

Miao Lu, University of Illinois
Jason Reeves, Dartmouth College
September 12, 2014











#### Outline

- The Basics
- Types Of Cyber Attacks
- Attack Artifacts
- Common Vulnerabilities
- Playing Defense

#### Outline

- The Basics
- Types Of Cyber Attacks
- Attack Artifacts
- Common Vulnerabilities
- Playing Defense

• First, a definition: What is a cyber attack?

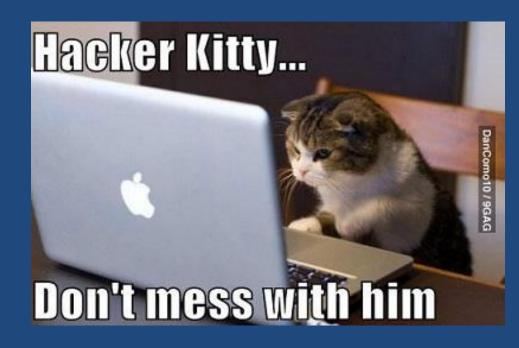
- First, a definition: What is a cyber attack?
  - —"[A] computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident on it."

—Kevin O'Shea, ISTS, May 7, 2003

http://www.ists.dartmouth.edu/library/107.pdf

Who launches cyber attacks?

- Who launches cyber attacks?
  - Classic Hackers



- Who launches cyber attacks?
  - Classic Hackers
  - Mercenary Hackers



- Who launches cyber attacks?
  - Classic Hackers
  - Mercenary Hackers
  - Hacktivists



- Who launches cyber attacks?
  - Classic Hackers
  - Mercenary Hackers
  - Hacktivists
  - Rogue Insiders
    - Not necessarily malicious!

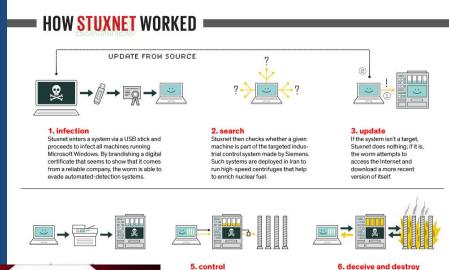


- Who launches cyber attacks?
  - Classic Hackers
  - Mercenary Hackers
  - Hacktivists
  - Rogue Insiders
    - Not necessarily malicious!
  - Nation-States



Prominent Cyber Incidents...





In the beginning. Stuxnet spies on the

uses the information it has gathered to

take control of the centrifuges, making

them spin themselves to failure.

operations of the targeted system. Then it

Meanwhile, it provides false feed-

back to outside controllers, ensur-

going wrong until it's too late to do

ing that they won't know what's

anything about it.



Prominent Cyber Incidents...and those to come?



#### Outline

- The Basics
- Types Of Cyber Attacks
- Attack Artifacts
- Common Vulnerabilities
- Playing Defense

- 1. Device Compromise
- 2. Service Disruption
- 3. Data Exfiltration
- 4. Bad Data Injection
- 5. Advanced Persistent Threat (APT)

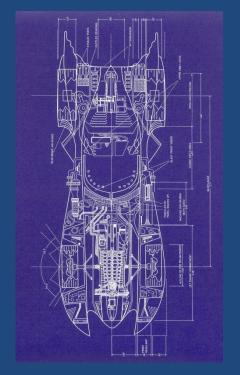
- Device Compromise
  - Goal: To obtain total control of a device.
  - Requirements:
    - Root credentials
    - Privilege escalation exploit
  - Powers Granted:
    - Arbitrary execution on compromised device
    - Network foothold
    - Ability to carry out other types of cyber attacks!



- Service Disruption
  - Goal: To prevent a device from performing its duties.
  - Requirements:
    - LOTS of computing power
  - Powers Granted:
    - Consequences of the device failing to do its job
      - Device downtime?
      - Revenue loss?
      - Public attention/shaming?
      - System failure?



