Why Everyone Is On The Security Team

Chris Todd
Unisys Canada Inc.

Who is Chris Todd?

- Security Consultant with Unisys Canada Inc
  - 10+ years experience in networking and security
  - GIAC Certified Firewall Analyst (GCFW), Incident Handler (GCIH), and Penetration Tester (GPEN)
  - Maintain a PCI DSS compliant environment
  - Provide security audit, vulnerability assessment and penetration testing services internally and externally

- SANS Mentor
  - Currently teaching Security 504: Hacker Techniques, Exploits & Incident Handling

Ready for a ride?

Security fail of the year
Honorable mention

Canadian federal government

- Finance Department and Treasury Board taken offline
- Defence Research and Development Canada another target
- Spear phishing senior Finance Department personnel

State of Texas

- PII of 3.5 million Texans publicly accessible for about a year
- Name, address, Social Security numbers, and possibly dates of birth and drivers license numbers
- Free credit monitoring offered could cost $21 million

Sony

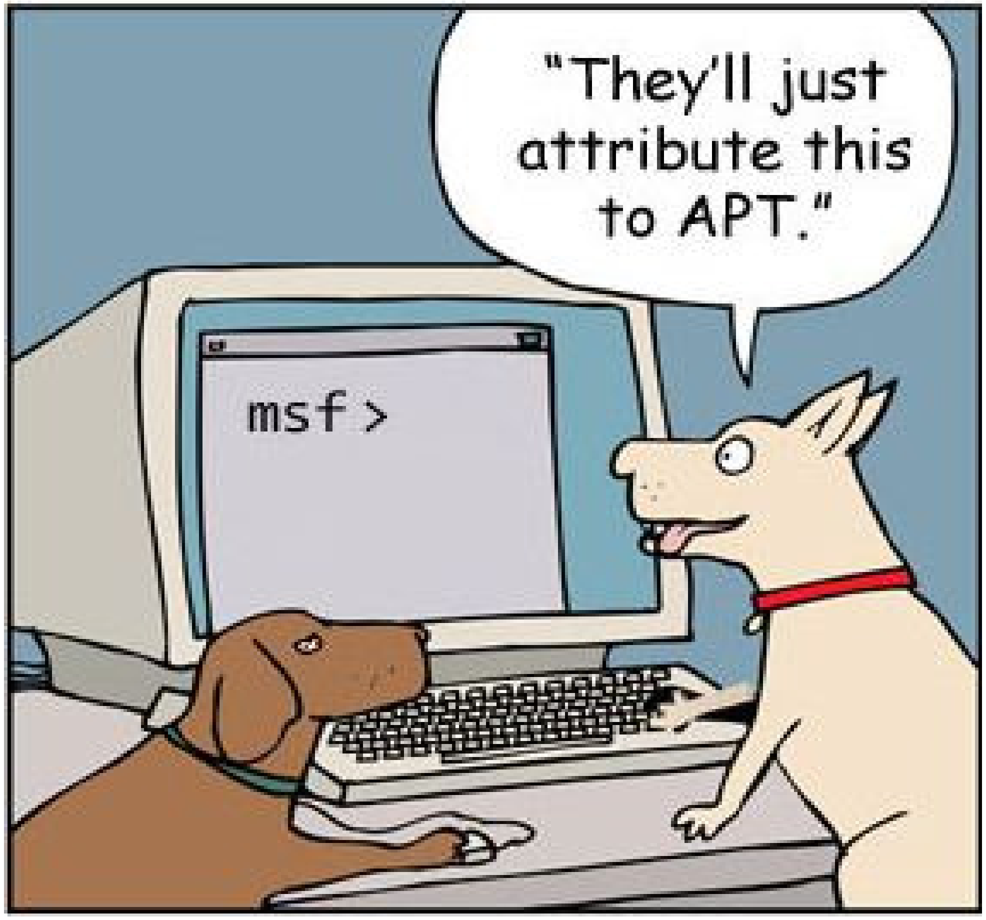
- PII and possibly cc of 77 million users stolen
- Replacement cc about $3 - $5
- Cost to Sony - $1.5 billion

Security fail of the year
Second runner up…

RSA

- Data stolen related to SecurID technology
  - RSA response:
    - *“confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers”*
  - That’s great, but...
    - *“this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack.”*
  - 40mil tokens deployed, 250mil mobile software versions
  - Claimed to be Advanced Persistent Threat (APT)
    - i.e. blame it on China

Another security pro’s take on APT



http://blog.zeltser.com/post/4523882852/apt-cartoon-two-dogs

‘Cause APT is too serious to be taken seriously.

