Principles and Practices of **Cybersecurity**

Christine Pommerening, Ph.D.


SPYWARE
UPDATE
VIRUS
SECURITY
SPAM
HACKER
IDENTITY
PHISHING
FIREWALL
INTERNET
PASSWORD

Overview

- Problem – How bad is it?
- History – How did we get into this mess?
- Solution 1 – What can we do about it?
- Solution 2 – What does the government do about it?

National Cyber Security Centre

NCSC Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the **@NCSC** Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit **www.ncsc.gov.uk/glossary**.

Antivirus

Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Botnet

A network of infected devices, connected to the Internet, used to commit co-ordinated cyber attacks without their owners' knowledge.

Bring your own device (BYOD)

An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

Cloud

Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services.

Cyber attack

Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber security

The protection of devices, services and networks - and the information on them - from theft or damage.

Denial of Service (DoS)

DoS

When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Digital footprint

A 'footprint' of digital information that a user's online activity leaves behind.

Encryption

A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End user device

Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.

Firewall

Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.

Internet of Things (IoT)

Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Macro

MACRO

A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

Patching

Applying updates to firmware or software to improve security and/or enhance functionality.

Phishing

Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Ransomware

Malicious software that makes data or systems unusable until the victim makes a payment.

Software as a Service (SaaS)

Describes a business model where consumers access centrally-hosted software applications over the Internet.

Social engineering

Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Spear-phishing

A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Trojan

A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.

Two-factor authentication (2FA)

The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

Water-holing (watering hole attack)

Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling

Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

Whitelisting

Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.

Zero-day

0

Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

Overview

- Problem – How bad is it?
- History – How did we get into this mess?
- Solution 1 – What can we do about it?
- Solution 2 – What does the government do about it?

2013-2016

- Target breach (“Citadel”)
- OMB breach (China)
- Anthem breach (China)
- Clinton campaign hack and dump (WikiLeaks)
- IoT device exploit and botnet (“Mirai”)
- Dyn ISP distributed denial-of-service attack (“Mirai”)

2017

- NSA tools release (Shadow Brokers)
- Windows XP exploit ransomware (“WannaCry”)
- Ukraine infrastructure attack/ransomware(“Petya”)
- Cloudflare customer data leak (“Cloudbleed”)
- Macron campaign hack and dump (Fancy Bear)
- Equifax KBA exploit and breach (TBD)

Overview

- Problem – How bad is it?
- History – How did we get into this mess?
- Solution 1 – What can we do about it?
- Solution 2 – What does the government do about it?

1960s……..2020s

Decade	Network Technology	Device Development
1960s	ARPANET	Mainframes
1980s	TCP/IP	Client-Servers
1990s	WWW	Personal Computers
2000s	Social Media Apps	Wireless Devices
2010s	Cloud	Shared On-Demand Space
2020s	IoT	Autonomous Devices

1993……..2018

"On the Internet, nobody knows you're a dog."

