A Look Towards Improving Resilience Within Cyber Systems: Methods and Approaches

Roland Varriale

Cyber Security Analyst

Argonne National Laboratory

Argonne NATIONAL LABORATORY

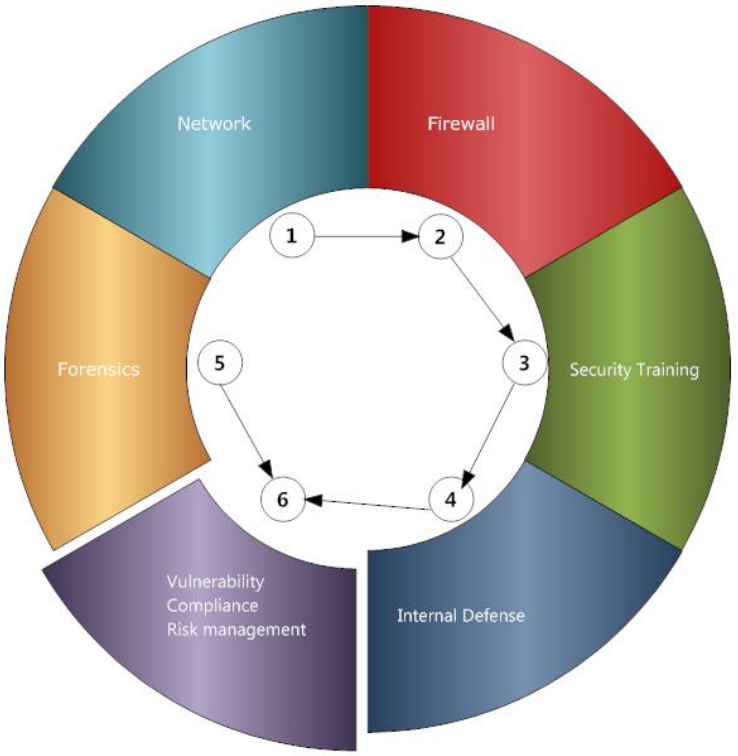
U.S. DEPARTMENT OF ENERGY

Just so we are on the same page

- When we discuss cyber within the context of this talk I am referring to the technological components that direct support business, or operational, functions
- Cyber is often a nebulous term that can be used to interchangeably describe
  - Information Systems (IS)
  - Information Technology (IT)
  - Using computer networks
  - Applied use of computer science
  - Etc
- Resilience can also have similar connotations so I will use it to refer to a System's ability to maintain normal functional operability under a variety of conditions
- Similar concepts that are often blurred are:
    - Robustness
    - Resistance
    - Etc.

Why is this so hard?

- Cyber related systems often combine services and technologies
- “The perimeter” is hard to define and hard to defend
- Security is constantly changing and evolving
- Aggregates of security layers often become unwieldy and cumbersome



Source: wikimedia

Business Vs Technology Vs Security

- It often seems that business and technology are at odds with each other
- To implement technology successfully there is a deployment cycle that often does not fit into the high-level business goals
- How do we support business operations while maintaining secure, resilient systems?

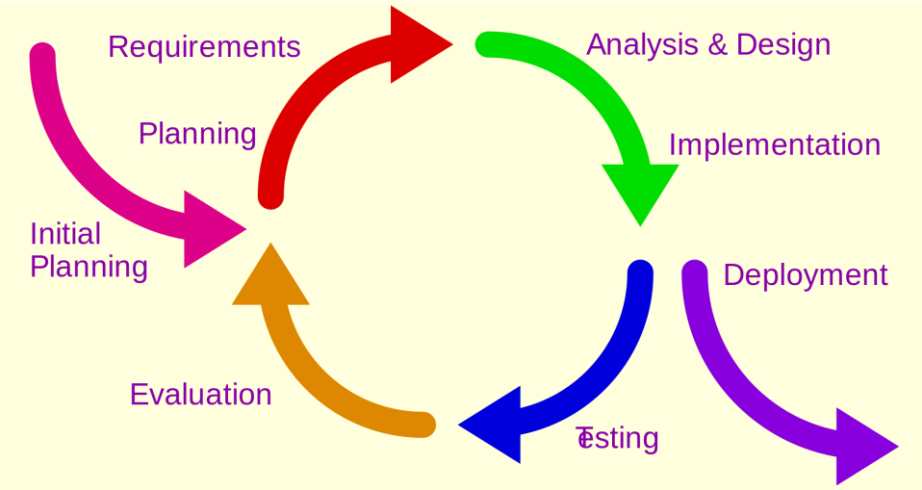


Image: wikimedia

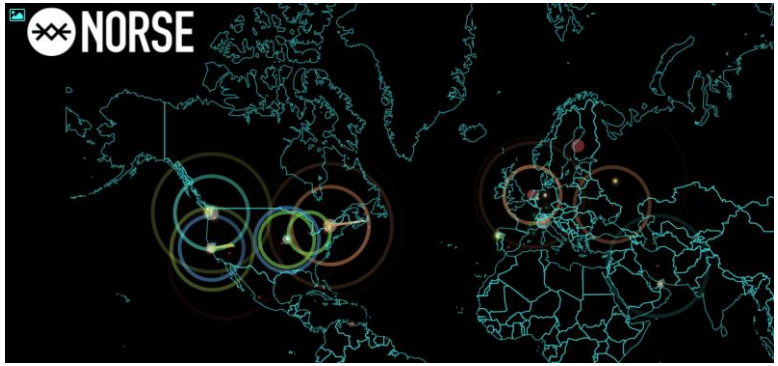
Security and Productivity are often at odds

- There is an observed inverse relationship between security and usability
- By increasing the security, often we decrease usability (and vice versa)
- This is an optimization problem that differs based on business needs

- How much risk are you comfortable incurring?
- Which services are critical/non-critical?

