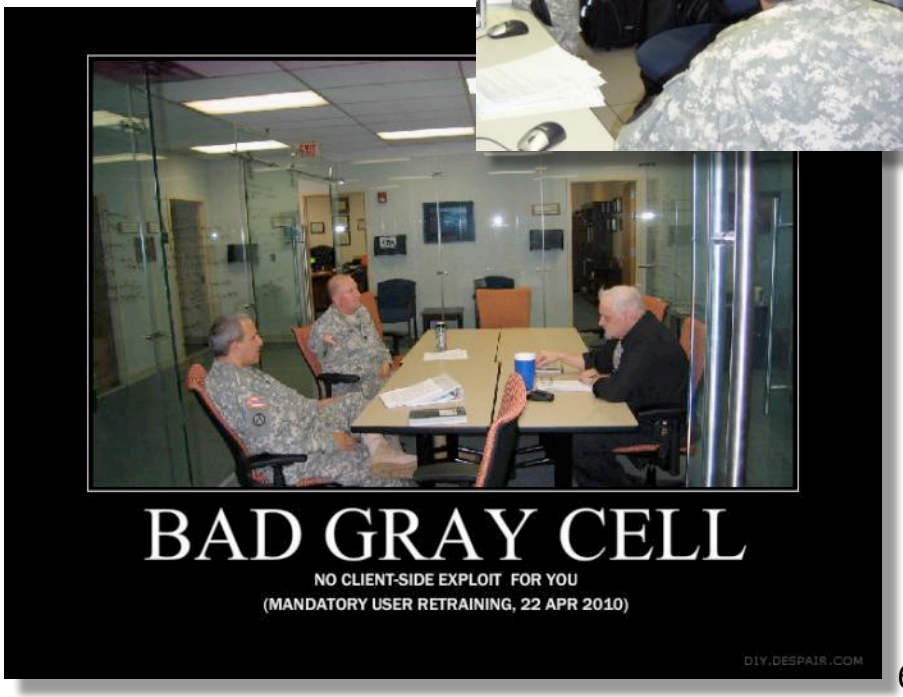


NSA/CSS Cyber Defense Exercise (CDX)

- Annual, week-long exercise
- Students design, implement and defend a 'Blue Cell' network
- NSA provides a headquarters 'White Cell' and attacking 'Red Cell'
- Scoring is based on preserving confidentiality, integrity and availability, plus accomplishing 'injected' security tasks
- CDX serves as our capstone exercise

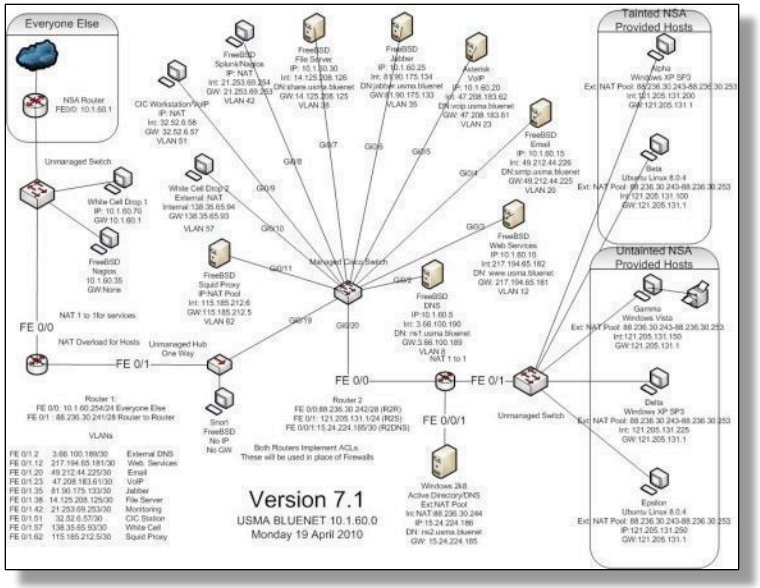
Updated Features in CDX 2010

- More realistic representation of client side threats
- Administrator "hands-off"
  - No 'process whack-a-mole'
  - Penalty for user disruption
- Patch freeze
  - Virtual 0-days
- Tainted hosts
- Live user 'Grey Cell'
- Acceptable use policies



