ForenSecure 17

Everything Old is New Again!

New Cyber attacks on the Same Old Technology

10/17/2016
Agenda

- Introduction
- Most Dangerous and Outdated Technologies
  - Anti-Virus
  - Passwords
  - Outdated and Misconfigured Systems
  - IoT / IIoT
- Attack Vectors
- Cyber FRAUD
- Social Engineering
  - Phishing
    - Goals, Examples, and Exploits
- Demonstration
  - WARNING
- Security Considerations
- Questions
- References
Who are we?

• **Prescient Solutions**
  • Information Technology (IT) Solutions Provider
  • Headquartered in Schaumburg, IL
  • Founded in 1996

• **Specializing in:**
  • Full-Time IT Department Outsourcing
  • Part-Time IT Support
  • Remote IT Managed Services
  • Cloud Computing
  • Collaborative Application Development
Most Dangerous/Old Technologies

- **Anti-Virus**
  - New devices continue to use same limited hardware solutions

- **Passwords**
  - New devices continue to use same limited hardware solutions

- **Outdated and Misconfigured Systems**
  - Small geography limits ability to add more functionality, including security

- **Internet of Things (IoT) / Industrial Internet of Things (IIoT)**
  - Designed to be fast and resilient
  - Perform specific functions with no additional code, i.e. plain text, no security.
Anti-Virus

• John McAfee: "Antivirus is dead"
  • May only detect 30% of known viruses
  • *Antivirus cannot keep up. AV-test estimates a whopping 12 million new malware variants a month.*

• New technology is required –
  • Endpoint Security may require multiple feature sets or add-ons
  • Existing AV can be used in combination with *Application firewalls*, *application white listing*, and increased access controls.
  • Additional tools are necessary to provide appropriate levels of security including: *Mobile Device Mgmt.* and *Data Loss Prevention (DLP)*
Passwords

• One of the biggest security threats to companies in 2016 is password management.
  • 90 percent of successful breaches analyzed by Verizon started with a weak or default password.
  • Implementation of weak passwords within the infrastructure environment and core systems; provide higher risks of not only the potential for stolen or lost data; but, also the possibility of complete remote access and control of devices within the environment.

• Authentication
  • Create unique and complex IDs and Passwords for all accounts
  • Use multi-form factor authentication
  • Follow the principals of least privilege, controlling and limiting user access
  • Disable Unused Accounts, Connectivity, Ports, Switches, etc.
Outdated and Misconfigured Systems

- More than 70% of cyber attacks exploit patchable vulnerabilities
  - Basic **cyber hygiene** can help prevent up to 80% of cyber attacks.
  - Cyber Essentials can make the difference between being a victim or not.
    - Regularly **patch** software,
    - **Scan** their applications for vulnerabilities
    - **Apply** other important security controls

- **Implement Automated Patch Management Solutions**
  - Install Most Current OS / IOS
  - Install All Updates and Patches
  - Install Most Current Applications
  - Update Firmware On All Devices Regularly

More than 150,000 people are using an OS from the last century
IoT and IIoT

Industrial Internet of Things

- **1950s – 60s:** Manufacturing Devices - SCADA, PLC, RBU and Numerical Controls
- **1980s – 2000s:** Industrial Control Systems (ICS) - Automation, Robotics, CNC

Consumer Internet of Things

- **1970s – 80s:** First “Smart House”, X10 – Used electrical lines to connect different home machines
- **1999 – 2000s:** Internet of Things (IoT) becomes Common Place
Vulnerabilities of IoT / IIoT

• **Age**
  • New devices continue to use same limited hardware solutions

• **Size**
  • Small geography limits ability to add more functionality, including security

• **Purpose Designed and Driven**
  • Designed to perform critical duties which limits down time to maintain and install patches

• **Protocols**
  • Designed to be fast and resilient
  • Perform specific functions with no additional code, i.e. plain text, no security.
Risks and Breaches of IoT / IIoT

