IMPACTS OF ENCRYPTION ON STREAMING VIDEO

A CAPSTONE PROJECT REPORT

VAIBHAV MISHRA

FACULTY OF SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTING SCIENCE AND DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

MASTER OF SCIENCE IN INTERNETWORKING

UNIVERSITY OF ALBERTA

2011

Abstract

The internet is growing rapidly and as a matter of fact, the number of devices connected to the internet are now more than the people on this planet. There is certainly an increase in the popularity of video-based communication in health, military and commercial sectors which may have some sensitive data that cannot be exposed to the vulnerable world of internet. Therefore VPN based security has become an integral part of the organizational network architecture.

Overhead is added to real time video by aggregation at a VPN concentrator, encryption at the concentrator, and decryption at the client. These steps result in extra bits being transmitted from the concentrator to the client, and extra delay in both the concentrator and client.

I have built a test network to measure the encryption latency and the additional network load introduced by VPN encryption on real-time video. This project report will provide you with the thorough explanation of test network architecture, methodology and measurements.

Acknowledgement

I would like to thank Dr. M. H. MacGregor for giving me an opportunity to work on a new platform and providing me with every possible resource to complete this project.

Table of Contents

1. Introduction

This project is an extension to the research paper reported by the National Research Council Canada in context of a broader project concerning the utilization of video applications within health care sector. Web-based video communication is increasingly becoming popular in health care, military and corporate sectors.

The health care sector has made it legally mandatory to deploy encryption for security and privacy of all patient-generated data and the patient information.

Internet Protocol Security (IPsec) based Virtual Private Network (VPN) can serve as a solution to the privacy and security requirements. It provides secure communication over internet by maintaining confidentiality, data integrity and Authentication.

The Quality of user Experience (QoE) may get affected due to the significant overhead introduced by the VPN based encryption on already delay-sensitive medium of video.

This project specifically reports on the affects of AES-256 encryption algorithm on streaming videos having different terms of proportion and quantities of frame types by a VPN concentrator.

I have created a testbed in the Master of Science in Internetworking lab at University of Alberta consisting of a VLC video server, client and a VPN concentrator that implements the AES-256 encryption algorithm. This testbed enabled me to look into the latency introduced at the concentrator and the additional traffic carried due to encryption.

2. Virtual Private Network (VPN)

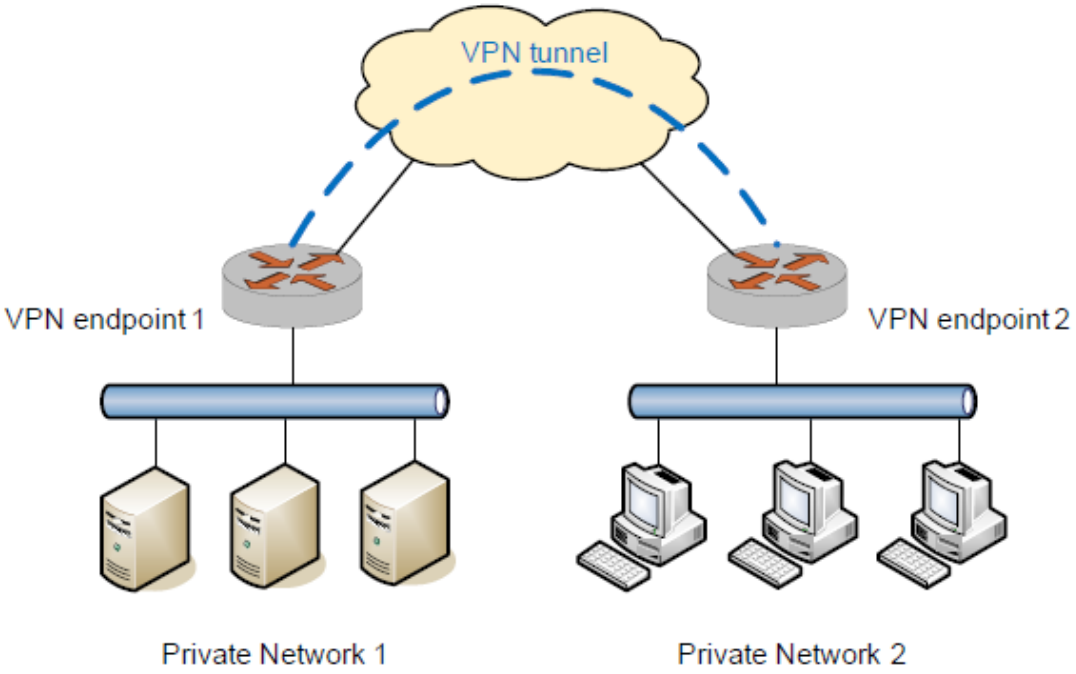
A VPN is a virtual network that uses existing physical networks as the internet, instead of leased lines to provide a secure communication media for data and IP information. This is often less expensive solution to facilitate secure data transfer between organizations or branch offices. Secure communication between remote telecommuters and the organization's server can also be offered by a VPN regardless of the telecommuter's location.

