Cybersecurity Key Principles

A Principled Approach to Cybersecurity Engineering

O. Sami Saydjari, Cyber Defense Agency, Inc.
17 June 2020

Introduction

- Goals
  - Understand 10 key cybersecurity engineering principles
  - See the big picture of principles to secure system design
  - Moving cybersecurity to an engineering discipline
- Background Basics
  - Confidentiality—Data whose value lies in its secrecy
  - Integrity—Ensuring data & system not changed maliciously
  - Availability—Ensure continued access to resources

1. Cybersecurity's goal is to optimize mission effectiveness; cybersecurity is never an end unto itself. [03.01]

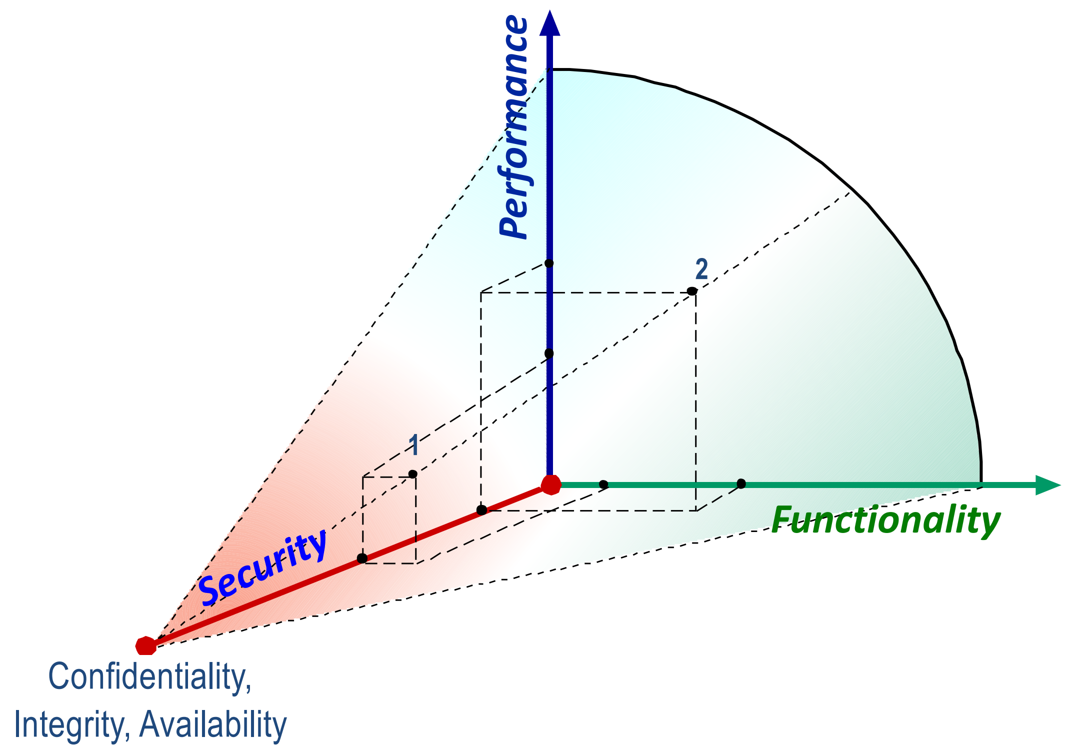
Description

Cybersecurity's goal is to optimize mission effectiveness; cybersecurity is not an end unto itself

- Systems have a primary mission
  - sell widgets, manage money, control chemical plants, manufacture parts, connect people, defend countries…
- Systems generate mission value
  - affected by probability of failure
  - from a multitude of causes, including cyberattack.
- The purpose of cybersecurity design
  - reduce probability of failure from cyberattack so as maximize mission effectiveness
- Rationale: Place security in collaborative vs adversarial role

The Challenge: Explicit Trade-off

- What does the cone look like?
- Where is the system located on the cone?

