Top 10 Dumbest Security Incidents

John Doan, CISSP

Sr. Program/Project Manager

Internal Revenue Service

Disclosures

- Information presented does not reflect the views or opinions of the Internal Revenue Service (IRS)
  - IRS does ask that I remind you to file and pay any taxes due by April 15

- No proprietary or confidential sources were used or referenced for the purpose of this presentation

About Me

1998 Kent State University Graduate, B.A. Psychology w/ Pre-Dentistry

Started career as Technical Recruiter for Tek Systems, Independence, OH

Certifications: A+, MCP, Citrix CCA, ArcSight, CISSP, ITIL v3

16+ years as IT Project/Program Manager
12+ years InfoSec/CyberSecurity

Married 12 years with 3 daughters, a cat and a leopard gecko

10 - Todd Davis

Impact: <10 Individuals

Root Cause: Poor judgment

Summary: Todd Davis admits to having his ID stolen at least 13 times. A thief used Todd's information to obtain a $500 cash advance loan. He was made aware of the breach when his wife received a call on her cell phone from a collection company. Additionally, Todd's information was used to obtain cell phone accounts which he also learned of through collection calls.

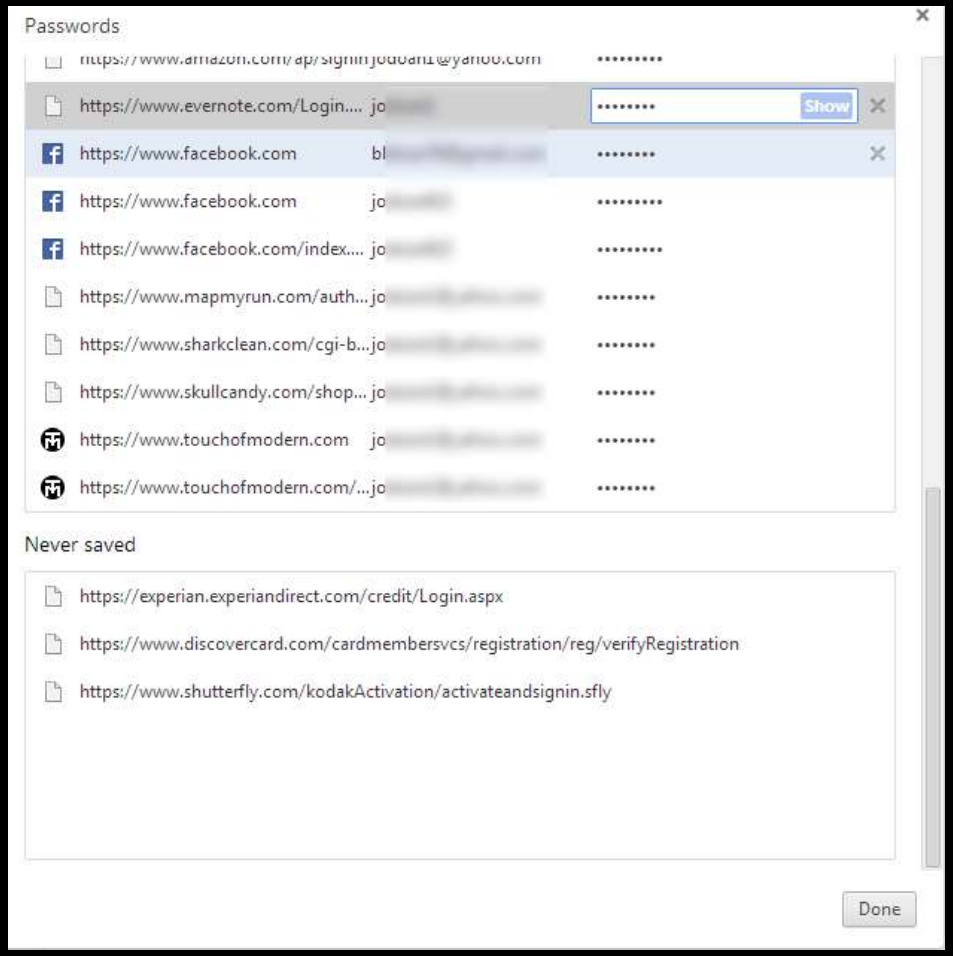
9 – Google Chrome Passwords

Impact: <10 Individuals

Root Cause: Application Vulnerability

Summary: Stored passwords in Google Chrome Browser can be accessed by all users with access to the machine by typing chrome://settings/passwords in the address bar. Google claims this is a feature and not a vulnerability.

Mozilla Firefox also enables users to see plaintext passwords. However, allows users to set a master password to access.



