NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Learning Principles for Cybersecurity Practice

January 29, 2020

NICE Framework Knowledge Descriptions

K0004: Knowledge of cybersecurity and privacy principles.

Center for Applied Cybersecurity Research

Learning Principles for Cybersecurity Practice

An Introduction to the Information Security Practice Principles

29 JAN 2020

POLL

Roadmap

1. Background
2. The Principles: Walkthrough
3. The Principles In Action

THE PRINCIPLES

1. **Comprehensivity** (“*Am I covering all of my bases?*”)
   Identify and account for all relevant systems, actors, and risks in the environment.
   Related concepts: Complete Mediation, End-to-end Encryption, Reconnaissance, Inventory
2. **Opportunity** (“*Am I taking advantage of my environment?*”)
   Take advantage of the actor relationships, material resources, and strategic opportunities available in the environment.
   Related concepts: Information Sharing, White Hat Testing, Deception, Common Tools
3. **Rigor** (“*What is correct behavior, and how am I ensuring it?*”)
   Specify the expected states, behaviors, and processes governing the relevant systems and actors.
   Related concepts: Governance, Requirements, Monitoring, Audits, Follow-Through
4. **Minimization** (“*Can this be a smaller target?*”)
   Minimize the size, quantity, and complexity of what is to be protected, and limit externally facing points of attack.
   Related concepts: Attack Surface, Compactness, Data Minimization
5. **Compartmentation** (“*Is this made of distinct parts with limited interactions?*”)
   Isolate system elements, and enable and control the interactions that are strictly necessary for their intended purposes.
   Related concepts: Modularity, Forward Secrecy, Least Privilege, Air Gapping, Cryptography
6. **Fault Tolerance** (“*What happens if this fails?*”)
   Anticipate and address the potential compromise and failure of system elements and security controls.
   Related concepts: Resilience, Failsafe Defaults, Defense in Depth, Revocability
7. **Proportionality** (“*Is this worth it?*”)
   Tailor security strategies to the magnitude of the risks, accounting for the practical constraints imposed by the mission and the environment.
   Related concepts: Risk Management and Acceptance, Usability

Background

Our purpose was to identify the underlying and invariant principles that inform cybersecurity and information security generally…

...those which have driven and guided information security decision-makers across technologies, sectors, and epochs.

Principle (n.)

A general law or rule adopted or professed as a guide to action; a settled ground or basis of conduct or practice; a fundamental motive or reason for action, esp. one consciously recognized and followed.

-Oxford English Dictionary, online

What is "Cybersecurity"?

1. Surprisingly contentious
2. Names are hard:
   a. "Information Security," "IT Security," "Computer Security," "Assurance"
      i. Do you hyphenate?
         1. One word or two?
            a. Nobody knows . . .
3. Blue padlocks are somehow involved
4. Goal: Mission Assurance

Why?

1. **Cybersecurity needs a foundational mental model.** Cybersecurity rarely has simple “right answers.” Our decision-making model must confront complex problems.
2. **Cybersecurity needs to support broad, novel analyses.** Cybersecurity canon is too often highly detailed/technical, narrowly applicable, and highly prescriptive.
3. **Cybersecurity needs a scalable model of education.** We cannot rely entirely on master-apprentice, mimetic transfer of knowledge and know-how. We need universal tools.
4. **Cybersecurity literacy is necessary for all decisionmakers.** People up and down the chain of command need to understand information security fundamentals.

Methodology

1. Feasibility review of prior work.
   - Has anyone else successfully unearthed and collected these principles? If so, how clearly, rigorously, and comprehensively? (*See, in particular*, Saltzer & Schroeder, 1975)
   - Where else have we found sets of principles that help communities frame and solve problems? (*See, e.g.*, Fair Information Practice Principles, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf) See pg. 45
   - Very broad search (across related fields and throughout history) for evidence of the principles.
2. Apply selection and tailoring criteria.

