
Major Cyber Attacks I

John E. Savage
Brown University
Outline

• 1988 Morris Worm
• 2003 Titan Rain exfiltration attack
• 2007 Estonian attack
• 2007 Aurora Experiment at US Facility
• SCADA Infrastructure Threats
• 2010 Stuxnet attack against Iran facility
Morris Worm

• One of the most important pieces of malware.
• William Morris launched it from MIT on 11/2/88 to estimate the size of Internet
• Because of design error, each computer infected too many times and Internet slowed to a crawl.
• Estimated 10% of Internet computers affected — Included NASA, Berkeley, MIT & Pentagon computers
Morris Worm Construction*

• It infected VAX and Sun 3 systems running variants of 4BSD Unix OS.
• Exploited known vulnerabilities in **finger**, **sendmail**, **rsh/reexec** and weak passwords.
• One of the first pieces of malware to exploit a buffer overflow vulnerability, in **finger**.
• It invoked bug in debug mode of **sendmail**.

Morris Worm Prosecution

• Morris was the first person convicted under the 1986 Computer Fraud and Abuse Act.
• US Government Accountability Office estimated the cost of the damage at $10M – $100 M 😊
• Sentenced to 3 year probation, $10K fine, and 400 days of community service.
• DARPA was prompted to establish Computer Emergency Response Team (CERT) Coordination Center at CMU as a result.
Titan Rain

• U.S. government name for attacks on American computers believed to come from China circa 2003-2006
• Purpose was exfiltration of information.
• Hackers penetrated computers at State Department, Homeland Security, Lockheed Martin, Sandia National Labs, NASA, FBI etc..
• Identity of Titan Rain attackers unknown although they used Chinese computers.
Titan Rain

• Sandia Labs analyst Shawn Carpenter followed hackers into routers in Guangdong, China.
• Discovered stolen schematics of propulsion systems, Mars Orbiter technology, and more.
• Titan Rain attacks were made on Brits, Canada, Australia, New Zealand.
• Carpenter was initially welcomed by FBI but later declared persona non grata and fired by Sandia.
• Did he violate US law or threaten USG?
Estonian Attack

• In April 2007 Estonia moved Soviet-era “Monument to the Liberators of Tallinn” from city center to a cemetery, provoking outrage among ethnic Russians. (Now called the “Bronze Soldier.”)
Cyber Attack on Estonia

- In April, May 2007 Estonian parliament, banks, ministries, papers, & broadcasters under DDoS.

- Second-largest instance of apparent state-sponsored attack at the time.

- Attack appears to come from Russia although at least half the packets originated in US.
2007 Aurora Generator Attack

- March 4, 2007 Idaho National Lab conducted a test (dubbed Aurora) to show that 27 ton diesel power generator could be destroyed in three minutes via its control computer.

60 Minutes Video: http://www.youtube.com/watch?v=rTkXgqK1l9A
Aurora Attack

• Thus, electrical grid can be an attack vector.
• If a generator is disconnected from grid, it will speed up. If reconnected when it is out of synch with the grid, it will experience huge stresses and destroy itself. This is a SCADA (Supervisory Control & Data Acquisition) system attack.
• SCADA is used throughout national critical infrastructures:
  – Water, oil & gas pipelines, oil refineries, chemical
A Key Critical SCADA Vulnerability

• Electric and water companies use the DNP3 protocol to communicate with SCADA systems
• A security vulnerability allowed investigator to infiltrate a power station’s control center.
• Remote system can be crashed, illustrating that poor implementation of standards can present a serious security hazard.

[External Link: Electrical Grid is Called Vulnerable to Power Shutdown, Nicole Perlroth, NYT10/18/13](http://bits.blogs.nytimes.com/2013/10/18/electrical-grid-called-vulnerable-to-power-shutdown/)
Threats to Critical Infrastructures

• Electromagnetic Pulse (EMP) will fry all electronics, killing the electric grid
  – Produced by nuclear explosions in space, solar flares, and military weapons over limited areas

• Former FERC Chief worries about grid
  – If fewer than a dozen major substations are destroyed, lights in US can be turned out for months
  – Solution is decentralized system

See Former FERC Chief Jon Wellinghoff Speaks Out on Grid Security and Distributed Generation, by Chip Register, FORBES http://www.forbes.com/sites/chipregister1/2015/02/03/
former-ferc-chief-jon-wellinghoff-speaks-out-on-grid-security-and-distributed-generation/
Olympic Games

• Goal: sabotage the Iran nuclear refinement facility in Natanz. Joint effort of USG and Israel
• In July 2010 Stuxnet discovered.
  – Designed to destroy centrifuges
• In September 2011 Duqu discovered
  – Highly collects control system info; similar to Stuxnet
• In 2012 Flame discovered
  – Designed primarily for reconnaissance in Natanz
• In 2014 Regin discovered
  – Designed for long-term reconnaissance
Stuxnet 1.x

• Computer worm discovered in July 2010; existed for ≥ 1 year.
• Designed to degrade and destroy centrifuges at Iranian uranium refinement facility.
• Stuxnet most advanced malware discovered – first serious cyber weapon.