CDX Preparation Phase

- Students design a network conforming to a network specification and a notional budget
  - Services: web, e-mail, DNS/AD, chat, file server, VoIP, PKI
  - Safeguards and infrastructure
  - 'Defensible' network architecture
  - COA development

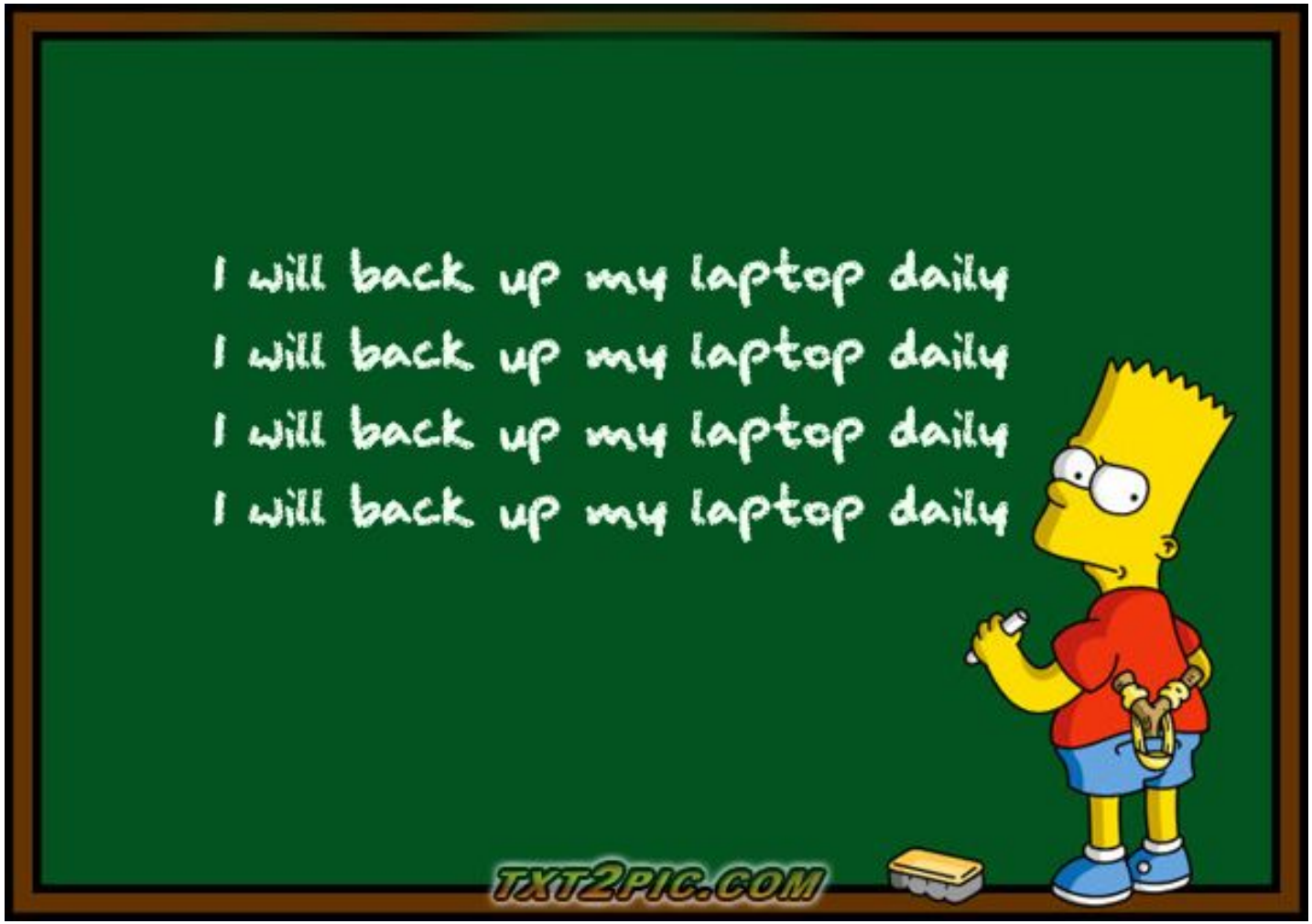


- Students implement their network from 'bare metal' and installation media

