CPSC 526: Network Systems Security: Introduction and Key Concepts

Michael E. Locasto

Agenda

Piazza Poll (75% of class has not taken 418)

HW1 is released, due 3 Oct.

Q: Why Piazza, why wiki?

QoD: how do you “sniff” a packet?

QoD: [many] How do you secure a network?

Lecture: Important Network Security Concepts

Lecture/Demo: The Deception Surface

QoD

"How do you ‘sniff’ a packet?”

wireshark (GUI)

tshark, tcpdump (cmd line)

libpcap

[whatever it is your OS+NIC does]

QoD (from W15)

"What is the most practical way to protect a network?"

QoDs (from F15)

How secured is a "secured" network?

How do I set up a secure network from scratch?

What is the relation between all elements in network to provide security? The big picture, elements and relations between them and weak points and bottlenecks, what to improve and how?

Since the network is not secure, so how can I secure myself?

Is there a way to secure a network such that the only possible attack left is social engineering

Can you envisage any circumstances wherein a network is completely secure?

How unsecure is our general WiFi at home?

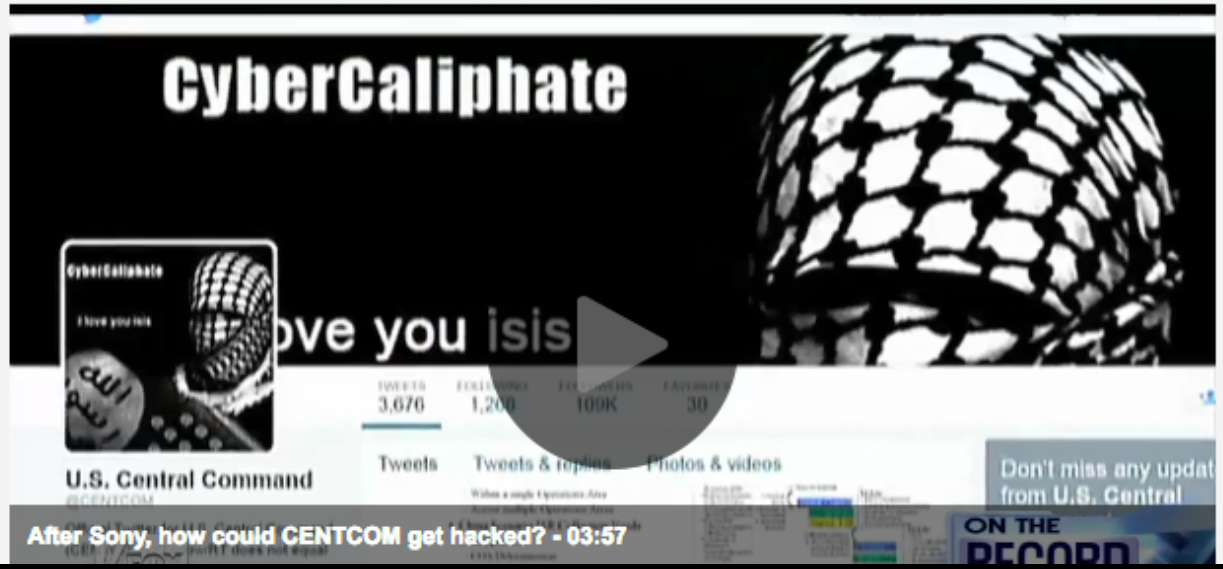
QoD

"What is the most practical way to protect a network?"