Resilience within Normal Cyber Systems

- Throughout the course of a day there can be several hundred to thousands of potential problems that can occur
  - Unwanted scans of your outward facing devices and computers
  - Visits to infected sites with malware
  - Phishing attempts
  - Drive by downloads
  - Use of business resources for personal use/gain
- Are there appropriate guards in place to support critical business functionality?
- Are there any single points of failure?



Continuity of Business

- Is there documentation in place to support your business operations throughout the entire continuity lifecycle?
- Are there disaster recovery solutions? Offsite?
- Are there clear instructions so that any on-site employee can restore critical system functions?
- Are there an plans in place to ensure reliable shut down of systems in emergencies to ensure configuration data does not become corrupt?
- What is the most efficient way to bring critical services back on line?

Source: wikimedia

A dependency based approach towards resilience

- Argonne has developed several analysis products that rely upon identifying dependencies in order to more fully support critical services, namely within Critical Infrastructure
- This allows for a technologically-agnostic approach towards solving resilience issues and maximizes flexibility
- The need for a specific threat based approach is not needed, and symptoms that underlie threats are identified

An Example

- Typical Question: “Do you have a firewall installed”
- The normal response would be within the domain {yes, no, I have to ask someone}
- Within a typical survey (such as PCI) you would be finished and move on to the next question or topic
- Within our survey tool there would be many follow up questions
  - Is the firewall maintained by a full time employee?
  - How often are the firewall rules updated?
  - Are the firewall rules checked for integrity (is there version control)?
  - Is there a process for decommissioning rules?
  - Who governs the implementation of new rules?
- All of these responses have weighted values that contribute towards a resiliency score

Underlying Services

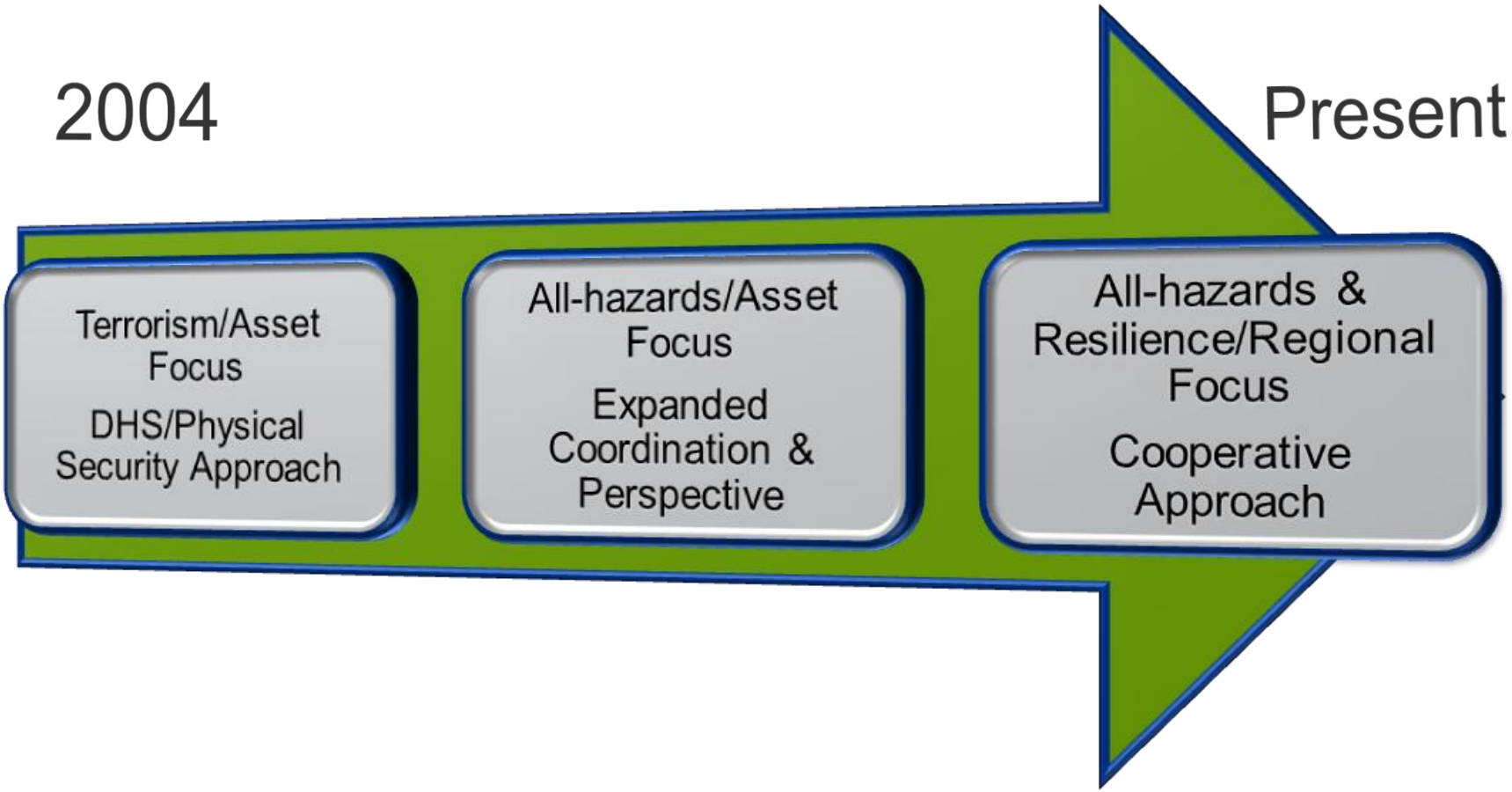
- Once a survey is completed the results are tabulated against the critical services or functions that were identified by the stakeholder
- In our previous example we examined firewalls
- If the critical service was: Payroll and transaction management
- Risks can be enumerated by correlating the responses to the survey with the critical services
- A dashboard is created that allows the stakeholder to see how comparable businesses fare and possible improvement areas

Is this selfish promotion?

