RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: PDAC-W04

How Poorly Managed Keys and Certificates Impact the Trust Model

Stephen Jordan

SVP/Technology Area Manager
Wells Fargo & Co
Enterprise Information Security
Engineering & Services

#RSAC

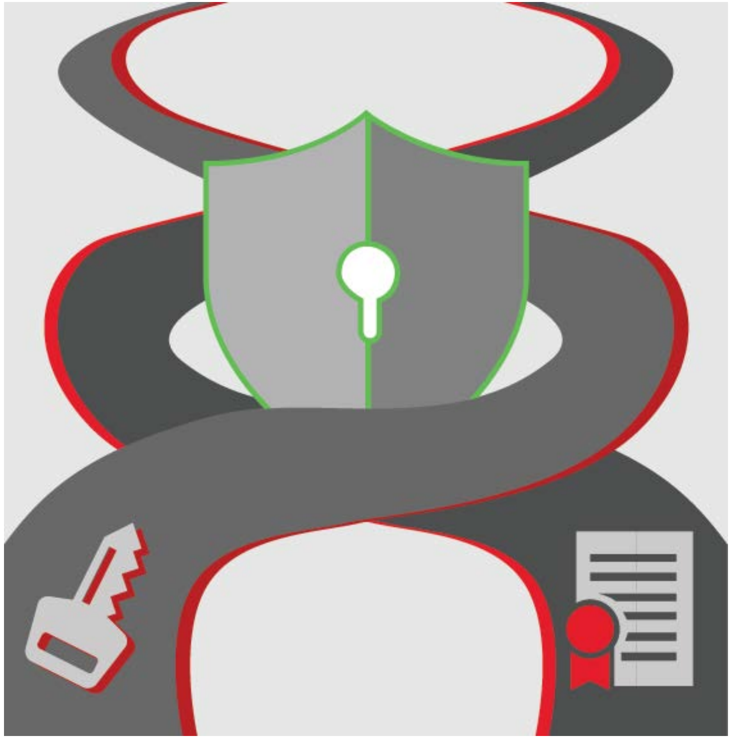
Key and Certificate Trust Model

- Used for secure communications, authentication, and authorization
- But when poorly managed, they jeopardize the trust they are meant to establish