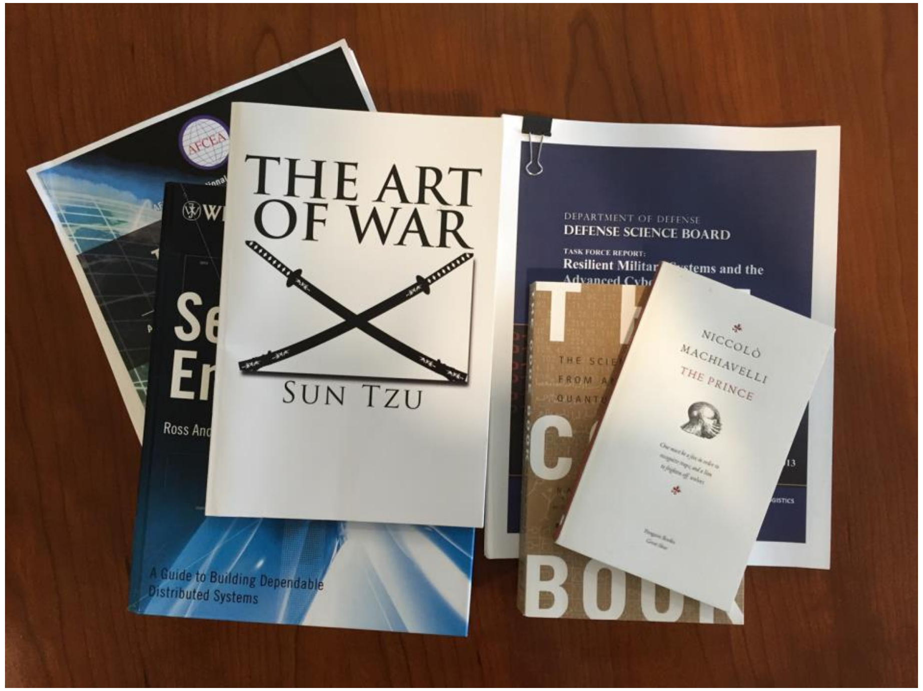
Selection and Tailoring Criteria (full set)

1. Sufficiently inclusive of the practice of information security. *Did we miss anything?*

2. Internal consistency. The principles must be able to logically interact, even if those interactions mean they come into conflict in practical application.

Selection and Tailoring Criteria (per principle)

1. Grounded in prior work
2. Guides action
3. Causally related to security outcomes
4. Work across time and space
5. Clarity for multiple audiences



Principles Overview

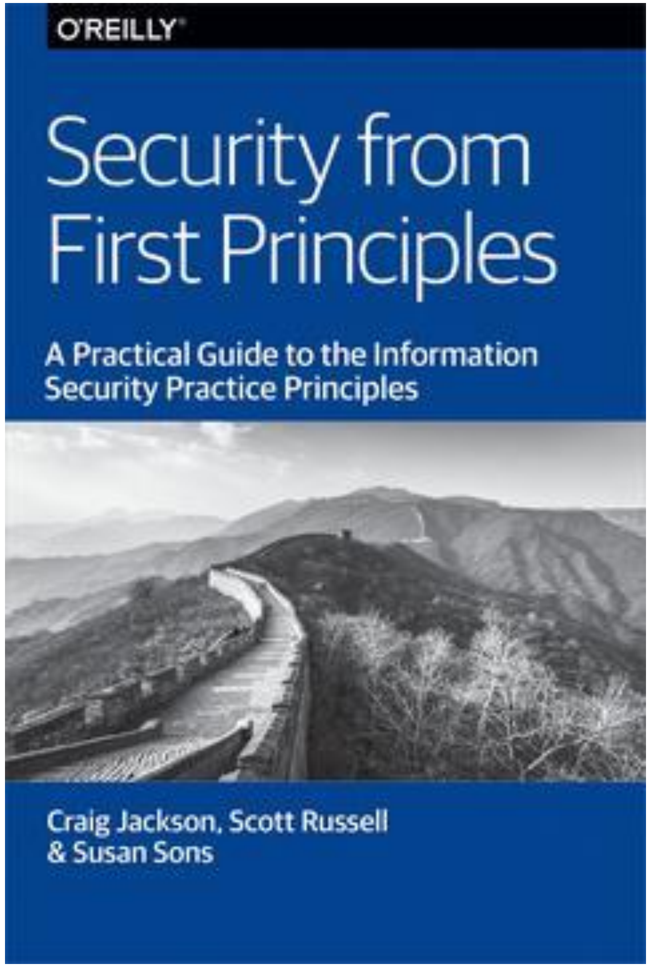
- **Mental Model:** The Principles structure how you think about cybersecurity
- **Decision-Making:** The Principles emphasize decision-making
    - Particularly when there is *limited time* or *no clear* best approach
- **A Set:** They work individually, but (more importantly) as a set.
- **General Purpose:** The Principles apply in every scenario, but are specialized to none; their use should be supplemented with *evidence*
- **Aspirational:** the Principles are not a state you achieve; they guide action