- Data Exfiltration
  - Goal: To steal sensitive information from a target.
  - Requirements:
    - Access (legit or otherwise) to device storing data
  - Powers Granted:
    - Arbitrary Data Operations!
      - Reconnaissance
      - IP Theft
      - Expose private information

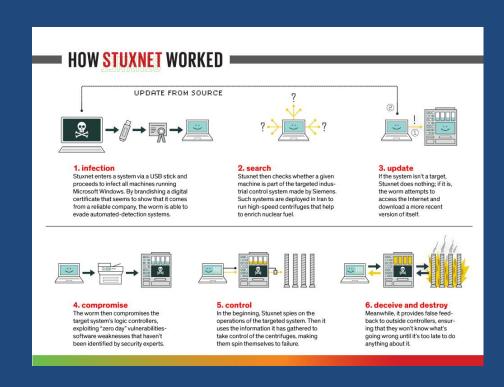




- Bad Data Injection
  - Goal: To submit incorrect data to a system without detection.
  - Requirements:
    - Access (legit or otherwise) to device storing data
  - Powers Granted
    - Determine the state of datadriven services!
    - Real-world consequences, potentially catastrophic



- Advanced Persistent Threat (APT)
  - Goal: To gain extended access to a device.
  - Requirements:
    - Time, patience, resources
    - Extensive target knowledge
  - Powers Granted:
    - Long-term reconnaissance
    - Ability to act on target quickly
    - Complete and invisible control of systems!



#### Outline

- The Basics
- Types Of Cyber Attacks
- Attack Artifacts
- Common Vulnerabilities
- Playing Defense

- Virus
  - Attaches itself to program and copies to other programs
  - Virus Phases:
    - Dormant: Waiting on trigger event
    - Propagation: Replicating on programs/disks
    - Triggering: By event to execute payload
    - Execution: Executing payload
  - Payload: The activity of the virus beyond the spreading
    - Installing software
    - Harvesting information

#### Worm

- Propagates copies of itself through a network from one computer to another
  - Self-directed propagation
- Dormant
- Propagation
  - Search for other systems to infect
  - Establish connection, and self replicate
- Triggering
- Execution

- Trojan Horse
  - Useful program containing hidden code that, when invoked, performs some unwanted or harmful function.
  - Often carrying payloads such as spyware

- Rootkits
  - A program used to hide the presence of other data and/or programs on a machine
    - Requires root privileges on the machine

#### Botnet

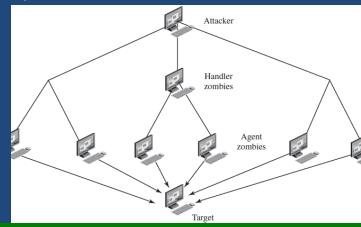
- bot is typically planted on thousands of computers belonging to unsuspecting third parties
- The collection of bots often is capable of acting in a coordinated manner, thus, the name Botnet
- Often used to launch denial-of-service (DoS) attacks

- Social Engineering
  - Infection mechanisms trying to make users to "click through"
  - tricking users to assist in the compromise of their own systems or personal information.
  - Usually in the form of Spam E-Mail

- Logic Bomb
  - Code embedded in the malware that is set to execute when certain conditions are met

- Time Bomb
  - Triggers action when specified time occurs

- Denial-of-Service Attack
  - an attack on a computer system or network that causes a loss of service to users
  - A DoS attack aims to overload or crash targeting system's network handling software
  - Source Address Spoofing
  - Distributed Denial-Of-Service (DDoS)



#### Outline

- The Basics
- Types Of Cyber Attacks
- Attack Artifacts
- Common Vulnerabilities
- Playing Defense

#### Buffer Overflow

- More inputs are placed into a buffer or data holding area than the capacity allocated, over writing other information
- Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system

- Weak Passwords
  - The more complex a password is, the harder it is to guess.
  - Password strength is a measure of how effective a password is in resisting guessing and brute-force attacks



#### SQL Injection

- Databases have a sophisticated interaction protocol called the Structured Query Language (SQL)
- In SQL injection attack, the user-supplied input is used to construct a SQL request to retrieve information from a database
- The hacker may input specifically crafted SQL commands with the intent of bypassing the login form barrier and seeing what lies behind it