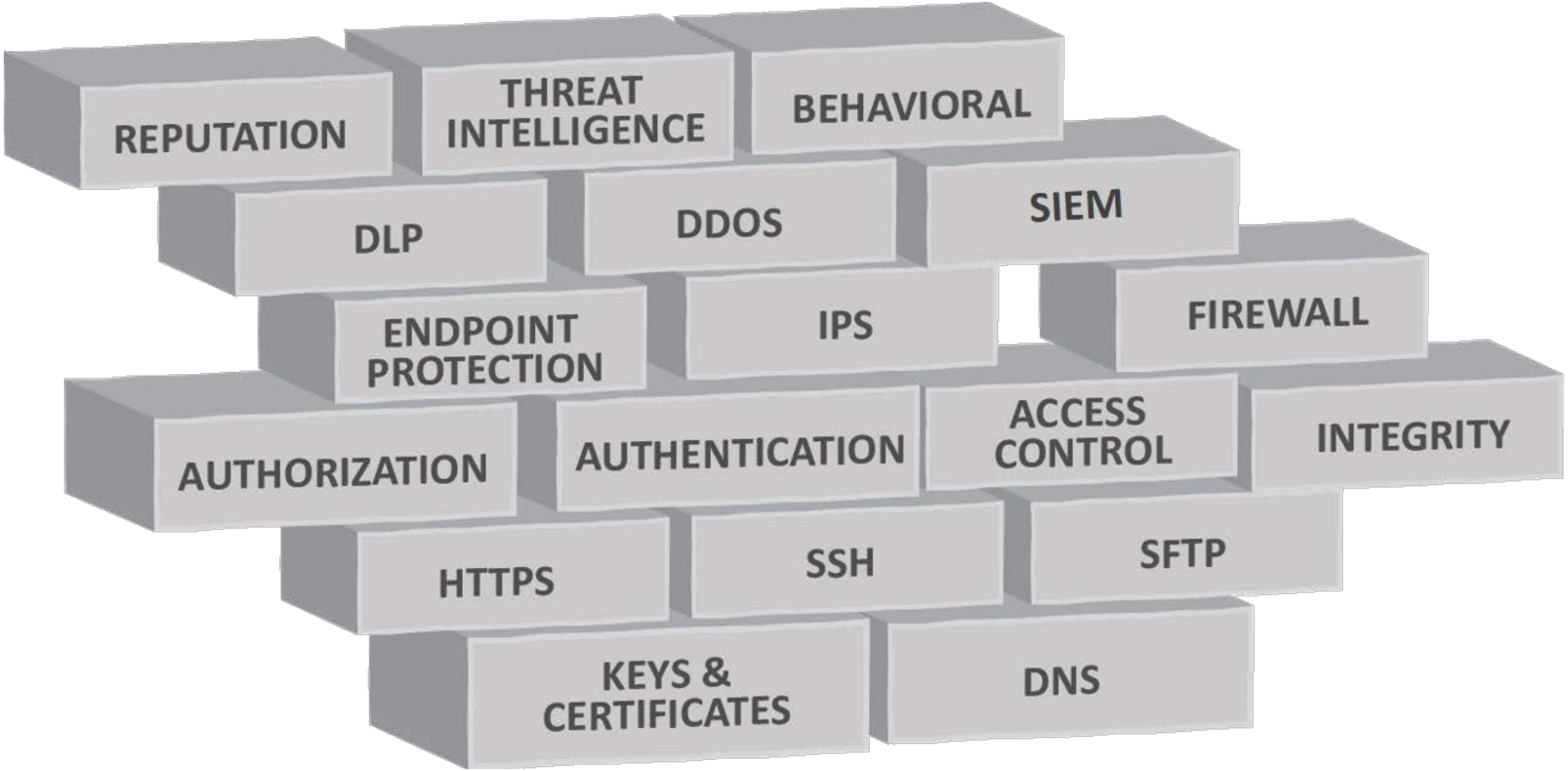
- SSL/TLS
- SSH
- Mobile devices
- WiFi &VPN access
- Etc.

Security Gaps

- Most security controls blindly trust keys and certificates
- Cyber criminals misuse keys and certificates to bypass security controls
- Do you trust all keys and certificates?



