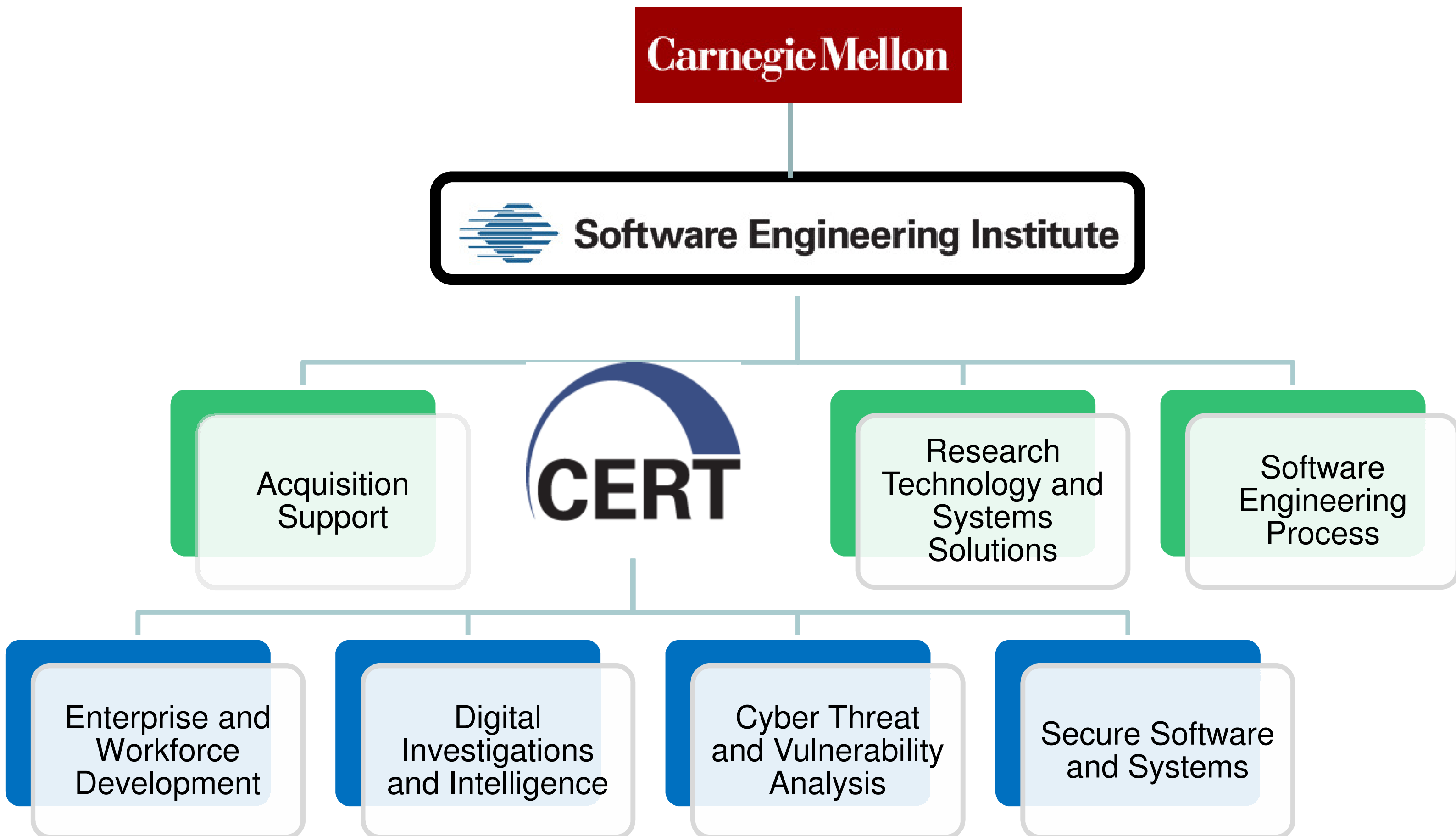
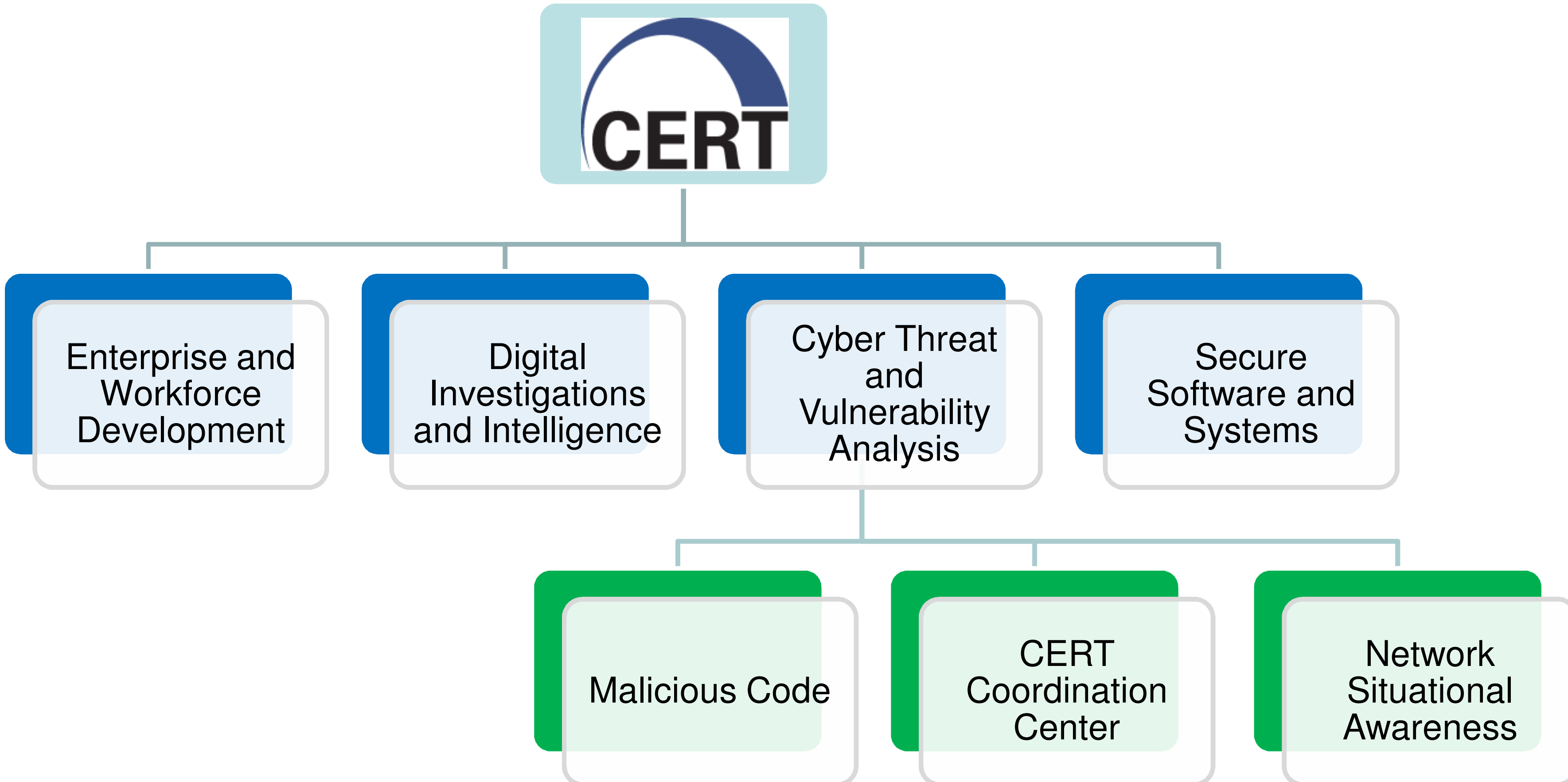
Building Security Into Closed Network Design

