Emerging Risks and Security Challenges: A Look at Current Cybersecurity Threats

Prepared and presented by: Tanya Baccam
CPA, CITP, CISSP, CISA, CISM, GPPA, GCIH, GSEC, OCP DBA
SANS Institute – Senior Certified Instructor
Baccam Consulting LLC
tanya@baccam.com

**Additional training opportunities can be found at: www.securityaudits.org/events.html
**** Penetration and Vulnerability Testing for Auditors offered February 6-8, 2017

Security Landscape

- The security landscape is constantly changing!
- You have to adapt and constantly be educating yourself

Emerging and Evolving Threats

- POS and data breaches
- Security device vulnerabilities
- Cyber Criminals leveraging APT techniques
- Encryption becoming more “standard”
- Mobile, mobile, mobile
- Application attacks
- SSL/TLS exploits
- Flash issues
- Hacking UEFI
- “Internet of Things” attacks
- New hacking hardware
- Infrastructure attacks
- Cloud… security???
- Ransomware

Target

- One of the most talked about data breaches
  - 40 million credit and debit cards stolen from Nov. 27 and Dec. 15, 2013
- At the time of the attack, none of the anti-virus solutions on the market would have, or did, detect the malware
- Logs did identify the attack… just no one was paying attention or knew what was being reported

Security Device Vulnerabilities

- Barracuda Backdoor
  - Several undocumented OS user accounts exist
  - Accounts couldn't be disabled
  - Barracuda says they are needed for customer support
- Juniper Backdoor
- Fortinet
  - Hard coded password - FGTAbc11*xy+Qqz27
  - Easy to exploit
- Cisco router
  - SynFull Knock
- Sonicwall
  - Multiple vulnerabilities including root command injection

Office of Personnel Management

Details

- They have been hacked multiple times
  - March 2014 – Chinese hackers obtained data on tens of thousands of people that had or had applied for Top Secret Clearance
  - June 2015 – 30 years of personal information on at least 4 million – and up to as many as 21 million current and former government employees
- Data included SS numbers, previous addresses, family information, financial history, personal information

What Controls Were Missing?

- No inventory of all the computer servers and devices with access to its networks
- No strong authentication for remote access
- Vulnerabilities scans not conducted regularly
- Data stolen was not encrypted
- Relying on “old” technologies
  - Signature based IDS
- Alerts, but no response
  - Logs not being reviewed
- 11 of the 47 computer systems that were supposed to be certified as safe were not “operating with a valid authorization”

Medical Data

- After the Office of Personnel Management breach, medical data was labeled as the "holy grail" for cybercriminals intent on espionage. "Medical information can be worth 10 times as much as a credit card number," reported Reuters. And now to steal such information, hospital networks are getting pwned by malware-infected medical devices.
- "[…] once an attacker has established a backdoor within our target blood gas analyzer, or any other medical device, almost *any form of manipulation* of the unencrypted data stored and flowing through the device is possible."
- "[…] medical devices "are closed devices, running out-of-date, closed, often times modified and likely insecure operating systems such as Windows 2000, Windows XP or Linux

Source: http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

Medical Data Value

- Data can be used to create fake IDs
- Buy medical equipment or drugs
  - Resell
- Create fake claims
- Harder to identify medical identity theft
  - Criminals have years to use the credentials

VTech

- More than 6 million children's accounts and 5 million parent's records were compromised on the Learning Lodge website
- Issues
  - Password hashes were weak
  - A true salt was not used - vtech or vtechvtech
  - Security architecture was out of date
- Response
  - Company focused on the fact that credit card and financial data hadn't been compromised
  - That misses the point - Identity, not credit, is the target of newer hacks

Priorities

- What about your information?
- What about your client data?
- What about your intellectual property?

- Anything that gives you a competitive advantage should be protected or you will lose that competitive advantage!