CDX Live Phase

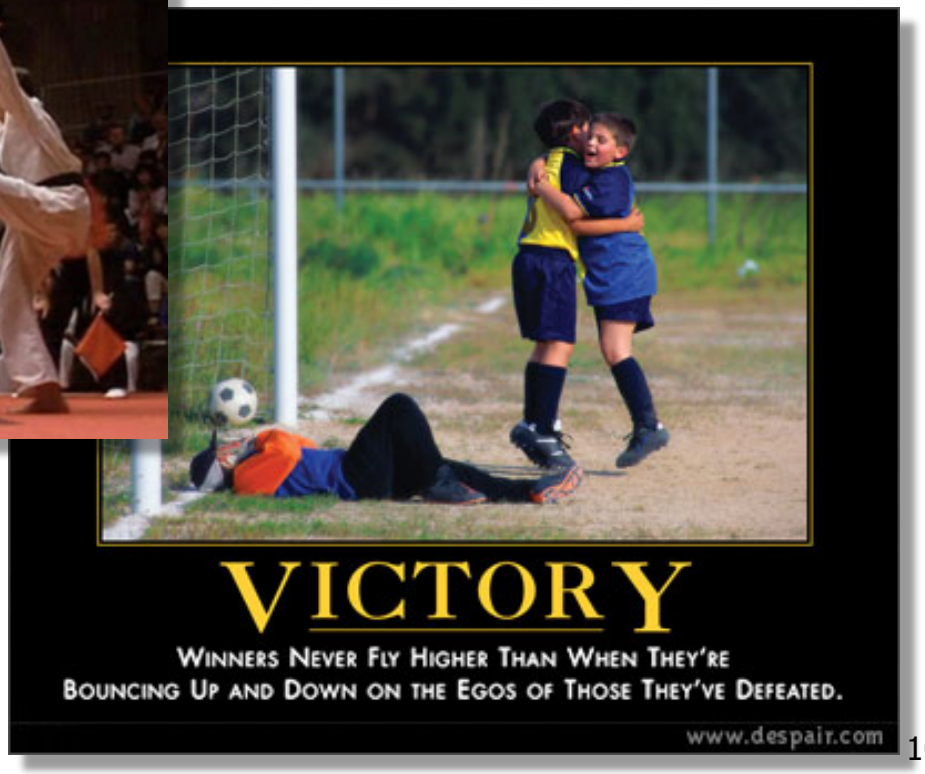
- Week-long, 0700 – 2200 daily
- Red Cell operates full time
  - Flooding DOS and on-site attacks are out of scope
  - Publicly disclosed vulnerabilities only
  - Limited social engineering
- Incident response
- Reporting
- Injects, e.g.
  - Forensic analysis
  - Technical orders
  - Web crawler
  - "General's laptop"