Applications

1. Cybersecurity Education & Training
2. Cybersecurity Assessments
3. Cybersecurity Decisionmaking
4. Cybersecurity Communication
5. Analysis of Frameworks/Best Practices

More Resources

- ISPP Foundational Whitepaper
    - Our most complete discussion of the Principles currently available.
    - Available at: https://cacr.iu.edu/principles/ISPP-Foundational-Whitepaper-2017.pdf
- O'Reilly "Security from First Principles"
    - Shorter, written for a more general technologist audience



O'REILLY

Security from First Principles

A Practical Guide to the Information Security Practice Principles

Craig Jackson, Scott Russell & Susan Sons

Q&A

POLL

The Principles

A walkthrough

1. **Comprehensivity** ("*Am I covering all of my bases?*")
   Identify and account for all relevant systems, actors, and risks in the environment.
   Related concepts: Complete Mediation, End-to-end Encryption, Reconnaissance, Inventory
2. **Opportunity** ("*Am I taking advantage of my environment?*")
   Take advantage of the actor relationships, material resources, and strategic opportunities available in the environment.
   Related concepts: Information Sharing, White Hat Testing, Deception, Common Tools
3. **Rigor** ("*What is correct behavior, and how am I ensuring it?*")
   Specify the expected states, behaviors, and processes governing the relevant systems and actors.
   Related concepts: Governance, Requirements, Monitoring, Audits, Follow-Through
4. **Minimization** ("*Can this be a smaller target?*")
   Minimize the size, quantity, and complexity of what is to be protected, and limit externally facing points of attack.
   Related concepts: Attack Surface, Compactness, Data Minimization
5. **Compartmentation** ("*Is this made of distinct parts with limited interactions?*")
   Isolate system elements, and enable and control the interactions that are strictly necessary for their intended purposes.
   Related concepts: Modularity, Forward Secrecy, Least Privilege, Air Gapping, Cryptography
6. **Fault Tolerance** ("*What happens if this fails?*")
   Anticipate and address the potential compromise and failure of system elements and security controls.
   Related concepts: Resilience, Failsafe Defaults, Defense in Depth, Revocability
7. **Proportionality** ("*Is this worth it?*")
   Tailor security strategies to the magnitude of the risks, accounting for the practical constraints imposed by the mission and the environment.
   Related concepts: Risk Management and Acceptance, Usability

Comprehensivity

Comprehensivity: What is it?

The Principle: Identify and account for all relevant systems, actors, and risks in the environment.

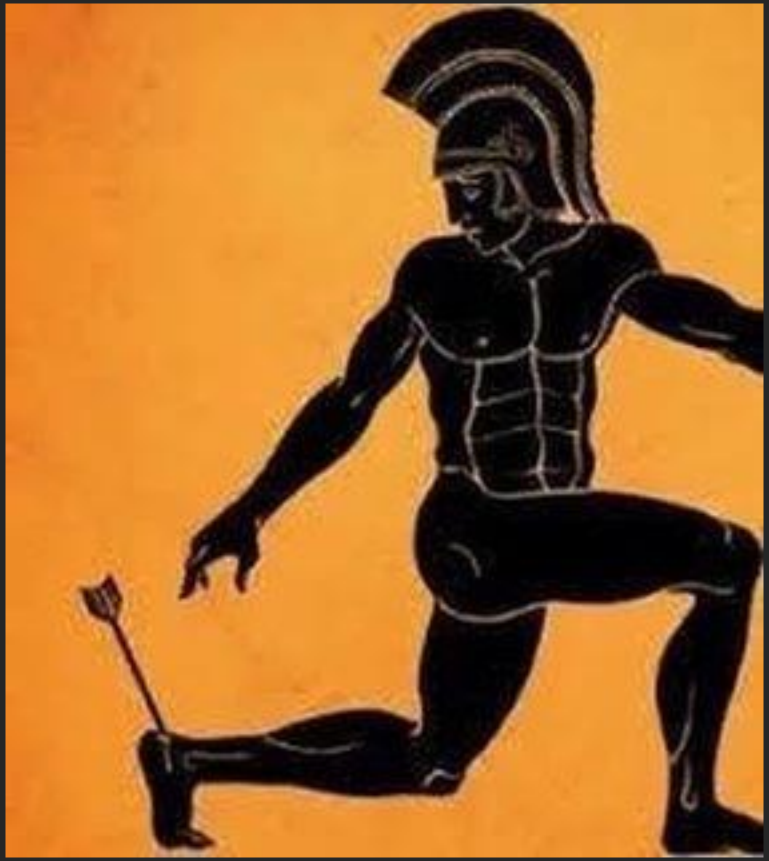
Key Question: Am I covering all of my bases?