Notable 2016 Breaches

- Yahoo Data Breach
  - 500 million user accounts
  - Security was not taken seriously
    - Better to risk annoying customers with product security measures than to leave their personal information open to data breaches
- SWIFT Network Attacks
  - SWIFT is a proprietary messaging system financial institutions use
  - Attackers remotely submitted billions of dollars in fraudulent money transfers
    - Only about $81 million went through
- DNC Hack
  - Lots of emails compromised
- FriendFinder Data Breaches
  - Email addresses and passwords obtained
    - Stored as plain text or hashed and converted to all lower-case
  - Stole company source code
  - Stole private/public key pair
- Wendy's POS Hack
  - Credit card information compromised at multiple locations

IOT

- Smart devices, dumb defaults
- Cars, lighting, refrigerators, bathroom scales, telephones, Supervisory Control and Data Acquisition (SCADA) systems, traffic control systems, home security systems, televisions, DVRs, etc.
- Risks
  - Disruption and denial-of-service attacks
  - Understanding the complexity of vulnerabilities
    - Webcams to spy on kids
  - IoT vulnerability management
    - Typically requires a firmware update
    - Default credentials
  - Identifying, implementing security controls
    - Remote connectivity to medical devices
  - Fulfilling the need for security analytics capabilities
    - What's normal and what's not?
  - Bandwidth requirements