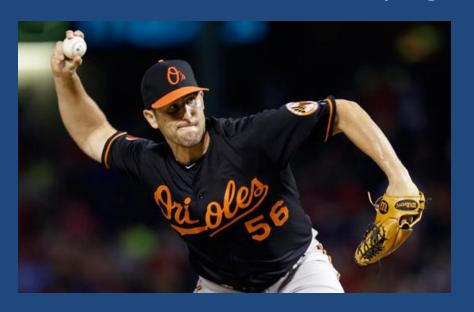
- Cross-Site Scripting (XSS)
  - Concerns input provided to a program by one user that is subsequently output to another user
  - Attackers can inject malicious code into Web pages viewed by others
  - Used by attackers to bypass access controls
  - Often used on wikis, blogs, where comment includes script code
  - Bypassing access control as blog comment, but acting as malicious script

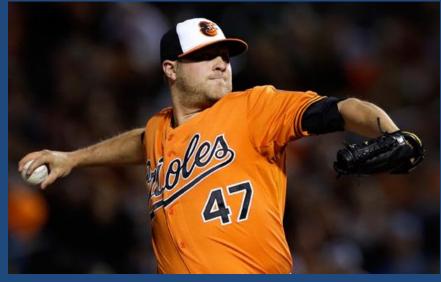
- Time-Of-Check-Time-Of-Use
  - a class of software bug
  - an attacker is able to make changes to the system between the checking of a condition and the use of the results of that check

A Word On Vulnerability Age:

### Common Vulnerabilities

#### A Word On Vulnerability Age:



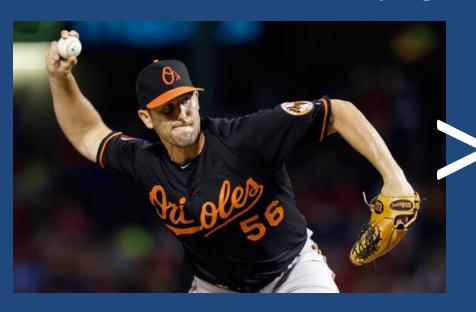


Darren O'Day 4-1 1.32 ERA 0.91 WHIP Evan Meek 0-3 6.75 ERA 1.66 WHIP

Stats from http://orioles.mlb.com. Current as of 12 noon on 9/11/14.

### Common Vulnerabilities

A Word On Vulnerability Age:





Darren O'Day 4-1 1.32 ERA 0.91 WHIP Evan Meek 0-3 6.75 ERA 1.66 WHIP

Stats from http://orioles.mlb.com. Current as of 12 noon on 9/11/14.

### Common Vulnerabilities

- A Word On Vulnerability Age:
  - Hacking works the same way!
  - A zero-day (or "O-Day") is a vulnerability that is previously unknown to the software community, and thus generally more effective at exploiting a target.
    - ...but this isn't necessarily true in the grid!
      - Vulnerabilities in SCADA equipment are sometimes left unmitigated for years!
      - Your local substation is vulnerable to Evan Meek!
    - Why?

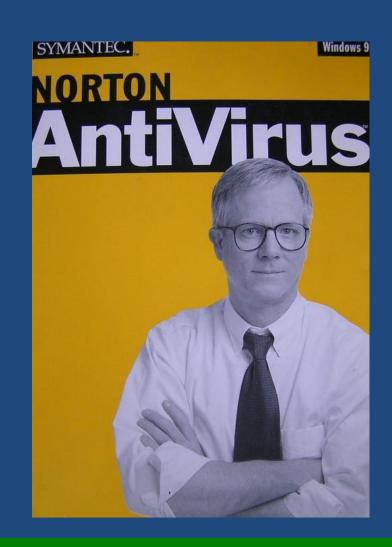
### Outline

- The Basics
- Types Of Cyber Attacks
- Attack Artifacts
- Common Vulnerabilities
- Playing Defense

- Patching
  - Updating software to fix vulnerabilities
- Power Grid Concerns
  - Devices may not be accessible
  - Patches may break legacy programs
  - Patches might require downtime



- Antivirus Software
  - Programs that monitor your system for malware
- Power Grid Concerns
  - Easy to circumvent
  - Added resource burden
  - Not made for some equipment



#### Firewalls

Programs that filter
 network traffic and block
 suspicious packets

#### Power Grid Concerns

- Have to know exactly what sorts of traffic are present
- Time is of the essence



- Intrusion Detection Systems (IDS)
  - Programs that monitor your systems for bad behavior
    - Host vs. Network
    - Signature vs. Anomaly
- Power Grid Concerns
  - Often require virtualization
  - Lots of false positives



- Training
  - Teach users proper computer hygiene!
- Power Grid Concerns
  - Humans not great at security operations
    - Passwords, anyone?
  - Easy to fake things
  - Cognitive biases?