Lessons Learned



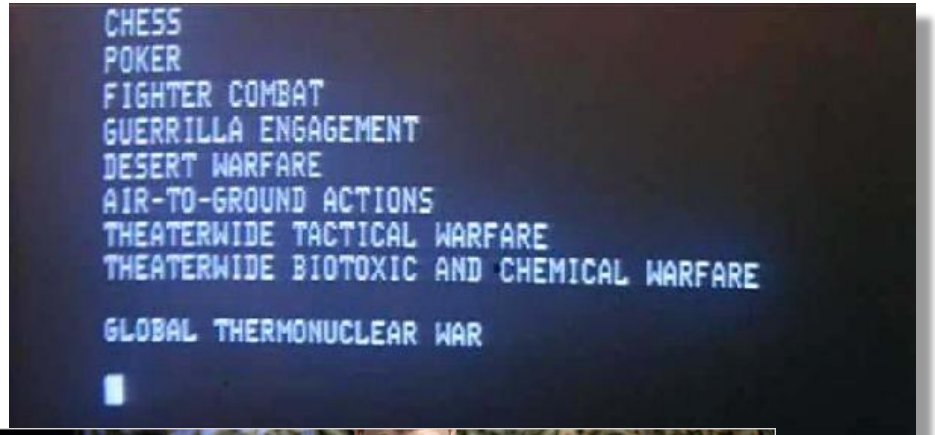
The value of competition

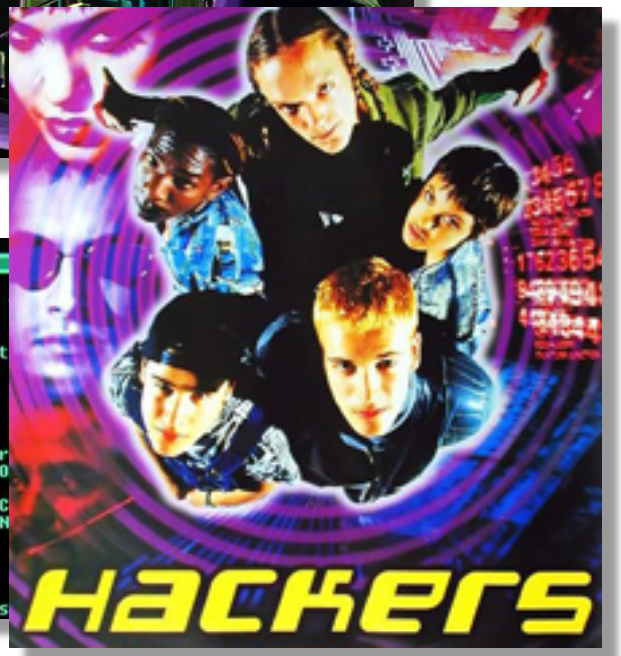
- Competitions capture the imagination
- We see greater effort than for grades alone
- Team working



Security makes the 'other stuff' more interesting

- Security can serve as a 'lure' that builds interest otherwise 'boring' material





They don’t know what they don’t know

- It is easy to underestimate the inexperience of undergraduates
- Assignments can guide students to producing deliverables they don’t know that they need

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told Weekly World News.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"As dangerous as this technology is right now, it's going to get much scarier," Yabenson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

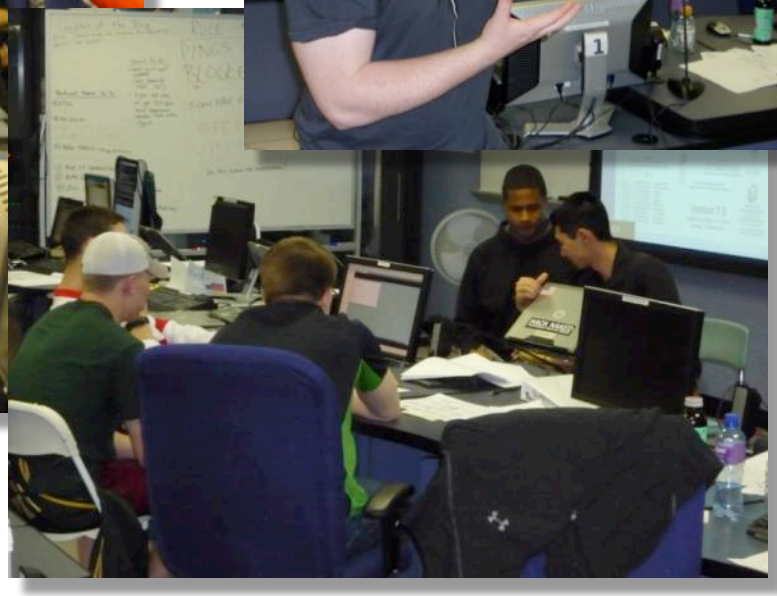
Sickos can wreak death and destruction from thousands of miles away!

Arnold Yabenson.

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

It takes longer than they think it will

- Time estimation is hard, especially for undergraduates
- Written estimates and back briefings
- Annual CDX 'death march' – not entirely bad…