OpenSesame

- Using hacked $12 kids' toy to open fixed-code garage door in 10 seconds

0

Car Hacking Made Easy

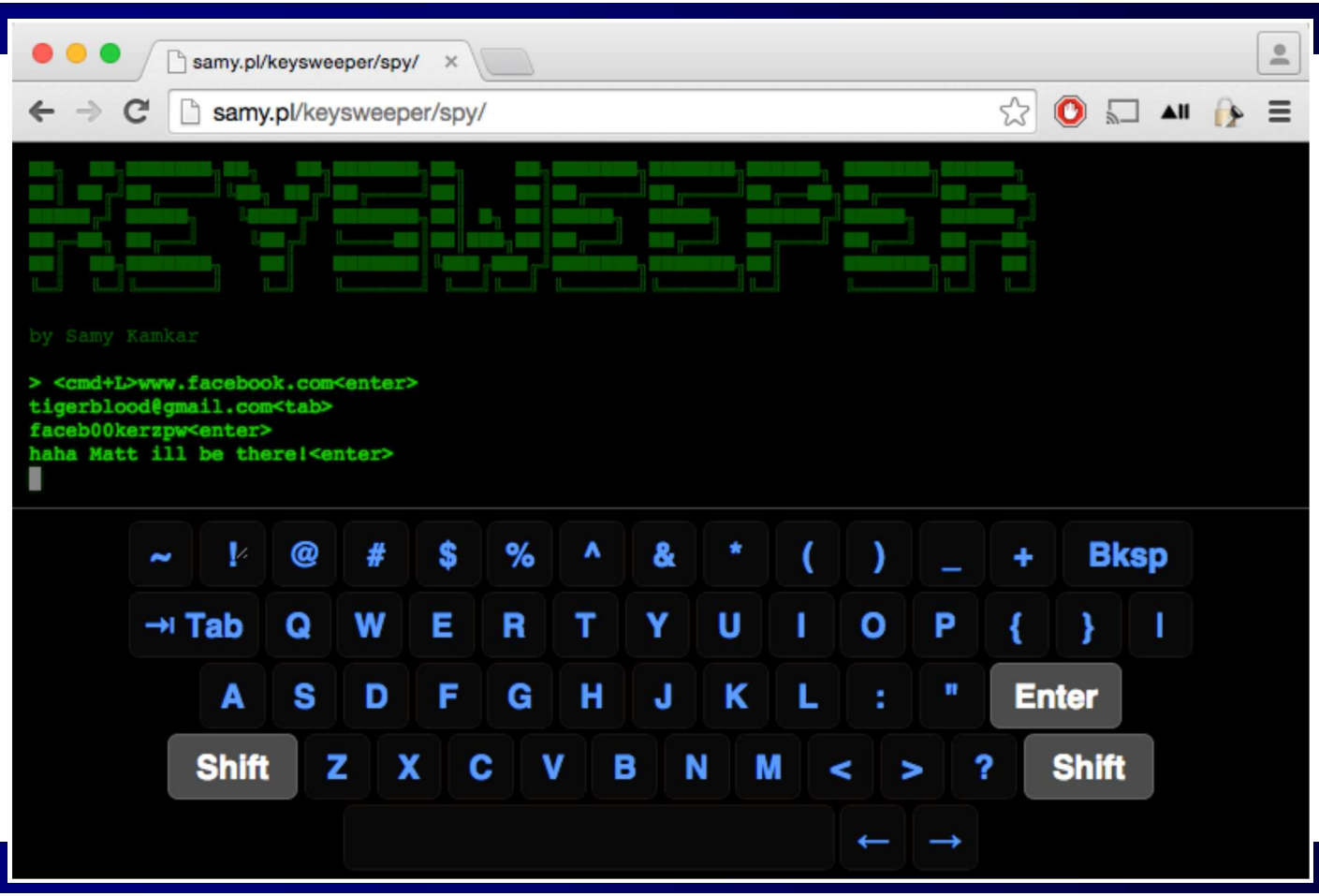
Jeep

- Took control of a Jeep SUV using the CAN bus
  - Exploited a firmware update
- Could speed up, slow down and even veer off the road
- Companies often ignore the security of peripheral devices or networks, the consequences can be disastrous

Mobile Devices

- Who doesn't have a mobile device today?
- Risks
  - Physical access
  - Users don't understand the risks
  - Untrusted apps and rooted phones
  - Phones that can't receive updates
  - Unlocked phones
  - Workstation infection
    - Essentially a portable USB stick
  - Insider threat
  - Lack of a governance framework

$10 Bluetooth Keyboard Sniffer



KeySweeper

- “it's a device disguised as a functioning USB wall charger that sniffs, decrypts, logs, and transmits all input typed into a Microsoft wireless keyboard.”
- “The device can either log the input on a chip for physical retrieval later, or it can use an optional GSM chip to transmit the keystrokes wirelessly to the attacker. For maximum efficiency, it can be programmed to send the operator SMS messages whenever certain keywords—think "bankofamerica.com," "confidential," or "password"—are entered.”
- “The entire sniffing device can be stashed inside an AC USB charger that powers the device. It recharges when plugged in and runs off of battery when not connected to a power source. To people being spied on, it looks like just another USB charger plugged into a wall socket.”

Source: http://arstechnica.com/security/2015/01/meet-keysweeper-the-10-usb-charger-that-steals-ms-keyboard-strokes/

Internet Of (Insecure) Things

- IoT botnet powered by Mirai malware caused a DDoS
  - September 20, 2016
  - Targeting Brian Kerbs' security blog
  - One of the largest on record - exceeding 620 gigabits per second (Gbps)
- Mirai malware continuously scans the Internet for vulnerable IoT devices, which are then infected and used in botnet attacks
  - Mirai uses a list of 62 common default usernames/passwords
  - Source code for Mirai is freely downloadable