George Warnagiris

Software Engineering Institute



Software Engineering Institute



Overview

CLOSED NETWORK DESIGN

Overview

Approach

Background

Findings

Conclusion

Approach

CLOSED NETWORK DESIGN

Building Security into Closed Network Design

Several common closed network design decisions adversely impact operational security

Closed network security can be improved by correctly making certain design decisions

Gathering Observations

Review the literature of network security best practices

Interview and survey closed network analysts

Observe production closed networks

Intended Audience

Network designers

Network architects

Information technology decision makers.

May also be interested:

- Network administrators,
- analysts,
- defenders,
- auditors,
- security officers, and
- information assurance personnel.

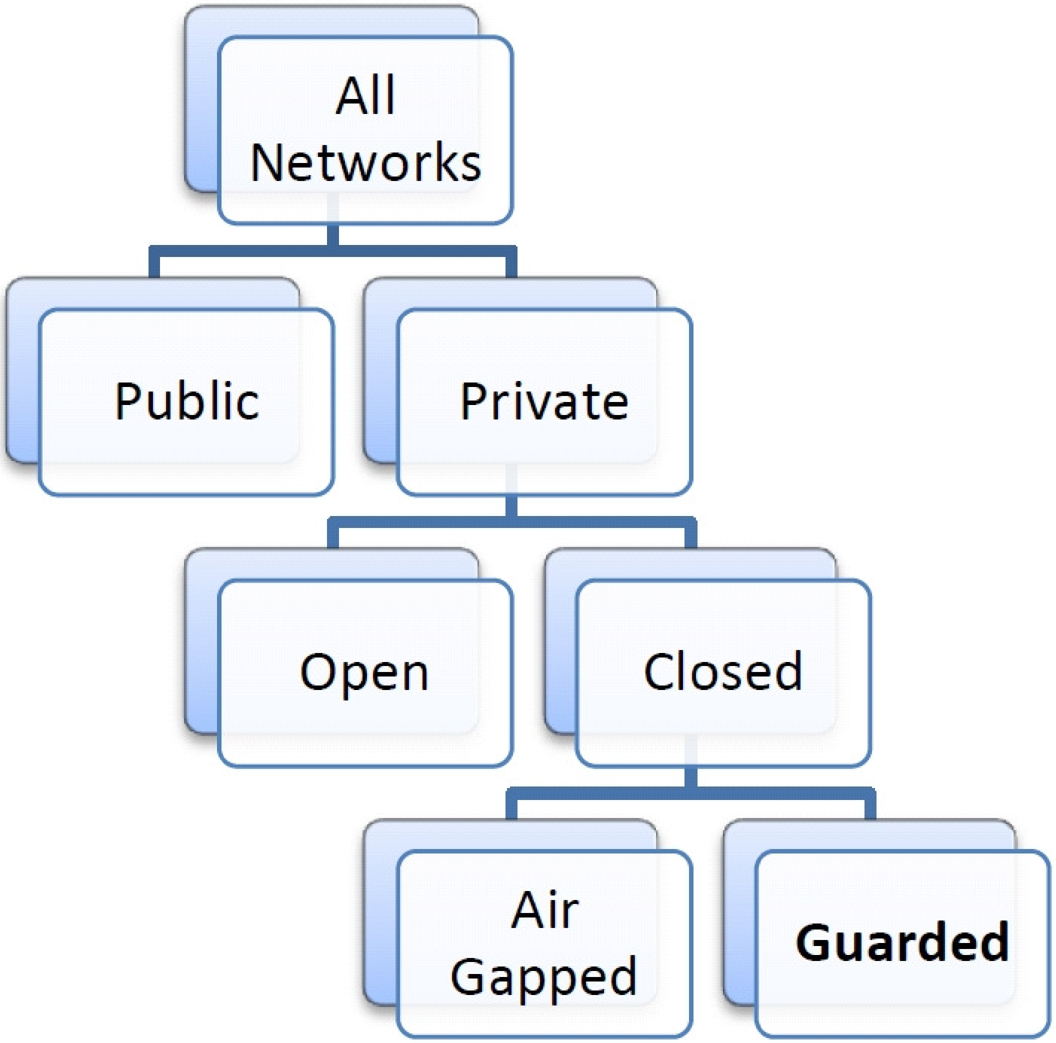
Background

CLOSED NETWORK DESIGN

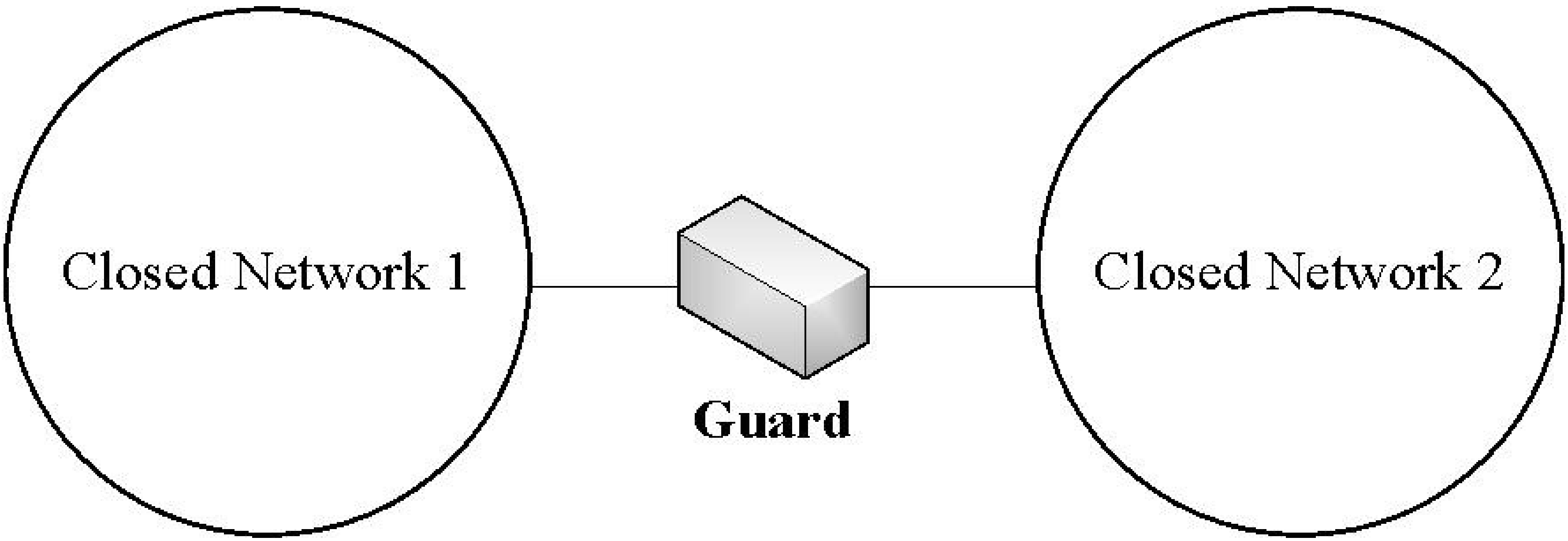
Closed Network Principles

A closed network is a private network which cannot access any other network or devices which are not managed by the designated authority. All nodes on the closed network operate under policy dictated by the designated authority. The closed network implements access restrictions which will prevent attempted communication with other networks.

Network Types



Network Guards



Cross Domain Violation

A *cross domain violation* occurs when controls are not properly enforced while moving data into or out of a closed network.

Exploits on a Closed Network

The presence of malware on the closed network means that a cross domain violation has occurred

Attribution in the Closed Environment

One key difference between closed and open networks is that in a closed network both and attacker and the target are on the same network

The Trust Trap