- The point I am trying to impress is that there are several ways at approaching resilience
- Identifying critical business services and what technologies support them is the key to understanding how you can improve your own resilience

- Do you need to take the our approach? No
- Do you need to identify critical services within your own operations? Yes

Critical Infrastructure Protection and Resilience



Homeland Security

Regional Resiliency Assessment Program

- The RRAP began in 2009 as a pilot program, out of efforts to assess security of individual critical assets
  - DHS recognized the need to better address the inherent connectivity of assets and systems and the merits of conducting assessments on a regional basis
- The goal of the RRAP is to identify opportunities for regional homeland security officials and critical infrastructure partners to strengthen resilience to all hazards
  - Achieved through a combination of vulnerability assessments, regional analysis, and research related to the RRAP focus area
- The RRAP process identifies critical infrastructure security and resilience gaps; dependencies; interdependencies; cascading effects; and State, local, tribal, and territorial government capability gaps
- DHS conducted 10 RRAP projects in 2014, including the Charlotte RRAP, which was the first to include a major cyber component

Past RRAPS

- Conducted 36 RRAPs from fiscal year 2009 – fiscal year 2013
  - Diverse and dynamic set of critical infrastructure topics, sectors, and regions
- Examined a wide array of factors affecting regional disaster resilience and security
- Major categories of key findings have included:
  - Identification and enhanced assurance of infrastructure dependencies (e.g., power, water, and communications required for critical functions)
  - Mitigation of physical vulnerabilities (e.g., susceptibility to manmade and natural threats, security gaps affecting transportation, mass gatherings, Government sites, and other infrastructure)
  - Closing gaps in planning, procedures, analysis, and training
  - Removing limitations in security and response expertise and equipment

RRAP Project Overview

- Primary activities are conducted over 1 year
- Regional partners build on initial project phase through follow-on analysis and activities
- Project elements include:
  - Partner awareness and outreach
  - Research and informed project scoping
  - Assessments of facilities critical to project focus
  - Multi-disciplinary workshops and subject matter expert interviews
  - Modeling and related data analysis
  - Documenting and briefing of project results
  - Risk mitigation training
  - Post-project activities and follow-up

Dependency Analysis Approach

- RRAP findings are derived from a unique approach designed to capture the complexities of infrastructure system resilience
- Dependency analysis is a core component of this approach
  - Dependencies are a fundamental consideration when assessing the resilience of critical infrastructure assets
  - Dependencies affect the resilience of regions, systems, or supply chains
  - RRAP methodology captures data on dependencies that allows for analysis of regionally significant cascading disruption impacts
  - Dependency data analysis can help determine potential disruption impacts over time and across sectors

Benefits of RRAP

- Data, analysis, and key findings can support existing or new infrastructure resilience enhancement efforts
  - Identify critical cross-sector issues, operational dependencies/chokepoints, planning/communications gaps, etc.
  - Confirm known resilience issues
  - Propose solutions inclusive of less traditional partners
- Unique opportunity for relationship building, enhanced coordination, and broader awareness among diverse yet interconnected stakeholders
  - Builds a stronger and more informed public-private partnership on infrastructure security and resilience issues

Homeland Security

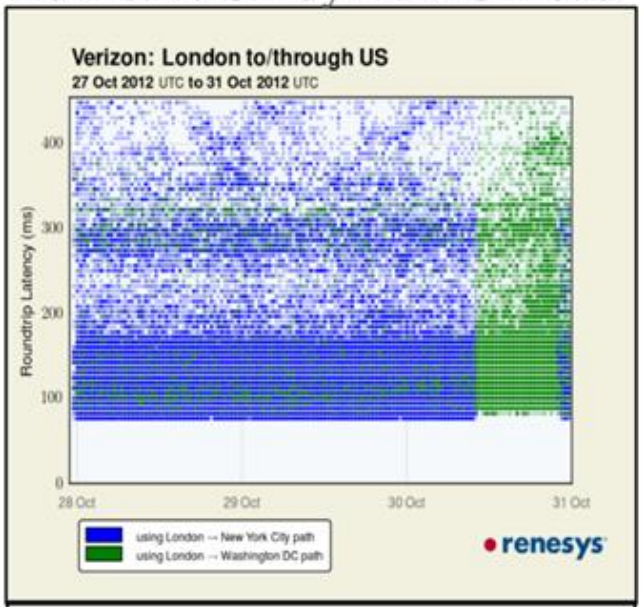
Value to Stakeholders

- Insight to decision makers on internal and external infrastructure dependencies for response planning
- Access to key study findings for collaborating utilities
- Potential planning tool and support for capital improvement funding proposals across the region
- Understanding of the implications of interdependencies among infrastructure systems
- Definition of cascading consequences of system operation including public health and economic value
- Identification of mitigation strategies for specific contingencies
- Evaluation of impacts on future system operational constraints
- Characterization of importance of interconnections to regional system stability

Ashburn, VA Data Center Cluster

- Ashburn-area data center cluster is a primary hub of Information and Communications Technology.
- Data centers and associated fiber are vulnerable to a variety of hazards.
- Develop better public-private partnerships to assist in mitigating potential vulnerabilities and improving communication and response during potential emergencies.
- Opportunity for collaboration with Office of Cybersecurity and Communications (CS&C) and Federal Protective Service (FPS).

Hurricane Sandy Data Offload



Once generators failed, NY data centers shed their load using a London to DC path,. Note the drastic and abrupt change when NY data centers shut down and the entire internet load shifted to Ashburn, creating a potential single point of failure.