An Amazing Variety of Examples…

Twitter account for US Central Command hacked, filled with pro-ISIS messages

Published January 12, 2015 · FoxNews.com 5828 1588 4174



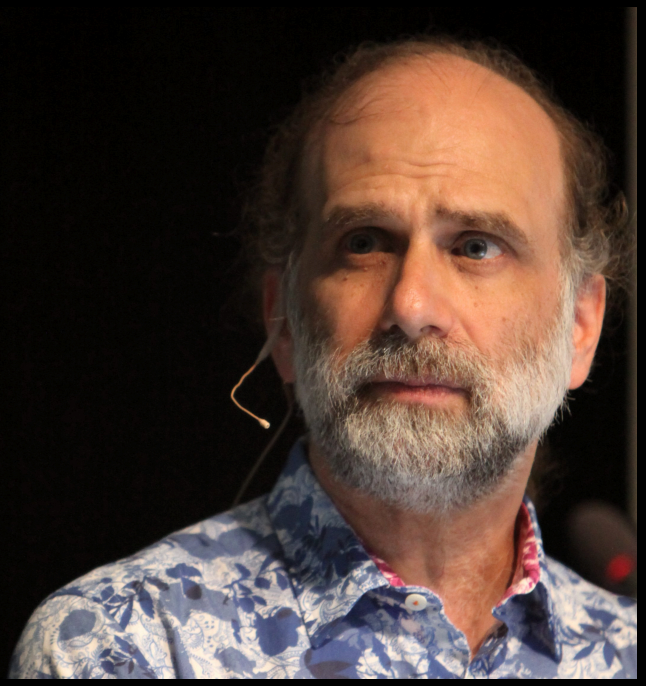
More on this...

CENTCOM Twitter, YouTube accounts hacked

Cyberattack embarrasses Obama, military

Bruce Schneier reminds us:

https://en.wikipedia.org/wiki/Bruce_Schneier#mediaviewer/File:Bruce_Schneier_at_CoPS2013-IMG_9174.jpg



"Security is a process, not a product."

QoD

"What is the most practical way to protect a network?"

QoD

"What is the most practical way to protect a network?"

practicality

protection

network

QoD

CryptoPro asks "What is the most practical way to protect a network?"

practicality (what kind of cost/benefit)?

protection (what security properties)?

network (what is a network, anyway)?

WHAT IS NETWORK SYSTEMS SECURITY?

NSS

Network systems security

Network systems security

ps. Network systems ***security***

Traditional Security

People, documents, property, money

- loss of control / availability (theft)
- loss of integrity (forgery)
- loss of secrecy / confidentiality (disclosure)

Locks, safes, walls, armed guards, forts, banks

- cf. The Great Train Robbery
- + Insurance, Redundancy

Important Concepts

Bellovin's Informal Law of Networking

- the network started as a benign environment

Malicious vs. accidental failure (Resilience, Fault tolerance, Byzantine Robustness)

Action at a distance

- attribution, identity

Security is about a cost / benefit analysis

No trust (I/O goes through enemy)

Bellovin's Laws of Networking

Networks Interconnect

Networks always interconnect

Interconnections happen at edges (i.e., no strict central control)

Security mechanisms often emerge from efforts to mediate access or interrupt connectivity

Threat Model

Achieving the "right" amount of security is ultimately a game of cost / benefit analysis

How powerful is the adversary? What are their capabilities? 10,000 GPUs? 5 mathematicians?

Rubber-hose cryptanalysis? Bribery? Blackmail? Undermining the standards process? The supply chain? The minds of students?

Two Primary Protection Problems

Isolation: Protecting / limiting access to resources (hosts, programs, channels, etc.)

Reliability: Protecting the conversation between Alice and Bob (integrity, confidentiality, availability)

Two Primary Protection Problems

In other words, ensure C-I-A of:

Data in flight
Data at rest
Network fabric (net elements are not dumb wires)

+ Execution integrity of communications endpoints

(and perhaps other properties like privacy, PFS, anonymity, non-repudiation, plausible deniability)

QoD: What is the most practical way to protect a network?

What threats do you expect? What assets are you protecting?

Best practices (firewalls, passwords, minimize vuln surface)

Unpredictable setup (don't trust defaults)

Strong cryptography & authentication

Limiting access in space and time

Simplicity of mechanism