Closed networks are inherently accessible only to trusted individuals which leads to decreased monitoring, decreased perceived risk, and decreased technical controls built into the network architecture*

* Stephen Band et al., "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," CERT Program, Carnegie Mellon Software Engineering Institute, Pittsburgh, Technical Report CMU/SEI-2006-TR-026, 2006

Design of Security

Security must be addressed from the outset

Experience shows that security usually cannot be retrofitted into systems for which it was not an original design goal

A Note About Topology

Physical topology, network topology, transport topology, and application topology

Application

Transport

Network

Access

The TCP/IP Model

Findings

CLOSED NETWORK DESIGN

Sensor Placement - Sink Holes

A sink hole gathers, analyzes, and drops traffic bound for unallocated, unused, or otherwise selected IP addresses and ranges

Sink holes are particularly effective in closed networks

Sensor Placement - Gaps

Sensor gaps force the network analyst to waste time trying to find missing data

Along these same lines, duplicate sensors are also a problem for the closed network analyst

Sensor Placement - Tunnels in the Closed Network

Tunneling protocols compromise the sensor fabric

Most closed networks are not equipped to deal with tunnels

Tunnel protocols

- e.g. Teredo, GRE or SSH

Subversive tunnels

- e.g. DNS, ICMP or HTTP tunneling

Sensor Placement - Application Proxies

Proxies prevent end-to-end monitoring and make attribution more difficult

Some closed networks do not capture proxy traffic logs or do not store it with other security data

Sensor Placement - Virtual hosts

Network layer taps are not sufficient to monitor virtual networks

Virtual sensors at the hypervisor level

"Virtual" data should be integrated with other data

Sensor Placement - Monitor at Multiple Levels

"Sensor" == "Snort"

A sensor stacks can also include:

- An IDS/IPS (for example Cisco MARS or Sourcefire)
- A flow monitoring and storing system (SiLK, Argus, or NFSen)
- A header capture and storage system
- A full packet capture and storage system (Nikson, NetWitness)
- An application layer monitor for critical applications (email guards, DNS monitors, SQL scrubbers, web proxies)
- A security information and event manager limited retrospective analysis

Topology - Data Consolidation

In closed networks, security data should be consolidated

Operations and security data should be stored together

Topology - Closed Network Zones

Closed networks should be divided into subnetworks of computer with similar security requirements

Enterprise services should be isolated in their own zone (DMZ)

Topology - Asymmetry in the Closed Network

Routing asymmetry has a significant impact on the ability to measure, model, and manage networks

Addressing - DHCP and NAT

Disallow DHCP and NAT on the closed network

If DHCP or NAT must be used, log and monitor and consolidate mappings with other security data

Addressing - IPv6

Avoid IPv6

IPv4 is more mature and better understood

The main benefits of IPv6 do not usually apply to the closed network

Addressing - DNS Names

Choose unique DNS names

Allows for identification of cross domain violations via DNS monitoring

Addressing - Monitor DNS

A DNS sensor is a rich source of information and is often overlooked on closed networks

Operations and Management - Operations vs. Defense

Network operations and network defense teams are often separated and sometime working towards opposing goals

Communication between netops and netdef is often poor

Operations and Management – Duplicate Responsibility

The tiered closed network security structure promotes

- Inefficient communication
- Ill-defined boundaries of responsibility
- Over reporting, and rework

Operations and Management - Lack of Security Budgeting

As closed networks grow, planners fail to account for personnel and sensors in expansion costs

Conclusion

CLOSED NETWORK DESIGN

Observations

Network Architectural Design Decisions that Impact Situational Awareness

Issue	Explanation	Recommendation
Topology		
Centralized monitoring	As opposed to the singular, opaque network core described in the traditional three-tier model, segregate backbone traffic by security profile.	Use multiple, parallelized cores to provide natural chokepoints that allow for in depth monitoring, a natural segregation of data, and centralized sensor data collection strategies.
Data Consolidation	Although data fusion is not a silver bullet, consolidation of data sources enables infrences that are not possible via each individual source. Consolidated data saves analysts' time.	Network designers can increase network defensibility by planning for data consolidation during the design phase.
Security Zones	A security zone is a subnetwork that contains devices with similar security profiles. Zones create network choke points that can be protected by an access control device and monitored by a guard.	The recommended approach is to segment similar users and similar devices into zones and to monitor those zones at the ingress/egress point.
Asymmetric routing	Asymmetric routing implies multiple paths through the network that allow the outbound portion of a flow to take a different path than inbound portion. Asymmetric routing hinders or prevents all except the most simple network monitoring tools.	Force traffic to flow symmetrically or marry both side of the conversations in the data repository.
Sensor placement		
Sink holes	A sink hole is a system that gathers, analyzes, and drops traffic bound for unallocated, unused, or otherwise selected IP addresses and ranges.	Architects should make accommodations for sink holes for use in directing attacks away from sensitive subnetwork and in improving situational awareness.
Sensor gaps	Sensor gaps imply that less than 100% of all traffic is being monitored. Sensor gaps force analysts to make assumptions about completeness. Gaps break some existing analysis products and decrease network situational awareness.	Ensure full sensor coverage so that every flow passes at least one sensor.
Tunnels	There are two types of tunnels, tunnel protocols (e.g. Teredo, GRE or SSH) and subversive tunnels (e.g. DNS, ICMP or HTTP tunneling). Tunnels thwart many monitoring technologies.	Place sensors on the "outside" of tunneling endpoints. Choose sensor technologies that can assist in the detect of subversive tunnels (YaF labeling?, Trickler?)
Application proxies	Proxies provide security and performance some applications such as web surfing.	Place sensors on the "outside" of proxies so that the conversation between the client and the proxy is visible. If this is not possible, provide proxy logs in near real time to security processes and applications.
Closed Network Clouds	Clouds are popular in classified networks too. Classified network clouds face some of the same challenges as Internet clouds.	Group similar clouds into security zones. Tighten access controls with the principles of least privilege.
Virtual hosts and networks and virtual sensors	VMWare has become a popular commodity in today's network design.	Network layer taps are not sufficient to monitor virtual networks. Plan for virtual sensors, create virtual security zones and network chokepoints.
Monitor at multiple levels of the stack	It is common for procurement and operations personnel to assume that "sensor" means "Snort" or "Sourcefire". While Snort operates at layer 2, and that allows it visibility into all the upper layers, other applications provide critical functionality that Snort does not provide.	We recommend that sensor stacks should include: - an IDS/IPS (for example Cisco MARS or Sourcefire) - a flow monitoring and storing system (SiLK, Argus, or NFSen) - A header capture and storage system (Trickler) - A full packet capture and storage system (Nikson, NetWitness) - An application layer monitor for critical applications (email guards, DNS monitors, SQL scrubbers, web proxies) - A security information and event manager
Addressing and naming		
Dynamic Host Configuration Protocol	Because of its transitory nature, DHCP complicates most traditional monitoring and analysis techniques. Attribution is much more complicated in dynamically addressed networks.	Avoid DHCP as much as possible. Set DHCP expiration to the maximum convenient levels. Maintain DHCP logs and make them available in near real time to security processes and applications.