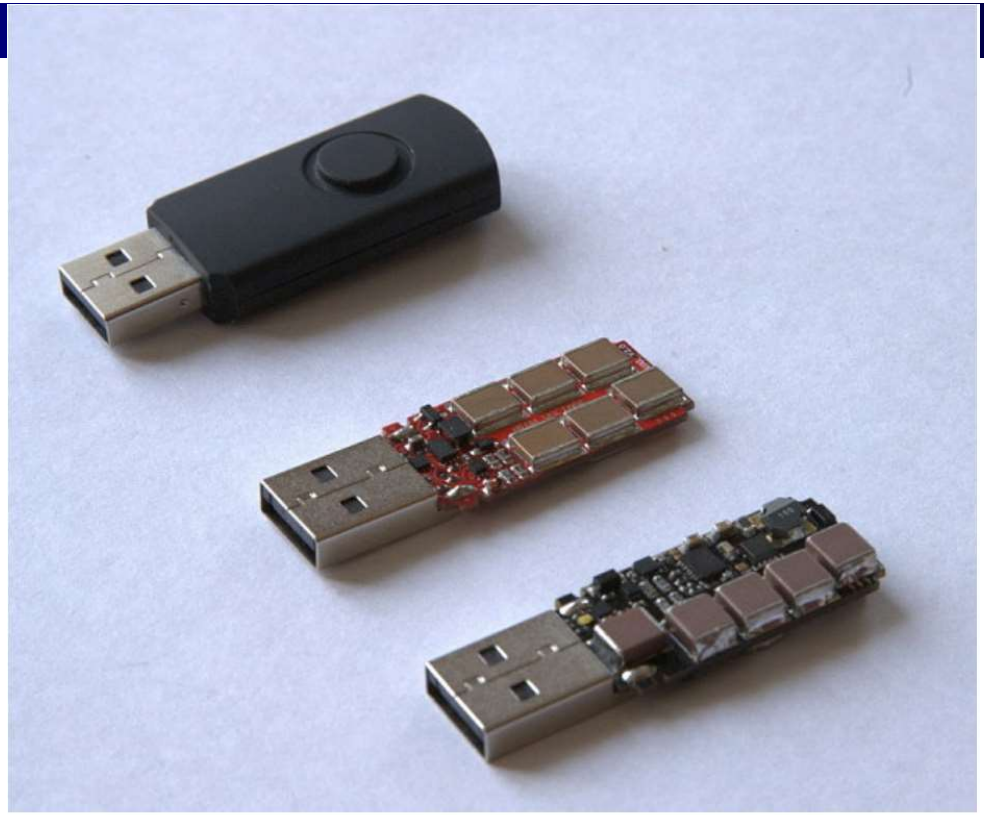
Mirai Mitigations

- Malware operates in dynamic memory, so a reboot will clear
- Change password for accessing device
- Reconnect to the network after rebooting and changing the credentials

Mirai Prevention

- Default credentials must be changed
  - Search Google
- Apply patches
- Disable UPnP whenever possible
- Purchase IoT devices from companies with a reputation for secure devices
- Know what a device can do
  - Know what devices can be access remotely or transmits data – medical devices at home, etc.
- Monitor ports 2323/TCP and 23/TCP for control channel
- Look for traffic on port 48101
  - Infected devices often attempt to spread malware using this port

Killer USB Sticks



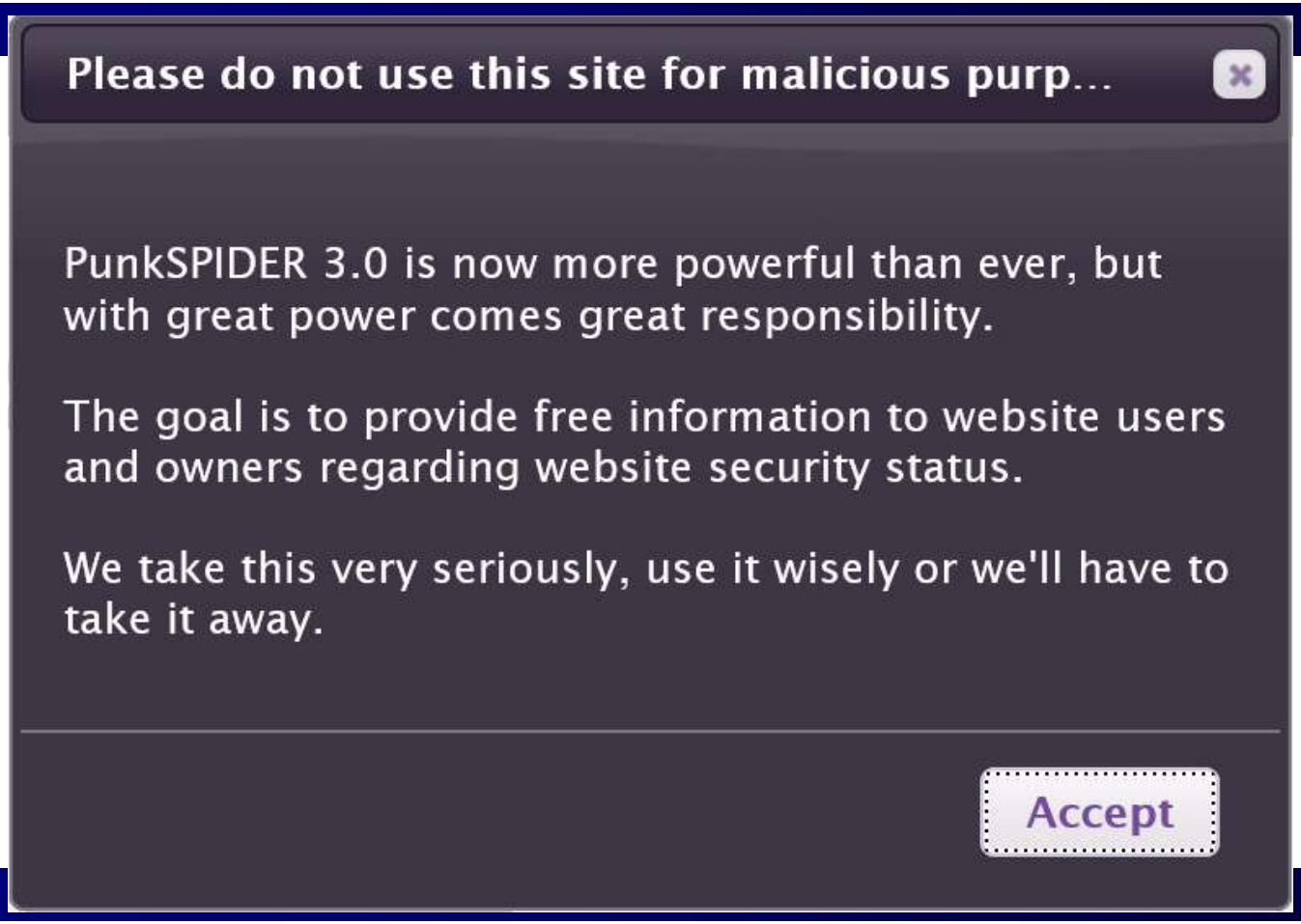
These 'killer' USB sticks can fry your laptop or phone in seconds, if plugged in.

