01:090:101 Section 51 Hill 120  Tuesday, 3:20-4:40

02: How to get infected. Phishing. Spearphishing. d0xed game.
03: Discuss the game elements. Erasing data forever. Lying.
04: The web of you. Who has it? What can they do with it? Good practices. Class presentation description.
05: Class presentations picking. What can I do with a little bit of you? Why the web can lie forever – wikipedia.
06: Social media. What’s good and bad practices.
07: The other side of the curtain – what are the responsibilities of the holders of data?
09: Presentations, part 1 (randomly selected.)
10: Presentations, part 2 (randomly selected.)

Dr. Casimir Kulikowski (kulikows@cs.rutgers.edu)
Not-at-all-Dr. Charles McGrew (mcgrew@cs.rutgers.edu)
How would you break in?
How would you break in?

- From the outside
  - Password guessing
  - -service defeating
- From the inside
  - let someone do it for you!
    email; web pages
    (NSA rules on windows machines)
    StuxNet
    Sony
What would you take?
What would you take?

• Username/password
• Credit card info
• Logins on other machines
What would you leave behind?
What would you leave behind?

- Easier way back in next time
- Encrypted files
- Alternative DNS path
- ???
StuxNet

• 2007: Iran announces it has 3,000 centrifuges enriching uranium
• 2008: Iran announces 6,000 more
• 2009: first StuxNet infections
• “Serious” Nuclear Accident in Iran (Natanz)
• 2010: 2,000 centrifuges decommissioned at Natanz; third StuxNet infection, Stuxnet discovered and announced
• 2011: Iran admits Stuxnet infection
• 2012: Stuxnet self-destructs
StuxNet

• Simple Infection (yes, but how?)
• Evolves
• Reports
• Infects others
• Infects target
• Ruins target, while lying to user
• Gets out by laptop(?) or many keys(?)
1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn’t a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system’s logic controllers, exploiting “zero day” vulnerabilities—software weaknesses that haven’t been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won’t know what’s going wrong until it’s too late to do anything about it.
Sony BMG in your Computer

• 2000: "The industry will take whatever steps it needs to protect itself and protect it revenue streams... It will not lose that revenue stream, no matter what... Sony is going to take aggressive steps to stop this. We will develop technology that transcends the individual user. We will firewall Napster at source - we will block it at your cable company. We will block it at your phone company. We will block it at your ISP. We will firewall it at your PC... These strategies are being aggressively pursued because there is simply too much at stake."[1] - Steve Heckler, Sony Senior VP

• 2005 Researchers discover a rootkit (XCP) on machines that have played a Sony CD, and quickly determine it came from the CD itself (autoexec.bat).

• XCP opens back doors that can be exploited by others; slows down the computer; reports to Sony on the user’s listening (and other) habits

• It has credentials that allow it to install itself as administrator and not tell you about itself, and hides itself from anti-virus programs. Oh, and occasionally blue-screen-of-deaths your machine.

• If you try to remove it without knowing exactly what you’re doing, it’ll make your disk unreadable.
Sony twists and turns

- Thomas Hesse, Sony BMG's president of global digital business (November 4, 2005)
  "Most people don't even know what a rootkit is, so why should they care about it?"
- Sony promises not to do it, and replace disks (November 14)
- Sony releases a “fix” that simply decloaks the rootkit, does not remove it
- Sony releases a second “fix” that removes the root kit, but leaves behind a second rootkit with even more exploitable vulnerability
- It is discovered that in attempting to “save copyright”, Sony violated copyright in the rootkit (which includes a “legal” mp3 player) they install
- Other anti-virus companies finally release removal tools.
[order of play]

1. [action]
   Take up to three actions.
2. [loot]
   Draw two [loot!] cards.
3. [patch]
   Draw and resolve [patch!] cards, as indicated by the [infocon] level.
4. [check]
   Discard, to obey the hand limit.

[winning]
If all players occupy the Internet Gateway tile, all four [digital asset] tokens have been recovered, and anyone plays a [zero-day exploit] card, you win. This is the only way to win: re-capture your stuff, escape to the Internet.

[losing]
You lose when either (1) the threat level reaches [infocon] level one, or (2) it becomes impossible for all players to win, including:
   • The Internet Gateway tile is decommissioned;
   • A [hacker] is ejected from the network, for any reason;
   • A [capture point] is decommissioned, such that it becomes impossible to [recover] some [digital asset].

[check]
At the end of your turn, you may hold at most five [loot!] cards when a hand limit check is performed. Discard any cards in excess of the hand limit to the [loot!] discard pile. You can play [zero-day exploit] cards before discarding them.

[layout]
You may layout the game pieces however you like. One possible layout is pictured on the back of this booklet.