BNSS Final Report

Martin Borek, Joel Gartner, Miguel Gordo, Yashu Sharma
Group V

March 21, 2016

1 Introduction

This document presents the analysis of ACME requirements as well as a brief design for a solution to the Building Networked Systems Security course project(EP2520). The document is divided in two sections: a section with a list of identified project requirements, and a final section that presents our solution design to address all identified requirements.

2 Project Requirements

Derived from the ACME project description, the following requirements have been identified:

- Corporate laptops and Mobile devices should be able to access the Stockholm's office web server from the London Office.
- Stockholm's web server should be accessible only to employees, both from computers at home and from corporate laptop from within the offices.
- When using a personal laptop from home, a two factor authentication scheme must be utilized with the corporate mobile devices in order to provide access to the network.
- Mobile devices should be able to transfer files between them, both when they're in the same network and also when one is located in the Stockholm and the other in London. The exchange must be authenticated, confidential and must preserve integrity.
- No host can connect to the corporate network if the address is not from either the London Office or the Stockholm office.
- Traffic between the two offices should be hidden from third parties.

- Network traffic must be logged, as well as access to Stockholm's web server.
- Stockholm office will be protected with an IDS that will log traffic and generate alerts.

3 Solution

In this section we will propose a design solution for ACME. We will address each requirement separately. Below you can find a network diagram with our proposed solution.

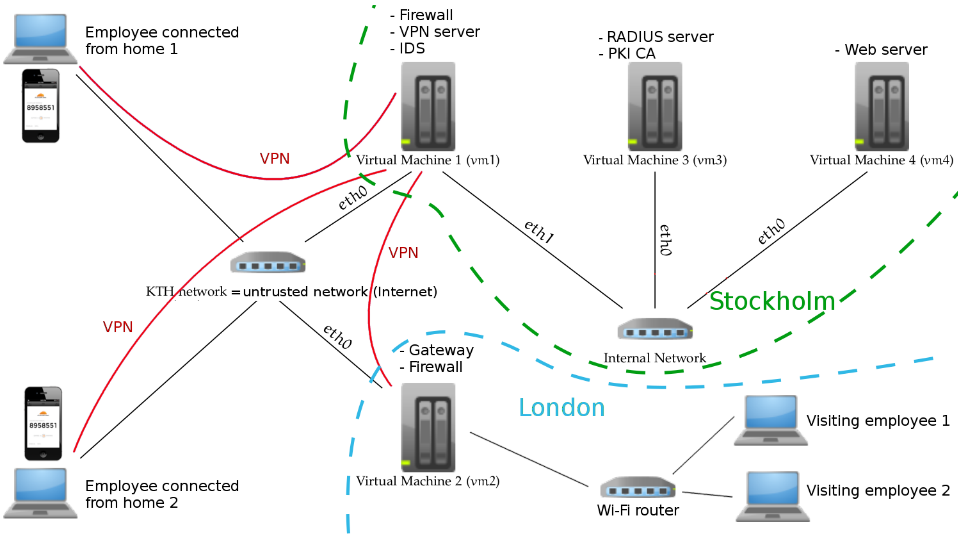

Figure 1: Network topology for the ACME Project

The topology is divided into three parts; the Stockholm network, the London network and the public (untrusted) network. The Stockholm network represents the headquarters, thus, most services are located there. All the Stockholm network is secured by a gateway (Virtual Machine 1) containing a Firewall and an Intrusion Detection System. Also, the VPN server is located there and all traffic directed to the inner network is secured by VPN. The Virtual Machine 3 is used as a RADIUS server and as a PKI CA server. The RADIUS server is used for authorizing visiting employees in London when connecting to the Wi-Fi and also for authorizing employees when connecting to the VPN from home. The last server in the Stockholm network, Virtual Machine 4, is designated the secured Web server. The London office consists of a gateway (Virtual Machine 2) that provides secure connection to the Stockholm network via VPN. It also includes a Firewall. Visiting employees connect to the network via a Wi-Fi router that is directly connected to the Virtual Machine 2. Employees connected from home are required to use a two factor authentication. This authentication is used for establishing a VPN connection to the Stockholm network (Virtual Machine 1).

- Authentication: We are using public key infrastructure model to authenticate the employees. The tools to enable this are digital certificates and public key cryptography. A digital certificate is given to all employees. By presenting their certificate in authentication steps it is ensured that only employees with valid certificates will be able to access the web server. Certificates are signed by the CA's private key. PKI CA is built in VM3. The software we are using is CFSSL, CloudFlare's open source PKI toolkit.