Homeland Security

Critical Infrastructure becomes a slightly larger problem

- Scenario: I want to update the firmware on my core switch/router

- **Possible solution 1**: I utilize my backup router while I upgrade the firmware. Once I have tested that the functionality that I require is preserved, I deploy back into the operational environment.
- Complications? Not really a problem since I have redundancy and functionality is completely maintained
- **Possible scenario 2**: I only have one router. There is expected downtime while I detach it from the network and update the firmware. When the update is complete there is additional downtime while I test the functionality OR there are possible compatibility issues if I test within my production environment.
- Complications? Possible corruption or incompatibility and need to roll back changes incurring additional, unexpected downtime

Scenario 2: I want to update my PLC

- Oftentimes there is no redundancy in place and operators are limited to the second scenario from before
- Two common choices:
  - (1) Don't update PLCs and incur additional risk of known security vulnerabilities
  - (2) Update PLCs and incur additional risk of incompatibility or corruption
- Neither of these is very desirable
- Redundancy is typically expensive

At a more abstract level

- Although PLCs, ICS, and SCADA systems are often difficult to upgrade and patch effectively, their supporting cyber systems are not
- As CI systems expand there is a need to include more diverse technologies
- Implementing these technologies without proper knowledge of the ramifications and testing can lead to unintended consequences

CI and Security through Obscurity

- Previously ICS/SCADA devices could hide behind the obscurity of the IPv4 space coupled with the proprietary port number of the service being utilized
- Until recently no one was able to successfully scan the IPv4 space in a reasonable amount of time
- Now – 4 hours

Image: eecs.michigan.edu

And now Searchable!!

- There is no more hide and seek
- Shodan and Censys are two heavily utilized “IoT Search Engines”
- Scan the entire IPv4 space and catalog responses from devices that they find
- Not only scan popular ports: Telnet, SSH, FTP, etc
  - Scan for Siemens, Rockwell Automation, Zigbee, Teletronics
  - Record responses from all of these ports and timestamp
  - Ability to save searches and export results
- Useful to increase your own resilience

SHODAN
Computer Search Engine

censys

Stuxnet: A study in resilience

- In the spring and summer of 2010, Israel unleashed the Stuxnet malware on uranium-enriching centrifuge farms in Iran, causing about a third of Iran's active centrifuges to explode, disrupting the others, and slowing down Iran's march to the bomb.
- The malware was propagated through use of USB drives

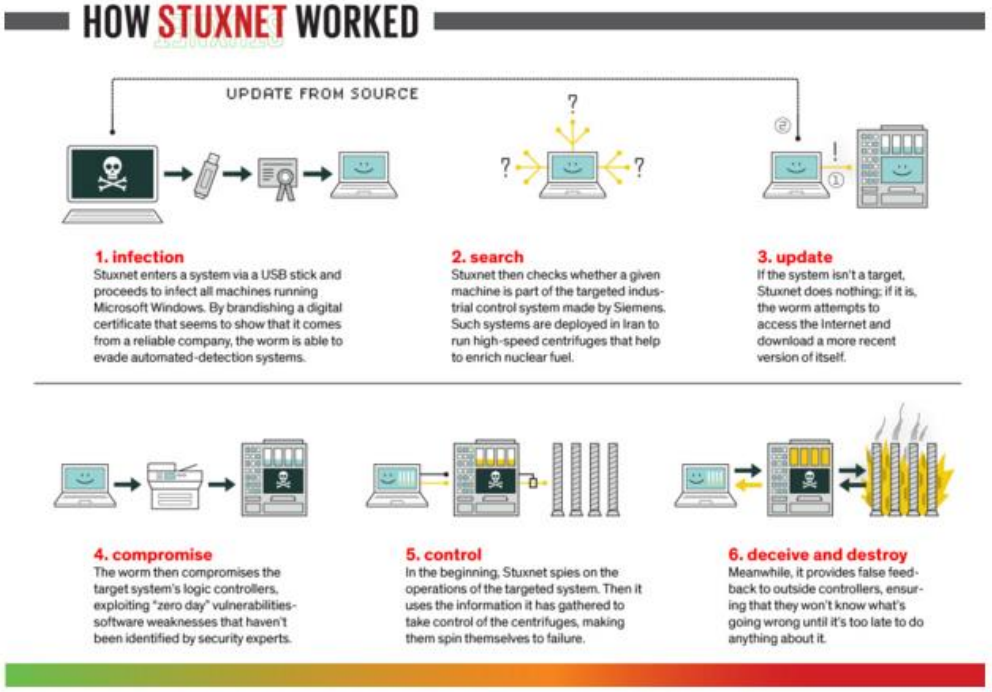


Illustration: L-Dopa, spectrum.ieee.org

Current state of deficiencies

- Cyber resilience lies in the ability to keep your systems and services protected which is usually accomplished by
  - Keeping systems up to date through software patches/updates
  - Maintaining communication between all necessary devices
  - Maintaining uptime and accessibility
- While not always directly related, the ability to restrict communication to only necessary personnel and systems can contribute to a degradation in overall resilience
- Externally facing systems are now readily viewable, and in some cases accessible

Shodan for resilience testing

- Shodan has the ability to be used to search by keyword, location, port/protocol, and several other criteria
- By combining keywords and other search criteria we can identify useful results
- I often perform self scans of the Argonne system to identify potential problems
- For example:
  - 2-19-2016 – 12 instances of Internet Key Exchange on externally facing computers

Cisco Security Advisory

Cisco ASA Software IKEv1 and IKEv2 Buffer Overflow Vulnerability

Critical

Advisory ID:	cisco-sa-20160210-asa-ike	CVE-2016-1287
Last Updated:	2016 February 16 23:06 GMT	CWE-119
Published:	2016 February 10 16:00 GMT	
Version 1.2:	Final	
CVSS Score:	Base - 10.0	
Workarounds:	No workarounds available	
Cisco Bug IDs:	CSCux29978	
	CSCux42019	

