How to Secure Electronic Data and Communications

Rotem Guttman

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

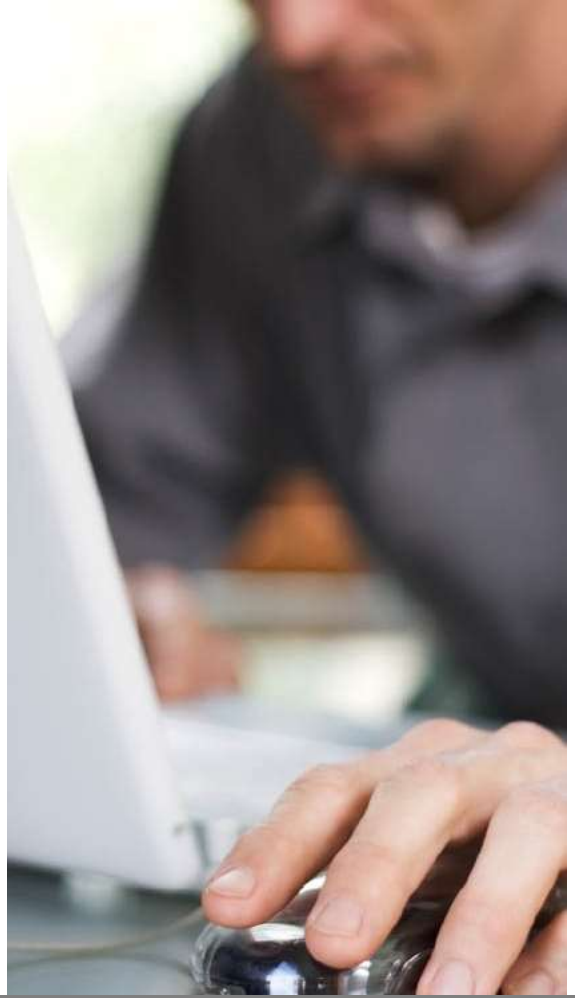
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-0617

How to Secure Electronic Data and Communications

- **Threat Models**
- **Defense Categories**
- **Defense Strategies**
- **Demonstration**

Disclaimer



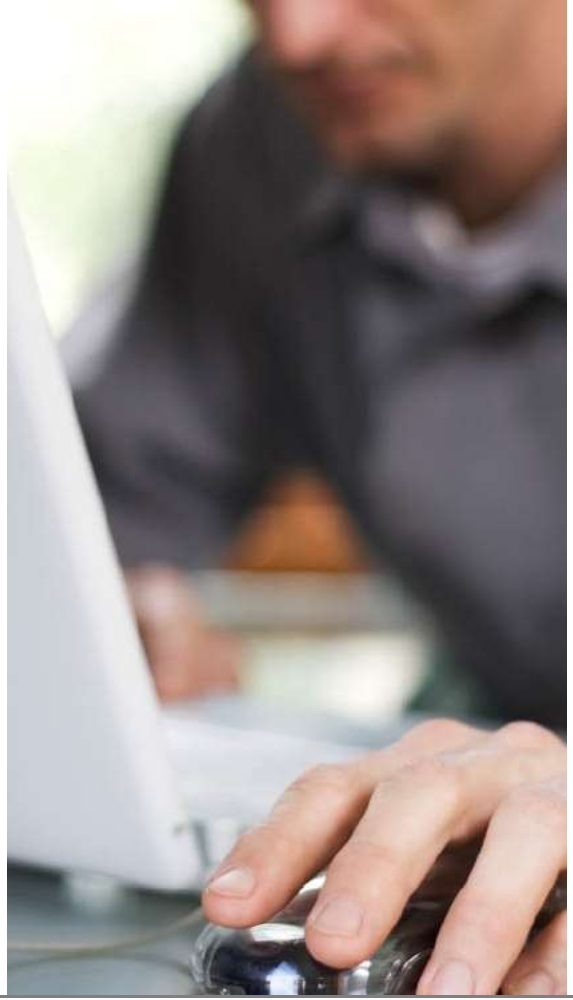
Disclaimer

This talk is aimed at a nontechnical audience and contains numerous simplifications and generalizations meant to convey complex subject matter in an understandable manner within the time constraints available.

Any comments made during this talk or the question and answer period should not be taken as an endorsement of any tool, company, or product. Any programs used in demonstrations are given as illustrative examples and their use should not be seen as an endorsement.

Threat Models

Know Your Enemy



Poll - Targeting

Know Your Enemy

- No one size fits all solution
- Identify critical assets
- Identify adversaries
  - Targeted vs Collateral

Considerations:

- Scale
- Collaboration needs
- Resource Availability

Know Your Enemy

- No one size fits all solution
- Identify critical assets
- Identify adversaries
  - Targeted vs Collateral

What is required for you?

What is required for your clients?