Related Concepts: Complete Mediation, End-to-End Encryption, Reconnaissance, Inventory, Threat Modeling

Comprehensivity: Example

Achilles’ Heel:

- A single vulnerability can undermine an otherwise “invulnerable system”
- Attackers will prioritize your weak points: so should you



Opportunity

Opportunity: What is it?

The Principle: Take advantage of the actor relationships, material resources, and strategic opportunities available in the environment.

Key Question: Am I taking advantage of my environment?

Related Concepts: Information Sharing, White Hat Testing, Deception, Common Tools

Opportunity: Example

DOD Bug Bounty Program:

- DOD has launched half a dozen bug bounty programs since 2016
- Researchers have identified more than 5000 flaws
- Program is now being expanded to include more sensitive DOD assets

Rigor

Rigor: What is it?

The Principle: Specify and enforce the expected states, behaviors, and processes governing the relevant systems and actors.

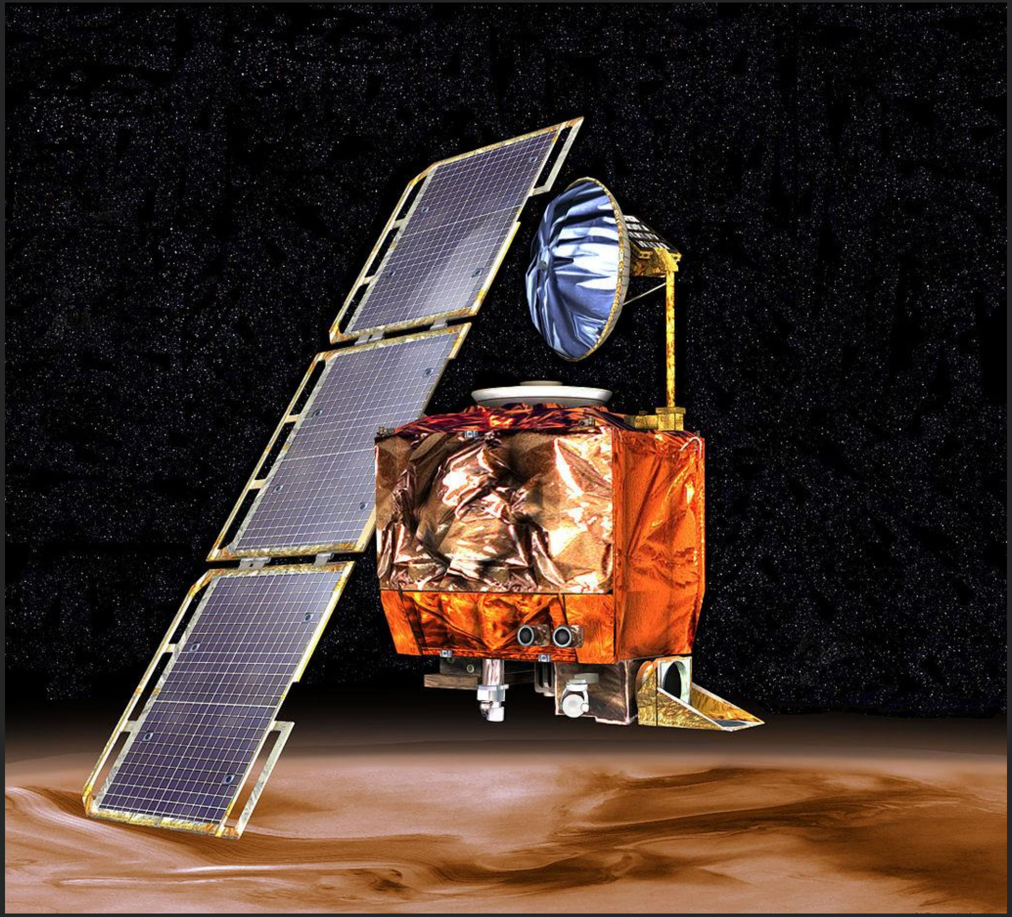
Key Question: What is correct behavior, and how am I ensuring it?

