

2013 DHS S&T/DoD ASD (R&E)  
CYBER SECURITY SBIR WORKSHOP

# Toward Agile and Informed Security Solutions

Intelligent Automation, Inc.  
Justin Yackoski, Ph.D.

*July 23, 2013*



Homeland  
Security

Science and Technology



# Company Profile

- Intelligent Automation, Inc. (IAI)
- 25 year old woman-owned small business
- 130+ professional staff, \$27M revenue in 2012
- Specialize in R&D
  - Cyber security and networks
  - Communications, sensors, robotics, air traffic, training, control, signals, modeling & simulation
- Strong record of excellence in developing and transitioning technology
  - Recent Rapid Innovation Fund technology sold to government, academic, and industry customers

# Customer Need

- Networks are under constant attack
- Networks will be compromised
  - 2012: two new remote access vulnerabilities affected **all** versions of windows
- A sophisticated attacker can easily spread undetected
- Disruption and containment is needed before detection
- Prevent initial successful attack of a network
- Prevent spread after initial attack succeeds
  - Significant focus on this case due to its inevitability

# Approach: Self-Shielding Dynamic Network Architecture (SDNA)

- It is possible to slightly modify the network architecture and significantly affect attackers
  - Network appears to be dynamic via cryptographically secure, IPv6-based techniques
  - Naming, addressing, routing, and other core aspects
  - Use a hypervisor or small embedded device to alter traffic entering/leaving each node
  - Transparently alter flow of packets in the network
- Prevent collection of actionable information
  - Identities, topologies, connectivity, etc.
- Maintain compatibility with existing OSs, applications, routers, switches

# Benefits

- Stop attacks without detection
  - SDNA stops both Microsoft vulnerabilities
- Prevents attacker from gathering actionable information about a network at their leisure
- Prevents scanning and mapping the network
- Prevents several common classes of attacks
- For attacks which cannot be fully prevented
  - Increases effort/resources required for success
  - Increases risk of detection
  - Contains spread of attack
  - Slows attack cycle to allow time to discover/detect



# Current Status



- Past
  - Under development since 2010
  - Demonstrated working in a representative network enclave scenario (compatibility)
  - Completed two external red-team evaluations
- Future
  - Revising software to add integration features
  - Creating embedded hardware device
  - Expect a product in the next 18-24 months

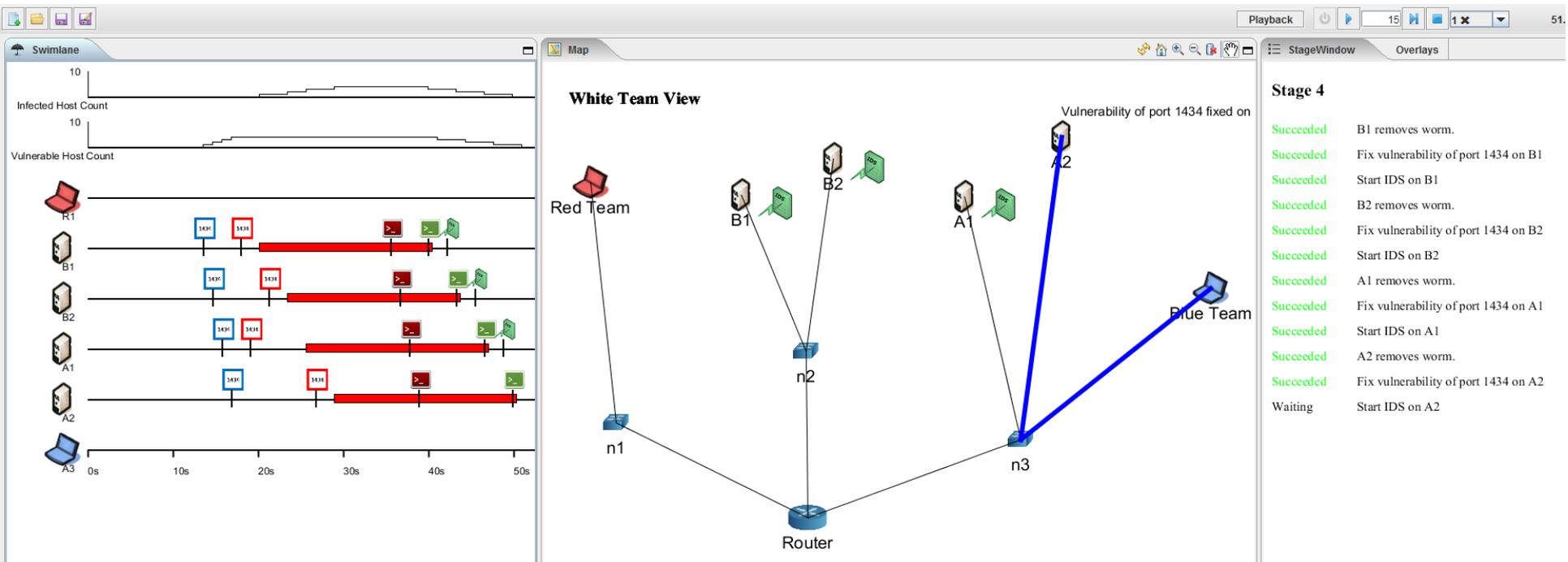
# Other Work – Traffic Resiliency

- Real-time Network Traffic Resiliency
  - Traffic and threat analysis using signature and anomaly detection
  - Divert malicious traffic using filtering present in deployed routing protocols (e.g. BGP FLOWSPEC)

# Other Work – Cyber T&E

- Hermes
  - Cyber security test event execution and analysis tool
  - Quickly build and debug complex network test scenarios
  - Automate configuration, execution, verification, and data collection
  - Provide recording, analysis, and demonstration capabilities
  - Support red-team testing

# Other Work – Cyber T&E (cont.)





# Next Steps



- SDNA:
  - Red-teaming and evaluation
  - Licensing and distribution channels



# Contact Information



- Jason Li (Senior Director)  
jli@i-a-i.com / 301-294-5275
- Justin Yackoski (Program Manager)  
jyackoski@i-a-i.com / 301-294-4251