2012 DHS S&T/ASD(R&E)
CYBER SECURITY SBIR WORKSHOP

Homeland Security
Science and Technology

Self-Shielding Dynamic Network Architecture (SDNA) and Other Efforts

Intelligent Automation, Inc.

Justin Yackoski, PhD

SDNA – Problem

- Computer networks are easy to attack
  - With enough patience, a vulnerability can be found and exploited
  - Once inside a network, an attack can easily spread

- To increase survivability, attack should be prevented and/or limited before detection

Source: unnecessaryquotes.com

SDNA – Overview

- Using an integrated architecture with multiple types of dynamics, SDNA changes the network's appearance continually
- An "SDNA Entity" protected by a hypervisor on each node prevents misuse of network, makes dynamics transparent to OS and user
- Cryptographically strong packet-level enforcement
- Decentralized operation

SDNA – Distinction / Goals

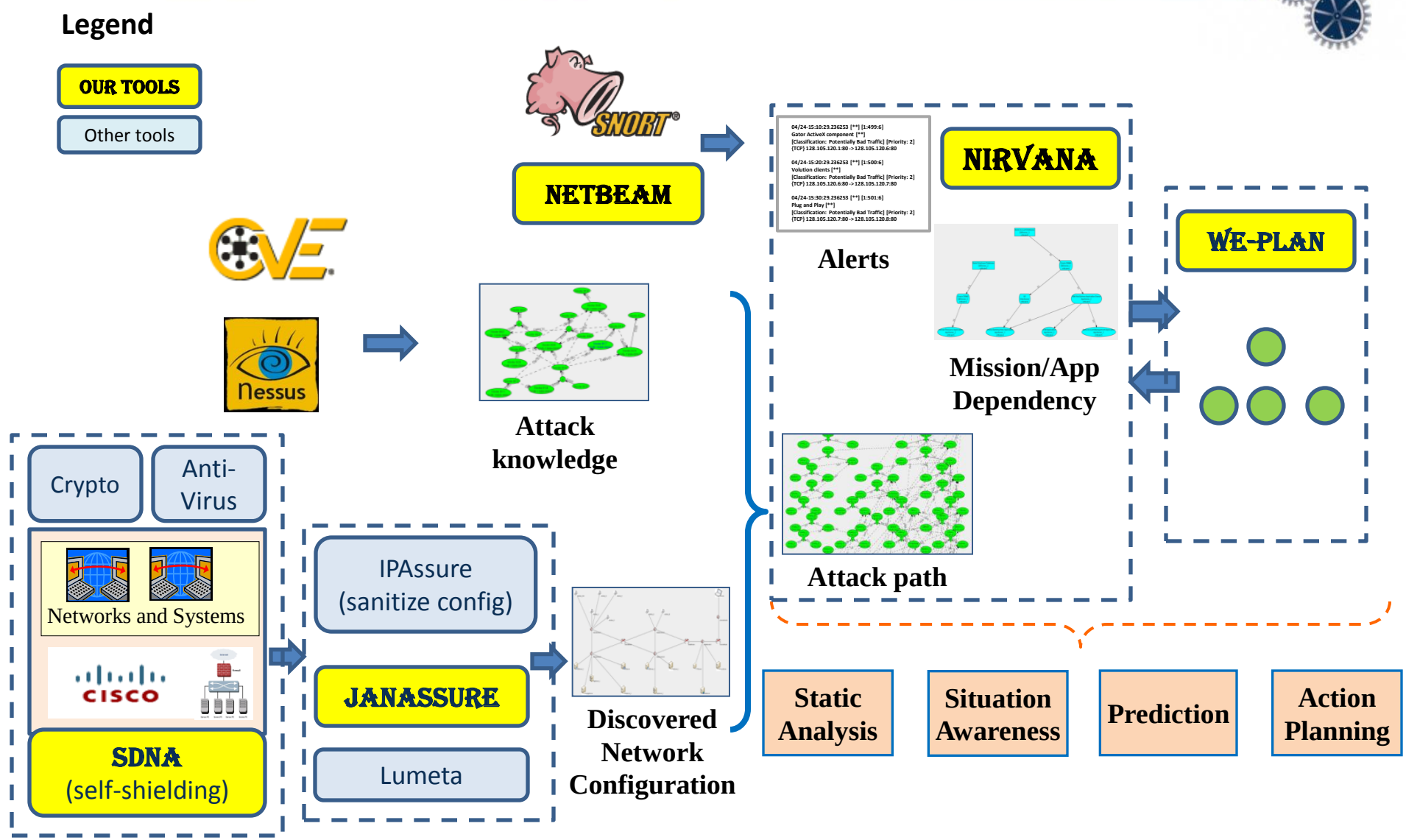
- Disrupt both planning and effectiveness of attacks
- A network is subject to many attacks:
  - Scanning
  - Worms
  - Brute force attacks
  - Cyber spies / spearfishing / etc.
- Prevent the first node from being attacked
- Prevent spread after a successful attack

SDNA - Benefits

- SDNA disrupts attack planning and reduces effectiveness of many classes of attacks
- Multiple dynamics increase total security
- Necessary changes to network behaviors can be implemented via a hypervisor providing translation

SDNA – Status

- Implemented as Linux-based Hypervisor

- Capabilities implemented:
  - Address dynamics via SDNA Bits
  - Naming dynamics via DNS response manipulation
  - Service redirection
  - Service-level availability
  - User authentication and interaction
  - Key exchange

IAI's Phase II Efforts on Cyber Security