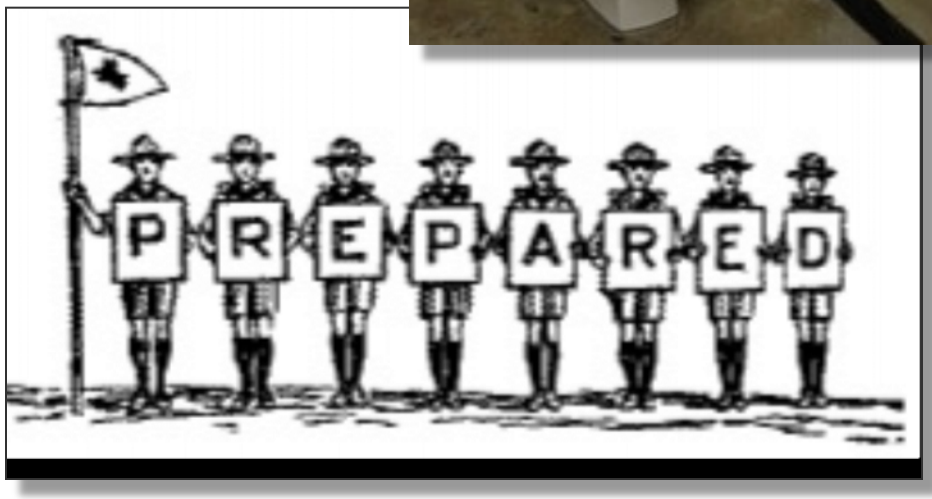


Students often miss the obvious, but learn from doing so

- Sometimes the 'easy way' really IS the easy way
- After action reviews are essential for learning from missing the obvious

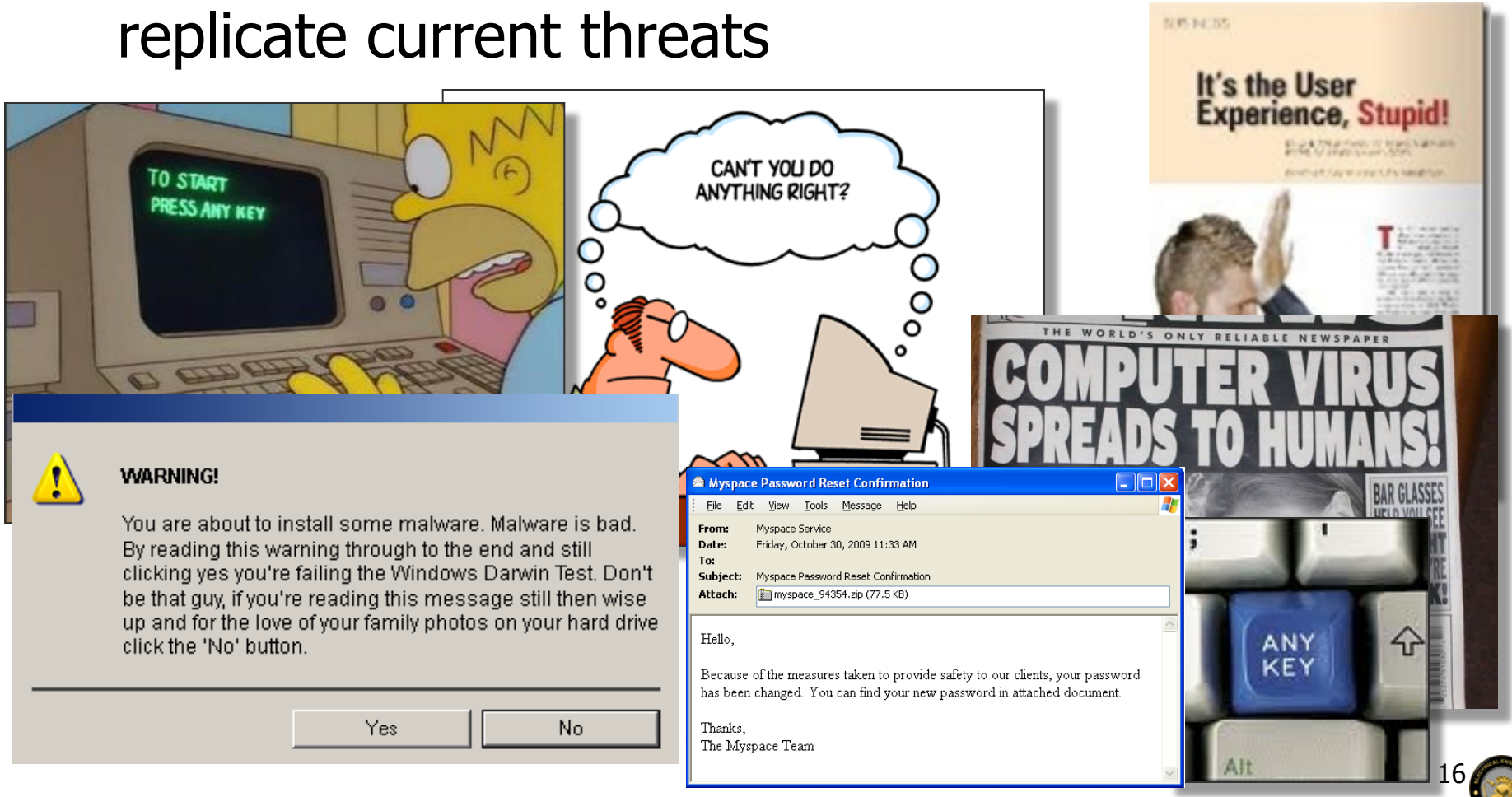
The value of preparation

- Preparation usually trumps inspired improvisation
- Have a plan….and a backup…or two



