Today’s session will be recorded.

An archive of today’s talk will be available at: [www.sercuarc.org/serc-talks/](http://www.sercuarc.org/serc-talks/)

Use the Q&A box to queue questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.

If you are connected via the dial-in information only, please email questions or comments to serctalks@stevens.edu.

Any issues? Use the chat feature for any technical difficulties or other comments, or email serctalks@stevens.edu.
The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense, ASD(R&E), nor the SERC.

No Warranty. This Stevens Institute of Technology Material is furnished on an “as-is” basis. Stevens Institute of Technology makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. Stevens Institute of Technology does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

This material has been approved for public release and unlimited distribution.
Securing the delivery pipeline
Agenda

1.1 What is Agile

1.2 Why Agile

1.3 Agile Improves Security

1.4 The Future
Goals

- Defend
- Detect
- Deter
Secure Agile Pipeline

With security integrated

Product Backlog

Automated Security tests Run daily

Definition Of Done (sprint)

Security checks

Definition Of Done (Release)

Security checks

Plan Design Build Test

Daily standup

Fuzzing

Static Analysis

Pen Test

Dynamic Analysis

Security checks

Threat Modeling

Secure Design Principles

Defensive Coding

Self Service Security scanning

Plan Design Build Test

Business Drivers

Enablers

Security Stories

Security

Scanning

Continuous Monitoring

Shippable Product

Secure Agile Pipeline with security integrated.
Activities as opposed to phases that have smaller batch sizes and are repeated.
Secure Solutions through Agile

Activities not Phases
Beginning our requirements with security in mind enables us to build trust early and prevent downstream friction.
Secure Requirements/Analysis

Cross-functional scrum team

Security

Dev

SM

Test

PO

Dev

Dev

Personas

Harry Hacker

Skills:
Proficient with the latest technology and enjoys leveraging their knowledge to exploit other’s weaknesses

Responsibilities:
- Stays current with latest technology
- Observant in nature
- Comfortable with change
- Constantly experimenting with new ideas and evaluating the results
- Identify weakness in people, process, and tools
- Constantly testing boundaries

Hacker Story
As a fraudster, I want to see the details of an order that is not my own so that I can learn another person’s private information.

Security Story
As a customer, I want to be sure that the credit card data that I provide for payments are processed and stored securely so that access by third parties or hackers is impossible.

Normal Story
As a customer I want to store my information in a profile so that I do not have to put information into the system every time I shop.

Enabler Story
As a team I want to have current security guidelines and procedures so that I can build security into the baseline.

Product Backlog

Ensure everyone on team Has security skills

Definition of Done

Definition of Done Policy / Description

All Work Items completed must meet the following criteria before moving the work item into the done column:

- All code / tests checked in trunk
- All Access controls checked
- High risk code reviewed by security
- All unit and integration tests passing
- Security Scanning complete
- Static analysis complete and with SLA's
- All acceptance tests written and passing
- Documentation complete
- Peer reviews complete
- Cycle time posted

© 2017 LOCKHEED MARTIN CORPORATION. ALL RIGHTS RESERVED
Secure Solutions through Agile

Activities not Phases
Design

Security by design moves team focus to vulnerability prevention from vulnerability detection

- Cross functional team
- Embedded security SME or security skills

- Threat Modeling
- Security Design Principles

- Open Design
- Security traceability matrix
- Security Service Catalogue
Secure Design

Security Design Principles

Product Backlog

Security Service Catalog

Threat Modeling

Security Matrix

© 2017 LOCKHEED MARTIN CORPORATION. ALL RIGHTS RESERVED
Secure Solutions through Agile

Activities not Phases
Moving from control gates to guardrails with automation and workflows
Secure Development Pipeline

- Defensive Programming
- Feature Toggles
- Secure Infrastructure

Product Backlog

Dev

- commit

Compile Build

Automated Unit Test

Digitally Sign Binary

Static Analysis

Peer Review

Alert High change

Test

Staging / Operations

- Chaos engineering
- Game day
- Red / Blue

- Smoke Test
- Targeted dynamic Scanning
- Automated Security Attacks
- Penetration Test
- API Fuzzing
Secure Solutions through Agile

Activities not Phases
Layered Security test levels reduces flaws in the systems we deliver
Security Testing

- Security Test Cases
- Static and Dynamic Analysis
- Fuzz Testing
- Triage Results
- Penetration Testing
- Risk Based Testing
- Automated Security Attacks
- Security Test Reports
Secure Solutions through Agile

Requirements / Analysis → Design
Operate / Monitor → Secure Agile Solutions
Deploy → Accreditation
Test → Development

Activities not Phases
Secure deployments take the stress out of delivery and allows use to deploy more often with smaller batches.

