Moving Target Reference Implementation

Software Engineering Institute, Carnegie Mellon University
Andrew O. Mellinger

December 17, 2014
Team Profile

• SEI Emerging Technology Center
  – Matt Gaston, PhD
  – Andrew Mellinger
  – David Shepard
  – Stephanie Rosenthal, PhD

• SEI CERT Division
  – Jose Morales, PhD

• Carnegie Mellon University
  – David Garlan, PhD
  – Bradley Schmerl, PhD

• Florida Institute of Technology
  – Marco Carvalho, PhD
Customer Need

Adoption + Ease of Development & Deployment

The government has made substantial investments into moving target and adaptive cyber defense and needs widespread adoption of these technologies.

Researchers need a secure, easy to use, and consistent development and deployment path for new techniques.
Approach

Iteratively build moving target middleware for parallel deployment into different lab environments. Moving target middleware supports installation, configuration, update, system monitoring, alerts, and optimization, and provides services for configuration management, knowledge management, ensembles of moving target techniques, and more.
Blend multi-agent systems and self-adaptive systems.

- Resilient
- Partition tolerant
- Localized performance
- Distributed load
- Incomplete view of data

- Centralized management
- Can hold “big picture”
- Can reason about all properties
- Central point of failure
Approach - Security

Properly designed middleware promotes secure design in extension components. **We want to make security easy.**

**Designed-In Security**
- Security architectures for middleware
- Secure design and coding practices
- Appropriate decomposition and privilege isolations
- Strong management and policy configuration
Transition Activities

The transition process is part of the project.

- Updates early and often
- Deploy Reference Implementation at the SEI
- Deploy Reference Implementation at DHS
- Collaborate with FIT on federation
- Start with AARC and HEZDP
Benefit

• **Measurable** improvements in **security** posture for real networks.

• New technologies can be **evaluated** in a standard environment.

• **Architecture** that is specific to MTD **promotes** useful research.

• Facilitates **experimentation**, prototyping, and **collaboration**.

• Facilitates bootstrapping of **commercial** solutions.
Related Work

• MTC2 from FIT (We are already collaborating with them.)
• Moving Target Defense Researchers
• Adaptive Cyber Defense Researchers
• Adaptive Systems Researchers
• Datacenter automation solutions
• Cloud solutions could also be adapted
Presenter
Andrew Mellinger
ETC
Telephone: +1 412-268-5161
Email: aomellinger@sei.cmu.edu

U.S. Mail
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Web
http://www.sei.cmu.edu
http://www.sei.cmu.edu/contact.cfm

Customer Relations
Email: info@sei.cmu.edu
Telephone: +1 412-268-5800
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257