Related Concepts: Governance, Requirements, Monitoring, Audits

Rigor: Example

Mars Climate Orbiter:

- Burned up in the Martian atmosphere rather than going into orbit
- Lockheed Martin engineers typically express force in pounds.
- NASA engineers assumed the software was converted to use metric units but was off by a factor of 4.5
- NASA soon abandoned “better, cheaper, faster” as their mantra



By NASA/JPL/Corby Waste - http://www.vitalstatistics.info/uploads/mars%20climate%20orbiter.jpg (see also http://www.jpl.nasa.gov/pictures/solar/mcoartist.html), Public Domain, https://commons.wikimedia.org/w/index.php?curid=390903

Minimization

Minimization: What is it?

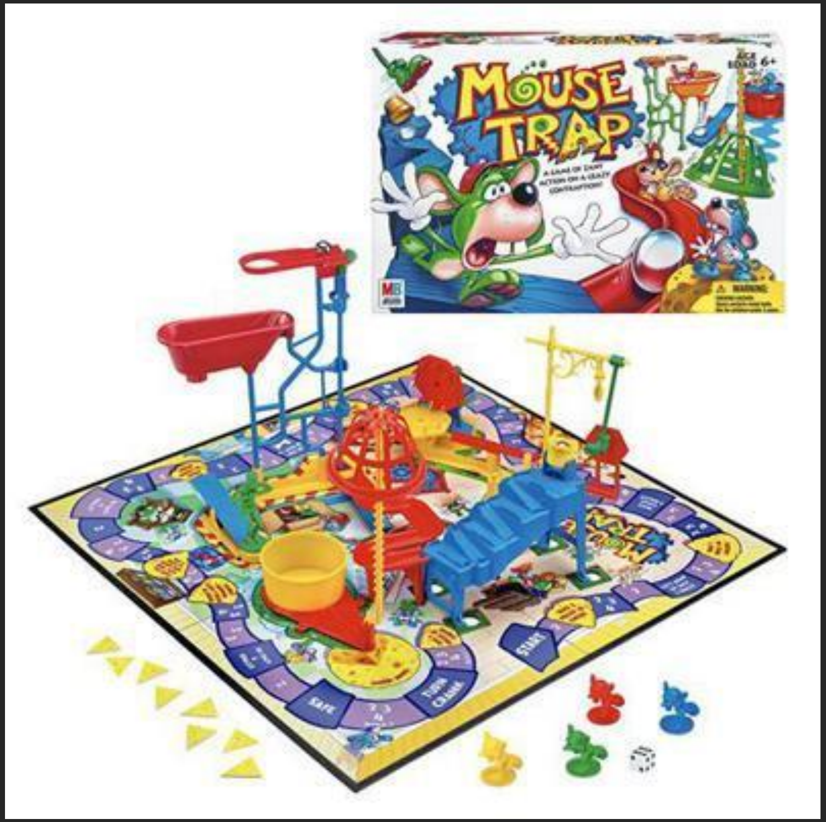
The Principle: Minimize the size, quantity, and complexity of what is to be protected, and limit externally facing points of attack.

Key Question: Can this be a smaller target?