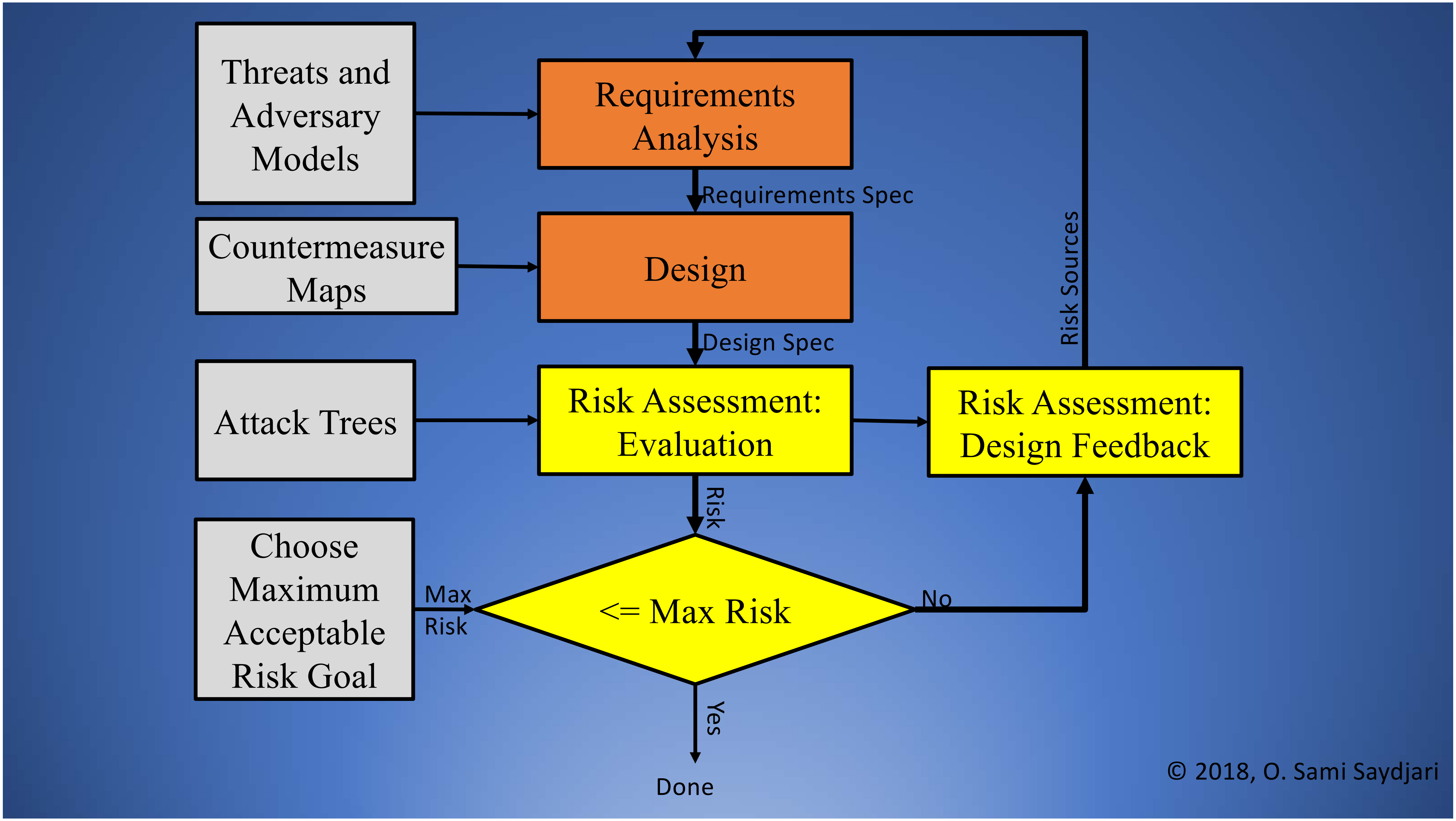


2. Cybersecurity is about understanding and mitigating cyberattack risk. [02.01]

Description

Cybersecurity is about understanding and mitigating cyberattack risk. [02.01]

- Risk is the primary metric of cybersecurity.
  - Understanding nature and source of risk is key to applying and advancing the discipline.
  - Risk measurement is foundational to improving cybersecurity {17.04}
- Cybersecurity risk
  - probability of cyberattacks occurring multiplied by
  - potential damages that would result if they actually occurred.
- Estimating both quantities is challenging, but possible
- Rationale: Engineering disciplines require metrics to characterize, evaluate, predict, and compare



Threats and Adversary Models
Requirements Analysis
Requirements Spec
Countermeasure Maps
Design
Design Spec
Attack Trees
Risk Assessment: Evaluation
Risk Assessment: Design Feedback
Risk Sources
Risk
Choose Maximum Acceptable Risk Goal
Max Risk
<= Max Risk
No
Yes
Done
© 2018, O. Sami Saydjari

3. Theories of cybersecurity come from theories of insecurity. [02.03]

Description

Theories of cybersecurity come from theories of insecurity. [02.03]

- Most important yet subtle aspects engineering discipline
  - understanding how to think about it
  - the underlying attitude that feeds insight
- As failure motivates and informs dependability principles
  - Cyberattack motivates and informs cybersecurity principles
- Approaches to defend a system
  - during design and operation,
  - must come from understanding how cyberattacks succeed
- Rationale
  - How to prevent attacks without knowing success mechanisms?
  - How to detect attacks without knowing how attacks manifest?

