CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

Appliance for Active Repositioning in Cyberspace (AARC)

Northrop Grumman Corporation

Jeff Foley

September 18, 2013

Homeland Security

Science and Technology

Team Profile

- **Northrop Grumman Information Systems**
  - Headquarters: McLean, Virginia
  - Annual revenues of approximately $7 billion
  - More than 19,000 employees
  - Offices in 49 states and 18 countries

Team Profile Cont.

- **Cyber Warfare R&D Team**
  - Location: Rome, New York
  - Focuses on computer network operations capabilities and penetration testing
- **AARC Project Team**
  - Principal Investigator: Jeff Foley
  - Co-Principal Investigator: Mike Lisi
  - Security Researchers and Engineers: Dan Martin, Anthony Miller-Rhodes, Michael Burke, Sean Radigan, and Zachary Harvey

Customer Need

- Moving Target Defense (MTD) needs to be transparent to the defender and as unpredictable as possible to the adversary
- Network-centric MTD (IP-Hopping) systems are often challenging to integrate into existing enterprise network infrastructures
- One reason for this issue is that few MTD systems have the typical functionalities that are expected from enterprise appliances.

Approach

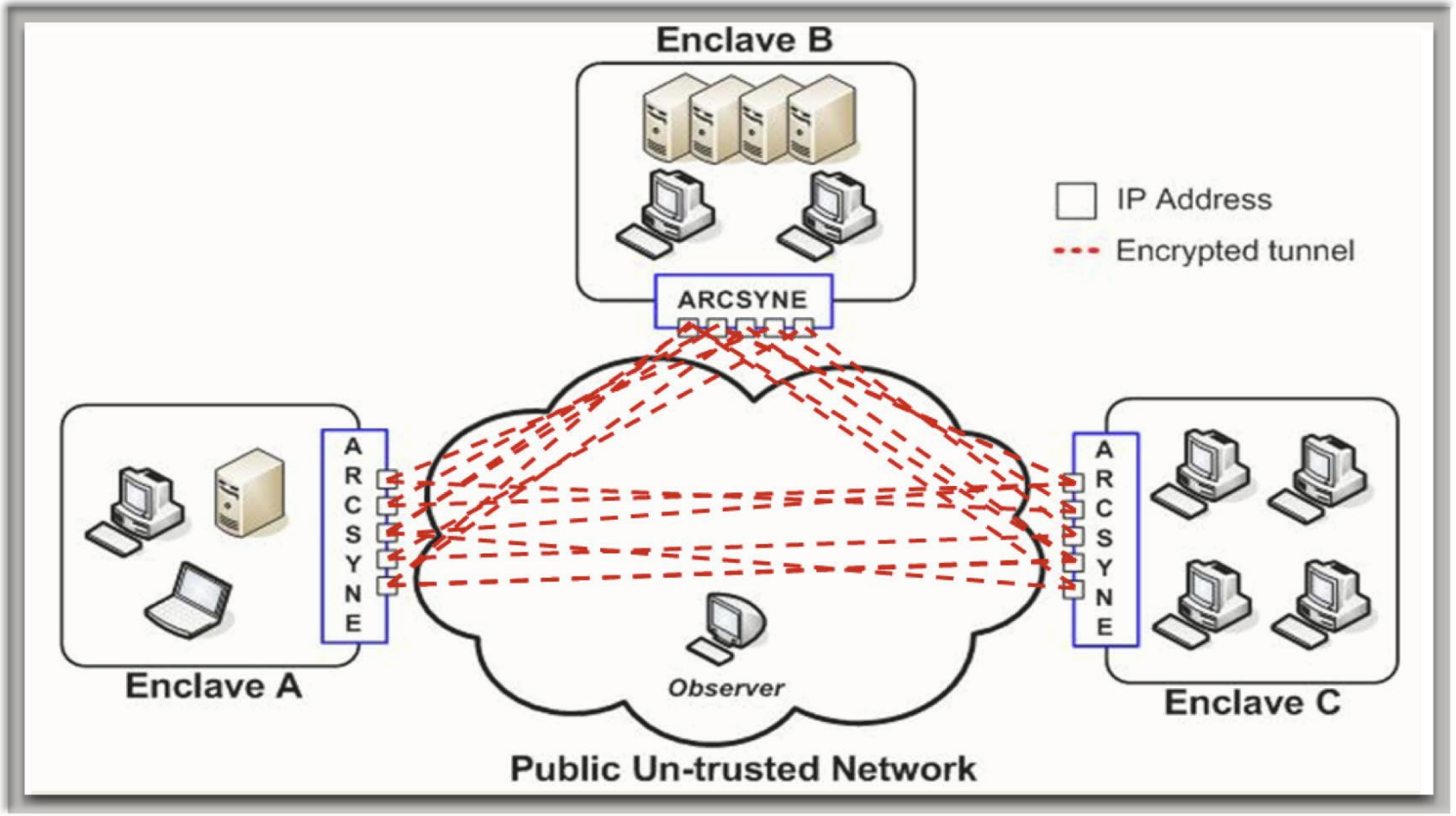
- The AARC project has addressed the practical requirements of deploying a moving target defense system into an enterprise environment

- It has taken an IP-Hopping MTD technology, originally developed by Northrop Grumman and AFRL (ARCSYNE), and matured its readiness for easy deployment

- This included bringing the technology to a high-performance network appliance hardware platform and developing configuration and status interfaces that are expected by network engineers.