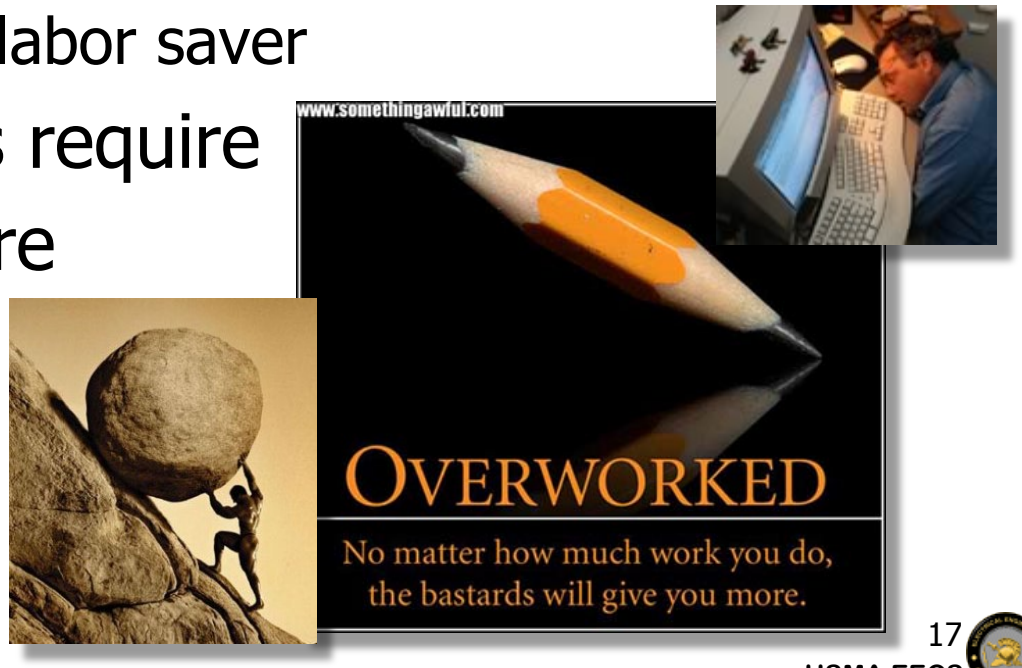
Replicating the client side is hard, but important

- The client side is as important as the server side
- Replicating users is difficult but necessary to replicate current threats