**People**
- Cross functional team
- Embedded security SME or security skills
- Hacking Skills
- Automated test SME or skills
- Operation (representatives)

**Process**
- Secure the Infrastructure
- Dark Roll-outs
- Canary Releases

**Tools**
- Immutable Infrastructure
- Containers
Secure deployments

Staging / Operations

Canary Release

Load Balancer

PKG A V 2.3
PKG B V 2.1
PKG A V 2.2
PKG A V 2.1
PKG A V 2.0
PKG B V 2.0

Image N

Immutable Infrastructure

Central Package Repository

New Feature

Feature Toggle

NextGenLM

© 2017 LOCKHEED MARTIN CORPORATION. ALL RIGHTS RESERVED
Secure Solutions through Agile

- Requirements / Analysis
- Design
- Operate / Monitor
- Secure Agile Solutions
- Development
- Deploy
- Test

Activities not Phases
Embracing a culture of continuous improvement results in secure systems
Secure Operations

Chaos Engineering

Game Day

Red/Blue Team
- MTTA
- MTTD
- MTTR

Bug Bounty
WANTED
100 000

Product Backlog

Feedback
Secure Solutions through Agile

Activities not Phases
Future

**DevOpsSec:** Seamlessly integrate security into the implementation pipeline; ensuring everyone takes responsibility while continuing to shorten feedback loops.
Automated Security Pipeline

Security
Compass, TMT

Threat Modeling

Manual Assess

Orchestrate

Prioritize

Bag of Holding (FOSS) App

Provision Security Services

Provision Security

• Fortify
• Coverity
• Checkmarx
• Klo
• Veracode

Static Analysis

Dynamic Analysis

Test Automation

Vulnerability Repository

Defect Tracker

Reporting Metrics

Governance
Compliance Reporting

Removal False Positives

Jira, V1, TFS

• RSA
• Qualsys
• Rackspace

Intake

Triage

Test

Deliver

© 2017 LOCKHEED MARTIN CORPORATION. ALL RIGHTS RESERVED
Lockheed Martin Cyber Kill Chain®

Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command & Control
Actions on Objectives

Effectiveness
Priority

Analysis
ROI
Prioritize
Measurement
Resiliency
Escalation
Investment
Dialogue
Culture

Threat Focused Operations Through Intelligence Driven Defence® are Critical
RMF (NIST Risk Mgt Framework)

1. Categorize
2. Select
3. Implement
4. Assess
5. Authorize
6. Monitor
Upcoming Events
16th Annual Conference on Systems Engineering Research

Hosted by: UNIVERSITY OF VIRGINIA, School of Engineering and Applied Science Department of Systems and Information Engineering
May 8 & 9, 2018

Theme: “Systems in Context”

Key Dates:

Final Paper Submission Due: April 13, 2018
Conference Registration Opens: February 1, 2018

Direct link to registration web page: http://edas.info/r24260

POCs:
Peter A. Beling: pb3a@virginia.edu
William T. Scherer: wts@virginia.edu
Cody H. Fleming: fleming@virginia.edu

Venue: University of Virginia Inn at Darden at the University of Virginia

Reserve rooms (referencing CSER) or online at this link.

For more information visit: https://cser2018.com/.
UPCOMING TALKS:
“Successfully Applying Agile Methods for High-Criticality Systems” Series

How Do You Use Agile Methods on Highly-Critical Systems that Require Earned Value Management?
Phyllis Marbach, INCOSE LA Chapter President; Senior Software Engineer at Boeing – Retired
June 6 | 1:00 PM ET | REGISTER NOW

CONTACT
Editor-in-Chief: Dr. Barry Boehm, University of Southern California – boehm@usc.edu
Ms. Maia Canlas, Stevens Institute of Technology – mcanlas@stevens.edu

Thank you for joining us!
Please check back on the SERC website for today’s recording and future SERC Talks information!
UPCOMING TALKS:

“Systems and Software Qualities Tradespace Analysis” Series

Barry Boehm, Chief Scientist, SERC; TRW Professor of Software Engineering and Director, Center for Software Engineering, University of Southern California
August 1 | 1:00 PM ET

Bill Curtis, Senior VP & Chief Scientist, CAST Software; Head of CAST Research Labs, Executive Director, Consortium for IT Software Quality (CISQ)
October 3 | 1:00 PM ET

Xavier Franch, Full Professor, Polytechnic University of Catalonia (BarcelonaTech)
December 11 | 1:00 PM ET

Please visit the SERC Talks page for more information and updates.