Attack Classes

- Computer Network Attacks
- Lifecycle/Supply Chain Attacks
  - Development
  - Integration
  - Operations
- Signals Intelligence Attacks
- Human Intelligence/Insider Attacks
- Social Engineering
- Electronics Warfare
- Kinetic Attack for Cyber Effects

4. Cyberspace espionage, sabotage, and influence are goals underlying cyberattack; prepare for all three. [06.02]

Description

Cyberspace espionage, sabotage, and influence are goals underlying cyberattack;

- Understanding adversaries = understanding their motivations and strategic goals
- Adversaries have three basic categories of goals:
  - espionage—stealing secrets to gain an unearned value or to destroy value by revealing stolen secrets,
  - sabotage—hampering operations to slow progress, provide competitive advantage, or to destroy for ideological purposes, and
  - influence—affecting decisions and outcomes to favor an adversary's interests and goals, usually at the expense of those of the defender
- Rationale: Knowing Adversary values → investments, targets, behaviors

5. Assume your adversary knows your mission and cybersecurity system better than you; the opposite assumption is folly. [06.05]

Description

Assume your adversary knows your mission and cybersecurity system better than you

- Secrecy is fleeting
  - never depend on it more than is absolutely necessary {03.05}
  - true of data, applies even more strongly to the system itself {05.11}
- Don't make rash and unfounded assumptions
  - safer to assume they know as much as designer about system
- Beyond adversary knowledge of the system,
  - Assume co-opted part of system sometime during its lifecycle
  - May have changed a component to have some degree of control
- Rationale
  - Many subversion opportunities during system's entire lifecycle
  - Design, Build, Test, Deployment, Maintenance

Programming tools used in the creation of executable programs are all subject to attack

Consider Lifecycle Attacks

Source Editor: Programming tool used to enter source code
Compiler: Translator from high-level language to object code
Linker: Links pre-compiled program libraries into the object code
Loader: Places executable code into memory and prepares for execution

6. Without integrity, no other cybersecurity properties matter.
[03.06]

Description

Without integrity, no other cybersecurity properties matter.

- Some cybersecurity engineers hyper-focused Confidentiality
  - to the exclusion of adequate attention to the other two pillars
  - particularly DoDers where protecting classified data is priority
- All system properties depend on system integrity ➔ primacy
- Reference monitor, requiring security-critical subsystems
  - correctly do required security functions,
  - non-bypassable so attacker cannot circumvent correct controls,
  - tamperproof so system cannot be altered without authorization.
- No matter what properties a system possesses when deployed
  - they can be immediately subverted by attacker
  - altering system, replacing properties with ones desirable to attacker

7. A cyberattacker's priority target is the cybersecurity system. [19.17]

Description

A cyberattacker's priority target is the cybersecurity system.