U.S. Steel Accuses China of Hacking (2016)
Steelmaker alleges Chinese government hackers stole plans for developing new steel technology

Hackers targeting industrial control systems (2016)
Researcher uses a network of simulated water pump systems to monitor how frequently industrial control systems are attacked

We watched a team of hackers 'fully compromise' a power company in less than 24 hours (2016)
From reconnaissance to 'fully compromised'

Intruders hack industrial heating system using backdoor posted online (2012)
Same control systems are used by FBI, IRS, and Pentagon.
Risks and Breaches of IoT / IIoT

Peeping into 73,000 unsecured security cameras thanks to default passwords (2016)
A site linked to 73,011 unsecured security camera locations in 256 countries to illustrate the dangers of using default passwords.

Flaws in Samsung’s “Smart” Home Let Hackers Unlock Doors and Set Off Fire Alarms (2016)

Botnet Uses IoT Devices to Power Massive DDoS Attacks (2016)
LizardStresser Ddos botnet used in attacks as large as 400 gigabits per second (Gbps) that leverage the power of IoT devices.

You can buy lock picks, Wi-Fi hacking tools, and more at the world's biggest hacking conference
Attack Vectors

An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

- DNS/ARP Poisoning
- Fuzzing
- Man-in-the Middle (MitM) / Session Hijacking
- Network Mapping
- Social Engineering
- SQL Injection
- Virus / Malware: Exploit Kits / Fileless / 0 Day
- Vulnerability Scanning
- Wardriving
- Weak Passwords - Brute Force - Dictionary
Common Types of Breaches

**Phishing**
- An estimated 91% of all hacks begin with Spear Phishing or Phishing (Verizon, 2016).
- Email Attachments, Embedded Links to Malware

**Drive By or Watering Hole Hack**
- Email Embedded Links to Malware, Website Links / Scripts

**Man-in-the-Middle (MitM)**
- Public WiFi, WiFi Auto Connect,
- Application redirection / Cross-Site Scripting
  (Browsers, Applications, Websites)
Phishing a Form of Cyber Fraud

**Fraud** - wrongful or criminal deception intended to result in financial or personal gain.

**Phishing / Social engineering** – Cybersecurity’s people problem

**Social engineering** – an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.
Categories of Social Engineering

- Phishing
- Vishing
- Spam Emails
- Popup Windows
- Interesting Software
- Non-Technical Attack Vectors
- Dumpster Diving
- Spying and Eavesdropping
- Acting as a Technical Expert
- Support Staff
- Hoaxing
Definitions and Forms of Cyber Fraud

“An estimated 91-percent of hacking attacks begin with a phishing…”

**Phishing** – defrauding an online account holder of financial information by posing as a legitimate company. Typically an email, with a malicious attachment or link is sent to a victim with the intent of tricking the recipient to open an attachment.
Definitions and Forms of Cyber Fraud

Spear-Phishing – an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data.

Whaling – a Spear-Phishing attack where the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Vishing – using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

Smishing – a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device.
Hackers Goal for Phishing!

- **UserID/Passwords**
  - All Accounts and Email Addresses
- **Personally Identifiable Information (PII)**
  - Financial Account Information
  - Credit Cards
  - SSN (Identity Theft)
- **Intellectual Property (IP)**
- **Remote Access to all systems**
- **Physical and Logical locations of users, facilities, systems, applications and data**
Phishing Email Examples

Phishing Email

Irvine, Jerry

From: [Redacted]
Sent: Tuesday, June 23, 2015 3:04 PM
To: [Redacted]
Subject: Fwd: Wire Payment
Attachments:

Are you able to process an international wire before the cutoff time?

John

-------- Original Message --------

Subject: Wire Payment
Date: 2015-06-23 13:55

John,

Per our conversation, attached is the wiring instructions. As you already know, the support for this will come in later. Let me know when this is processed.