Download CVRF

Download PDF

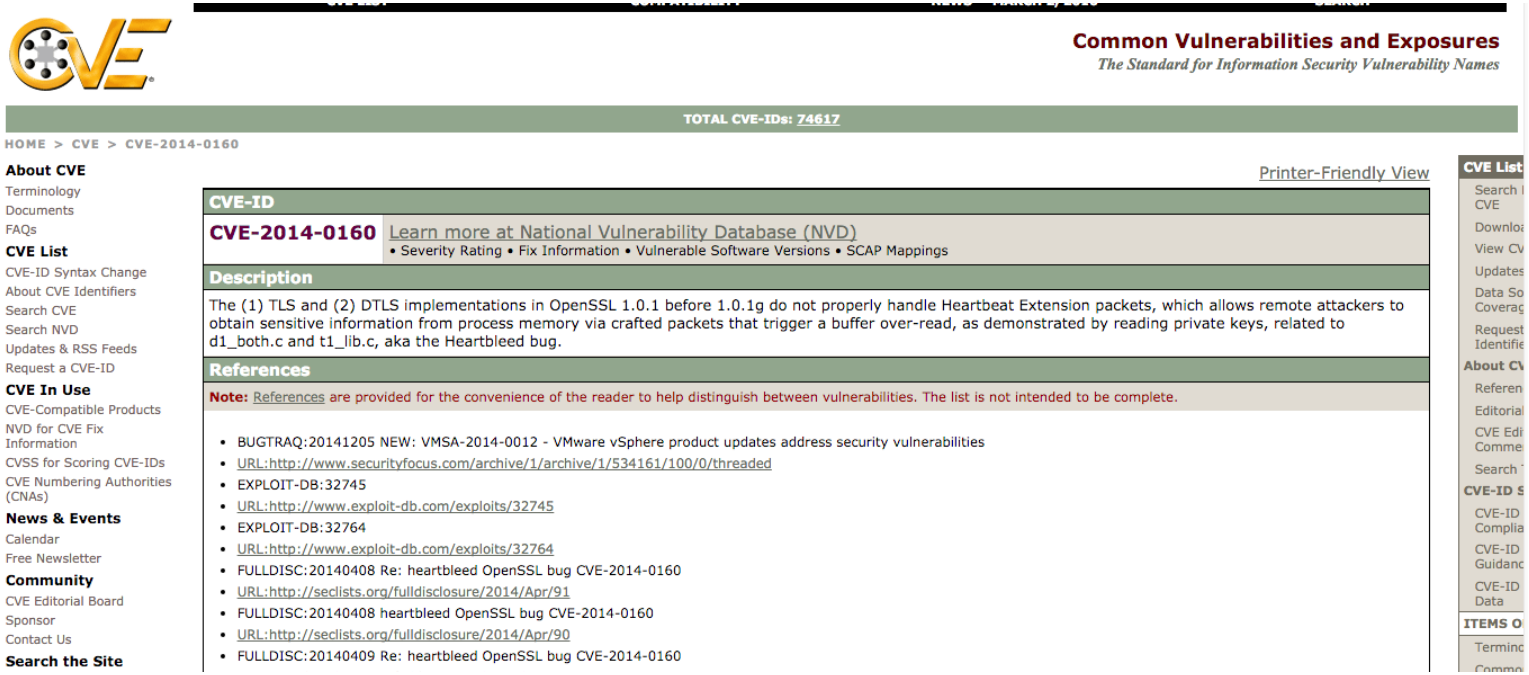
Email

Testing for remote access on ICS

- During research I have found symptoms of unsecured outward facing ICS devices
- The most likely cause was lazy operator access
- ICS/SCADA devices were not initially built for networked access
- This could be secured using any of the following:
  - Access Lists/Whitelists/Restricted Ips
  - Authentication
  - VPN
    - Internal access only (intranet)
- By leaking information about your system you are inherently increasing your risk
- How does the resilience of your system deal with the increase in traffic that may be caused by being indexed?

Knowledge is power

- Common vulnerabilities and Exposures (CVE)
- Help identify vulnerable software and services



Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

TOTAL CVE-IDs: 74617

HOME > CVE > CVE-2014-0160

About CVE
Terminology
Documents
FAQs
CVE List
CVE-ID Syntax Change
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID
CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVSS for Scoring CVE-IDs
CVE Numbering Authorities (CNAs)
News & Events
Calendar
Free Newsletter
Community
CVE Editorial Board
Sponsor
Contact Us
Search the Site

Printer-Friendly View

CVE-ID

CVE-2014-0160 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- URL:http://www.securityfocus.com/archive/1/archive/1/534161/100/0/threaded
- EXPLOIT-DB:32745
- URL:http://www.exploit-db.com/exploits/32745
- EXPLOIT-DB:32764
- URL:http://www.exploit-db.com/exploits/32764
- FULLDISC:20140408 Re: heartbleed OpenSSL bug CVE-2014-0160
- URL:http://seclists.org/fulldisclosure/2014/Apr/91
- FULLDISC:20140408 heartbleed OpenSSL bug CVE-2014-0160
- URL:http://seclists.org/fulldisclosure/2014/Apr/90
- FULLDISC:20140409 Re: heartbleed OpenSSL bug CVE-2014-0160

Moving Target Defense:

Based on the common missile defense technique
changing services every *n* seconds
Service can be OS, application stack, network device, IP, firewall

Reduces the Exposure and Consequences of a Zero Day Exploit
Multiple moving elements allow vulnerable elements to be removed pending patching and qualification / certification – Overall system / application stays up on unaffected platforms.

