

Day 1 Introduction to workshop topic

Abstract: Agile Security Adaptable to Attack Evolution

Jack Ring, OntoPilot, INCOSE Fellow. jack@ontopilot.com

Agile security must be reactively resilient and proactively composable at the pace of unpredictable and evolving adversarial attackers and their attack methods. The adversarial at-tack may originate from outside the system or, particularly in system of system scenarios, from inside the system. This idea encompasses information systems, cyberphysical systems, physical systems, infrastructure systems, and national defense systems. Success demands close collaboration and co-learning by system engineering and security engineering interests. System engineering seeks sustainable systems. Security engineering seeks sustainable system defense. It takes both to succeed against agile adversaries. The respective practitioners march to separate drum beats. Security engineering must educate systems engineers on the kinds and sources of threats and needs for detecting and defeating them. System engineering must satisfy new demands on system architecture, system design, systems engineering, and security engineering. All need to better understand their requisite interoperability.

What stands in the way of synergistic engineering cooperation? What are the requirements for an effective engineering-team approach? What can systems engineering do to enable and facilitate the needs of agile-security engineers? What can security engineering do to enable and facilitate engagement with systems engineers?

This workshop will explore values and needs for cooperative agile-security engineering, identify the inhibiting barriers, suggest concepts that any effective solution must address, and open a dialog on potential solutions.

Jack Ring



Managing Member, Educe LLC, a WOMO enterprise

Managing Member, OntoPIlot LLC, enabling fault-free software

Explorer, Model Centric Systems Management, Systems That Learn, and Sociotechnical Systems that Do No Harm.

Auditor, Third Party Facilitation, ASU Com691

Fellow, INCOSE 2003

Agile security:
adaptable/adaptive
to adversary attack evolution

Jack Ring

Session Moderator

Collaborative Knowledge Exchange Summit

10/28-29/2016

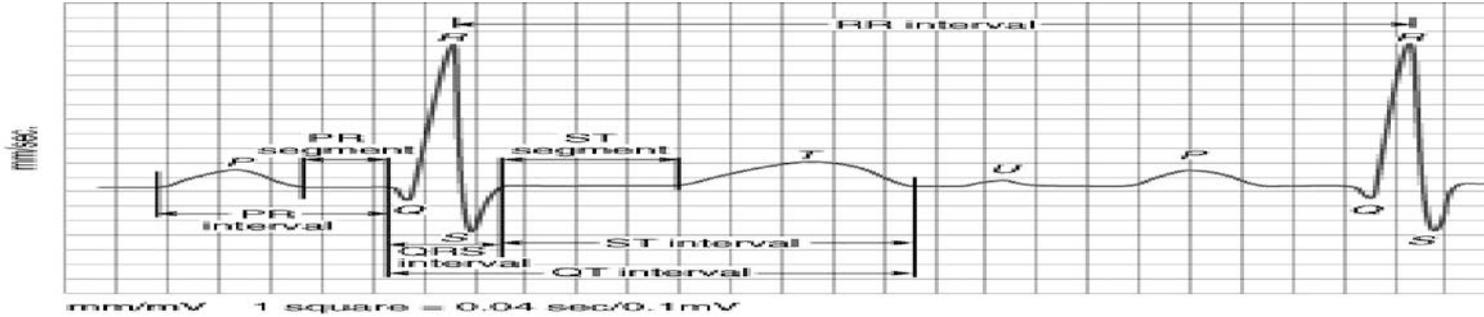
Socorro, NM

Adaptable to adversary attack evolution.

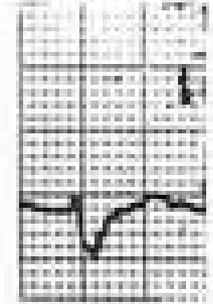
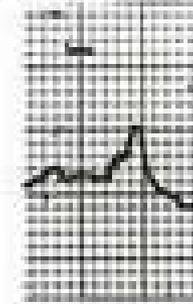
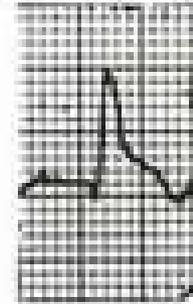
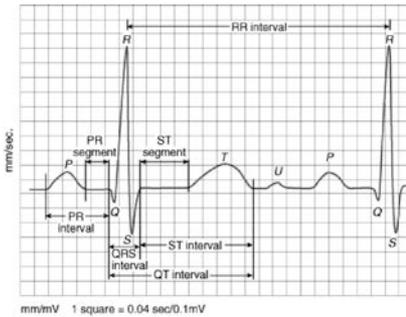
Circa 1878