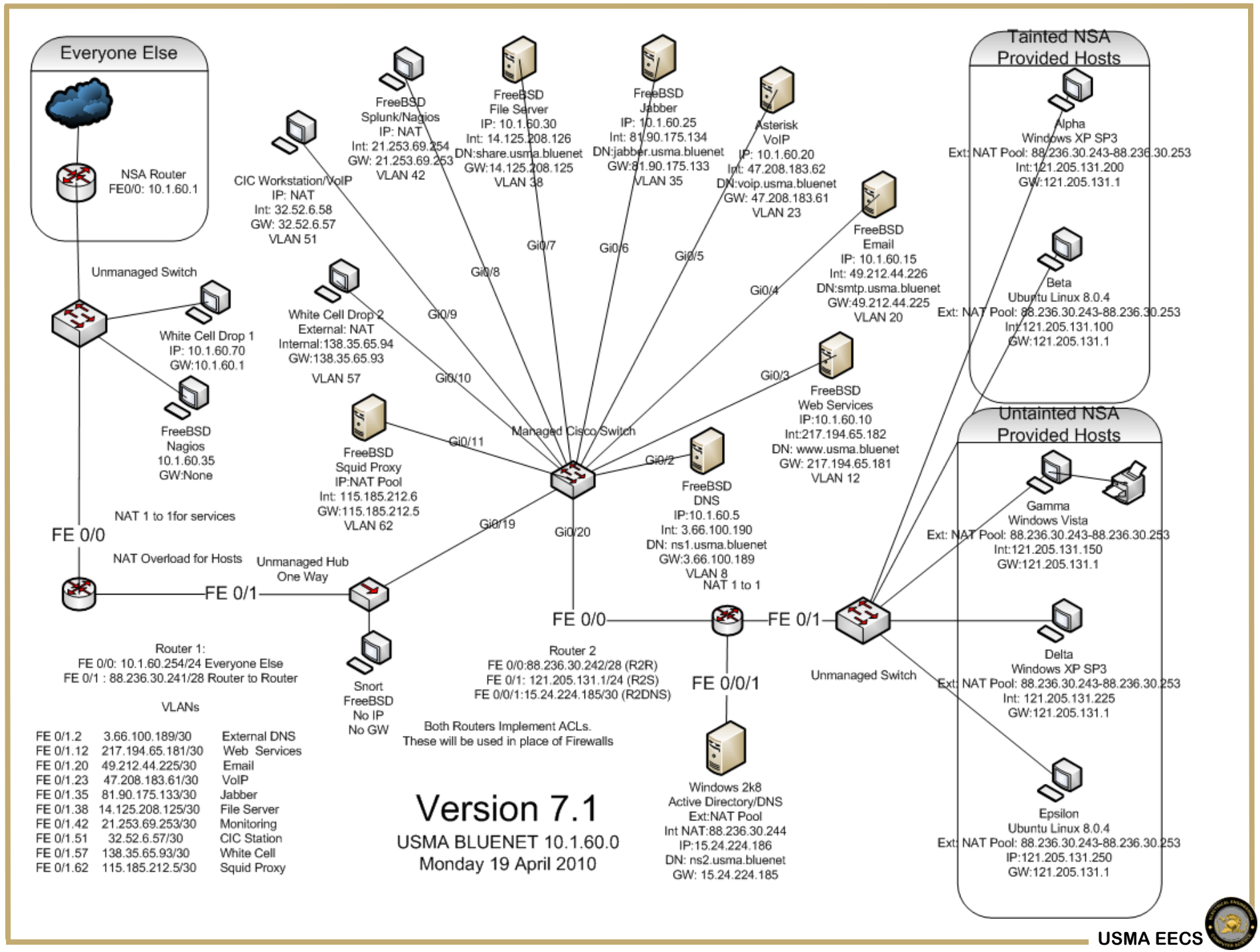
Security courses are among the most time consuming and resource intensive

- Some subject areas need little updating
- Security principles may change little, but practical details change constantly
  - New technology, protocols, software
  - Threats, exploits and vulnerabilities; new and obsolete
  - Virtualization is a key labor saver
- Competitive exercises require even more effort, but are worthwhile



Experiences with practice-focused undergraduate security education

Robert L. Fanelli and Terrence J. O'Connor
Department Electrical Engineering and Computer Science
United States Military Academy, West Point, NY, USA


