SY110
Pillars of Cyber Security

Major Brian Hawkins, USMC

U.S. Naval Academy

Fall AY 2018

Outline

What **is** security?

Protecting computers?

- If we were *only* interested in safeguarding the physical machines, a safe would solve our problems. . .
- . . . but a powered-down machine in a safe isn't useful.

Protecting data?

- If we *only* needed to protect data, we could lock up the hard drive. . .
- . . . but this isn't useful either; the hard drive needs to be read by a computer to access the data.

Information Systems

What we're really trying to secure is an **information system**, something that can store, process, and transmit data other parts of the network.

What **is** security?

Protecting computers?

- If we were *only* interested in safeguarding the physical machines, a safe would solve our problems. . .
- . . . but a powered-down machine in a safe isn't useful.

Protecting data?

- If we *only* needed to protect data, we could lock up the hard drive. . .
- . . . but this isn't useful either; the hard drive needs to be read by a computer to access the data.

Information Systems

What we're really trying to secure is an **information system**, something that can store, process, and transmit data other parts of the network.

What **is** security?

Protecting computers?

- If we were *only* interested in safeguarding the physical machines, a safe would solve our problems. . .
- . . . but a powered-down machine in a safe isn't useful.

Protecting data?

- If we *only* needed to protect data, we could lock up the hard drive. . .
- . . . but this isn't useful either; the hard drive needs to be read by a computer to access the data.

Information Systems

What we're really trying to secure is an **information system**, something that can store, process, and transmit data other parts of the network.

What **is** security?

Protecting computers?

- If we were *only* interested in safeguarding the physical machines, a safe would solve our problems...
- ...but a powered-down machine in a safe isn't useful.

Protecting data?

- If we *only* needed to protect data, we could lock up the hard drive...
- ...but this isn't useful either; the hard drive needs to be read by a computer to access the data.

Information Systems

What we're really trying to secure is an **information system**, something that can store, process, and transmit data other parts of the network.

Cyber Security

In general, we talk about the "Five Pillars of Cyber Security"

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Authentication

Confidentiality

What is it?

The protection of information from disclosure to unauthorized individuals, systems, or entities. **Data oriented**.

Examples

- Credit card data stolen from Target hack.
- An eavesdropper snooping on a conversation.
- Passively capturing unencrypted traffic on a public wireless network.

Confidentiality

What is it?

The protection of information from disclosure to unauthorized individuals, systems, or entities. **Data oriented**.

Examples

- Credit card data stolen from Target hack.
- An eavesdropper snooping on a conversation.
- Passively capturing unencrypted traffic on a public wireless network.

Integrity

What is it?

Protection of information, systems, and services from unauthorized modification or destruction. **Data oriented**.

Examples

- Stuxnet worm – modified Iranian centrifuge control system programs
- Flipping bits in an encrypted email
- Unauthorized users modifying data
- Server crashes that corrupt files

Integrity

What is it?

Protection of information, systems, and services from unauthorized modification or destruction. **Data oriented**.

Examples

- Stuxnet worm – modified Iranian centrifuge control system programs
- Flipping bits in an encrypted email
- Unauthorized users modifying data
- Server crashes that corrupt files

Availability

What is it?

Timely, reliable access to data and information services by *authorized* users. **Service oriented**.

Example

- Russia's *Denial-of-Service (DoS)* attack on Georgian infrastructure.
- Redundancy of services provided – *e.g.* a backup mail server in case primary fails

Availability

What is it?

Timely, reliable access to data and information services by *authorized* users. **Service oriented**.

Example

- Russia's *Denial-of-Service (DoS)* attack on Georgian infrastructure.
- Redundancy of services provided – *e.g.* a backup mail server in case primary fails

Non-repudiation

What is it?

The ability to correlate, with high certainty, a recorded action with its originating individual or entity. **Entity oriented**.

Examples

- Manipulating/deleting access log files of a computer or network
  - Makes it difficult or impossible to determine who made certain changes within a system.
- Manipulating/deleting financial transaction logs
  - Makes it difficult to prove that an action took place, like transfers of money or purchases of stock, etc.

Non-repudiation

What is it?

The ability to correlate, with high certainty, a recorded action with its originating individual or entity. **Entity oriented**.

Examples

- Manipulating/deleting access log files of a computer or network
  - Makes it difficult or impossible to determine who made certain changes within a system.
- Manipulating/deleting financial transaction logs
  - Makes it difficult to prove that an action took place, like transfers of money or purchases of stock, etc.

Authentication

What is it?

The ability to verify the identity of an individual or entity. **Entity oriented**.

Examples

- Using stolen credentials to access files or areas on a system for which a user doesn't have authorization.
- RSA security services compromised in 2011 – allowed attackers to log into systems at Lockheed and other companies using stolen credentials of employees.

Authentication

What is it?

The ability to verify the identity of an individual or entity. **Entity oriented**.

Examples

- Using stolen credentials to access files or areas on a system for which a user doesn't have authorization.
- RSA security services compromised in 2011 – allowed attackers to log into systems at Lockheed and other companies using stolen credentials of employees.

Services vs. Security

There is always tension between the services that are provided to users versus the risk brought by providing these services.

- Physical-world example
  - A building with no doors or windows
- Cyber example
  - A shut down computer in a vault

Often, there is no "right" answer, and the decision of whether to allow a service is based on the potential risk.

Services vs. Security

There is always tension between the services that are provided to users versus the risk brought by providing these services.

- Physical-world example
  - A building with no doors or windows
- Cyber example
  - A shut down computer in a vault

Often, there is no "right" answer, and the decision of whether to allow a service is based on the potential risk.

Services vs. Security

There is always tension between the services that are provided to users versus the risk brought by providing these services.

- Physical-world example
  - A building with no doors or windows
- Cyber example
  - A shut down computer in a vault

Often, there is no "right" answer, and the decision of whether to allow a service is based on the potential risk.

Questions

Questions?