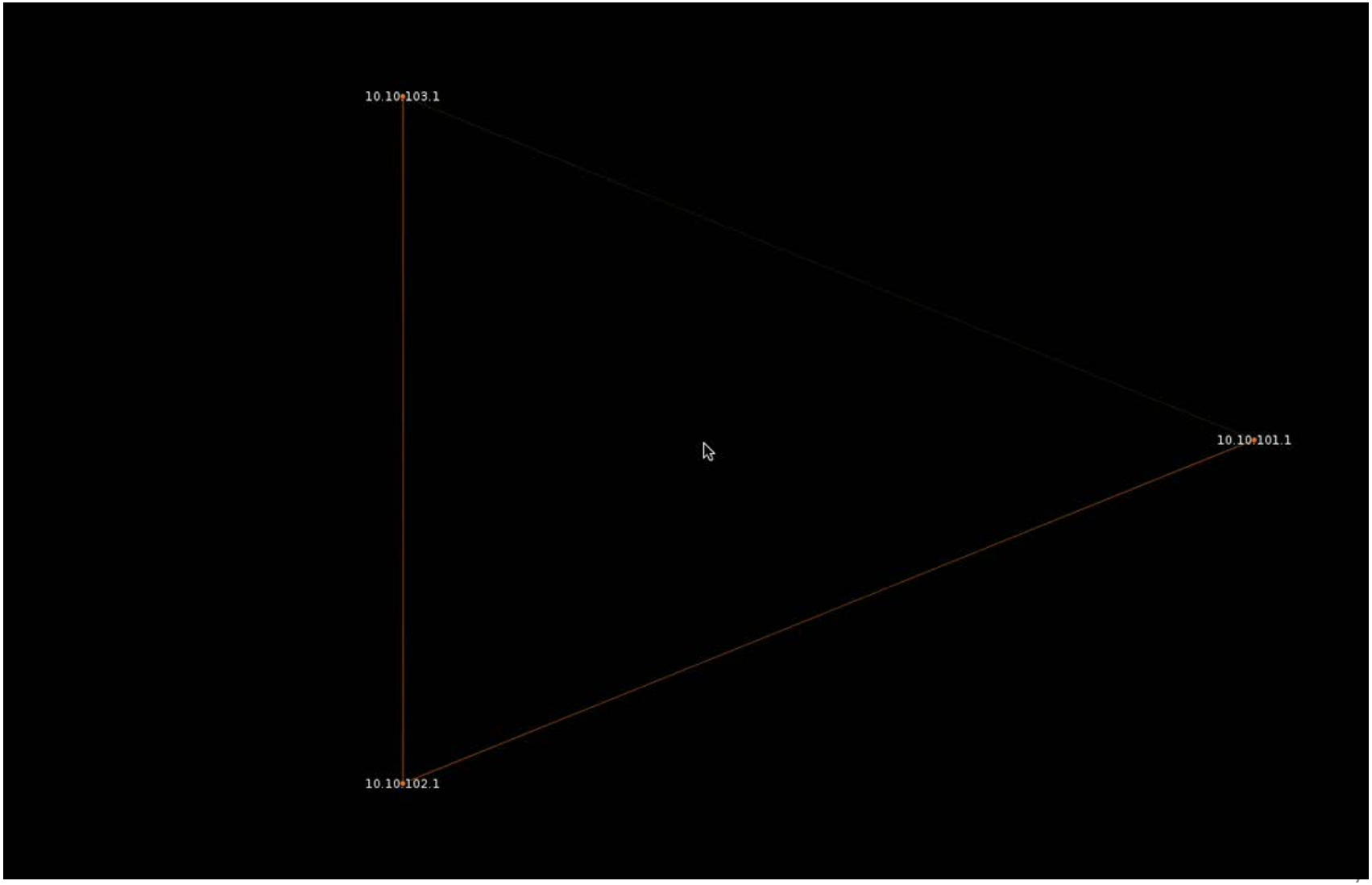
Approach Cont.

Approach Cont.



AFRL/RIGA Diagram of the Developed IP-Hopping System.

Approach Cont.



Benefits

- The AARC project has brought MTD technology to an easy to use appliance
- This allows enterprises to maneuver their cyber assets in cyberspace
- Maneuver allows for repositioning, which can dictate the tempo of a conflict, and preempt enemy actions
- Effective tactical maneuver continually poses new problems for the enemy.

Current Status

- During the 12 month effort, the following has been accomplished:
  - Encapsulated the MTD capability into a 2U rack-mountable network appliance chassis
  - Ported the MTD technology to FreeBSD
  - Developed a web configuration interface
  - Integrated LCD status output into the appliance
  - The appliance can be configured through SNMPv3
  - Enhanced situational awareness syslog output.

Next Steps

- This team is looking forward to working with DHS during the testing and piloting of this product
- This effort has taught us important lessons, and we are looking forward to enhancing the technology further with this knowledge
- Strategic investment planning is currently underway to determine the next step in AARC commercialization.

Contact Information

- Northrop Grumman Cybersecurity: CyberGroup@ngc.com

- Jeff Foley – Security Architect
  - P: 315-338-5404
  - E: Jeffrey.L.Foley@ngc.com
  - W: www.linkedin.com/in/caffix/

- Mike Lisi – Security Engineer
  - P: 315-338-5419
  - E: Mike.Lisi@ngc.com
  - W: www.linkedin.com/in/mikelisi/