Adaptive to adversary attack evolution



$\sigma \approx 7\%$



Agenda 10/28

- ✓ Me < 30 minutes: Explore; Purpose, Prompts, Groundrules:
- ✓ You 30 minutes: Reflection and Outlook;
 - Key objectives of Agile Security.
 - Impediments to communication, invention and innovation that did or will impact agile security negatively?
- ✓ Us 30 minutes: Objectives for achieving Agile Security: Prepare Chart for 10/29 Agenda

Session Groundrules

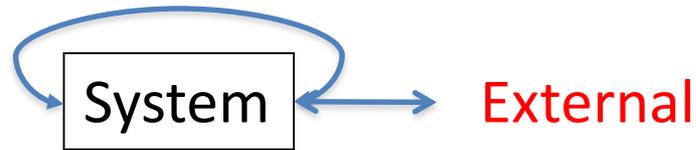
- 1) Learn from one another.
- 2) Listen to others fully, even when you disagree.
- 3) Beware your body language and nonverbal responses.
- 4) Speak for yourself, not as representing an authority.
- 5) Ask questions for clarification. No rhetorical or 'gotchas.'
- 6) No arguing. Tell alternative stories instead.
- 7) Search for assumptions (especially your own).
- 8) Defer decision OODA.

1. Purpose: 30 minutes

Agile security adapt(able/ive) to adversary attack evolution.

External and Internal Attacks

Admin & Maint



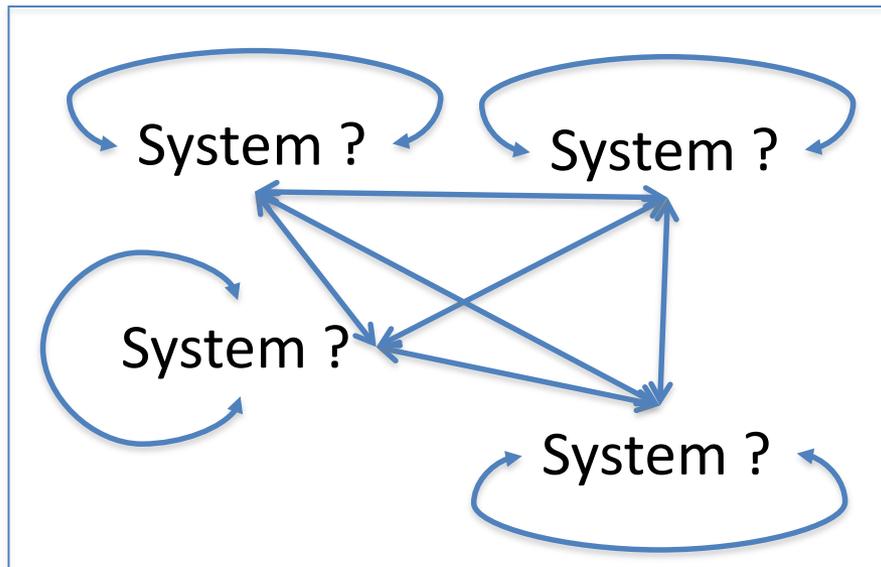
System of Systems

External

External

External

External



Autonomy for Non-deterministic

- ✓ Operational Pull vs. Technology Push.
- ✓ Trustworthiness and Trust in Autonomous Systems.
- ✓ Self-explanatory systems.
- ✓ Do No Harm.

Significance?

DARPA director Arati Prabhakar says the DoD can't keep up with rapidly advancing adversaries because DoD systems **“take too long to develop, too long to troubleshoot, and too long to update.”**

<http://breakingdefense.com/2016/02/faster-than-thought-darpa-artificial-intelligence-the-third-offset-strategy/>

The other half of necessary and sufficient action is to remove all exploitable vulnerabilities from our systems while preventing introduction of further ones.

Eventually every new line of code introduced into any system must be considered a cyberattack until confirmed otherwise.



Urgency?

CERT Situational Awareness Symposium, 10/26/2016

“One of the biggest [sic] challenges facing cyber defenders today is keeping up with attackers who have developed automated mechanisms to morph malware, distribute attacks, and continually alter signatures, domain names, and IP addresses.

With the expansion of fully autonomous systems in other highly complex and volatile public domains such as fraud detection, stock trading, utility management, and driverless cars, the time is right to explore the possibilities of automated cyber attack identification, categorization, and response.”