Know Your Enemy

- No one size fits all solution
- Identify critical assets
- Identify adversaries
  - Targeted vs Collateral

Who would target you?

- Untargeted attacks
  - Internet Background Radiation
- Unskilled attackers
  - Script Kiddies
- Skilled attackers
  - Cybercriminals
  - Cyber-activists
  - Nation-states
- Insider threats
  - Not just YOUR insiders

Know Your Enemy

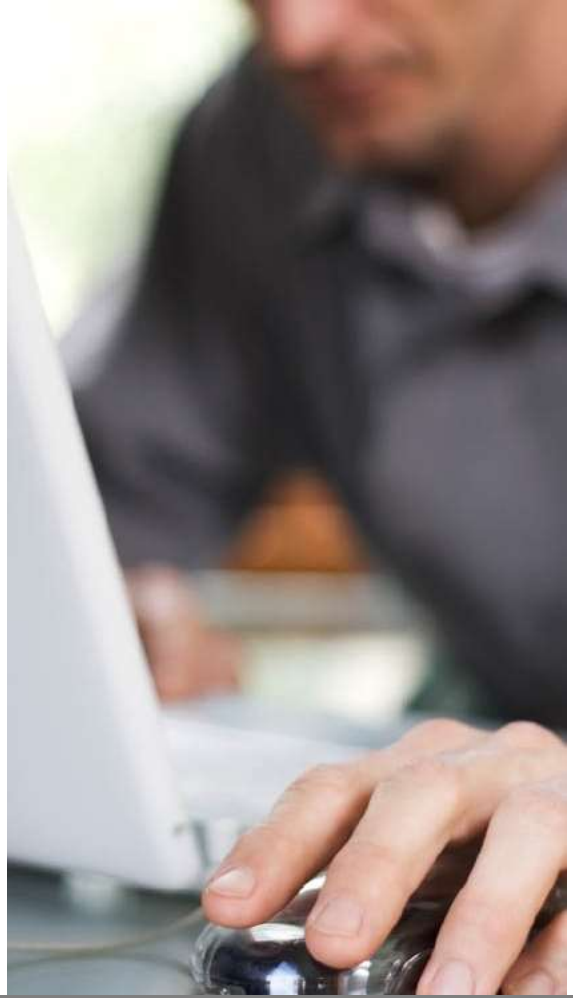
- No one size fits all solution
- Identify critical assets
- Identify adversaries
  - Targeted vs Collateral

You are all targets:

- Insider trading
- Client Extortion
- Ransomware
- Crypto-mining

Defense Categories

Security is Fractal…



Security is Fractal…

..every part of it is as complicated as the whole.

- Weakest Link Problem

- Data at Rest
- Data in Transit
- Data in Use

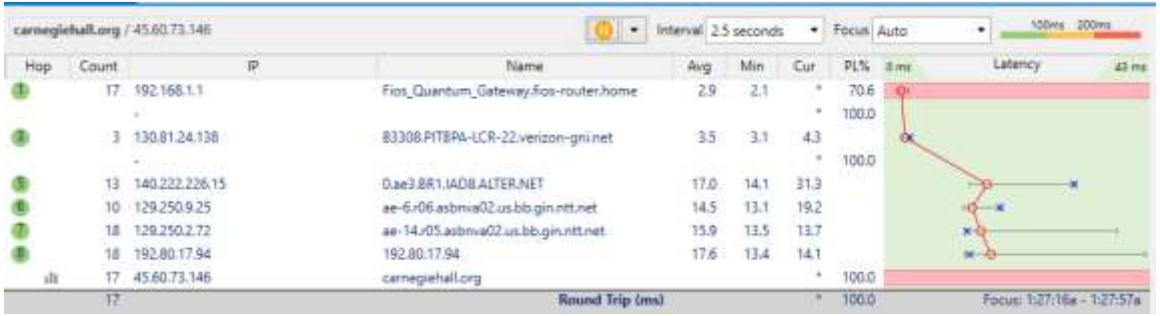
Data in Transit

"The internet"

- Translation:
  The "not your net"
- Routing

Alphabet Soup

- SSL/TLS
  - Encrypted tunnel



Data in Transit

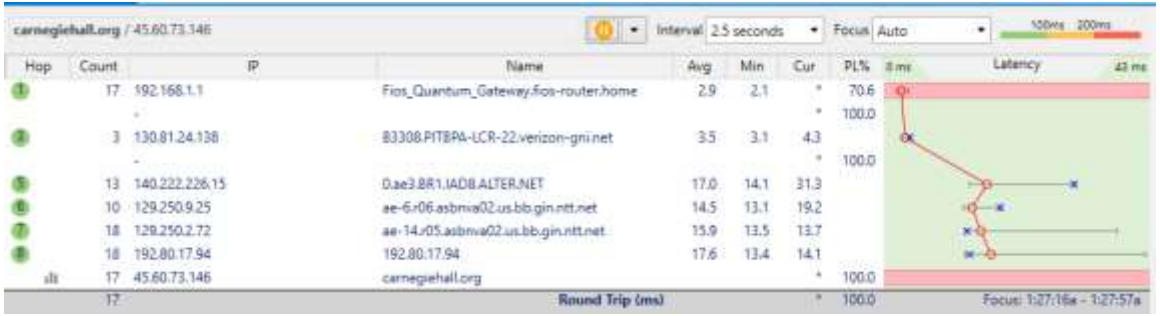
"The internet"