Foundation of Layered Security



REPUTATION

THREAT INTELLIGENCE

BEHAVIORAL

DLP

DDOS

SIEM

ENDPOINT PROTECTION

IPS

FIREWALL

AUTHORIZATION

AUTHENTICATION

ACCESS CONTROL

INTEGRITY

HTTPS

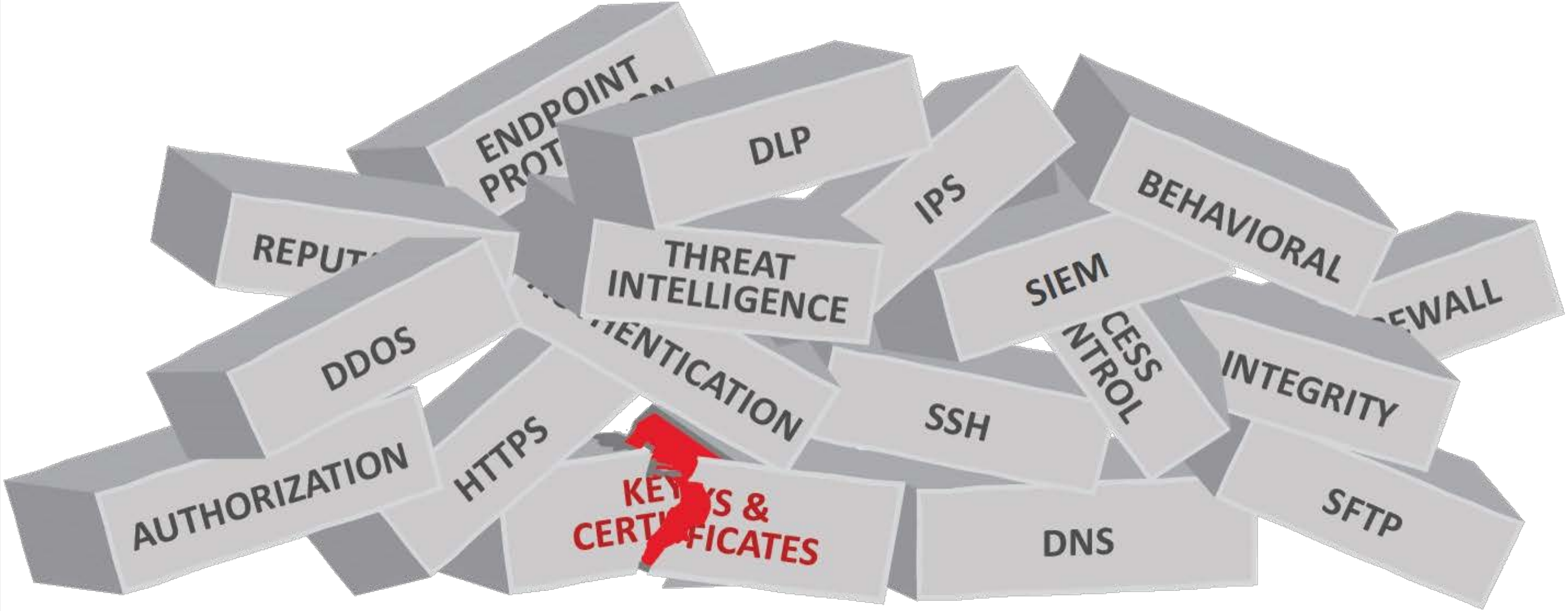
SSH

SFTP

KEYS & CERTIFICATES

DNS

When the Foundation Isn’t Protected

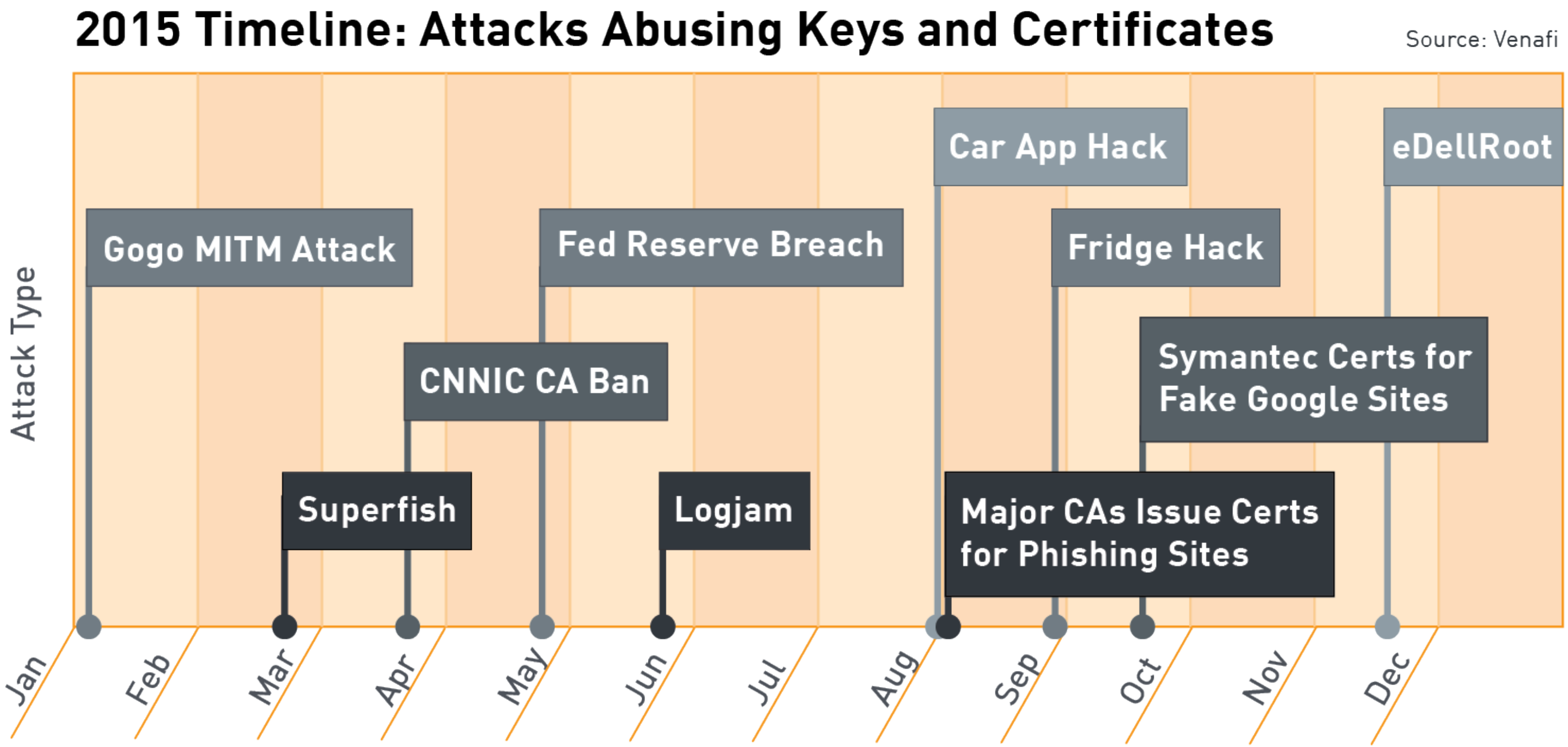


Cyber Criminal Activity

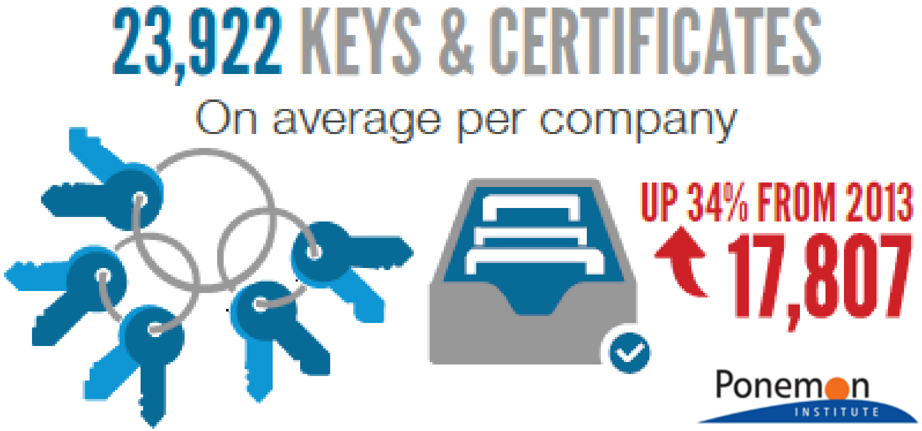
Cyber Criminals Misuse Unmanaged / Unprotected Keys and Certificates:

- Abuse their trusted status
- Hide in encrypted traffic—e.g., transmit malware or steal data
- Eavesdrop using man-in-the-middle (MITM) attacks
- Code-sign malware
- Spoof websites in phishing attacks

Increasing Attacks



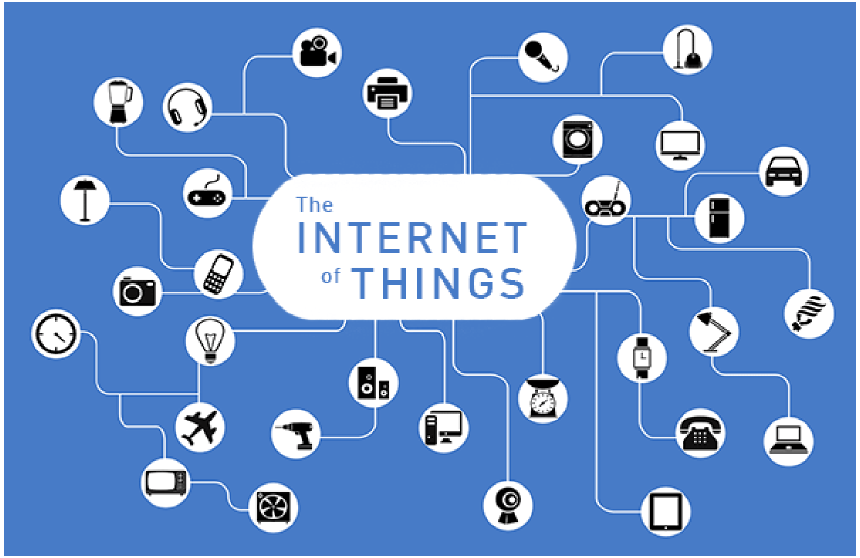
The Problem



- Increased management complexity
- Lack of knowledge/management of the trust model
- Human error/lack of education

Ponemon Institute. *2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point*. 2015.

