Society of American Military Engineers

A New Way of Thinking: Consequence-driven, Adversary-tolerant Lifecycle Engineering

Arlington, Texas
2 February 2018

Daniel J. Ragsdale, Ph.D.
Director, Texas A&M Cybersecurity Center
Professor of Practice, Computer Science and Engineering
Texas A&M Cybersecurity Center (TAMC²) Mission:

Make outsized contributions to social good by:

– Producing highly skilled cyber leader-scholars

– Facilitating the conduct of ground-breaking, basic and applied cybersecurity research

– Developing novel and innovative methods for cybersecurity education and work force development

– Building mutually beneficial partnerships with commercial, governmental, and academic partners
Inquiring Minds...

• Are we increasingly dependent on cyber systems?

• Are we disproportionately dependent on cyber systems

• Are we losing ground?

• Why?
Fill in the Blank...

- _______ Infrastructure
- _______ Cites
- _______ Roads
- _______ Bridges
- _______ Power Plants
- _______ Cars
- _______ Homes
- _______ Thermostats
- _______ Crock Pots
- _______ Engineers

https://gen.com/~/media/GIG/GCN/Redesign/Articles/2017/January/smartinfrastructure.png
Obligatory Einstein Quote

“The definition of insanity is doing the same thing over and over again and expecting different results.”

Albert Einstein

Obligatory Lincoln Quote

"The problem with quotes on the Internet is that no one can confirm their authenticity."

–Abraham Lincoln

What we've been reading...

"Hacking Nuclear Systems Is The Ultimate Cyber Threat. Are We Prepared"

~The Verge, 23 Jan 2018

- "Unless we start to think more creatively, more inclusively, and have cross-functional thinking ...we’re going to stay with a very old-fashioned [security] model ..."
- "[We don't] have the luxury of banking on probabilities...even a minor attack ... could further erode public confidence."
What we've been reading...

"Hacker takes control of hundreds of rooms in hi-tech 5-star Shenzhen hotel"

~South China Morning Post, 29 July 2014

- "A San Francisco-based cybersecurity expert claims he has hacked and taken control of hundreds of highly automated rooms at a five-star Shenzhen hotel"
- "I'm an ethical hacker... explaining why he didn't immediately plunge the entire hotel into darkness or switch every television to the same channel."
Definition System Lifecycle

Includes all phases of system to include:

- System conception
- Design
- Development
- Production
- Operation
- Maintenance and support
- Retirement
- Phase-out and disposal  [1]

Warning: Whiplash Alert!

https://cdn1.medicalnewstoday.com/content/images/articles/174/174605/whiplash-anatomy-diagram.jpg
Commander/Staff Actions During an "Operation's Lifecycle"

- Planning and Execution

- Risk Management
  - During Planning:
    - MDMP - "Operation Design"
      - COA Development / Analysis Selection
      - War gaming
  - During Execution:
    - Continuously monitoring and ongoing assessment of red and blue activities

- They manage risk, in part, by continuously listening to...
  - ...the voice of the adversary!
Definition: Risk

• "The anticipated [and quantifiable] loss or damage to an asset associated an event"

Risk Components?

• $P(\text{Event})$

• Impact$(\text{Event})$
Risk Strategies

• Accept
• Avoid
• Transfer
• Mitigate
  – Reduce
  • probability (likelihood)
    and/or
  • consequence (impact)

https://www.google.com/search?biw=1707&bih=844&tbs=isz

TAMU | TEXAS A&M CYBERSECURITY CENTER

TAMU | TEXAS A&M ENGINEERING EXPERIMENT STATION
Cyber Risk

"The anticipated quantitative loss or damage to an asset associated with a specific cyber threat event(s)"

Risk Associated with a Cyber Threat Event (CTE)

- A Function of:
  - $P(CTE)$
  - Consequence($CTE$)

- Mitigate a cyber risk?
  - Reduce the probability (likelihood) AND/OR
  - Reduce the impact (consequence)

Warning: Whiplash Alert!

https://cdn1.medicalnewstoday.com/content/images/articles/174/174605/whiplash-anatomy-diagram.jpg
Risk Associated with a Cyber Threat Event (CTE)

$$\text{Risk}(\text{CTE}) = P(\text{CTE}) \times \text{Consequence}(\text{CTE})$$

- **P(CTE)** is a function of:
  - $P($The vulnerabilities associated with a CTE are present$)$
  - $P($Threat has the capability and intentionality to cause a CTE$)$
  - $P($Threat has access to the vulnerabilities that are associated with a CTE$)$

- **Consequence(CTE)** is influenced by:
  - Plan/Design
  - Operational Decisions

- I.e., an "operation's lifecycle"
Risk Perspectives

Assets
- Consequences
- Vulnerabilities
- Accessibility

Threats
- Capability and Intentionality

Inward Looking  Inward and Outward Looking  Outward Looking
How does these cyber risk considerations relate to design?
Why Do Systems Fail?

• Bad design!

• What contributes to bad design?
  – Invalid assumptions
  – Lack of knowledge
  – Sole focus on functionality
    • In cyberspace, failure to understand and adequately consider vulnerabilities, threats, and consequences

https://static.seattletimes.com/wp-content/uploads/2015/11/eedc84cc-84e0-11e5-b53b-a576789c5b7f-780x605.jpg
Elements of Design

Fundamental elements of the design process:
- Establishment of objectives and criteria
  - Assumptions
  - Constraints
- Synthesis
- Analysis
- Construction
- Testing and evaluation
[ABET]
The Root Cause of the Cybersecurity Problem...

- The most serious of all invalid design assumptions and famous last words:
  - "No one would ever..."
  - "That can't happen..."
So how can we do better?
Tolerance for Failures

• **Fault Tolerance:**
  – The ability to continue to function correctly in the presence of component failures caused by random events

• **Adversary Tolerance:**
  – The ability to continue to function correctly in the presence of component failures caused by [purposeful and ongoing] adversary activities
Continuous Cyber Consequence Analysis

• Identify set of negative consequences

• Determine the adversary actions that could produce the consequence
  – Requires knowledge of adversary cyber tactics, techniques, and procedures (TTPs)
    • Aka Kill chain, plays, etc.
Consequence-driven Adversary Tolerant Life Cycle Design

• Focus on consequences

• Always include an adversarial perspective
  – "Voice of the Threat"

• Conduct continuous formal and Informal "War gaming"

• Analyze EVERY lifecycle decision, in all phases, to determine the degree to which the decision influences risk

• More broadly, perform continuous risk assessment throughout a system lifecycle taking into account:
  – Consequences
  – Threats
  – Accessibility
  – Vulnerabilities
Questions?