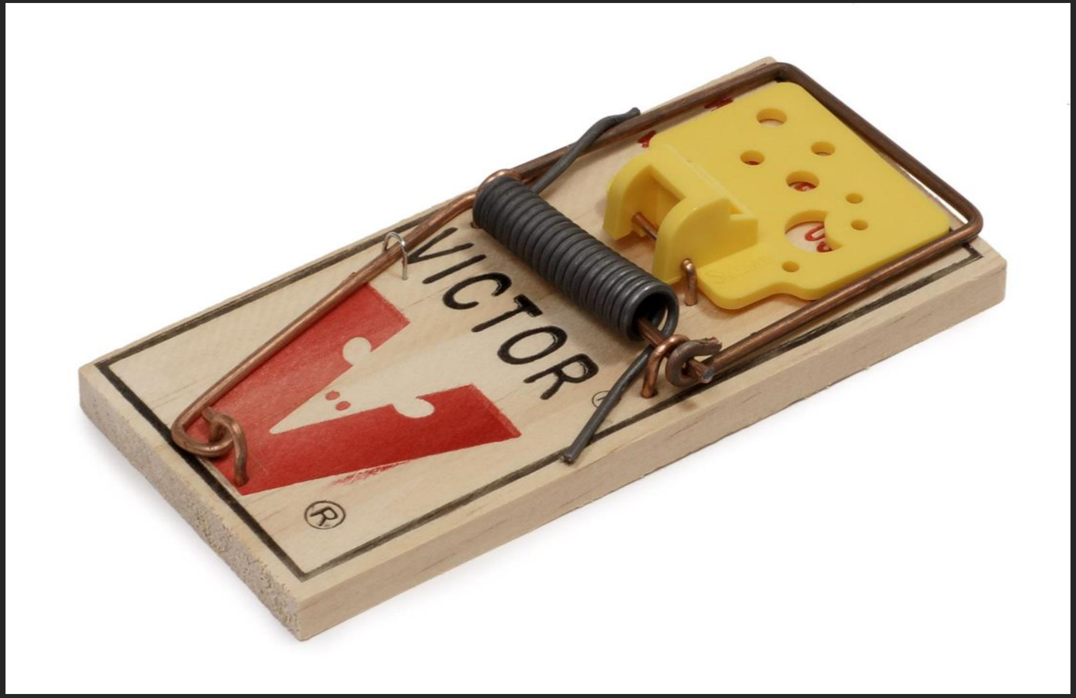
Related Concepts: Attack Surface, Compactness, Data Minimization, Simplicity

“I have yet to see a house that lacked sufficient storage. The real problem is that we have far more than we need or want.” - Marie Kondo

Minimization: Example



vs.



Minimization: NTP Rescue

Network Time Protocol:

- Rescue effort on reference implementation
- Removed unreachable or obsolete code
- Dodged 85% of vulnerabilities *that the team hadn’t found* before disclosure

Compartmentation

Compartmentation: What is it?

The Principle: Isolate system elements, and enable and control the interactions essential for their intended purpose.

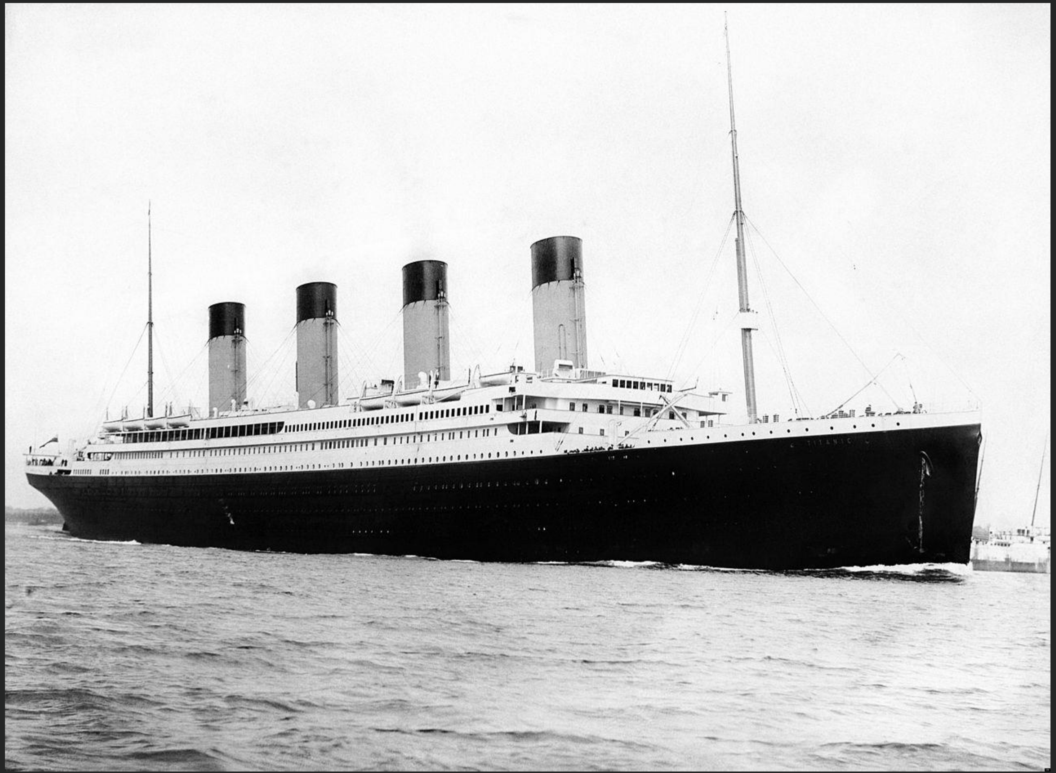
Key Question: Is this made of distinct parts with limited interactions?

