
Michael E. Locasto
Agenda

Piazza Poll update (1/3 class has not taken 418)
Scribe request
Week 1 Reading: Chapter 23 in Kaufman et al.

QoD
Lecture: Important Network Security Concepts
offline: CEH exam, Q1-5
QoD

CryptoPro asks "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
Bruce Schneier reminds us:

“Security is a process, not a product.”
QoD

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

CryptoPro asks "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?

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 vulnerability)
Unpredictable setup (don’t trust defaults)
Strong cryptography & authentication
Limiting access in space and time
Simplicity of mechanism