IT Security @ Cornell

IT Security Office
Wyman Miles, CISO
Glenn Larratt, Sr. Security Engineer
Overview -- ITSO

• Part of the IT@Cornell organization
• 9 staff – CISO, Deputy, 5 Sr. Security Engineers & 2 Operations Engineers
• Works closely with Counsel, Audit, law enforcement, etc.
• Responsible for the security of Cornell information, operational stability of the IT ecosystem, IT Policy, certain aspects of Privacy
IT @ Cornell

- Central: 270 employees
- Departments: 670 employees
- On any given day, 65000 devices active on campus
  - 35000 of those are on wireless
Security Incidents

• 500 system compromises per year
  – \(\frac{3}{4}\) are student systems on wireless
  – Almost all are drive-bys, heavily weighted towards Windows
  – Fortunately, very few put regulated data at risk

• Another 1500 password thefts per year

• Assorted web defacements, stolen devices, and other events account for 100+ more incidents/yr
Threat Landscape

- Cybercrime
- Espionage – Industrial and National
- Hacktivism
- Attacks against the university (50K/day, typically)
- Attacks from the university (???)
- Internal actors, direct and incidental
Regulatory Landscape

• We are a 30000 person city that runs its own bank, insurance company, medical clinic, refuse collection, power generation, potable water treatment, hotel, animal hospital, law enforcement agency, and hazmat team

• Oh, and the next Nobel Prize lurks somewhere within its 100 buildings and 2800 acres

• You name it, it applies: FERPA, HIPAA/HITECH, PCI, SOX, GLBA, FISMA, FERC/NERC, …
Guiding Principles: The Textbook

- Confidentiality, Integrity, and Availability
- Or, as most people think of it:
  - Secrecy
  - Get Security Out of the Way
  - Huh?
- Administrative, Technical, Physical
- Defense in Depth
- Least Privilege
Guiding Principles: Cornell

- Separation of Duties
- Minimal Access to Log Data, Zero Access to Content
- Data Stewardship
- *We are a cog in the risk management apparatus of the university*
1988: Morris Worm
1998: Melissa
2003: Sasser
2006: Drive-Bys
2009: USB Bot
2011: Zeus, ZeroAccess

Exploits are an educational experiment
Exploits are an ego experiment
Exploits drive an underground economy
(Revealed) Exploits are a matter of national security

Computers are the target
People are the means
People are the target
The Objective is Data
Defending Cornell: Now

- Rudimentary network filtering across 80% of networks
- Network intrusion detection
  - FireEye
  - SIEM
  - Homegrown
- Log analysis
- Managed Antivirus
- Managed Encryption
- Vulnerability Scanning
- University Policy
  - Data classification and safeguards
  - Network registry
  - Accounts and access control
  - Data Governance
Defending Cornell: Future

- We need to shift to a preventative posture
  - *Risk Assessments, Risk Assessments, Risk Assessments*
  - *Re-align the program with FISMA, FedRAMP, and NIST*
  - *Application vulnerability management*
  - *Penetration testing*
  - Firewalls with Unified Threat Management – *coming 2015*
  - Virtual Desktops
  - Increased encryption
  - Data-loss prevention
  - Multifactor Auth

- Policy re-aligned to meet new threats: espionage and cybercrime
(Hopefully) Interesting Reading

- NIST-800: http://csrc.nist.gov/publications/PubsSPs.html
- FISMA: http://csrc.nist.gov/sec-cert/
IT Security Ops – Priorities / Customers

• “The Data” is our first priority
  – Networks designed based on data contained therein
  – First question we ask in incident response
  – Data types and data stewards

• Our customer base
  – End users
  – Netadmins / local Sysadmins
  – Investigative/administrative units within the University
IT Security Ops – Defense in Depth

• There is no, no, **NO** silver bullet
• …nor fire-and-forget
• Layered defense – one layer catches what another misses
• Firewalls, encryption, and AAA are obvious layers
• Less obvious layers include policy, detection, incident response, and trained analysts
IT Security – Services

• Antiphishing / SafeDNS
• Network Quarantine / PASS
• Endpoint Protection
• Remote Access via VPN
• Full-disk and other encryption
• Edge ACL’s
• Proactive vulnerability scanning
IT Security – SIEM

• Security Information/Event Management
• Listens to network traffic at the core
• Receives AAA, IDS, and other logs
• Correlation / Corroboration / Investigation
IT Security – Detection (Network)

• Tap on the network core, feeding:
  – Flow processor of our SIEM
  – FireEye IDS
  – Bro IDS

• NetFlow – Server Farm and Border routers
  – Spike alerts
  – Traflog
IT Security – Detection (logs)

- AAA logs from most systems on campus
  - Look for obvious patterns of compromise

- IDS logs from our several such systems
  - Postprocess, correlate, check with bad actor info
IT Security - Consulting

• “How do I use this service?”
• “Why doesn’t my network work as expected?”
• “Is this (old) firewall really giving me any value?”
• Security Assessments
• Security planning for new IT projects
IT Security – Incident Response

- Again – it’s the data
- What data was there?
- What capabilities did the attacker have?
- Analyze a large volume of technical data…

…to reach a simply-stated likelihood of data loss, for a committee of university executives
Incident Response

- Volatile data is important
- Modern malware is encrypted
- Acquire RAM and disk image
- Contain communications
- Restore user work environment
Threat Landscape

• Older
  – Trojan horses
  – Viruses
  – Worms (network, USB)
  – Denial of Service (DoS) attacks

• Newer
  – Phishing
  – Drive-by downloads
  – Distributed Denial of Service (DDoS) attacks
  – Web application attacks
Phishing

• Trick the user into giving information (social engineering)
• Trick the user into executing malware
• Methods
  – URLs in
    • e-mail, instant messages, social media, SMS
  – Attachments
  – Phone calls
You will not be able to send/receive more emails until you visit the below helpdesk link to restore your email access within 48-hours.