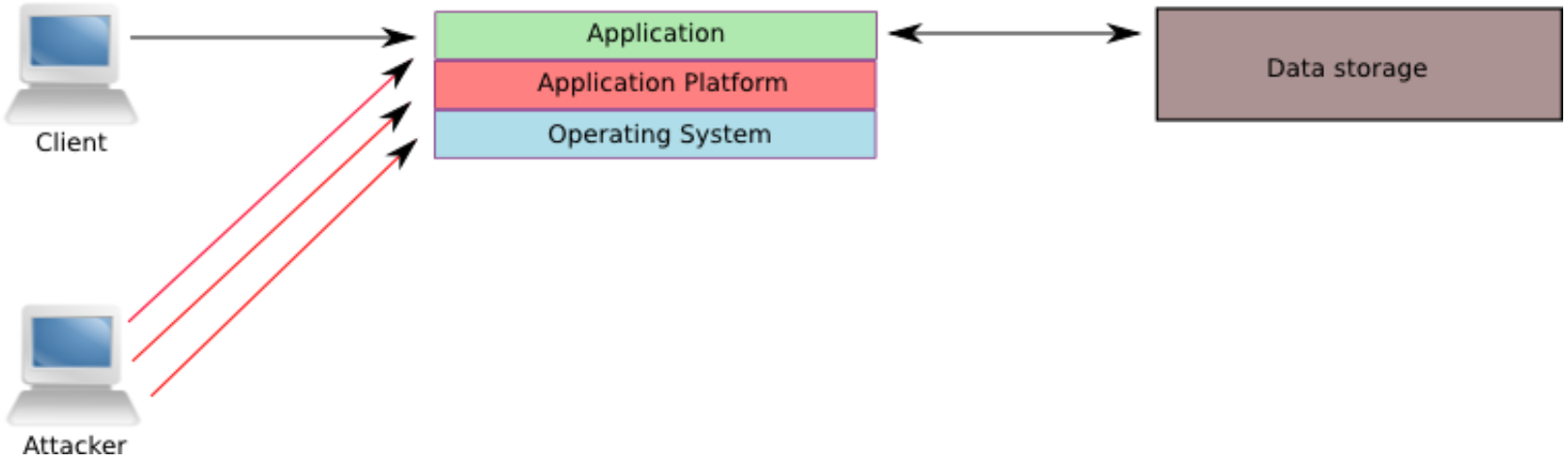
Rotation environment allows uptime during normal outage events
Quarantining of exploited systems for forensic analysis with zero downtime.
Patching, updating, and testing can be done offline with updated systems added post certification with zero downtime.

A Proactive Approach to Cyber Security
Current Collaborators: Argonne National Lab, Infrastructure Assurance Center, University of Buffalo, Iowa State University, and University of IL Chicago

Visualizing the Attack Surface:

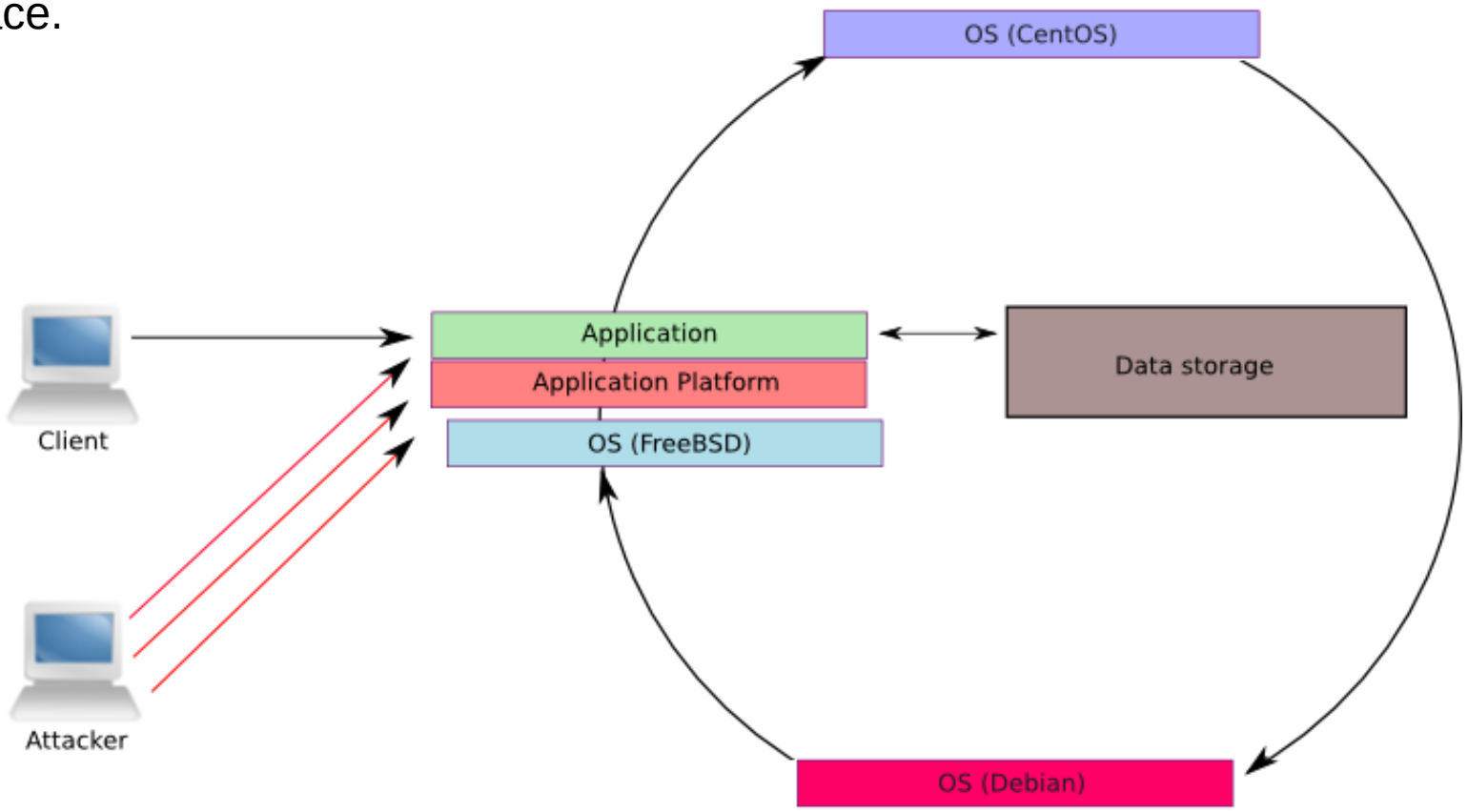
In a normal client/server application, the typical client is only concerned about the application itself, where the attacker's goal is to gain a foothold wherever he can.

