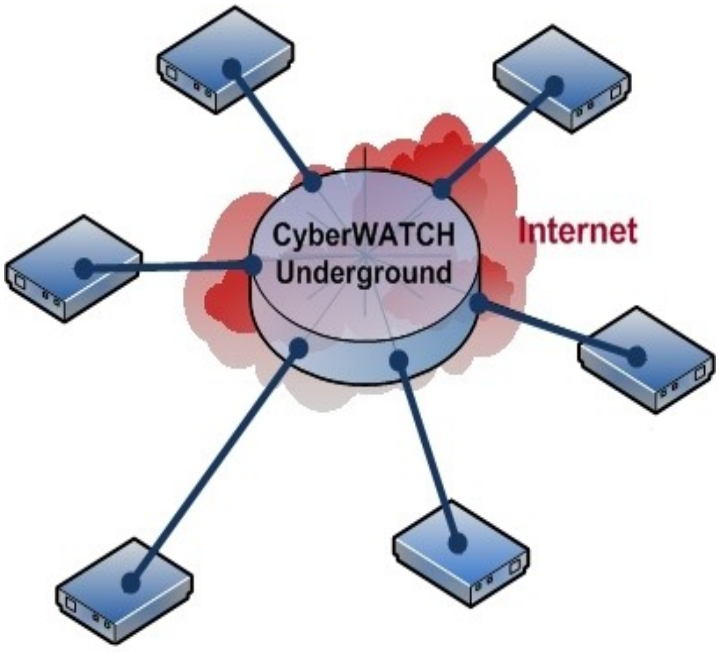
The CyberWATCH Underground

A Proposal for a Cooperative Testbed Network to Facilitate Information Assurance Education and Cooperation



Mark Matties and Sharad Sharma
Bowie State University
Dept. of Computer Science

Introduction

CyberWATCH has enjoyed much success since it inception. In particular, Prof. Casey O'Brien has run a Mid-Atlantic Regional competition for the Collegiate CyberDefense Competition. Many other members have arranged or directly provided courses, seminars, faculty development and other activities around Information Assurance education.

To sustain cooperative activities beyond these meetings once participants have gone home, members would need to create ad hoc network connections between them. Even with the wide range of knowledge and skills among the CyberWATCH members, expertise in network engineering may be out of reach. They may also need to convince their local Office of Information Technology to create a firewall rule exception to allow a one off network connection.

We propose a secure testbed network – the CyberWATCH underground – that will provide a means for ongoing collaborative activities. The CyberWATCH Underground takes its name from the London Underground – the name of the subway system in that city. Using this network, CyberWATCH members – and other approved institutions – . The CU also encourages "buy in" from the local administration through a Memorandum of Understanding, giving CyberWATCH members a better chance of cooperation from their local OIT.

The mission of CyberWATCH encourages "... members collaborate to share best practices, methodologies, curricula, course modules and materials, and provide faculty training and support to schools who want to develop an information security/assurance curriculum". The CyberWATCH Underground will serve as the "last mile" resource that facilitates all manner of ongoing cooperation between participants.

Architecture Overview

The CU is a secure overlay network (see Figure 1). That is, it is an independent, logical network that runs over existing physical network facilities between participating sites. It employs a number of security appliances (one at each participating site) that create and maintain the CU network. The appliance, termed the CyberWATCH Underground Tunnel Server (CUTS), is a modest computer. Each CUTS will be sent to the participating site pre-configured, fully ready to drop into the site's network.

The CUTS runs the Linux operating system and creates the CU network through either a Layer 3 or Layer 4 secure tunnel. The CUTS also provides network health information via SNMP to a health monitoring server.

The CU is a separate logical network, but uses the campus/ISP (physical) connection of the local site. Ideally, the CUTS will be placed in the lab of a CyberWATCH member. Each site determines which of its resources, if any, it will connect to the CU, when they will connect and for how long. The CU requires no dedicated computing resources except for the CUTS and an ISP connection. The network behind the CUTS may be as simple or as complex as desired.

While the CU runs over existing physical network connections at each site and through the Internet, it is designed to be a *closed network*. It does not and will not provide connectivity to the Internet and is not designed. Note that the CUTS does not co-opt the Internet connection at its placement site. The CUTS

operates in parallel with existing network connections.

