Agile Security Adaptable to Attack Evolution

Facilitator: Rick Dove, Paradigm Shift Int'l, INCOSE Fellow. rick.dove@parshift.com

Rick Dove, INCOSE Fellow, was co-PI on the original work which identified Agility as the next competitive differentiator, in a 3-month industry-collaborative workshop funded by the US Office of the Secretary of Defense in 1991 at Lehigh University. He went on to organize and lead the US DARPA-funded industry collaborative research at Lehigh University's Agility Forum, developing fundamental understandings of what enables and characterizes system's agility.

He authored *Response Ability – The Language, Structure, and Culture of the Agile Enterprise*. He has employed these agile concepts in both system architecture and program management for large enterprise IT systems, for rapid manufacturing systems and services, and for self-organizing security strategies.

For Stevens Institute of Technology he teaches graduate courses in basic and advanced agile-systems and agile systems-engineering, at client sites. He is CEO/CTO of Paradigm Shift, an applied research firm specializing in agile systems concepts and education. He chairs the INCOSE working groups on Agile Systems and Systems engineering, and on Systems Security Engineering.

Day-2 Workshop Participants

Luis Arvizu	**UTEP**	**laarvizu@miners.utep.edu**
John Brtis	**MITRE**	**Jrbrtis@JohnBrtis.com**
Rick Dove	**PSI**	**dove@parshift.com**
James Musick	**Harris**	**jdmusick@earthlink.net**
Tyler Werne	**NMTech**	**TylerWerne40@gmail.com**

Day-1 Intro and Results Poster

Agile Security Characteristics

Knowledgeable awareness of external threats

Knowledgeable awareness of internal threats and vulnerabilities

Quick detection of attacks

Resilience after attack

Quick reconfiguration of attack surface

Quick composability of attack-response options

Food For Thought

Facilitator may suggest a concisely articulated problem statement – for modification or replacement by Day-1 participants.

Poster

1. **Articulate the unresolved problem-need for resolution.**
   The bad guys think up new attacks faster than we can detect/respond?
   Security is not a high priority taken seriously?
2. **Identify the customer(s) for a solution (provides context).**
   Who can/should/want such a decision?
3. **Issues within the problem area for Day-2 intended focus.**
   1. **Organization doesn’t have security as sufficient priority?**
   2. **Agile security has no guidance for implementation?**
   3. **You can’t (affordably?) buy effective agile security?**
   4. **Security viewed as productivity impediment?**

Agile Security Adaptable to Attack Evolution
Day-1 Brief Out Poster

1. **Unresolved problem-need:**

   A strategic approach to security is missing in the face of complex systems environments given opportunistic agents with competing objectives.

2. **Customers – who can/should/want this solved:**

   Top authority, and all stakeholders that demand functionality.

3. **Issues within the problem area for Day-2 intended focus.**
   1. **Lack of value proposition, impedes proper prioritization.**
   2. **Integration of agile security into enterprise/systems engineering.**
   3. **Socio-technical dependence on systems without any control over them.**

Day-2 Workshop

Participants

Luis Arvizu	UTEP	laarvizu@miners.utep.edu
John Brtis	MITRE	Jrbrtis@JohnBrtis.com
Rick Dove	PSI	dove@parshift.com
James Musick	Harris	jdmusick@earthlink.net
Tyler Werne	NMTech	TylerWerne40@gmail.com

Topic: Agile Security Adaptable to Attack Evolution

Modified Day-1 Focus Development

1. Unresolved problem-need:

A strategic approach to security is missing
in the face of complex systems environments
with opportunistic agents and competing objectives.

2. Customers – who can/should/want this solved:

Top authority, and all stakeholders that demand functionality.

3. Issues within the problem area for Day-2 intended focus.

1. Lack of value proposition, impedes proper prioritization.
2. Integration of agile security into enterprise/systems engineering.
3. Lack of customer emphasis on security (change from Day-1)

Lack of Value Proposition

- Impediments
  - No clear definition
  - Hasn’t been fielded (no experience to point at, no empirical data)

- Requirements
  - Value proposition should appeal emotionally and rationally. If only one – emotional.
  - Create a clear definition of agile security
  - Develop case studies

- Notes
  - Value statement: addresses advance persistence threat and future unknown threats
  - Emotional appeal: reduce IP loss

Integration of Agile Security into SE

- Impediments
  - SEs don’t understand security
  - SEs driven by contract satisfaction not problem space satisfaction

- Requirements
  - Educate Systems Engineers in agile security.
  - Become part of security standard
  - Use a recognized and authoritative source on agile security

- Notes
  - Systems Engineering
    - Concerned about functionality
      - Add consideration of threat condition to SE life cycle
      - Nominal condition vs threat condition
    - Systems Engineers should consider agile security

Lack of customer emphasis on security

- Impediments
  - Cost to implement
  - Customer Perception of Risk/Reward
  - Culture of Secrecy

- Requirements
  - Develop cost expectations
  - Statement of Agile security principles that can be applied contractually
  - Presentation to customer shall include vulnerabilities/threat assessment
  - TBD

- Notes
  - Customer differences
    - May be in denial
    - Example: Banking System
      - Protective nature – security is natural
      - Distrustful
    - Example: Healthcare Software
      - HIPPA Regulation

Action Plan

Agile security working group project instigation:

- **Create a clear referenceable definition of agile security**
- **Develop some case examples**
- **Consider appendix to NIST 800-160 for agile security like the appendix section on resilient security**

Other Notes

Impediments to Implementation

- Cost to implement
    - Costs visible and concrete, benefits are amorphous.
    - Is it?
    - Solution:
        - Make architecture cheap and reconfigurable.
        - Quality vs. price.
        - Incremental benefit vs. cost
- Risk Perception
    - Underestimation of risk
    - Solution:
        - Insurance companies could require more security
- More Restrictions
    - Sharing of information
        - DoD and DoE don’t talk to each other and themselves

Impediments to Implementation (contd.)

- **Defining the customer base**
  - **May be in denial**
  - **Solution:**
    - **Scare/Educate them**
      - **Free Red Team**

- **Defining the agile security benefit**
  - **Agile security addresses advance persistence threat and future unknown threats**
  - **Addresses threats that normal security cannot.**
  - **Recovery consideration**

- **Proof of agility**
  - **Red teams**

- **Standards**