And It’s Only Getting Worse…



4.9 Billion Connected "Things" in 2015—
up to 25 Billion by 2020

Gartner

Gartner Press Release. *Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015*. Nov. 11, 2014.

Real-world Case Study #1

As reported by Time, Bloomberg, and others, known Chinese cyber-espoinage operator, APT18, compromised a Fortune 200 American health services organization and stole data on 4.5 million patients.

Reconstructed by: Raxis CYBER SECURITY

Real-world Case Study #1

Attack Stage 1: Stole Private Keys

Attackers used

HEARTBLEED

To compromise private keys.

MANY STILL VULNERABLE
All those that did not replace all keys and certificates following Heartbleed

ATTACKERS BYPASSED SECURITY CONTROLS

In addition to Heartbleed, they could have used any of millions of malware variants that steal keys and certificates to bypass security controls.

Real-world Case Study #1

Attack Stage 2: Gained Access

ATTACKERS BREACHED THE COMPANY

Using stolen private keys and VPN credentials. The private keys were used to decrypt live data.

ATTACKERS BYPASSED SECURITY CONTROLS

Circumventing firewalls, authentication, and other security controls.

Real-world Case Study #1

Attack Stage 3: Expanded Foothold

ONCE IN, ATTACKERS WORKED TO ELEVATE PRIVILEGES AND EXPAND ACCESS

Stole or created new SSH keys and certificates for future backdoor access and exfiltration of data.

ATTACKERS BYPASSED SECURITY CONTROLS

Including firewall, authentication, VPN, and privileged access controls by using stolen keys and certificates to hide their activity.

Real-world Case Study #1

Attack Stage 4: Exfiltrated Data

ATTACKERS EXFILTRATED DATA USING SSL

Most security controls do not conduct SSL inspection or have ALL of the keys necessary to decrypt ALL traffic, leaving a huge blind spot

ATTACKERS BYPASSED SECURITY CONTROLS

Used encrypted SSL/TLS communications to bypass security controls, including DLP, IDS/IPS, threat detection, sandboxing, etc.

Real-world Case Study #2

Russian hacking group stole an SSL private key to conduct an effective phishing campaign of a Fortune 100 bank.

The attack went undetected for months and led to the loss of account information for tens of millions of customers.

Reconstructed by: Raxis CYBER SECURITY

Real-world Case Study #2

Attack Stage 1: Getting a Private Key

PURCHASED ON THE UNDERGROUND
Attackers purchased an SSL private key for a wildcard certificate for a Fortune 100 bank

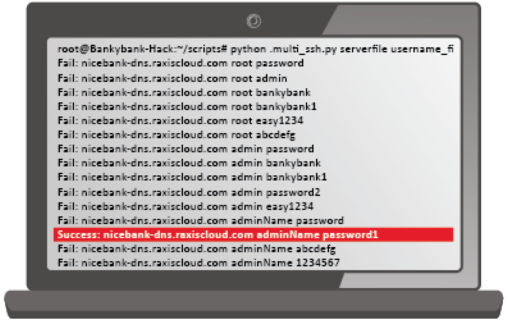
$1000 PRICE TAG
For a stolen certificate in the underground marketplace

ABUSING TRUST
How did the private key wind up for sale on the underground marketplace? Most likely it was stolen by malware or it might have been sold by an employee.