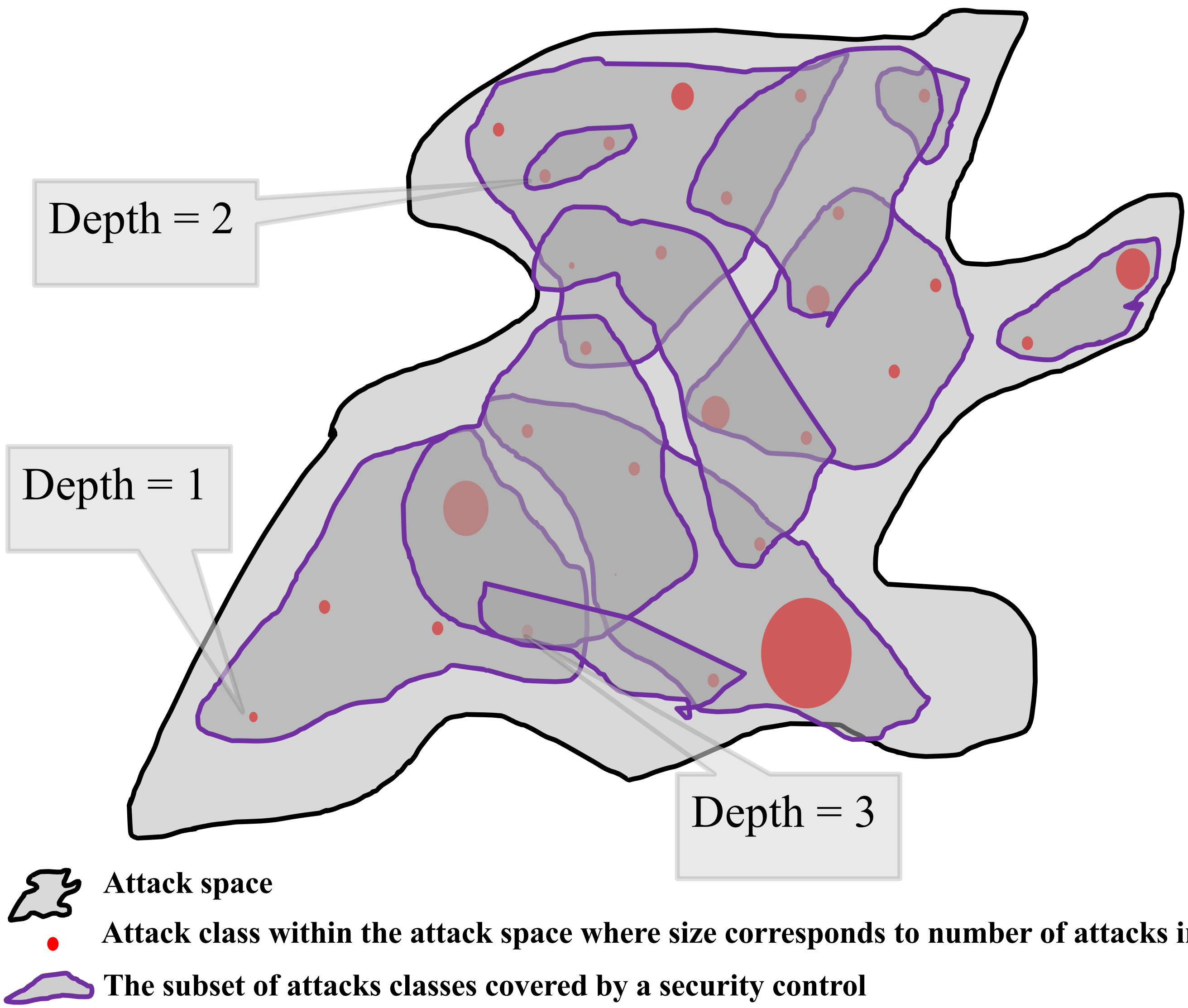
- Criticality of cybersecurity subsystem
  - Closely following from primacy-of-integrity principle {03.06}
- To attack the mission
  - it is necessary first to disable any intervening security controls
  - clearing adversary's attack path from defense
  - including security controls that defend the security subsystem itself
- Protect & monitor cybersecurity subsystem carefully {23.12}
- Cybersecurity subsystem protects the mission system
  - Attacks on cybersecurity harbinger attacks on mission system {22.08}
  - Cybersecurity system is key to attacking mission system
  - Example: attacks on audit logs to erase evidence