Related Concepts: Modularity, Forward Secrecy, Least Privilege, Air Gapping, Cryptography

Compartmentation: Example

RMS Titanic

- Utilized 16 watertight compartments
- But could only survive flooding four . . .
- Actually a partial Compartmentation success story



Fault Tolerance

Fault Tolerance: What is it?

The Principle: Anticipate and address the potential compromise and failure of system elements and security controls.

Key Question: What happens if this fails?

Related Concepts: Resilience, Failsafe Defaults, Defense in Depth, Revocability, Incident Response, Business Continuity and Disaster Recovery, Murphy’s Law

Fault Tolerance: Example

NotPetya & Maersk:

- Massive ransomware attack.
- Only one Maersk domain controller was unaffected.
  - Because of a power outage in Ghana.
- That one machine was used to restart their entire operation.
- Fault Tolerance by accident?

Proportionality

Proportionality: What is it?

The Principle: Tailor security strategies to the magnitude of the risks, accounting for the practical constraints imposed by the mission and the environment.

Key Question: Is this worth it?

Related Concepts: Risk Management and Acceptance, Usability

Proportionality: Example

Airport Security:

- Too much security is bad for the mission.
- Good security finds an appropriate balance between the risks faced, the security obtained, and the cost and hassle the security imposes.
- Airports went overboard, and so the general public was frustrated by them.

Q&A

POLL

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The Principles

In Action

Ransomware Targets Local Government

Welcome to the plucky but under-funded cybersecurity staff of Anytown, USA.

You’ve been asked for a plan to prevent ransomware attacks from disrupting the town’s most critical services, to be implemented within the coming year.

Mayoral Top Priorities:

- Water and Sewer Service
  - including billing for same
- 911 Service
- Police Activities
- Volunteer Fire Service
- Electronic Scoreboard for Little League Games

1. **Comprehensivity** (“*Am I covering all of my bases?*”)
   Identify and account for all relevant systems, actors, and risks in the environment.
2. **Opportunity** (“*Am I taking advantage of my environment?*”)
   Take advantage of the actor relationships, material resources, and strategic opportunities available in the environment.
3. **Rigor** (“*What is correct behavior, and how am I ensuring it?*”)
   Specify the expected states, behaviors, and processes governing the relevant systems and actors.
4. **Minimization** (“*Can this be a smaller target?*”)
   Minimize the size, quantity, and complexity of what is to be protected, and limit externally facing points of attack.
5. **Compartmentation** (“*Is this made of distinct parts with limited interactions?*”)
   Isolate system elements, and enable and control the interactions that are strictly necessary for their intended purposes.
6. **Fault Tolerance** (“*What happens if this fails?*”)
   Anticipate and address the potential compromise and failure of system elements and security controls.
7. **Proportionality** (“*Is this worth it?*”)
   Tailor security strategies to the magnitude of the risks, accounting for the practical constraints imposed by the mission and the environment.

Mayoral Top Priorities:

- Water and Sewer Service
  - including billing for same
- 911 Service
- Police Department Activities
- Volunteer Fire Service
- Electronic Scoreboard for Little League Games

Q&A

Thank You!

Email:

- Craig Jackson: scjackso@iu.edu
- Scott Russell: scolruss@indiana.edu
- Susan Sons: sesons@iu.edu

Principles home page: https://cacr.iu.edu/principles

O’Reilly Book: http://go.iu.edu/282b

Q&A

Thank You for Joining Us!

Upcoming Webinar: “The Intersection of the Privacy and Cybersecurity Workforce”

When: Wednesday, February 19, 2020 at 2:00pm EST

Register: https://nist-nice.adobeconnect.com/webinarfeb20/event/registration.html

nist.gov/nice/webinars