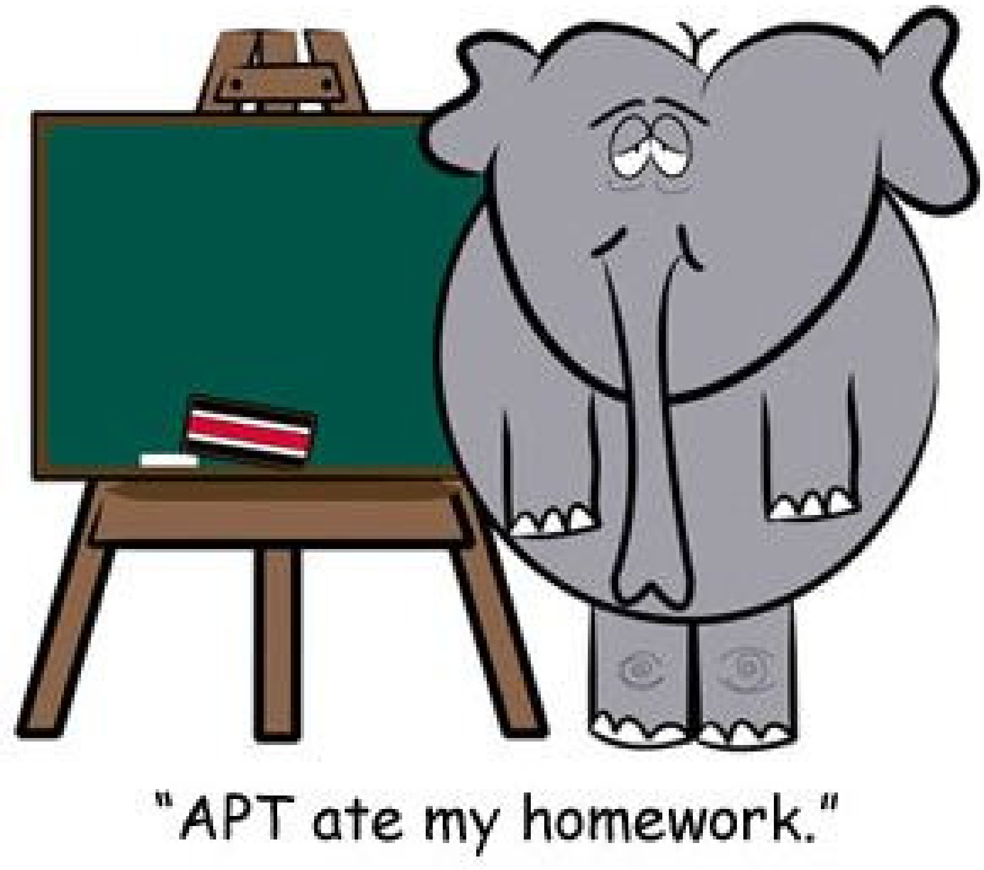
– *Lenny Zeltser*

Security fail of the year
First runner up…

Comodo

- Attacker used a valid username and password to issue nine valid SSL certificates
  - mail.google.com, login.live.com, www.google.com, login.yahoo.com, login.skype.com, addons.mozilla.org
- Calls into question entire SSL infrastructure
  - 1500 CA certificates controlled by 650 organizations (eff.org)
  - You trust all of them!
- Initially blamed on APT, but this time from Iran
  - A lone Iranian hacker took credit for the attack
  - Hacked into InstantSSL.it, an RA for Comodo

The APT scapegoat



http://blog.zeltser.com/post/4599814825/apt-cartoon-sad-elephant

Security fail of the year WINNER! (so far)

HBGary Federal

- A security company that sells its services to various three-letter federal agencies
- Pwned for poking “the Anonymous hive”
  - No APT!
- Anonymous intent on embarrassing them
- Let’s see how everyone is on the security team

Management

- Hbgaryfederal.com used a custom-built CMS
  - Plethora of COTS products benefit from a large user base
  - This decision was the entry point for the attack

- Also share responsibility for other areas of fail
  - Perhaps proper policies and procedures were not in place
  - Perhaps adherence to such was not sufficiently validated
  - Either way, basic security practices were not followed

Management – lessons

- Every application must be viewed as a potential target or entry point into your environment
  - Treat as such from product evaluation to production operation
    - And everywhere in between

- Ensure organization has what it needs to operate securely
  - Policies and procedures
  - Staff training
  - Validation – audit, pen test, etc.