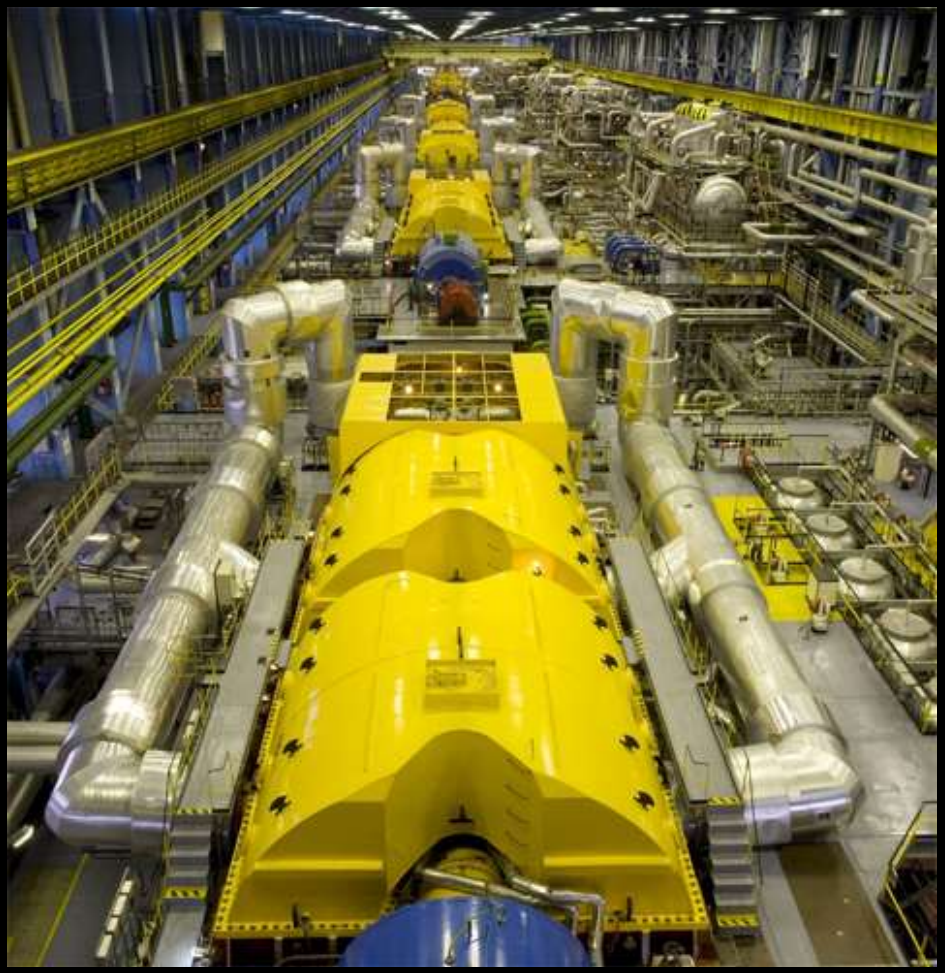
8 – US CERT

Impact: Unknown

Root Cause: Malware

Summary: US CERT reported a Stuxnet-like virus shuts down a power-plant when a contractor uses an infected USB drive to update a turbine control system. The workstations were not backed-up (ever) and were not running AV software.

Anti-malware was not installed on the workstations because according to CERT, they are not connected to the Internet.