- LangSec
  - Treat inputs as a formal language, and verify them!
- Power Grid Concerns
  - Have to retro-fit legacy programs
    - ElfBAC!



### **Image Credits**

- Research Cat: http://bethanish.files.wordpress.com/2011/10/research-cat-lolcat.jpg
- Hacker Kitty: http://yahbh.files.wordpress.com/2013/02/hacker-kitty.png
- Wario: http://wac.450f.edgecastcdn.net/80450F/arcadesushi.com/files/2013/03/Video-Game-Money.jpg
- Anonymous: http://blogs-images.forbes.com/thumbnails/blog\_1011/pt\_1011\_5662\_o.jpg?t=1343922794
- "Red button doesn't dispense cheeseburgers:" http://icanhascheezburger.com
- NSA HQ: http://media4.s-nbcnews.com/i/streams/2013/December/131206/2D9860010-130606-NSA-headquarters-tight-730a.jpg
- Owned computer: http://wiki.elon.edu/download/attachments/14156666/virus1.gif
- Batmobile Blueprint: http://www.chickslovethecar.com/images/topblueprint.jpg
- Jennifer Lawrence: http://upload.wikimedia.org/wikipedia/commons/4/4f/Jennifer\_Lawrence\_at\_the\_83rd\_Academy\_Awards\_crop.jpg
- EMR Example: http://www.emr-ehrs.com/images/screenshots/gastroenterology-electronic-health-records.jpg
- Aurora Generator: http://2.bp.blogspot.com/ gCayFzinbX8/Rv14Pgog0rl/AAAAAAAAAAfs/BnnDUNJZEqw/s400/Generator+Test+-+Aurora.jpg
- Stuxnet: http://spectrum.ieee.org/img/03OLHowStuxnetWorked-1360963061216.jpg
- Target: http://media.northlandsnewscenter.com/images/470\*264/NNC TARGET.jpg
- Metasploit Shell: http://2.bp.blogspot.com/-TJUUt5 0eG4/UdfY1Yjgmkl/AAAAAAAAB7Y/WlAxaE5fXxo/s1600/3.png
- Jim Harbaugh: http://media.jrn.com/images/620wtmj\_harbaugh.jpg
- Bert: http://www.blogcdn.com/cars.aol.co.uk/media/2011/11/bert-and-ernie.jpg
- John Boehner: http://dc.streetsblog.org/wp-content/uploads/2011/06/john-boehner-gaveljpg-6706b1f02a6d1dab.jpg
- Stephen Colbert: http://media.salon.com/2014/03/stephen colbert5.jpg
- Joe Biden: http://a.abcnews.com/images/Politics/AP joe biden tk 130812 16x9 608.jpg
- Grandpa Jones: http://jamesdmccallister.files.wordpress.com/2013/10/grandpa-jones.jpg
- Charlie Brown: http://www.chud.com/wp-content/uploads/2011/03/CBTHANKS6.png
- Sergey Bratus: http://upload.wikimedia.org/wikipedia/commons/4/43/2013-12-28 30C3 Sergey Bratus 2915.JPG
- Russell Wilson: http://www.rochelleriley.com/wp-content/uploads/2014/02/russell-wilson2.jpg
- Unikitty: http://img3.wikia.nocookie.net/ cb20131123061837/lego/images/e/e0/Unikitty.jpg
- Utility Control Center: http://www.smartgridnews.com/artman/uploads/1/pjm control center.jpg
- Darren O'Day: http://orioles.mlb.com/images/players/525x330/503285.jpg
- Evan Meek: http://orioles.mlb.com/images/players/525x330/457425.jpg
- Road Patches: http://lgam.wdfiles.com/local--files/road-photos/Patches-01.JPG
- Peter Norton: http://www.technologizer.com/wp-content/uploads/2014/06/image5.jpg
- Furwall: http://icanhascheezburger.com
- Stop Weird Machines: http://www.cs.dartmouth.edu/~sergey/langsec/occupy/WeirdMachines.jpg
- All clipart originally from Microsoft corporation.

### Thank You!

- Questions?
- Comments?