On the Internet, someone knows you're a dog

This Is Us


Add to Cart
or 1-Click Checkout
Buy now with 1-Click®


Click Here to Like us on Facebook!
facebook

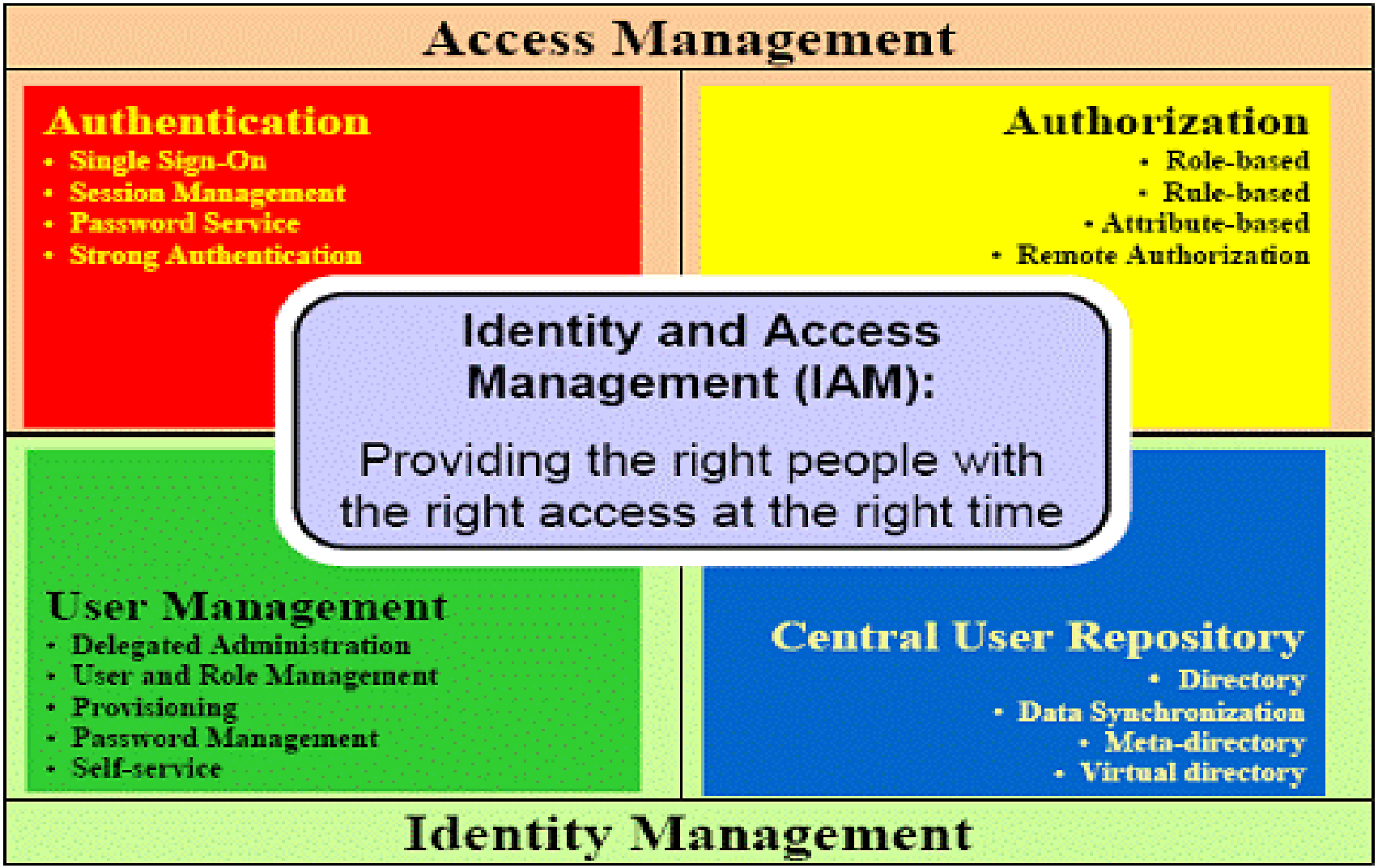

nest
AIRWAVE
74


UBER
UBER

Overview

- Problem – How bad is it?
- History – How did we get into this mess?
- Solution 1 – What can we do about it?
- Solution 2 – What does the government do about it?

I A M


Access Management
Authentication
• Single Sign-On
• Session Management
• Password Service
• Strong Authentication
Authorization
• Role-based
• Rule-based
• Attribute-based
• Remote Authorization
Identity and Access Management (IAM):
Providing the right people with the right access at the right time
User Management
• Delegated Administration
• User and Role Management
• Provisioning
• Password Management
• Self-service
Central User Repository
• Directory
• Data Synchronization
• Meta-directory
• Virtual directory
Identity Management

I A M

- What do ***you*** use?
- What have ***others*** used?

USER:	PASS:	USER:	PASS:
root	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbzd
root	54321	root	anko
support	support	root	zlxx.
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	ikwb
user	user	root	dreambox
admin	(none)	root	user
root	pass	root	realtek
admin	admin1234	root	00000000
root	1111	admin	1111111
admin	smcadmin	admin	1234
admin	1111	admin	12345
root	666666	admin	54321
root	password	admin	123456
root	1234	admin	7ujMko0admin
root	klv123	admin	1234
Administrator	admin	admin	pass
service	service	admin	meinsm
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		
guest	12345		


From:
Amazon <management@mazoncanada.ca> on behalf of
not an Amazon email address
(note the missing A in Amazon)
To: @sheridanc.on.ca
Cc:
Subject: Suspension
amazon.com
Dear Client,
Generic non-personalized greeting
We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.
To confirm your identity with us click the link bellow:
https://www.amazon.com/exec/obidos/sign-in.html
Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"
Sincerely,
The Amazon Associates Team
© 1996-2013, Amazon.com, Inc. or its affiliates

I A M

1. Be strong – Use strong and dedicated passwords
2. Be aware – Know your accounts
3. Beware – Check before you click
4. Double up – Use two-way authentication
5. Update – Keep software up to date
6. Backup – Have important info elsewhere
7. Unplug – Turn off devices when not needed
8. Privacy, please - Sharing is not caring

Overview

- Problem – How bad is it?
- History – How did we get into this mess?
- Solution 1 – What can we do about it?
- Solution 2 – What does the government do about it?

FISMA

- Federal Information Security Management Act of 2002
- Mandatory for all information systems owned or operated by a federal government agency in the executive or legislative branches, or by a contractor or other organization on behalf of a federal agency in those branches
- Key security standards and guidelines include FIPS 199, FIPS 200, and NIST SP 800-53 et al.

NIST-CSF

- National Institute of Standards and Technology – Cybersecurity Framework v.1.1
- Voluntary industry adoption
- Five Core Functions:
  - **Identify**
  - **Protect**
  - **Detect**
  - **Respond**
  - **Recover**
- Basic risk management approach
- Risks are probabilities related to specific threats, vulnerabilities, and consequences

NIST-CSF


software
objectives
improved
implemented
performed
detection
devices
systems
lessons
policy
internal
impact
security
recovery
analysis
communications
awareness
maintained
cybersecurity
information
stakeholders
vulnerability
documented
personnel
support
understood
monitored
consistent
response
responsibilities
incorporating
business
identified
events
strategy
activity
users
event
incidents
used
critical
risk
established
protection
timely
activities
vulnerabilities
determined
incident
procedures
external
processes
detect
manner
planning
plans
tested
unauthorized
roles
potential
data
understand
adequate
assets
ensure
physical
integrity
access
parties
policies
managed
mission
control
detected
organizational
learned
system
network
communicated
organization's
appropriate
partners
requirements
protected
management
maintenance
organization
coordinated
environment
authorized
executed
prioritized
operations

Conclusion

- The bad news:
  - There is no 100% security, or privacy
  - The government can (and should) only do so much
- The good news:
  - Even small measures make a difference:
    - Add a few extra characters to every password
    - Change passwords regularly, including hardware
    - Delete apps and accounts you don't need
  - Everyone can decide which trade-offs to accept:
    - Convenience versus control
    - Cost versus benefit