Real-world Case Study #2

Attack Stage 2: Gain Access to DNS

SSH BRUTE FORCE: Conducted an SSH brute force attack to get a username & password.



```
root@Bankybank-Hack:~/scripts# python .multi_ssh.py serverfile username_fi
Fail: nicebank-dns.raxiscloud.com root password
Fail: nicebank-dns.raxiscloud.com root admin
Fail: nicebank-dns.raxiscloud.com root bankybank
Fail: nicebank-dns.raxiscloud.com root bankybank1
Fail: nicebank-dns.raxiscloud.com root easy1234
Fail: nicebank-dns.raxiscloud.com root abcdefg
Fail: nicebank-dns.raxiscloud.com admin password
Fail: nicebank-dns.raxiscloud.com admin bankybank
Fail: nicebank-dns.raxiscloud.com admin bankybank1
Fail: nicebank-dns.raxiscloud.com admin password2
Fail: nicebank-dns.raxiscloud.com admin easy1234
Fail: nicebank-dns.raxiscloud.com adminName password
Success: nicebank-dns.raxiscloud.com adminName password1
Fail: nicebank-dns.raxiscloud.com adminName abcdefg
Fail: nicebank-dns.raxiscloud.com adminName 1234567
```

PRIVATE KEY WITH ROOT ACCESS: Searched the home directory tree and revealed a tarfile with a system backup, containing an SSH private key for root access.

MATCHING DOMAIN NAME TO CERTIFICATE: Inserted a DNS entry into the system zone file and the IP Address of a hacked server into the production DNS system.

Real-world Case Study #2

Attack Stage 3: Build a Phishing Website

A BELIEVABLE PHISHING WEBSITE

Attackers cloned a legitimate, reputable production website, but used the phishing URL.

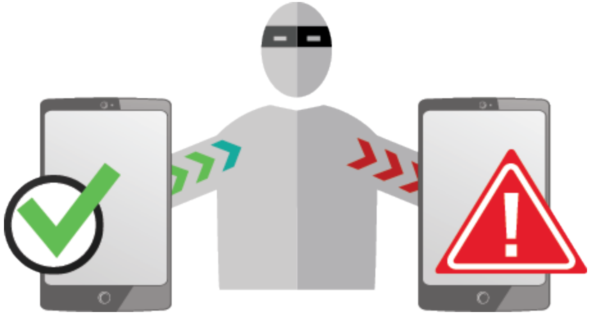
ABUSING TRUST

Using the stolen SSL certificate enabled the phishing site to display a valid certificate—along with a valid domain name and SSL/TLS encryption, this made a convincing phishing site.

Real-world Case Study #2

Attack Stage 4: Lure Victims

ROUTING USERS TO PHISHING SITE
Emails were sent to harvested email addresses for the bank's customers and employees.



ABUSING TRUST
When a user and password combination were entered, the fake site then redirected the end user to the legitimate site through a MITM approach.

What’s Needed

Protect Your Business

- Establish visibility, awareness, and a centralized inventory of keys and certificates
- Get control with enforced policies & workflows for certificate management
- Automate certificate lifecycle actions
- Educate, educate, educate

Benefits of Better Management

- Increase operational efficiencies
  - Avoid outages—increase system uptime
  - Reduce certificate lifecycle timeline

- Improve security
  - Know what should and shouldn’t be trusted
  - Strengthen investment in other security controls
  - Reduce attack vector with tighter control
  - Leverage trust model → don’t blindly trust everything

Apply What You Have Learned Today

- **Next week:**
  - Identify your current key and certificate management approaches
  - Read the full Raxis attack reconstructions to better understand vulnerabilities
- **Within three months:**
  - Conduct a full inventory of all keys and certificates, including a vulnerability assessment
  - Develop a management strategy, including policies and workflow
  - Evaluate tools to help automate key and certificate management & security
- **Within six months:**
  - Implement management & security tools
  - Begin phased approach to vulnerability remediation

Tips

- Don’t boil the ocean, it is a journey, one step at a time
- Educate, educate, educate
- Rinse and repeat—this is not a one time event

Questions

Case Study #1

Real-world Attack Case Study: Misuse of Keys and Certificates Bypass Critical Security Controls

http://research.crn.com/content51270

Case Study #2

Real-world Attack Case Study: Private Keys and Digital Certificates Used for Phishing and Breach of a Global Bank

http://whitepapers.fiercecio.com/content50888