Copy/click [http://www.strud.com/forms/forms/form1.html](http://www.strud.com/forms/forms/form1.html)

System Administrator
201.285.2331

This message is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged, confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy, or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately either by phone (803-469-8536 or 803-469-6900) or reply to this email and delete all copies of this message.
This message was sent with High importance.

From: FedEx Delivery Post <info@fedex.in>
To: Recipients
Cc: 
Subject: We Have A Package For You On Our Desk
Attachments:  FEDEX PARCEL.doc (27 KB)

Open Attached
Claim Your Tax Refund Online

We identified an error in the calculation of your tax from the last payment, amounting to $419.95. In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.
Registration

Please attach a card to your account by entering the details below. (on this card you will receive your refunds)

NOTE: On this card you will receive your refunds.

*Cardholder Name (Required):

*Card Number (Required):

*Card Expiry Date (Required):

3 digit number found on the back of your card

Continue

e-services Privacy Policy
CUWebLogin

NetID: 
Password: 
Login

What is this?
I forgot my password!
I don't have a NetID, now what?

To log out, you must Exit or Quit your browser.

Caution: Always check your browser's address bar before you enter your NetID password to make sure the address starts with https://web*.login.cornell.edu/ (where web* is either web1, web2, web3 or web4).

CUWebLogin is a component of Cornell University's central authentication service. If you are unsure of the authenticity of any online University service, please contact the IT Service Desk.

This service and the services to which it provides access are for authorized use only. Any attempt to gain unauthorized access, or exceed authorized access, to online University resources will be pursued, as applicable, under campus codes and state or federal law.

© 2006 Cornell University. All Rights Reserved.
Drive-by Downloads

- Installs malicious software without user’s knowledge or consent
- Vector typically is a compromised web site or malicious advertisement
- Goal: exploit a vulnerable system and execute a “dropper” that downloads malware du jour
How do they work?

- Web-based exploit kits
- Hidden iFrame or redirect to malicious Javascript, usually obfuscated
- JS determines environment
  - OS platform, browser version, plugins installed
- Delivers tailored exploits based on results
- Exploits typically attack
  - Web browser
  - Plugins
    - Java
    - Adobe Flash
    - Adobe Reader
Popular Malware on Campus

- Fake anti-virus
- FBI ransomware
- ZBot
- ZeroAccess
- Flashback
DDoS

• Use voluminous resources around the Internet to conduct attack
• Source can be
  – Botnet
  – Open or insecure services
    • DNS
    • SNMP
**Distribution:**
Attacker's Botnet Hosts

**Reflection:**
SNMP Vulnerability

**Target:**
Hit With Reflected Amplification DDoS Attack

Results for Target:
- Network
- Hosts
- Websites
- Applications

Step 1:
Attacker Sends Command to Botnet
"Send Forged SNMP Query to All Bots" at ISPs 1 - 4

Step 2:
Bots Send SNMP Queries to All SNMP Devices at ISPs 5 - 8, Using Forged IP Address of Target

Step 3:
Vulnerable Devices Respond to Forged Queries, Repeating En Masse to Target
DNS Amplification Attack

Step 1: Attacker sends signal to activate bots.

Step 2: User’s Primary DNS Servers (Recursion Allowed).
Question: What is the IP Address of some-webserver.com?
Answer: Here is the IP Address of some-webserver.com.

Step 3: Question: Where can I find the IP Address of some-webserver.com?
Answer: I don’t know but .com NameSpace should have the answer.

Step 4: Not authoritative for some-webserver.com.

Step 5: Question: What is the IP Address of some-webserver.com?
Answer: Primary DNS Server of some-webserver.com knows it.

Step 6: Question: What is the IP Address of some-webserver.com?
Answer: Primary DNS Server of some-webserver.com knows it.

Step 7: Question: What is the IP Address of some-webserver.com?
Answer: Here is the IP Address of some-webserver.com.

Step 8: Answer: Here is the IP Address of some-webserver.com.

Step 9: Answer: Here is the IP Address of some-webserver.com. Each reply can be amplified up to a factor of 73.

Step 10: Victim’s Server Victim IP Address.
Case: SpamHaus

- Largest DDoS reported in history
- Estimated that over 30,000 resolvers were used
- Each 36 byte query resulted in a 3 kilobyte response (100x amplifier)
- Over 90 Gb/s smashed SpamHaus servers
  - More than 300 Gb/s at Tier 1 and 2 providers
Web Application Attacks

• OWASP

• Common attacks
  – SQLi
  – XSS
  – CSRF

• Common goals
  – database access
  – credential stealing
  – malware hosting
  – spam hosting
Prevention

• It’s all about the layers
  – Nextgen firewall
  – Endpoint protection
  – Patch management
  – Vulnerability management
  – Awareness training

• OS protection
  – ASLR
  – DEP
  – EMET (Windows)

• Penetration Testing