Developers/DBAs

- The custom-built CMS had a gaping SQL injection hole
  - The exact URL was used to break in was: http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27
  - Sample SQL query
    - select [field] from [table] where [variable] = ‘[value]’;
  - The above URL could have been a SQL query something like:
    - select * from pages where pageNav = ‘2’ AND page = ‘27’;
  - One or other or both handled incorrectly by the CMS
    - Attackers grabbed the user database containing usernames, email addresses and password hashes
      - Simple MD5 password hashes, no iterative hashing or salting
      - Bring on the rainbow tables!
      - More on passwords shortly

Developers/DBAs – lessons

- Follow secure coding and database management practices
  - Plenty of guidance in this area – OWASP
  - Take advantage of it

- Ensure everything is coded securely
  - Even if it doesn’t seem important
  - Maybe everything on hbgaryfederal.com was for the public
    - But usernames, email addresses and passwords were not!

Security/test team

- HBGary sells security services
  - Should have had the skills on their security or test team to find SQL injection flaws
- Why wasn’t the SQL injection hole found earlier?
  - Was the security/test team careless and just missed it?
  - Or was the CMS never tested and the work of this third-party never validated?
- Why wasn’t the attack stopped earlier?
  - Took a few weekend hours to execute
  - Targets in various locations
  - Who really has a team that could stop that?

Security/test team – lessons

- Eat your own
- Validate third-party work
- Don’t skip step 1
  - Steps 2-6 of the incident handling process are crucial
    - Identification, containment, eradication, recovery, and lessons learned
  - But they won’t bail you out if you skip step 1
    - Preparation!

Password pop quiz

- True or False
  - Q1 - Your password should be kept short and simple so it's easy to remember.
  - Q2 - That simple password should be used everywhere so you never forget it.

(Please tell me you didn’t answer true!)

- Knowing what SHOULD be done ≠ what IS done
- Case in point, HBGary Federal CEO and COO

CEO and COO

- Passwords cracked for HBGary Federal CEO Aaron Barr COO Ted Vera
- Why?
  - Six lower case letters and two numbers
    - Available in any self-respecting rainbow table
    - FYI, mleafs67 is NOT a strong password
- Result?
  - Same password for email, Twitter, and LinkedIn
  - Vera – ssh access to support.hbgary.com
  - Barr – Google Apps email admin
    - Torrented email of Barr and HBGary CEO Greg Hoglund's email

CEO and COO – lessons

Pretty straight forward:

- Use long, strong passwords
  - >14 characters and complex not likely in rainbow tables
    - Maple-Leafs-'67 is much better
- Don't share them across systems
  - Especially those with different security requirements

System administrators

- support.hbgary.com fail
  - Ted Vera’s password gave external ssh access
  - Privilege escalation flaw provided root access
    - Patch released Nov 2010
    - Rated important, i.e. not critical
    - Typical vendor rating
  - Gigabytes of research and backup data purged
- rootkit.com fail
  - A site owned by HBGary CEO Greg Hoglund
  - Greg’s email used to social engineer sys admin
  - Stole email addresses and MD5 password hashes of registered users