- Translation:
  The "not your net"
- Routing

Alphabet Soup

- SSL/TLS
  - Encrypted tunnel

How do you get to Carnegie Hall?



Data in Transit

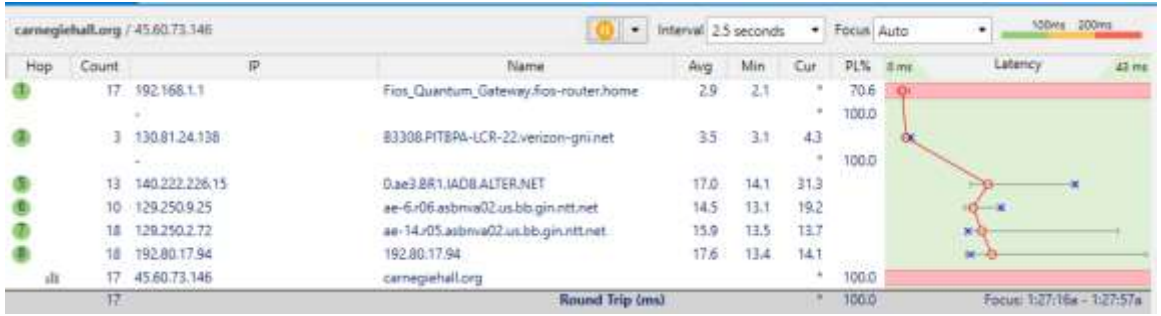
"The internet"

- Translation:
  The "not your net"
- Routing

Alphabet Soup

- SSL/TLS
  - Encrypted tunnel

How do you get to Carnegie Hall?



Practice, Practice, Practice

Data in Transit

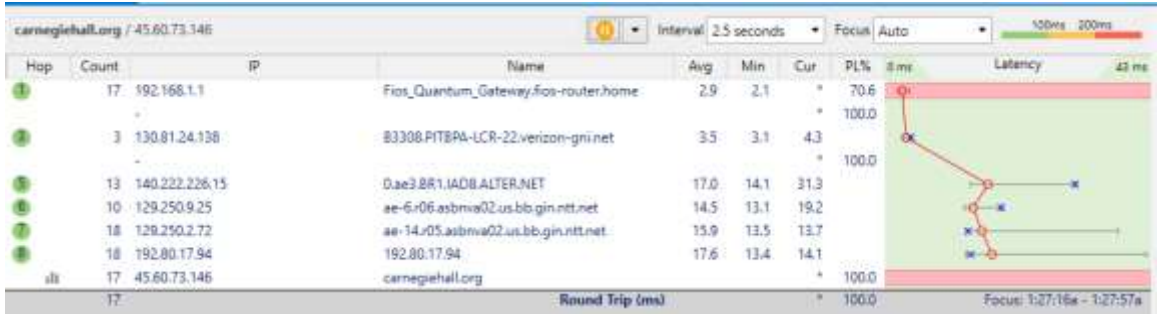
"The internet"

- Translation:
  The "not your net"
- Routing

Alphabet Soup

- SSL/TLS
  - Encrypted tunnel

How do you get to Carnegie Hall?



~~Practice, Practice, Practice~~
Correction: Via Japan.

Data at Rest

Encryption

- File
- Partition
- Drive

- Storage Devices
  - Mobility
- Storage Locations
  - Jurisdiction(s)
    - sshfs example
- Storage Services
  - “The Cloud”