Network Architectural Design Decisions that Impact Situational Awareness

Issue	Explanation	Recommendation
Network Address Translation	NAT complicates most traditional monitoring and analysis by obfuscating the source and/or destination addresses. It also frustrates some analysis techniques such as operating system identification. Even if it is possible to associating native to translated addresses, the process is manual and time consuming in most of the networks studied.	Avoid NAT where possible. Arrange for end-to-end connectivity. If NAT is necessary, monitor both sides or make detailed NAT logs available in near real time to security processes and applications.
IPv6	IPv4 is recommended because it is more mature and understood, because vendors provide better support for v4, and because there is an industry-wide lack of expertise with IPv6. Furthermore, IPv6 depends on a suite of immature and less understood supporting protocols.	Use IPv4 whenever possible.
Choose unique DNS names	Unique domain names allow for identification of cross domain violations via DNS monitoring. If classified and unclassified DNS names are the same, this detection is more complicated.	Monitor public networks for the appearance of classified name requests and monitor the classified network for the appearance of unclassified name requests.
Harvesting DNS queries and responses	Some networks we studied do not take advantage of DNS monitoring. DNS data enables inventorying the name space and the identification of malicious behavior, malicious content distribution, and anomalous IP addresses.	Monitor DNS and create DNS query and response repositories of historical information. See also, Sinkholes
Operations and Management		
Stovepiped network knowledge	Diagrams, device configurations, and address inventories are incomplete, not maintained, and/or unavailable in the networks we've studied. Sometimes this type of information is not shared freely, hoarded by internal competing interests (operations, assurance, security, etc.). We found that there is no standardization for diagrams and inventories. These problems lead to duplication of effort and increased effort when responsibilities change or during audit time.	Architect documentation processes into the design. Utilize network inventorying tools so that documentation processes are automated. Create standardization and sharing policies.
Eliminate duplicate monitoring responsibility	Many networks spend duplicate effort (and duplicate equipment) monitoring at multiple network tiers. Enclave networks promote effort duplication. A streamlined security monitoring system is more efficient because it does not incur division of labor overhead.	Consolidate monitoring responsibility.
Account for personnel and sensors in expansion costs	Many classified networks fail to anticipate the increased workload and equipment costs when planning for network growth.	Consider the impact of expanded functionality when designing the network. Include personnel costs in classified network upgrade budgets.

Hypothesis

Several common closed network design decisions adversely impact operational security

Therefore, closed network security can be improved by selecting certain design aspects

Predictions

- Zoning of closed networks will lessen the number of machines affected in a malware worm attack.
- Data consolidation will allow for the creation of new analysis techniques and increased situational awareness.
- The collection of sinkhole data will allow discovery of policy violations that were not possible before.
- Elimination of NAT allows for faster attribution.
- As duplication of effort is decreased, closed network defense becomes less expensive and more reliable.

Future Work

CLOSED NETWORK DESIGN

Experiment

Create test closed networks and compare operation

Use production closed networks as a test bed

Future Work

Security Capability Model for Networks

- Maturity Level 5 – Optimized Closed Network
  - Guard Validation
  - Topology Verification
  - Sensor Placement
  - Addressing Planning
  - Operations
  - Organizational Training
  - Risk Management

Security Capability Model for Networks

- Maturity Level 4 – Defined Border Mgt
  - Guard Management
  - Topology Requirements Development
  - Sensor Optimization
  - Addressing Management
  - Operations