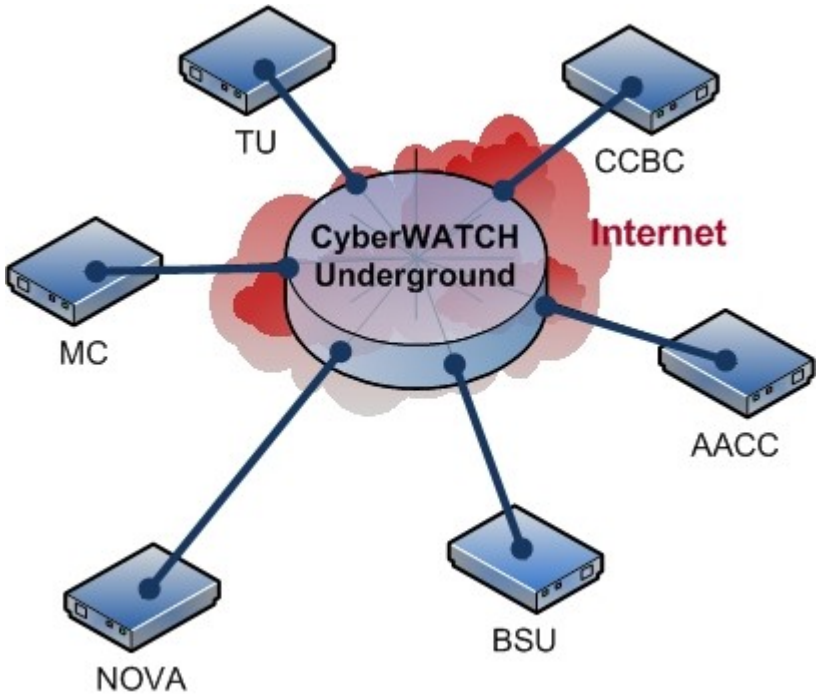


Figure 1: CyberWATCH Underground inter-site logical network diagram. Site names are for demonstration purposes only.

An example of CU use is shown in Figures 2 and 3 below.

The CyberWATCH Underground Tunnel Server (CUTS)

Hardware	TBD
Operating System	Linux (RHEL 5), *iptables* (firewall), *iproute2* (traffic shaping/policing)
Tunnel Software	IPSec (or OpenVPN, if necessary)
Health Monitoring Software	Net-SNMP, Nagios. Cacti, RRDtool

ISP connection

A site that wishes to connect to the CU must provide its own physical (ISP/Internet) network connection. We are happy to lend technical assistance when requested. However, we cannot advise anyone to circumvent their institution's AUP.

CU Connection Options

Preferred Option	IPSec
Alternative Option	OpenVPN

IPSec is much preferred to OpenVPN since the former has reduced packet overhead and is routed normally between CU sites. In particular, OpenVPN requires a fully connected mesh network of point to point links as well as a central VPN server, which would present a single point of failure. It may be possible that a site cannot (for whatever reason) connect to the CU using IPSec. In such a case, OpenVPN may provide a workaround until IPSec can be implemented.

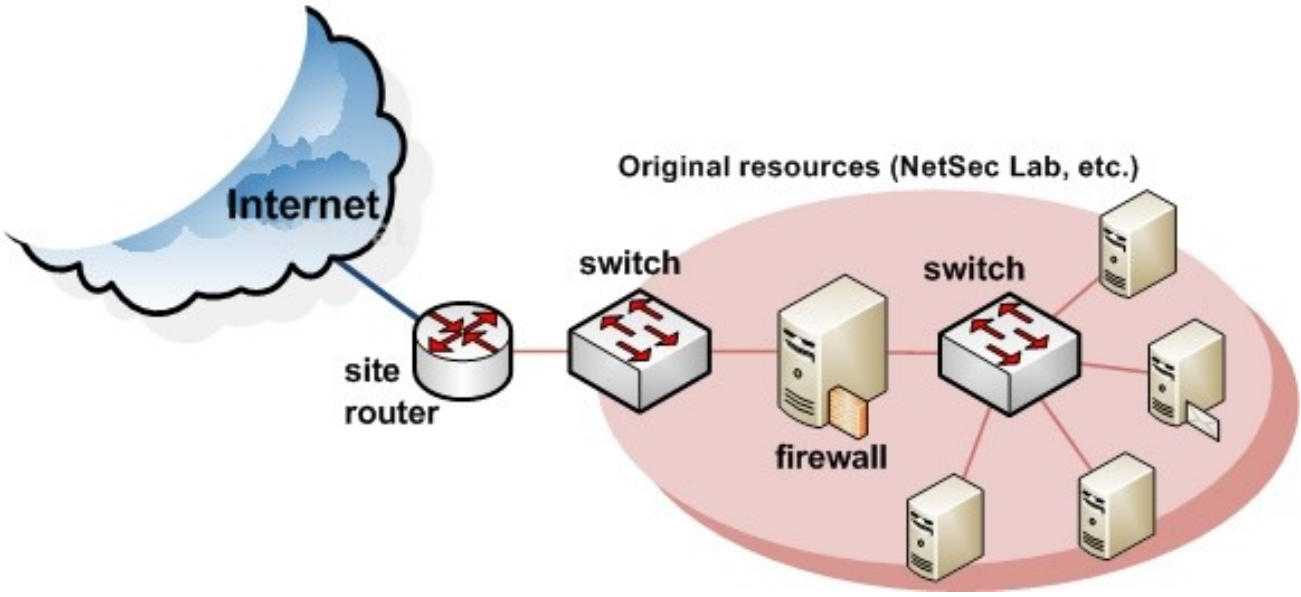


Figure 2: Example of site resources before joining CyberWATCH Underground.

