# SECURITY OBJECTIVES

EN.600.424

Fall 2018

Lecture Notes

# NETWORK SECURITY GOALS

- Confidentiality
- Integrity
- Availability

- These are goals incorporated into policy

# *NOT* CRYPTO FEATURES

- Confidentiality
- Integrity
- Authentication

- Related, but not identical to system objectives

# CONFIDENTIALITY

- What is it?

  Confidentiality is a ***requirement*** whose purpose is to keep sensitive information from being disclosed to unauthorized recipients. (Nap)

- Why is it important?
- How do we enforce it?
  - ***NOT JUST CRYPTO!!!***

# CONFIDENTIALITY IN NETWORKS

- Typically, we're interested in ***data in motion***
- However, network protocols can expose data at rest (heartbleed)
- Examples?

# INTEGRITY

- What is it?

  Integrity is a requirement meant to ensure that information and programs are changed only in a specified and authorized manner. (Nap)

- Why is it important?
- How is it enforced?

# INTEGRITY IN NETWORKS

- Typically, ensuring that a message isn’t altered enroute
- But, also ensuring that remote parties are authenticated
- Other examples?

# AVAILABILITY

- What is it?

  Availability is a requirement intended to ensure that systems work promptly and service is not denied to authorized users (Nap)

- Why is it important?
- How is it enforced?

# AVAILABILITY IN NETWORKS

- Typically, controlling bandwidth consumption
- But also preventing individual systems from overload

# WHERE DOES NETWORKING END?

- Applicability to "network" security is broad
- Vulnerabilities of host applications, O/S, etc matter
- We will primarily focus on communication protocols

# IAAA

- Identification
- Authentication
- Authorization
- Accounting (audit)

# IDENTIFICATION

- Security goals are meaningless without identities
- Historically, an identity is a “label” tied to a principal
- I am a principal, I have different labels on different systems
- Some labels are becoming global (e.g., email address)
- Labels can also be role-based, etc

# AUTHENTICATION

- The process by which a label is determined/assigned
- A principal connects to a system. What label do they get?
- Typically, a principal claims a label and then proves ownership

# AUTHORIZATION

- Permissions
- What is a principal, authenticated under a label, able to do?
- Can also determine QoS, etc

# ACCOUNTING (AUDIT)

- Record/Trace activities of the authorized/authenticated ID
- Good for forensics
- But also good to enforce accountability
- In earlier days, was used to charge for computer use

# ACCESS CONTROLS

- Access controls are "center of gravity" for security
  - Primarily focused on Authorization and Audit
  - Authenticated identity is typically assumed
  - Goal is to enforce limits
- Most of our familiarity is for access to systems
- Access controls are also used in networks

# QUICK OVERVIEW IN SYSTEMS

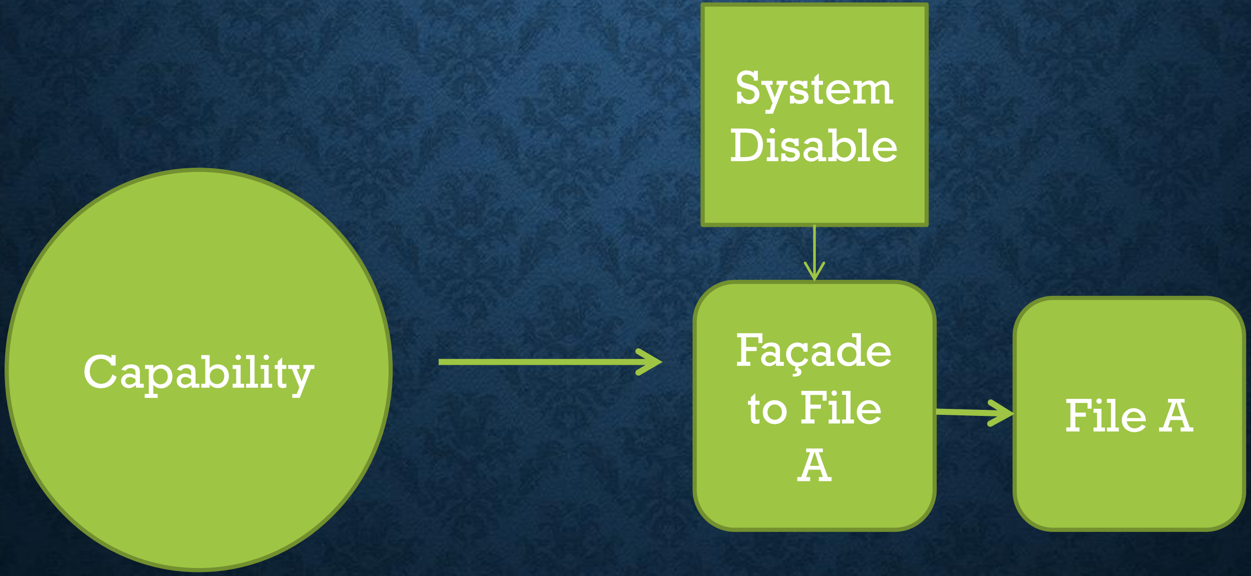
- Hardware
- O/S
- “Middleware”
- Application

# TWO TYPICAL APPROACHES

- Access control model
    - Columns for resources
    - Rows for identities
    - At each matrix element stores permissions
- Access control list
    - Store by column (e.g., per resource)
- Capabilities (less common)
    - Store by row (e.g., per identity)

# CAPABILITY ARGUMENT

- Opponents of capabilities argue that you cannot change a file's status
- They just don't understand capabilities



Capability

System Disable

Façade to File A

File A

# NETWORK ACCESS CONTROLS

- Identification mechanisms
  - Address/attribute
  - Session identifiers
  - Systems (portals, RADIUS, authenticators)
- Access controls
  - Mostly “connect” (e.g., send/receive)
  - Could envision “modify” (e.g., for routers)

# RADIUS AND NAS

- Remote Authentication Dial-in User Service (orig 1991!)
- Network Access Server
  - Control access to network resources
  - Sends RADIUS Access Request for Authentication/Authorization
  - Sends RADIUS Accounting Request for Audit

# APPLICATION IAAA

- Distributed applications require AAA
- Often rely on network protocols for some elements of AAA
  - TLS often provides some authentication for servers
  - Mutual TLS is used for some machine-to-machine stuff
- Moreover, sessions are *trusted* to maintain authentication!

# FIREWALL ACCESS CONTROLS

- Attribute based (address, size, type)
- Identity based (using a portal or a client-side cert)
- Authorizations include
  - Access to networks, machines, and ports
  - Audit levels
  - Trust levels