8. Defense in depth without defense in breadth is useless; breadth without depth, weak. [08.02]

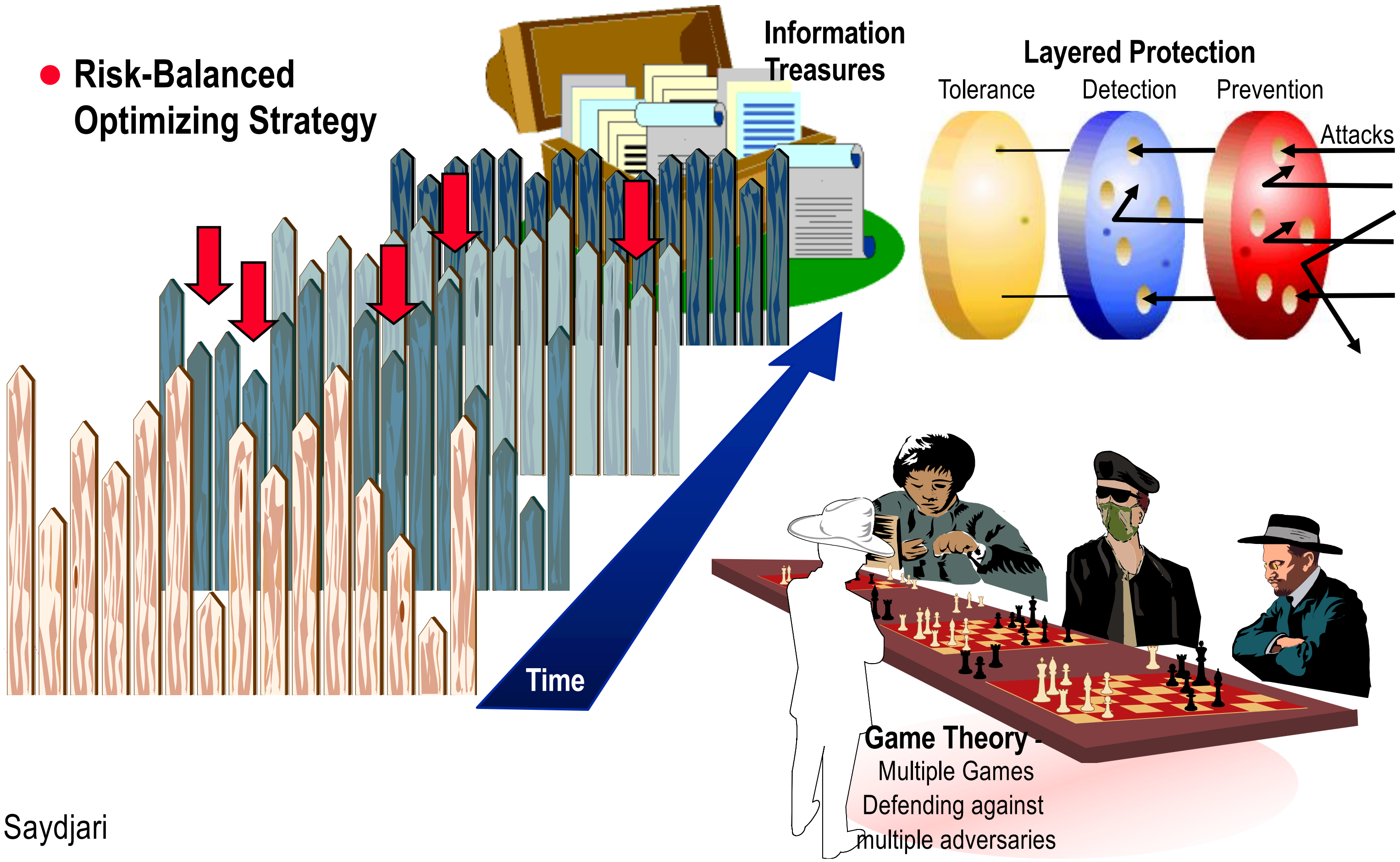
Description

Defense in depth without defense in breadth is useless; breadth without depth, weak.

- Much ado about *defense in depth*
  - Vaguely defined as layering cybersecurity approaches (people, tech)
  - Need precision to be useful in design process: layer how, WRT what?
  - WRT cyberattack space covering gamut of possible attack classes
- Mechanisms useful against one attack class is useless for others
- Thus, companion principle: *defense in breadth*.
  - creating depth to point of making a class of attack prohibitive
  - adversary may simply move to an alternative attack
- Ideally, the depth will cause adversary equal difficulty
  - For all avenues of attack, For all attack classes…
  - Be above the cost and risk thresholds of the attackers


Depth = 2
Depth = 1
Depth = 3
Attack space
Attack class within the attack space where size corresponds to number of attacks in the class
The subset of attacks classes covered by a security control

Cyber Security Principles



9. Failing to plan for cybersecurity failure guarantees catastrophic failure. [20.06]

Description

Failing to plan for cybersecurity failure guarantees catastrophic failure

- System failures are inevitable {19.01, 19.05}.
  - pretending otherwise is almost always catastrophic.
  - applies to mission system and cybersecurity subsystem that protects it
  - cybersecurity systems, like all systems, are subject to failure
- Engineers must understand how their systems can fail, including
  - failure of underlying hardware (microprocessors, internal buses)
  - other systems on which they depend (network, memory, ext storage)
- A student of cybersecurity is a student of failure {07.01}, dependability
  - Security requires reliability; reliability requires security {05.09}
- Cybersecurity mechanisms not endowed with nonfailure magical powers
  - Subject to same Engineering-V failures as all system
  - Security code handle complex timing issues, hardware control