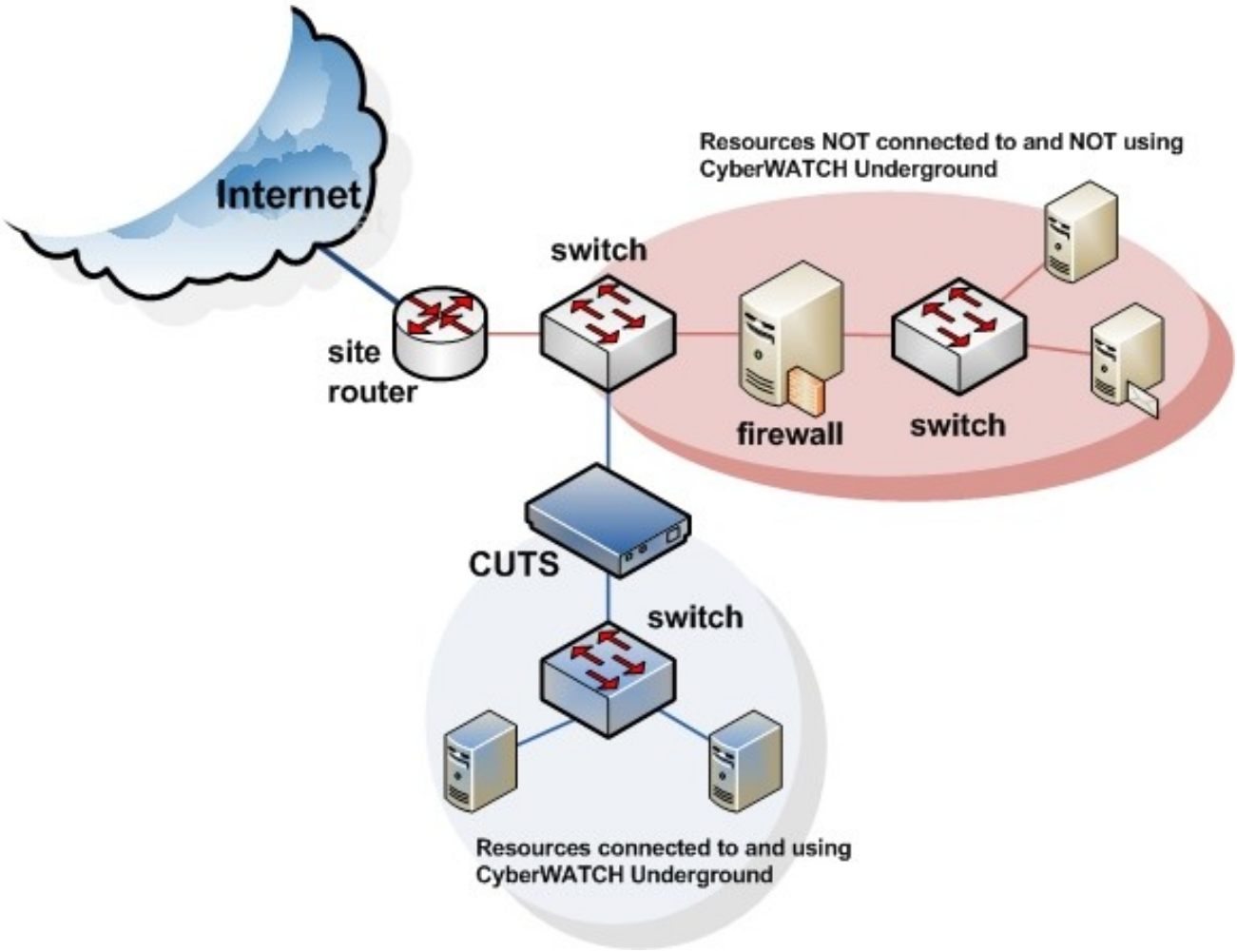


Figure 3: Example site resources after joining CyberWATCH Underground. Note that resources may be moved in and out of the CU at the discretion of local site personnel.