  Our system of trust is based on a PKI using internally-hosted CA. Firstly, a certificate and private key are generated for CA. To generate a certificate, a json input file containing the information about the subject organization is created and passed to genkey command which creates the private key in pem format and Certificate Signing Request (CSR). CSR is then presented to CA for signing. CA uses the sign command to sign the CSR and outputs the signed certificate in pem format. For signing, CA takes its configuration file and database configuration file in json format as input. The configuration file provides the policy for a certificate (e.g. validity period, key usages). We also added an authentication key to this signing policy. This authentication key should be kept private. The API key is a basic authentication mechanism that prevents unauthorized parties from requesting certificates. The DB config file contains the information about connection to the database. An entry is added to Certificates table once CA signs a certificate. For revoking a certificate, revoke command is used. Using OCSPrefresh command, entries are added to OCSPResponse table that shows status of certificates; good or revoked.

- Secure Wireless Access: In order to connect to the corporate network via Wi-Fi from the London Office, a FreeRADIUS server will be installed in VM3. In this way, wireless access with mobile devices and laptops will be authenticated, ensuring only ACME employees can access the network. Wireless router at the London Office will be tasked to communicate with the RADIUS server. Additionally, if time allows, we will set up a backup FreeRADIUS server so that in case the VPN tunnel between London and Stockholm is broken both offices can still authenticate and use the wireless network.

- VPN: VPN is used in this design to provide the confidentiality, the integrity and the authenticity when connecting to the Stockholm network from outside of the internal network. The VPN server and the gateway are located in the VM1. VPN client is running at the VM2 that represents the gateway in the London office. This VPN client is connected to the VPN server in VM1. Thus, it establishes a secure tunnel between the Stockholm and the London offices. All traffic between these offices goes through this VPN tunnel. The VPN server is used also for employees that want to connect to the Stockholm network from home. An IP address assigned to a VPN client belongs to the Stockholm office range. As a result, the private laptop is granted access to the corporate network.

VPN in this design is provided by the OpenVPN that uses the SSL/TLS. The authentication is done by the RADIUS server that is used also for authenticating users when connecting to the Wi-Fi in the London network. To establish a connection from home, two factor authentication needs to be used. This is described in the bullet point below.

For the final solution, VM2 has been substituted by a personal laptop that achieves the same functionality. This decision was taken because of the difficulties that arose from trying to set up the communication between the London router and VM2, since KTHOpen is in between, whereas in our diagram a direct connection is assumed. Since the solution to this problem involved changing the router's firmware with little spare time left, we chose using a personal laptop instead, and from it we set up a VPN tunnel to VM1.

- Two factor authentication: In order to reduce the risk of intrusion, two factor authentication is required when connecting from home. This means that an employee can securely connect to the Stockholm network only if he/she is in possession of a mobile device with pre-installed application that generates authentication tokens together with authenticating to the RADIUS server by username and password. Upon successful authentication a secure VPN connection with the Stockholm network is established. The two factor authentication is achieved by Google Authenticator that is used together with the OpenVPN.

- File sharing: In order for the mobile devices to share files between each other, the certificates are used. The devices use these to establish a TLS connection between each other which can be used for the actual file sharing process which then will be confidential and preserve integrity. The implementation uses the java security with spongy castle distribution of the bouncy castle library as a security provider. The implementation also uses a server in order to enable the users to connect to each other without entering another users IP-address. The connection to this server is established with TLS and when doing the actual file transfer another TLS connection is established with the user who actually is supposed to receive the file.

- Firewall: In order to prevent connections to the corporate network from devices which don't have an address in any of the offices, an instance of IPTables is used. It is placed in VM1 and filters out all undesired traffic. All the Stockholm office is behind the firewall. In order to get access to the resources in this network from the outside, employees are required to use the VPN.
- Intrusion detection: Snort will be deployed in VM1 in Stockholm in order to detect possible network attacks on it, as well as log all traffic that goes in or out. This system will alert the administrator in case an anomaly is detected with the help of the installed web interface snorby.

A Changes after review

- Added specification for FreeRADIUS and IPTables as the RADIUS server and firewall program to be used, respectively.
- Added setting up of an intermediate FreeRadius server as the back up if main radius server is down as an additional requirement if time permits.
- Second factor explained in the 2-factor authentication.
- Explanation added to the VPN about IP addresses assigned to VPN clients.
- Peer-Review mentions that a personal laptop does not need to be able to have access to the internal network. However, according to the project specification, the main web server can be accessed by employees from their homes. For a higher security, the web server is located inside of the Stockholm network in our design. Therefore, the peer-review recommendation is not applicable.