7 – Apple IOS/OS X Goto Fail

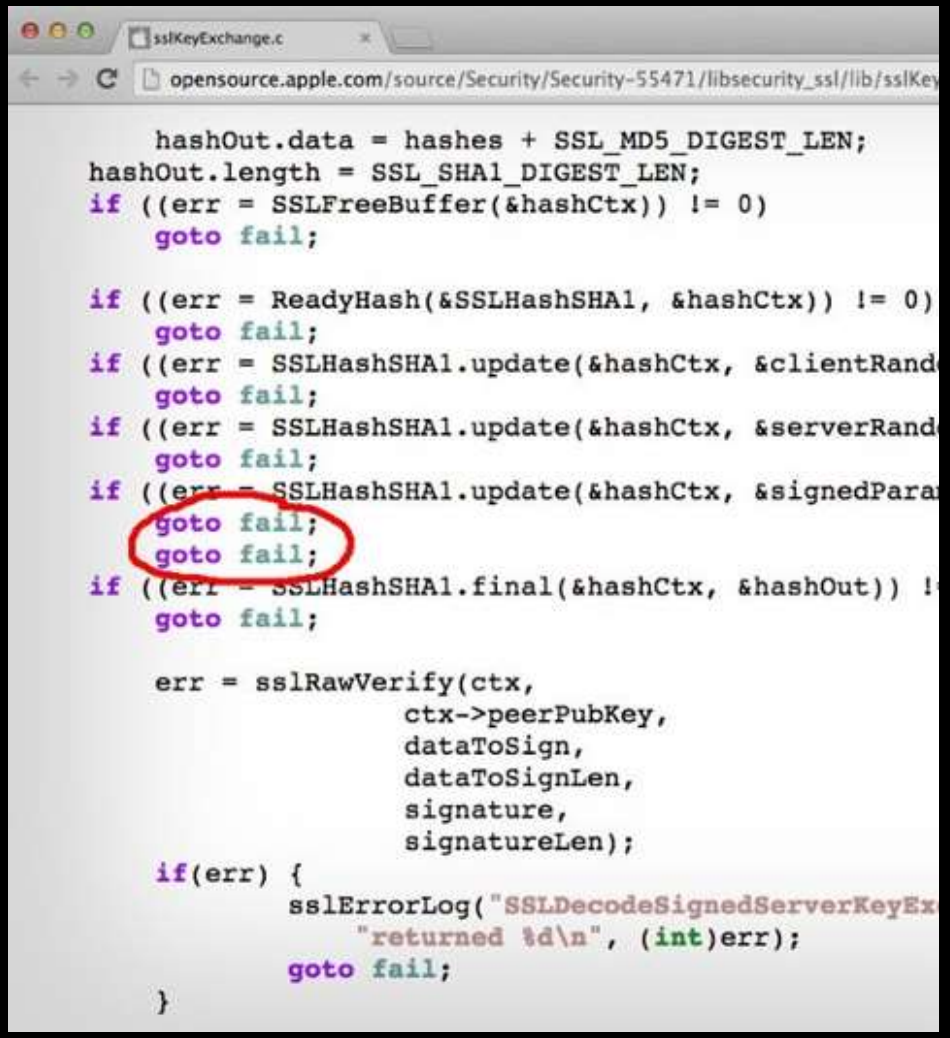
Impact: 100M+

Root Cause: Bad Code

Summary: Apple issued an emergency patch to fix an SSL vuln in IOS version 6+. The vuln breaks the SSL allowing a man-in-the-middle attack.

The vuln also affected OS X and remained unpatched for four days.

Timing of code introduction aligns with addition of Apple to NSA's PRISM program



6 – Healthcare.gov

Impact: 4M+

Root Cause: Bad Code, Denial, Politics

Summary: Numerous vulnerabilities that make the site susceptible to PHI and PII data leakage.

Kevin Mitnick writes, "It's shameful the team that built the Healthcare.gov site implemented minimal, if any, security best practices to mitigate the significant risk of a system compromise.“

Less than ½ of 1 vuln addressed in 3 months after launch.

5 – Experian

Impact: 1M+

Root Cause: Bad Process

Summary: Superget.info offered to sell millions of PII and credit cards it obtained from Court Ventures.

Experian acquired court ventures and allowed access to its database for over a year before Secret Service contacted them regarding the ongoing investigation.

Payment to Experian was in form of wire transfers from Singapore.

4 – US Dept of Veterans Affairs

Impact: 26.5M, $100M-$500M

Root Cause: Negligence

Summary: An employee copied the records of 26.5M veterans and active duty military personnel and spouses to an unencrypted laptop and external hard drive.

Records contained name, address, SSN and date of birth.

Largest US Government breach to date.

3 – EMC/RSA

Impact: 40M Tokens, $66.3M

Root Cause: Phishing

Summary: A phishing email was used to install backdoor Trojans allowing hackers to compromise their SecureID authentication platform.

Hackers subsequently used their knowledge to attack Lockheed Martin.

RSA sells security products that would have prevented the security breach.

2 – Sony PlayStation Network

Impact: 77M, $171M-$24B

Root Cause: Unpatched Systems

Summary: PSN was DDOS'd shortly after filing legal proceedings against George Hotz for system mods.

Sony has not stated explicitly the root cause of the attack but many security researchers conclude combination of SQL injection, unpatched backend servers and compromised accounts.

Customer name, email address, phone number and date of birth were stored in plain text.

Honorable Mention

Meetup

Meetup is currently unavailable

Update 3/2/14 at 8:09 pm EST

Over the past several days, Meetup has suffered a prolonged denial of service (DDoS) attack, resulting in intermittent service outages for our website and apps. We're working urgently to bring Meetup back and restore full functionality. We appreciate your patience.

For the latest information on the situation, we recommend that you follow Meetup on Twitter, Facebook, or check our blog.

Target

Impact: 70M, $3.6B

Root Cause: Malware, Unpatched Systems

Summary: Malware running on Target's POS systems were able to capture credit and debit card information. If a PIN was used, that information was also collected. Credit/debit cards may also contain name and address information of cardholder on its magnetic strip.

This attack could have been prevented if the US issued credit/debit cards contain smartchips (EMV). Target piloted the use of EMV cards but ultimately decided against the technology

References

http://www.eweek.com/security/usb-storage-drive-loaded-with-malware-shuts-down-power-plant/

http://gizmodo.com/5976680/two-us-power-plants-hit-by-malware-attacks

http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/