Suggests at Least Eight Dimensions for our Dialog

Agile security adapt(able/ive) to adversary attack evolution

System IS secure:
→ Sustain it

System NOT secure:
→ Gain it

Purposeful Attacks

Unintended Consequences

System Generator Chain

- S0 Operational SoS
- S1 Deployed System
- S2 System @ Realized Model, Concept
- S3 Sociotechnical That Generates S2
- S4 Social System That Enables S3

Kinds of Systems

Kinds of People

Challenges

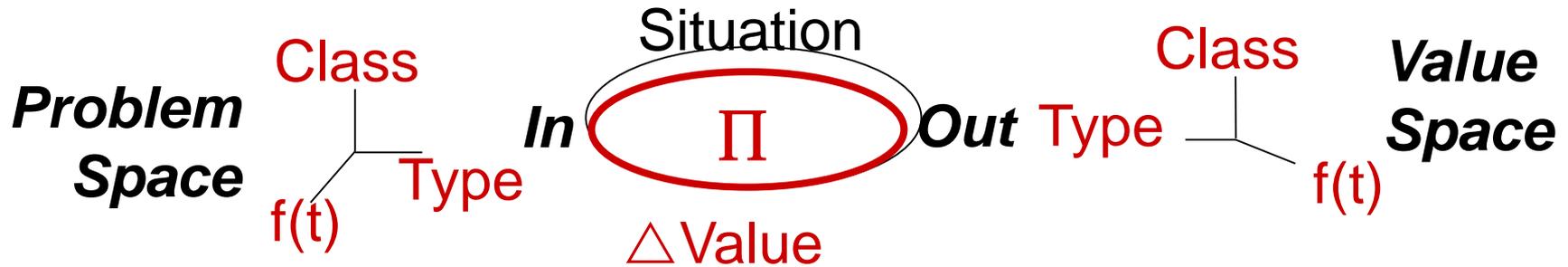
ConOps,
Strategy,
Design,
Architecture
Activation
Adaptation

Example: Kinds of People



Motivation	Results	Mediators
Co-evolve	Morphing toward Win-Win-Win	Joy-enabled Level of Consciousness
Co-facilitate	Value Out/Value In $\approx e^N$	N party stewardship
Co-learn	Meaningful reflection	Shared knowledge claims
Collaborate	Help one another	Desire to serve
Co-celebrate	En-joying one another	Time & Space, F2F
Cooperate	Compatible actions	Willing to wait
Commit	Principled relationship	Courage to plan
Converge	Compelling purpose	Shared self-respect
Communicate	Share interests & values	Common language
Connect	One discover another	Accessible attributes

Example Kinds of Systems



$\Pi = f(k) = \text{ballistic}$

$\Pi = f(O) = \text{governor}$

$\Pi = f(I) = \text{anticipatory}$

$\Pi = f(\text{Sit}, O) = \text{homeostatic}$

$\Pi = f(\text{Sit1}, O) = \text{homeorhetic}$

$\Pi = f(\text{Val}) = \text{goal-seeking}$

$\Pi = f(\text{Pr}) = \text{self-organizing}$

$\Pi = f(\text{Pr}, \text{Val}) = \text{value-seeking}$

$\Pi = f(\text{all}) = \text{autocatalytic}$

Pr = Problem Space
 Val = Value Space
 S = Stimulus
 R = Response
 Sit = Situation
 Π = System Transfer Function

2. Your Perspectives: 30 minutes

Purpose:

Mutually discover the barriers to effective leveraging of group knowledge that impact negatively in complex, problem solving situations?

1. Requirements for system and security strategy that will enable response with at least the agility of the adversary?
2. Implications for ConOps, design, and architecture?
3. Understanding problem and solution spaces of the topic area better—barriers to solution, cultural incompatibility and push back, systemic inertia, misaligned forces, and solution value propositions, objectives, and requirements.

Agile Security Adaptable to Attack Evolution

Moderator: Jack Ring

Day-1 Brief Out (as decided Friday, subject to change during Saturday)

Planned Primary Workshop Issues to Explore

- Clarity of Purpose: Attributes of secure system and Acceptance Criteria
- Accountability of the system producers, administrators and users
- A Compelling Value Proposition to sponsor sufficiently agile secure system

Potential Secondary Workshop Issues to Explore

- Which stage of the system generation chain is critical
- Systems that Do No Harm
- Competencies and Current awareness of the Threats

- Objectives for Saturday
- Ways and means for generating sufficient sponsorship (Value Proposition)
- Ways and means for generating sufficient accountability.
- Grand Challenge

Agile Security Adaptable to Attack Evolution

Moderator: Jack Ring

Day-2 Brief Out

For Agile Security Adaptable to Attack Evolution we shall:

Objective: Value proposition

Impediment: Convincing the community

Resource/Action: Fast prototype(in order to survive evolutionary attack you must have agility in your security)

Order of Battle: 1. Test prototype

Objective : Clarity of Purpose e.g. Operational availability

Impediment: Complex confusing situation (agility, vulnerability, virulence)

Resource/Action: Generate an insight article that brings what operational availability means in the agile security space

Order of Battle: 2. Test prototype

Objective : Accountability of all actors

Impediment: Metrics of agility and accountability

Resource/Action: Develop and publish an RFI to INCOSE CAB members and its collaborative associates

Order of Battle: 3. Test prototype