Services Provided by the CyberWATCH Underground

1. Technical services related to the CU proper and its direct infrastructure, including technical consultation with local site staff (e.g, OIT) and technical planning
2. CUTS configuration, testing, deployment consultation, maintenance and troubleshooting
3. CU Network Health Monitoring
   Including, but not necessarily limited to :
   - CU Status (sites up/down)
   - CUTS status (up/down)
   - Inside + Outside Interface status (up/down),
   - Inside + Outside Interface bytes sent/received
   - CPU and Memory utilization (health monitor for encryption)
   - General hardware health (internal temperature, swap use, etc)
   - Verification of proper configuration
4. Reporting of Monitoring/Status
5. Maintenance of site contact list
6. Maintenance of policies and procedures

Services NOT Provided by the CyberWATCH Underground

The responsibility of the CU ends with the CUTS. The CU does not provide regular technical consultation on systems attached to the CUTS. That said, the personnel maintaining the CU will likely either be involved in collaboration on projects using ther CU or otherwise informally available at theoir own discretion.

The CyberWATCH Underground is a closed testbed network. As such, it does NOT provide service to public networks, such as the Internet. This policy is meant to prevent sites from circumventing their local site's AUP by routing their Internet traffic through a another site whose AUP may be less restrictive. More importantly, it is meant to reduce the amount of network traffic over the CU that is not directly related to CyberWATCH cooperative activities.

Policies and Procedures

This document contains an early proposal for the CyberWATCH Underground. All policies and procedures are, at this point, suggestions. Since the CU is a cooperative endeavor, its members will develop and approve policies and procedures.

Becoming a CyberWATCH Underground Site

To become a participating member in the CU, a site must designate one point of contact, who will then apply to the CU. This person will hold responsibility for communicating local site concerns and question for reporting information back to others at the local site. In practice, we expect that the local point of contact will be the sole (faculty or staff) person making use of the CU.

Although signature of a CU MoU by a representative of the site's administration is not a precondition of joining the CU, we very strongly recommend doing so. Signing on in this way demonstrates interest of the site's administration and helps smooth over potential problems at the local site related to installation of the CUTS and substantial, active participation in CU.

Current Status
The technologies comprising the CU are well established. We have previously made tests to other sites (CCBC and HCC), demonstrating feasibility. The next steps are to create the CU as formal part of CyberWATCH, enlist sites for participation and execute the implementation plan below.

Steps to Implementation
A sample implementation plan is attached in Appendix A. Example steps are
General

- Select a common hardware platform
- Purchase hardware
- Create a standard software image
- Develop test plans for pre-shipment and post-installation of CUTS
- Develop MoU template
- Write documentation
  - Template for local site documentation (customized with local site info)
  - Policies and procedures for CU
- Create monitoring server
- Create web site for monitoring

Site specific

- Admit new site to the CU
  - Identify a local point of contact (LpoC)
  - Sign MoU
  - Gather local network information from LPoC
- Install and configure a CUTS
  - Install standard software image on hardware
  - Customize software for local site (IP addresses, tunnel method)
  - Perform pre-shipment test of CUTS
- Ship CUTS
  - Install CUTS at local site
  - Perform post-installation test of CUTS
  - Certify CUTS
- Add certified CUTS to monitoring pool

Appendix A: Sample Project Plan Work Breakdown Schedule

CyberWATCH Underground

Company: CyberWATCH
Manager: Mark Matties
Start: November 17, 2008
Finish: December 16, 2008
Report Date: November 17, 2008

Gantt Chart

WBS	Name	Work	Week 48, 2008							Week 49, 2008							W	
			17	18	19	20	21	22	23	24	25	26	27	28	29	30	1	2
1	**General tasks**	**45d**																
1.1	Select common hardware platform	3d																
1.2	Purchase hardware	4d																
1.3	Create standard software image	3d																
1.4	**Develop test plans**	**10d**																
1.4.1	Pre-shipment burn-in test	5d																
1.4.2	Post-installation test	5d																
1.5	Develop MoU template	5d																
1.6	**Write documentation**	**20d**																
1.6.1	Local site documentation template	10d																
1.6.2	CU policies and procedures	10d																
2	Create monitoring server	5d																
3	Create web site for monitoring	3d																
4	**Site Specific Tasks**	**15d**																
4.1	**Admit New Site to CU**	**8d**																
4.1.1	Identify local point of contact (LPoC)	2d																
4.1.2	Execute Memorandum of Understanding	5d																
4.1.3	Gather localnetwork information from LPoC	1d																
4.2	**Install and configure CUTS**	**7d**																
4.2.1	Procure hardware	1d																
4.2.2	Install standard software image	1d																
4.2.3	Customize software for local site (IP addresses, tunnel method)	1d																
4.2.4	Perform pre-shipment burn-in test of CUTS	4d																
5	Ship CUTS	1d																
6	**Local installation of CUTS**	**4d**																
6.1	Install CUTS at local site	1d																
6.2	Perform post-installation test of CUTS	2d																
6.3	Certify CUTS	1d																
7	Add certified CUTS to monitoring pool	1d																
8	Certify site to send / receive traffic over CU																	