See W32.Stuxnet Dossier, Nicolas Falliere, Liam O Murchu, and Eric Chien, Symantec
Stuxnet Objective

- Stuxnet targeted centrifuge systems used to separate U235 from U238 using centrifuge tubes spinning at high speeds.
- Speed of tubes is critical.
  - Too fast and they disintegrate
  - Too slow and low separation rate
- Stuxnet manipulates speed.
- About 60% of targets in Iran.
Spread of Stuxnet

• Stuxnet targeted five different Iranian sites.
• First spread by USB drive.
• By July 2010 any Windows machine could have been infected.
• Spreads if autorun off or can’t run app from USB
• Spreads whether or not systems are up to date or whether anti-virus software running.
• Uses five different vulnerabilities, four zero-day.
• Hides its tracks.
Spreading of Stuxnet

• Stuxnet dormant unless it is on a computer
  – Running a version of Windows,
  – Running Siemens Step 7 software,
  – Connected to Siemens programmable logic controllers (PLCs), and
  – Controlling Fararo Paya (Iran) or Vacon (Finland) frequency controllers.

A PLC is a simple computer designed for control systems. Programmed with bits.
Stuxnet Degraded Operation

- Normal controller frequency: 807Hz to 1210Hz
- Stuxnet cycles the frequency from 1064Hz (normal) up to 1410Hz; down to 2Hz; up to 1064Hz
  - It is in abnormal range for ≤ 50 minutes each time.
  - System is sabotaged by this variation in frequency.
- Typically Stuxnet waits ~13 days after the initial infection before starting sabotage. Each additional step occurs after ~27 days.
- Variation either cause centrifuges to disintegrate or produce low-grade results.
Stuxnet Damage

• Stuxnet code targeted 984 Natanz frequency converters
  – When IAEA inspectors visited Natanz in late 2009, they found 984 centrifuges had disappeared.

• President Ahmadinejad confirmed in November 2010 that cyber attack had damaged centrifuges.
  – Apparently permanent damage is limited.

• On 11/29/10 Prof. Shahriari, head of Iranian team combating the Stuxnet virus, was assassinated by motorcyclists on streets of Teheran.

• On 1/11/12 Ahmadi-Roshan, supervisor of Iranian uranium enrichment department, was assassinated.
Clues to Origins of Stuxnet

• Kaspersky Lab speculates Israel behind Stuxnet.
• Value 19790509 is used to decide whether to infect a machine; it may denote May 9, 1979.
  – Date when Jewish-Iranian businessman Habib Elghanian executed in Iran after convicted of spying for Israel.
• Code has file b:\myrtus\src\...\guava.pdf
  – Wikipedia says “Esther was originally Hadassah (which) means ‘myrtle’ in Hebrew.” Esther “told the king of Haman’s plan to massacre all Jews in the Persian Empire” who pre-empted the plot by killing plotters.
• But has a primitive command & control system, not typical of a sophisticated Western power.
Origins of Stuxnet

• **U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site**, David Sanger (NYT, Jan 10, 2009)
  – This article says that President Bush deflected a request from Israel to provide it with bunker-busting bombs to attack Iran’s main nuclear complex.
  – It also says that US turned down by Israel to fly over Iraq and into Iran.

• Iran admits it has run into serious problems at Bushehr nuclear reactor, a site it has admitted was infected by Stuxnet.

New York Times Scoop

• 2012 NYT Report:* President Obama ordered attacks on Iran’s nuclear enrichment facilities.

• Code-named Olympic Games in Bush admin.

• NYT says although Stuxnet discovered in summer 2010, Obama authorizes two new versions of Stuxnet be launched.

• Obama said to be aware of Stuxnet precedent!

• NYT: CIA tried to inject faulty parts into facilities

* [http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html](http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html)
New York Times Scoop

• NYT says US develops software to “phone home” electrical blueprints of Natanz centrifuge plant.
  – Is this Flame cyber espionage malware found in ‘12?
• NSA and Israeli Unit 8200 develop Stuxnet worm
• US tests worm on its Pakistani P-1 centrifuges
• First cyber attack to cause physical damage, according to Michael Hayden, former CIA chief.
• Iranians confused by random failures.
Stuxnet Sources


• W32.Stuxnet Dossier, Nicolas Falliere, Liam O Murchu, and Eric Chien, Symantec, 2011

Review

• 1988 Morris Worm
• 2003 Titan Rain exfiltration attack
• 2007 Estonian attack
• 2007 Aurora Experiment at US Facility
• SCADA Infrastructure Threats
• 2010 Stuxnet attack against Iran facility