Building Security Into Closed Network Design

George Warnagiris
NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.
Software Engineering Institute

Carnegie Mellon

Software Engineering Institute

- Acquisition Support
- CERT
- Research Technology and Systems Solutions
- Software Engineering Process
- Enterprise and Workforce Development
- Digital Investigations and Intelligence
- Cyber Threat and Vulnerability Analysis
- Secure Software and Systems
Software Engineering Institute

Enterprise and Workforce Development

Digital Investigations and Intelligence

Cyber Threat and Vulnerability Analysis

Secure Software and Systems

Malicious Code

CERT Coordination Center

Network Situational Awareness
CLOSED NETWORK DESIGN

Overview
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

- All Networks
  - Public
  - Private
    - Open
    - Closed
      - Air Gapped
      - Guarded
Network Guards

Closed Network 1

Guard

Closed Network 2
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 an 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*

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

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
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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Explanation</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Topology</strong></td>
<td>As opposed to the singular, opaque network core described in the traditional three-tier model, separate backbone traffic by security profile.</td>
<td>Use multiple, parallelized cores to provide natural choke points that allow for in-depth monitoring, a natural segmentation of data, and centralized sensor data collection strategies.</td>
</tr>
<tr>
<td><strong>Centralized monitoring</strong></td>
<td>Although data fusion is not a silver bullet, consolidation of data sources enables analysts that are not possible via each individual source. Consolidated data saves analyst’s time.</td>
<td>The recommended approach is to segment similar users and similar devices into zones and monitor those zones at the ingress/egress point.</td>
</tr>
<tr>
<td><strong>Data Consolidation</strong></td>
<td>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.</td>
<td>Force traffic to flow symmetrically on both sides of the conversation in the data repository.</td>
</tr>
<tr>
<td><strong>Security Zones</strong></td>
<td>Asymmetric routing implies multiple paths through the network that allow the outbound portion of a flow to take a different path than the inbound portion. Asymmetric routing renders or prevents all except the most simple network monitoring tools.</td>
<td>Architects should make accommodations for sink holes for use in directing attacks away from sensitive subnetwork and in improving situational awareness.</td>
</tr>
<tr>
<td><strong>Sensor placement</strong></td>
<td>A sink hole is a system that gathers, analyzes, and drops traffic bound for unallocated, unused, or otherwise selected IP addresses and ranges.</td>
<td>Ensure full sensor coverage so that every flow passes at least one sensor.</td>
</tr>
<tr>
<td><strong>Sink holes</strong></td>
<td>Sensor gaps simply mean 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 increase network vulnerabilities.</td>
<td>Place sensors on the “outside” of tunnel endpoints. Choose sensor technologies that can assist in the detection of subversive tunnels (YAF labeling, T rickler?).</td>
</tr>
<tr>
<td><strong>Sensor gaps</strong></td>
<td>There are two types of tunnels: tunneled protocols (e.g., Teredo, GRE or SSH) and subversive tunnels (e.g., DNS, ICMP or HTTP tunneled). Tunnels thwart many monitoring technologies.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Tunnels</strong></td>
<td>Application proxies provide security and performance some applications such as web surfing.</td>
<td>Choose 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.</td>
</tr>
<tr>
<td><strong>Application proxies</strong></td>
<td>Clouds are popular in classified networks too. Classified network clouds face some of the same challenges as internet clouds.</td>
<td>Some networks use classified DNS data enables inventorying the name space and the identification of malicious behavior, malicious content distribution, and anomalous IP addresses.</td>
</tr>
<tr>
<td><strong>Closed Network Clouds</strong></td>
<td>VMW are not just a commodity in today’s network design.</td>
<td>Monitor at multiple levels of the stack. Consider the impact of application functionality when designing the network.</td>
</tr>
<tr>
<td><strong>Virtual hosts and virtual sensors</strong></td>
<td>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 a visibility into all the upper layers, other applications provide critical functionality that Snort does not provide.</td>
<td>Monitor all sensor levels to ensure effective monitoring and security processes.</td>
</tr>
<tr>
<td><strong>Addressing and naming</strong></td>
<td>Dynamic Host Configuration Protocol</td>
<td>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.</td>
</tr>
</tbody>
</table>

Network Architectural Design Decisions that Impact Situational Awareness

<table>
<thead>
<tr>
<th>Issue</th>
<th>Explanation</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAT</strong></td>
<td>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 associate native to translated addresses, the process is manual and time consuming in most of the networks studied.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Translation</strong></td>
<td>IPv6 is recommended because it is more mature and understood, because vendors provide better support for IPv6, 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.</td>
<td>Use IPv6 whenever possible. Monitor public networks for the appearance of unclassified packets and monitor the classified network for the appearance of unclassified packets.</td>
</tr>
<tr>
<td><strong>IP addresses</strong></td>
<td>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.</td>
<td>Monitor DNS and unclassified DNS and response repositories of historical information. See also, Snortholes.</td>
</tr>
<tr>
<td><strong>Distributed Intrusion Detection System (IDS)</strong></td>
<td>Many network monitoring tools are not sufficient to monitor virtual networks. Plan for virtual sensors, create virtual security zones and network choke points.</td>
<td>Many networks spend duplicate effort (and duplicate equipment) monitoring at multiple network tiers. Enclose networks promote effort duplication. A streamlined security monitoring system is more efficient because it does not incur divisions of labor overhead.</td>
</tr>
<tr>
<td><strong>Operations and Management</strong></td>
<td>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 shared freely, learned by internal computing interests (operations, assurance, security, etc.).</td>
<td>Diagrams, device configurations, and address inventories are complete. NA</td>
</tr>
</tbody>
</table>
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