B Tools and programs used in the project

- VPN: OpenVPN Access Server 2.0.24, Google Authenticator 4.44
- Firewalls: The version for the firewalls used is IPTables v1.4.12
- RADIUS: The RADIUS server used for the final set up is FreeRadius version 2.1.10. To run it up the command to be used is `sudo freeradius -X &`
- IDS : Snort version 2.9.2, barnyard2 version 2.1.14, snorby
- Router: The router has been set up in WPA2 Enterprise mode in order to support wireless authentication with independent user accounts.
- PKI: Public Key Infrastructure Certificate Authority is implemented using CFSSL software, CloudFlare's open source PKI toolkit. Go 1.4 is installed prior to the installation of CFSSL. SQLite3 is installed for the configuration database of CA.

C Configurations

C.1 VPN Access Server

- Mode: Layer 3

- Authentication: RADIUS
- Google Authenticator for employees connecting from home.
- All VPN clients have access to private subnet 192.168.0.0/24.
- VPN clients are allowed to communicate with each other.

C.2 PKI

- CA has a certificate with expiry set to 365 days; ocsp url set to VM3, port 8888; usages set to signing, key encipherment, server auth and client auth.
- Each server and employee has a certificate with following configuration: algorithm used for key generation: RSA, key size: 2048, issuer CA: ACME CA, expiry: 365 days.

D IP addresses

- VPN server and VPN client web server: 172.31.212.109
- London VPN client: 192.168.1.254
- Employees connected from home: 192.168.2.1-254
- London office users: 192.168.1.0/24
- Stockholm Office: 192.168.0.0/24
- Webserver in Stockholm Office: 192.168.0.4
- RADIUS server and CA: 192.168.0.3

E Additional Details

E.1 File Transfer

The file transfer application is working with the help of a server. This server is set to run at VM3 (IP 192.168.0.3). The purpose of this server is to allow the different users to connect to each other without knowing each others IP-addresses. This allows users to transfer files between each other without having another channel of communication with each other.

The security of the transfer is ensured by using TLS for all communication. This is done with client authentication enabled which makes it so that only clients with valid certificates will be able to access the server and thus perform the file transfer. The keys which are used for the TLS-communication are stored in bouncy castle key stores which are saved as "/sdcard/keystore.bks" on the phones. This keystore has to be secured with the password "password" as this is currently hard coded into the application. The user is identified by the first alias in this keystore which is not equal to "acme ca" and this alias is what will be shown to other users connecting to the server. The phones also need a copy of the CA:s public key, which is the trusted certificate they use to validate the server and any person which they perform file transfer with. This key has to be saved in another bouncy castle keystore as "/sdcard/trusted.bks" and be protected by password "password" as well.

The server also has to have a copy of the CA's public key as to validate that all clients which are connecting are approved by the company. The server also needs it's own private key to authenticate itself to the clients.

When a user chooses another user and a file to transfer to that person the other user first has to approve the transfer. When this is done the server sends a request to both users that they should connect to a specific port on the server. When both users have connected to this all traffic is forwarded between the users while passing the server. On this connection between the users which passes the server there will be a SSL-handshake and an TLS connection between the users will be established. This allows a secured connection to be established between the users with the server as a middle man. This connection is then used to transfer the actual file between the users.

E.2 Snort

Snort is set up and running on VM1. This is configured to output to a binary file which is then read by barnyard2 in order to read this binary file to a MySQL database. This database is then read by snorby which is used to give a web interface where all warnings can be shown. Installed is also pulled pork which can be used to download rules for what the system should detect. This has been used to download the community rules which are available without an API key, but no rules which require an API-key to download with PulledPork were installed.

E.3 Firewall

The firewall was configured to block all traffic which wasn't specifically allowed. As such the rules consisted of a list of allowed traffic. The traffic which was allowed was

- All traffic to VM3 from Stockholm or London office, for file exchange

- SSH traffic to all virtual machines, for remote configurations of machines
- Access to the web server on VM4 for all ACME network users
- Access to the snorby web interface on VM1 for all ACME network users
- All traffic which is part of an ESTABLISHED connection
- All traffic which is RELATED to an established connection
- VPN traffic to VM1 from any source