Phishing Attachment

BRAND WIRING INSTRUCTIONS

Hang seng Bank
83 Des Voeux Rd,
Central, Hong Kong

Swift Code: HASEHKHH
Account #: 788-482172-883

Credit to: Brand Inc Limited
Major KNOWN Phishing Hacks

Massive Target Hack Traced Back To Phishing Email

Investigators Suspect Anthem Breach Began with ‘Phishing’ of Employees

Alleged Bank Hack Tied to Phishing? - Suspected JPMorgan Breach Raises Risk Awareness

JPMorgan Chase Customers Targeted in Phishing Scheme

Ashley Madison Users victims of extortion and phishing
Common Phishing Exploits

• **Attachment Payloads**
  • Malware, Mal-Vertising, Viruses
  • Ransomware
  • Embedded URLs

• **Website and Application attacks**
  • Drive by Downloads
  • Watering Hole

• **Man in the Middle (MitM)**
  • Session Hijacking
  • Cross-Site Scripting (XSS)
  • URL Redirection
I will be performing a live presentation.

Host devices with WiFi adapters turned on may be detected.

No External systems will be viewed, connected to or exploited.

Note: Demonstrating MitM attack on IoT since MOST COMMON BREACHES can be completed with MitM
Issues with Public WiFi

- Hackers are looking for easy targets – and WiFi is EASY!!!
- Wireless Access Points (AP) can span the whole network

- Hackers may be able to scan from one building and see wireless devices throughout the network.
**Man in the Middle Demo**

**Issues with Public WiFi**

- Midway International Airport
- WiFi IP Range is set up for 64,000 Devices
- Can Scan from baggage claim and see A, B, & C
- Multiple Open WiFi’s to Spoof
- A Hacker can get on any Open and perform a MitM on all of them.
Man in the Middle Demo

Issues with Public WiFi

• Midway International Airport
• Scanned for 20-30 seconds and found hundreds of devices
Man in the Middle Demo

Man-in-the-Middle Attack using WiFi Pineapple -
Man in the Middle Demo

Man-in-the-Middle Attack using WiFi Pineapple -

1. Scan for and Enter Open Network SSID Information
2. Attack local Targets or go to a Target Company
3. Scan for Target devices that are connected to the Open network or setup to “Automatically Connect” to Open Networks
4. Inject host device between Target and Internet
5. Insert Payload
Man in the Middle Demo

DEMO
Man in the Middle Demo

Spoof Access Point SSIDs so Client Devices see them

Spoofed SSIDs

Windows Detected SSIDs
Client Devices that are set to autoconnect Connect...

Once the Client Device is connected, the hacker can copy data, define vulnerabilities, and even insert payloads for remote control.
Man in the Middle Demo

IF YOU SEE THIS, YOU JUST MIGHT BE HACKED!!!!!!
With the right Tools – Anyone Can HACK!
Seven Strategies to Effectively Defend Your Systems*

1. IMPLEMENT APPLICATION WHITELISTING
   (Anti-Virus, Malware, Application Firewall)
2. ENSURE PROPER CONFIGURATION / PATCH MANAGEMENT
3. REDUCE YOUR ATTACK SURFACE AREA
   (Segmentation)
4. BUILD A DEFENDABLE ENVIRONMENT
5. MANAGE AUTHENTICATION
   (Multiform factor Authentication)
6. IMPLEMENT SECURE REMOTE ACCESS
   (No Public WiFi, VPN, HTTPS)
7. MONITOR AND RESPOND

(NCCIC, 2016).
THANK YOU

Jerry Irvine, CIO – Prescient Solutions, Inc.
CISSP, CeH, HCISPP, CISM, CISA, CGEIT, GICSP, CRISC, CBCP, CASP, CIPP/IT, MCSE, CCNA, CCNP, CCDA, CCDP

jirvine@prescientssolutions.com
847.571.7065