Source: http://www.telegraph.co.uk/technology/internet-security/11932793/Killer-USB-stick-destroys-your-computer-in-seconds.html

Web Applications

- OWASP Top 10
- Application vulnerabilities abound

PunkSpider



Ransomware

- Restricts access to the system or a portion of the system and demands a ransom to remove the restrictions
  - Encryption
  - Lock the system
- $$$
  - 2013 – CryptoLocker – earned an estimated $3 million before it was taken down
  - 2014 – Cryptowall – estimated to have accrued over $18 million by June 2015
  - 2015/2016 – Fusob – pretends to be an accusatory authority and demanding payment of a fine
    - Often users pay $100-$200 instead of facing the fictitious charge
    - Masquerades as a pornographic video player
    - Estimates are the healthcare organizations have paid of $1,000,000 in 2016 due to ransomware - https://lazarusalliance.com/data-breaches-2016/

Closing Thoughts…

- We need to think about how to address security threats that are constantly changing
- We must continually adapt
- No barrier is impenetrable
- The number of vulnerabilities continues to increase

Mandiant M-Trends

- Attackers maintained access for an average of 205 days prior to discovery
  - Better than the 416 days from the prior year
- Significant evidence of organizations being compromised repeatedly
  - Incomplete eradication
  - Re-compromised in numerous cases by the same adversary

What should you do?

- **Compromise is inevitable**
- Accept that your organization can be compromised
  - Any large, complex, valuable organization is likely already compromised
- Then how can we possibly hope to win?
  - Change the definition of winning…
- Old goal: Preventing compromise
- **New goal: Prevent adversary success**

A New Security Paradigm

- It's not enough for an attacker to break into a network
  - They are going after data and information
  - Focus on detecting the adversaries goal of going after data and respond quickly
- Approaching security with these goals in mind is the only way to win this fight
- Tools of the new security paradigm
  - Defensible Security Architecture
  - Network Security Monitoring
  - Continuous Security Monitoring

Take Away…

Be afraid… be very, very afraid…

and go do something about it!

Thank you!

Prepared and presented by: Tanya Baccam
CPA, CITP, CISSP, CISA, CISM, GPPA, GCIH, GSEC, OCP DBA
SANS Institute – Senior Certified Instructor
Baccam Consulting LLC
tanya@baccam.com

Additional training opportunities can be found at: www.securityaudits.org/events.html
**** Penetration and Vulnerability Testing for Auditors offered February 6-8, 2017