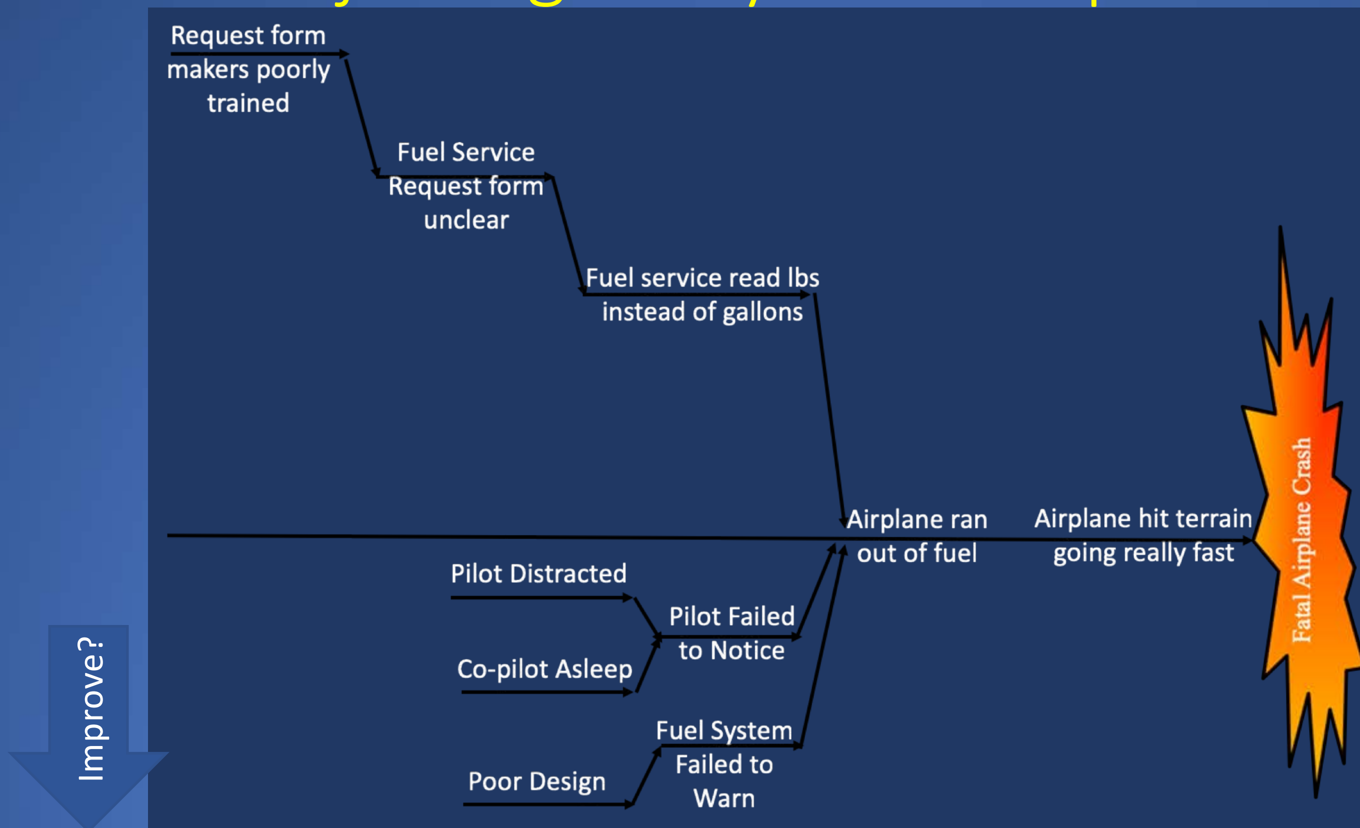
10. Cybersecurity strategy and tactics knowledge comes from deeply analyzing cyberattack encounters. [01.09]

Description

Cybersecurity strategy and tactics knowledge comes from deeply analyzing cyberattack encounters

- Good cybersecurity operations is as important as good design
  - Cybersecurity mechanisms are highly configurable (e.g., FW rules)
- What are optimal settings of all various mechanisms?
  - Depends on variations in mission, system environment, attack status
  - Settings = trade-off space for addressing entire spectrum of attacks
  - No static optimal setting for all cyberattack scenarios under {22.07}
- Dynamic control → complex control-feedback system {23.11}
- Knowledge to set parameters according to situation?
  - analyzing cyberattack encounters: real + simulated, yours + others
  - Theory: game theory, control theory
  - Strategic knowledge to guide default postures & future designs
  - Tactical knowledge to improve quality and speed of response

Projecting Analysis for Improvement



Aircraft Design

Pilot Training

Air Traffic Control

Cockpit Design

Support System