Data in Use

Keys to the Kingdom

- Access to variety of data

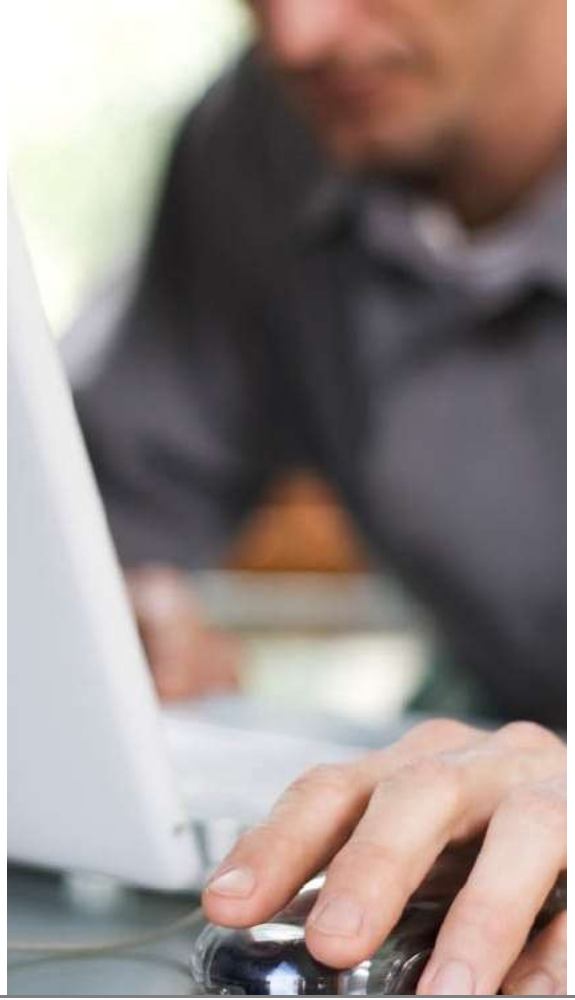
Bypasses Encryption

- Data must be decrypted to be useful*

* Not including homomorphic encryption solutions, or working memory encryption solutions.

Defense Strategies

(Fire)walls are not enough



Poll - Devices

Defense Strategies

- Must match threat model
- Defense in Depth
- Principal of Least Privilege
- Minimize Attack Surface
- Situational Awareness

- Each client may require updating the adversary model
- Asymmetric Capabilities
- Due Diligence for traffic tickets looks different than for political dissidents

Defense Strategies

- Must match threat model
- Defense in Depth
- Principal of Least Privilege
- Minimize Attack Surface
- Situational Awareness

- The border is not sufficient
- Minimizes damage when compromised
- Multifactor

Defense Strategies

- Must match threat model
- Defense in Depth
- Principal of Least Privilege
- Minimize Attack Surface
- Situational Awareness

Need to know basis, and you don't need to know!

- Applications
  - Run as a limited user
- Users
  - Minimal permission
  - Timely Revocation
- Devices
  - BYOD?

Defense Strategies

- Must match threat model
- Defense in Depth
- Principal of Least Privilege
- Minimize Attack Surface
- Situational Awareness

Once again…

- Applications
  - What needs to run?
- Users
  - Who needs to do what?
- Devices
  - Where is it allowed to be done from?

Defense Strategies

- Must match threat model
- Defense in Depth
- Principal of Least Privilege
- Minimize Attack Surface
- Situational Awareness

If you were compromised, would you know?

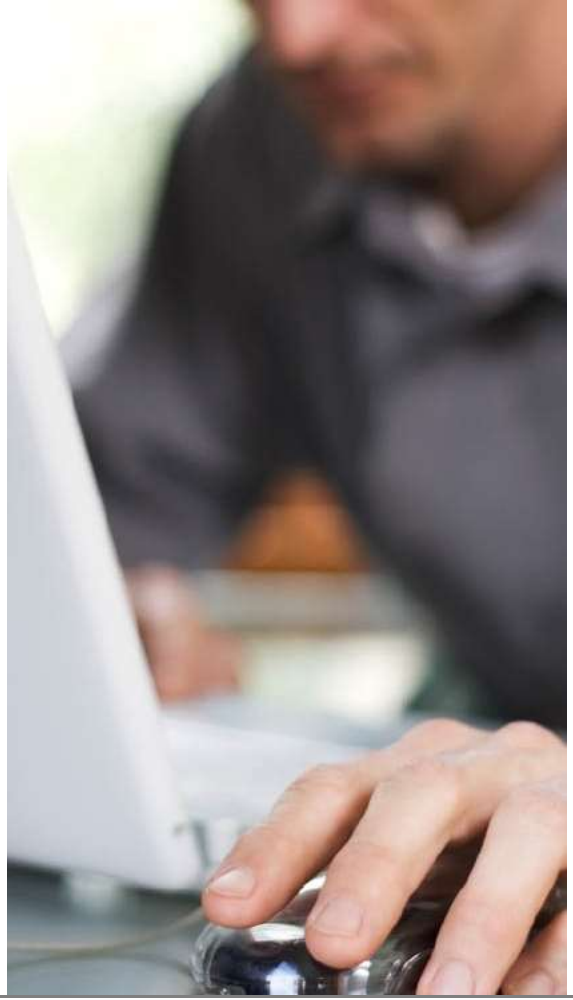
Average time from exploit to detection: **206 days***

* IBM - 2019 Cost of a Data Breach Report

How to Secure Electronic Data and Communications

Demonstration

Tool Use



Data At Rest

Data in Transit

Questions