Everyone Else
NSA Router
FE0/0: 10.1.60.1
Unmanaged Switch
White Cell Drop 1
IP: 10.1.60.70
GW:10.1.60.1
FreeBSD
Nagios
10.1.60.35
GW:None
NAT 1 to 1for services
FE 0/0
NAT Overload for Hosts
FE 0/1
Unmanaged Hub
One Way
Snort
FreeBSD
No IP
No GW
Router 1:
FE 0/0: 10.1.60.254/24 Everyone Else
FE 0/1 : 88.236.30.241/28 Router to Router
VLANs
FE 0/1.2 3.66.100.189/30 External DNS
FE 0/1.12 217.194.65.181/30 Web Services
FE 0/1.20 49.212.44.225/30 Email
FE 0/1.23 47.208.183.61/30 VoIP
FE 0/1.35 81.90.175.133/30 Jabber
FE 0/1.38 14.125.208.125/30 File Server
FE 0/1.42 21.253.69.253/30 Monitoring
FE 0/1.51 32.52.6.57/30 CIC Station
FE 0/1.57 138.35.65.93/30 White Cell
FE 0/1.62 115.185.212.5/30 Squid Proxy
CIC Workstation/VoIP
IP: NAT
Int: 32.52.6.58
GW: 32.52.6.57
VLAN 51
FreeBSD
Splunk/Nagios
IP: NAT
Int: 21.253.69.254
GW: 21.253.69.253
VLAN 42
FreeBSD
File Server
IP: 10.1.60.30
Int: 14.125.208.126
DN:share.usma.bluenet
GW:14.125.208.125
VLAN 38
FreeBSD
Jabber
IP: 10.1.60.25
Int: 81.90.175.134
DN:jabber.usma.bluenet
GW:81.90.175.133
VLAN 35
Asterisk
VoIP
IP: 10.1.60.20
Int: 47.208.183.62
DN:voip.usma.bluenet
GW: 47.208.183.61
VLAN 23
FreeBSD
Email
IP: 10.1.60.15
Int: 49.212.44.226
DN:smtp.usma.bluenet
GW:49.212.44.225
VLAN 20
FreeBSD
Web Services
IP:10.1.60.10
Int:217.194.65.182
DN: www.usma.bluenet
GW: 217.194.65.181
VLAN 12
White Cell Drop 2
External: NAT
Internal:138.35.65.94
GW:138.35.65.93
VLAN 57
FreeBSD
Squid Proxy
IP:NAT Pool
Int: 115.185.212.6
GW:115.185.212.5
VLAN 62
Gi0/9
Gi0/8
Gi0/7
Gi0/6
Gi0/5
Gi0/4
Gi0/3
Gi0/10
Gi0/11
Gi0/2
Gi0/19
Gi0/20
Managed Cisco Switch
FreeBSD
DNS
IP:10.1.60.5
Int: 3.66.100.190
DN: ns1.usma.bluenet
GW:3.66.100.189
VLAN 8
NAT 1 to 1
FE 0/0
FE 0/1
Router 2
FE 0/0:88.236.30.242/28 (R2R)
FE 0/1: 121.205.131.1/24 (R2S)
FE 0/0/1:15.24.224.185/30 (R2DNS)
FE 0/0/1
Windows 2k8
Active Directory/DNS
Ext:NAT Pool
Int NAT:88.236.30.244
IP:15.24.224.186
DN: ns2.usma.bluenet
GW: 15.24.224.185
Both Routers Implement ACLs.
These will be used in place of Firewalls
Unmanaged Switch
Tainted NSA Provided Hosts
Alpha
Windows XP SP3
Ext: NAT Pool: 88.236.30.243-88.236.30.253
Int:121.205.131.200
GW:121.205.131.1
Beta
Ubuntu Linux 8.0.4
Ext: NAT Pool: 88.236.30.243-88.236.30.253
Int:121.205.131.100
GW:121.205.131.1
Untainted NSA Provided Hosts
Gamma
Windows Vista
Ext: NAT Pool: 88.236.30.243-88.236.30.253
Int:121.205.131.150
GW:121.205.131.1
Delta
Windows XP SP3
Ext: NAT Pool: 88.236.30.243-88.236.30.253
Int: 121.205.131.225
GW:121.205.131.1
Epsilon
Ubuntu Linux 8.0.4
Ext: NAT Pool: 88.236.30.243-88.236.30.253
IP:121.205.131.250
GW:121.205.131.1
Version 7.1
USMA BLUENET 10.1.60.0
Monday 19 April 2010

CS482 Topic Listing

- Incident Handling
- Security Fundamentals
- Network Fundamentals
- Lab 1: Network Concepts Review
- Securing Unix PE
- Network Tools
- Network Tools PE
- Securing Windows PE
- Lab 2: Domain Name System
- Securing Web Apps
- Audit and Vulnerability Assessment PE
- Confidentiality and Cryptography
- Encryption Protocols and Tools
- Lab 3: Active Directory
- Encryption Protocols and Tools PE
- MITM / Session Hijacking PE
- Vulnerabilities and Exploits
- Metasploit PE
- Lab 4: Securing Services
- Hiding Data / Covering Tracks
- Hiding Data / Covering Tracks PE
- Network Security Monitoring
- Network Security Monitoring PE
- Lab 5: CTF Scrimmage
- Defensible Network Design
- William Cheswick Presentation
- CDX COA Briefings
- Ed Skoudis Presentation
- Lab 6: CDX Implementation
- Digital Forensics
- Wireless Security