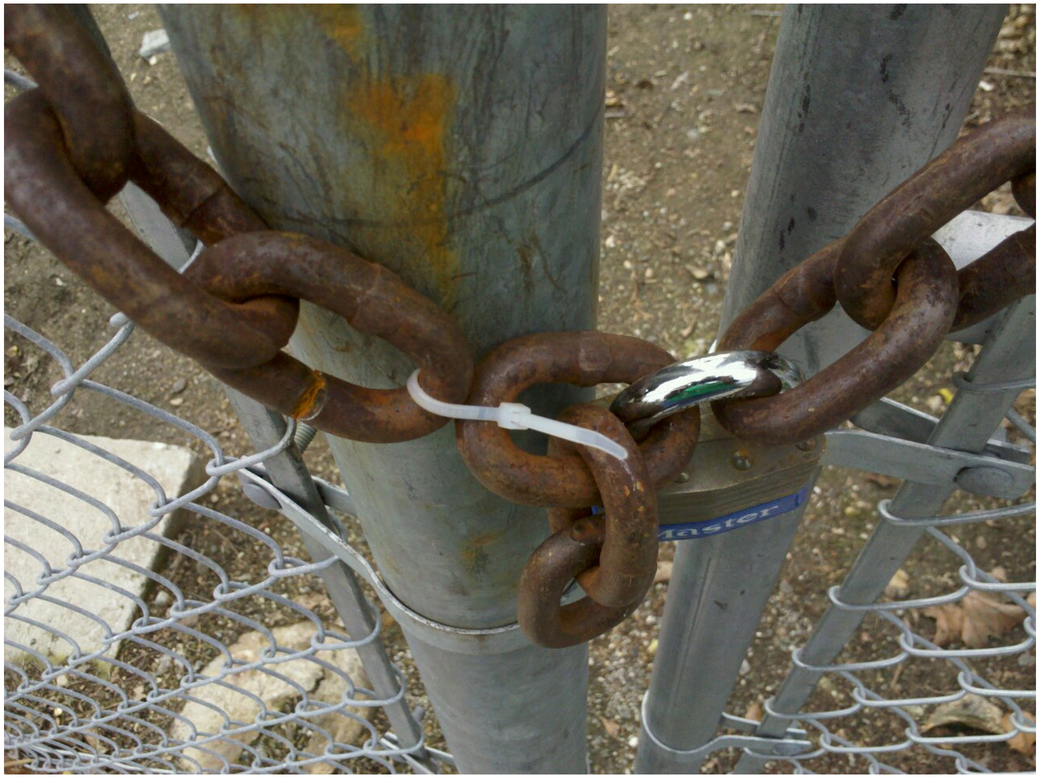
System administrators – lessons

Key term: two-factor

- Remote access
  - Require two-factor authentication
- Password resets
  - Require two-factor verification of requestor
    - Or at least one undisputable factor
- Admin access
  - May have prevented the email compromise
  - Supported in Google Apps since Sep 2010

Fail recap

- Management
- Developers/DBAs
- Security/test team
- CEO and COO
- System Administrators
- Miss anyone?
  - The janitor perhaps?
    - That’s for another day



Don’t be the zip tie!

Fail summary

EPIC FAIL
A fail that overflows fail's integer
and wraps right around and into a win.

Lesson recap

- Everyone must have knowledge of basic security practices
  - But it's not enough.
  - You all passed the pop quiz, right?
    - I'm sure Aaron and Ted would too

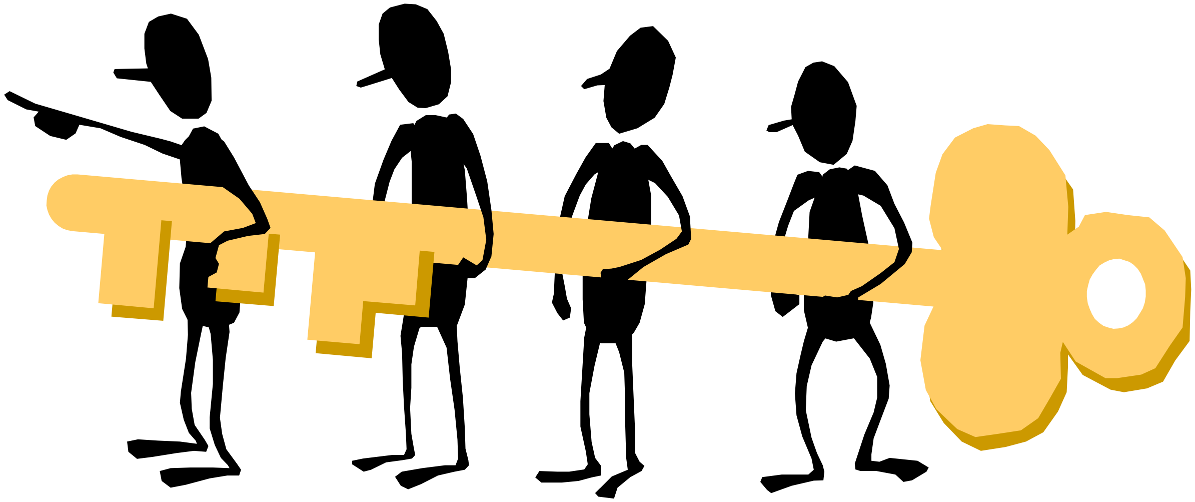
- Everyone needs to understand why what they do really affects an organization’s overall security posture
  - Ask the CMS developers or whoever decided to go with a custom-built CMS in the first place if they believe this

Lesson recap (cont)

- Everyone needs to appreciate that one careless or lazy move on their part can have dire consequences
  - Configuring ssh to use public keys takes about 2 minutes
  - A phone call takes 1
  - Too much to ask of the sys admins?
- Everyone needs to act with the care and rigor of a finely tuned security team
- Everyone needs to appreciate that they play an integral part in securing their organization

Lesson summary

Everyone is on the security team!



And the result

Or if you prefer...

Conclusion

Chris Todd

chris.todd@unisys.com
902-421-2460