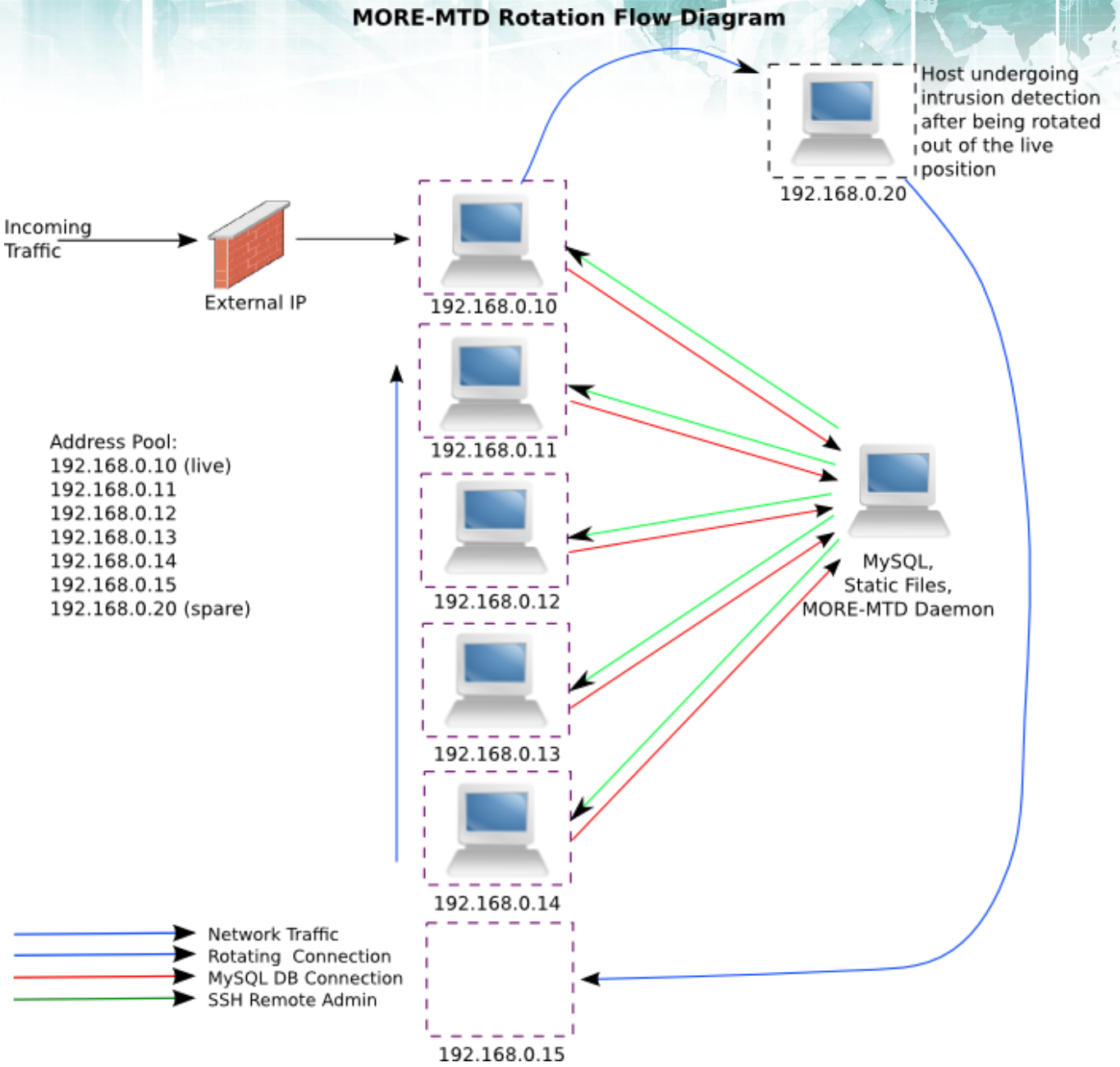
Since an application developer has a limited amount of control over the platform and operating systems their application runs on, these are natural attack vectors for “hackers” to target.



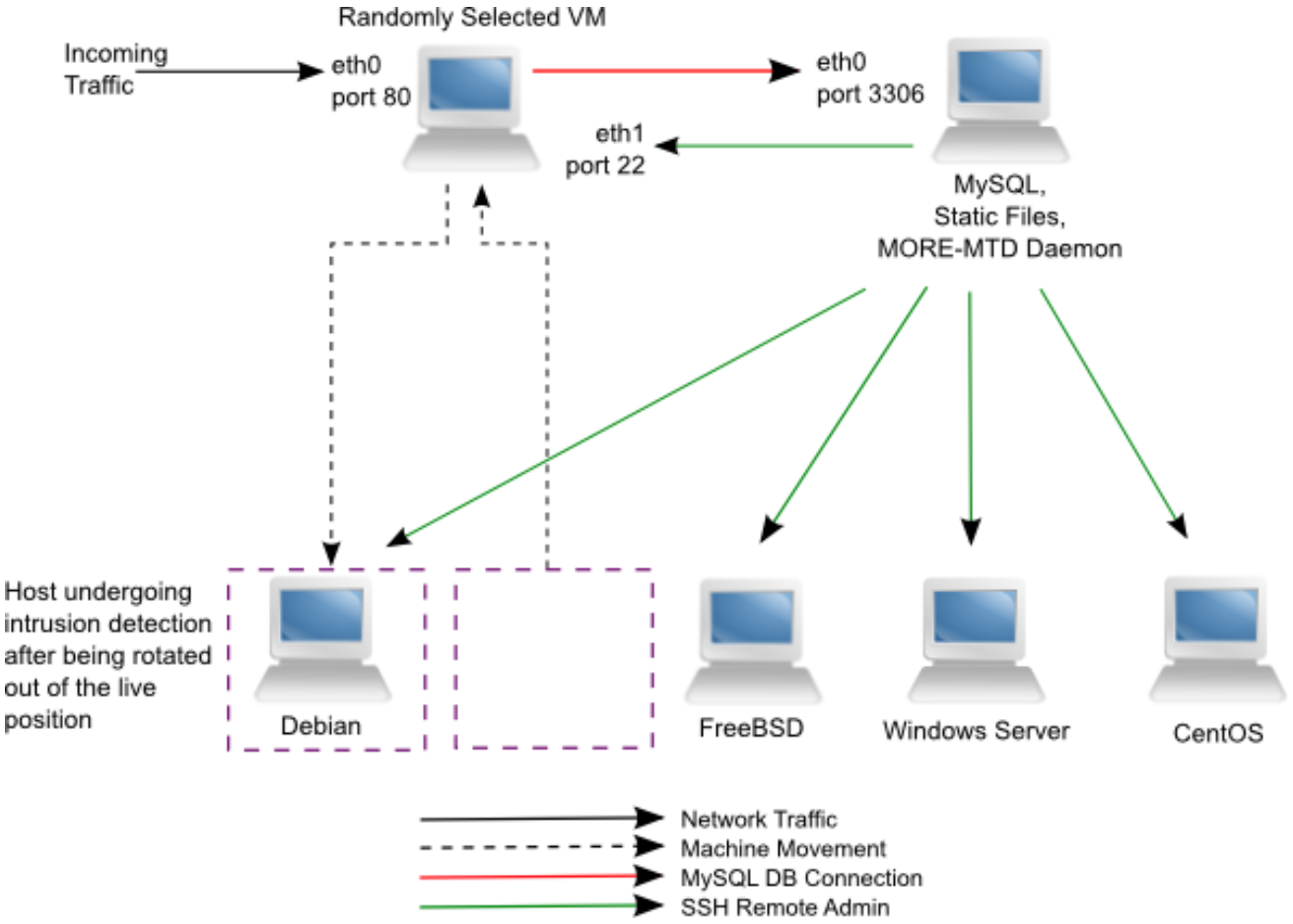
Multiple OS Rotational Environment:

Our idea: since neither the user nor the application (in many cases) rely on or care about the OS, decouple the OS from the stack and rotate that part of the attack surface.



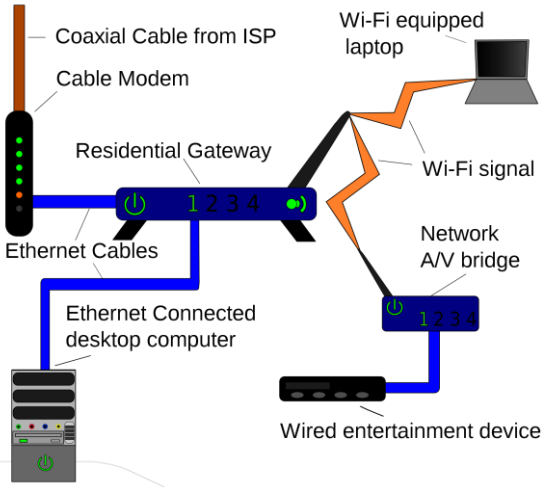

MORE-MTD Rotation Flow Diagram
Host undergoing intrusion detection after being rotated out of the live position
192.168.0.20
Incoming Traffic
External IP
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.15
Address Pool:
192.168.0.10 (live)
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.15
192.168.0.20 (spare)
MySQL, Static Files, MORE-MTD Daemon
Network Traffic
Rotating Connection
MySQL DB Connection
SSH Remote Admin

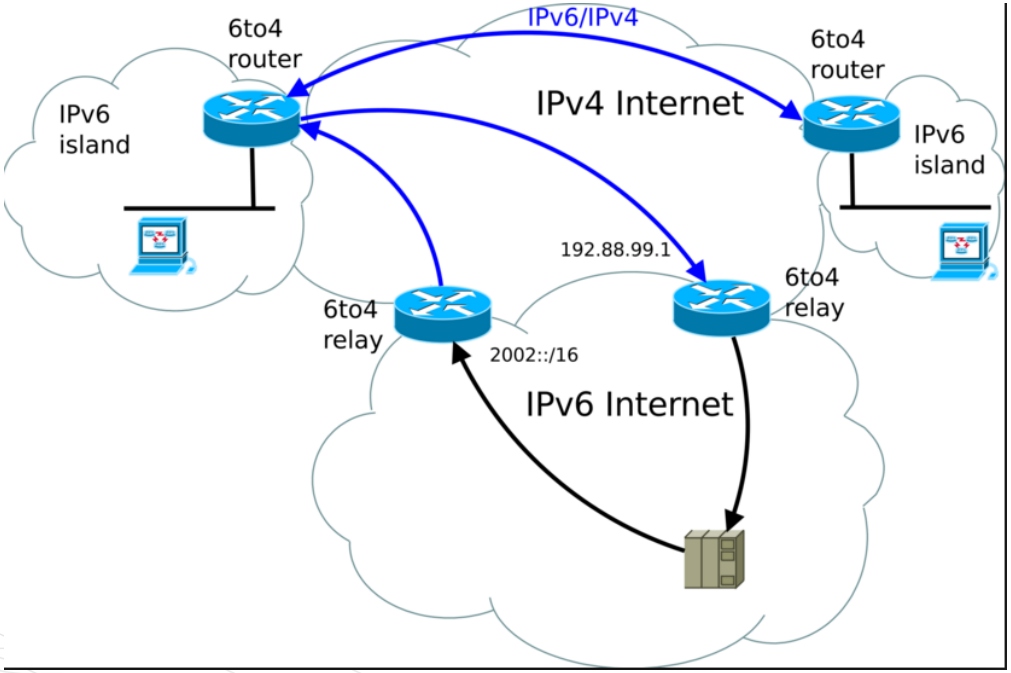
MORE MTD with Random Rotation Ordering



Devices and the IoT

- It's a scary world out there
- As we move to IPv6 every device will gain an external IP address and has the possibility of being globally routable
- Security will be pushed onto individual devices and routers will have a smaller footprint





Moving forward

- How can you protect yourself and increase your own resilience?
  - Patch systems whenever possible
  - Test to ensure that proper business operations are maintained
  - Create plans for deployment of software and devices that include enumerations of problems that occur and how to remediate
  - Maintain communications between business operations and technology teams to ensure that security is preserved and business operations do not suffer
- Should resilience include a human or social aspect to reduce social engineering?

Thank you for listening

- Any questions?

- Probably not