VPNs can use both symmetric and asymmetric forms of encryption. Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses separate keys for encryption and decryption. Asymmetric encryption is a very strong encryption algorithm but at the same time it is very inefficient for our router processor. A combination of asymmetric (Diffie Hellman Group 2) and symmetric encryption (AES-256) is used in this project to achieve efficient encryption and router performance.

2.1. Types of VPN

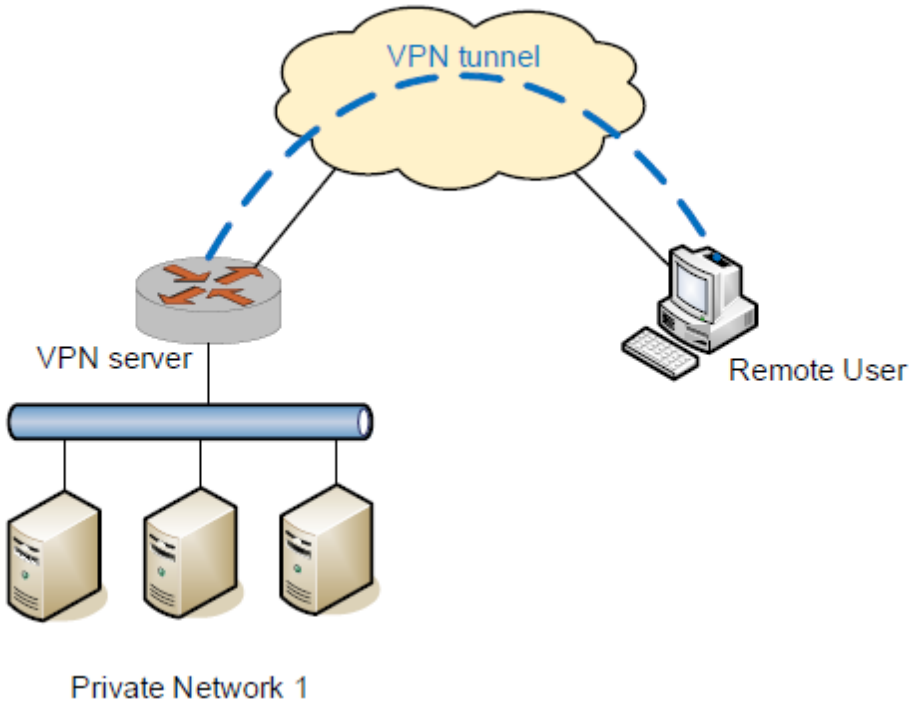
Site-to-site VPN

Site-to-site VPN allows you to connect two or more sites securely separated by the internet such that they appear to be on a single private network. One VPN endpoint is deployed on each site which establishes a secure virtual tunnel for data transfer. VPN endpoints are responsible for encapsulating and decapsulating the packets.



Remote access VPN

Remote access VPN connects a mobile remote user to the organization's server through a secure tunnel over internet. A dedicated VPN server is deployed at the organization to support secure remote users connections. Remote users on individual workstations perform tunnel peer function with the VPN server.



3. Internet Protocol Security (IPsec) Site-to Site VPN

IPsec is a protocol suite that allows us in protecting communications over IP networks by:

- **Authentication:** Authentication guarantees that the other side is who they say they are and not someone who is pretending as the source.
- **Data integrity:** Data integrity ensures correct transmission without modification or tempering. Hashing provides "checksum" for encrypted data which maintains data integrity.
- **Confidentiality:** Confidentiality using encryption ensures that the data which is being sent is not exposed on the public network.

There are three main components of IPsec architecture:

- The Authentication Header (AH) protocol
- The Encapsulating Security Payload (ESP) protocol
- The Internet Key Exchange (IKE) Protocol

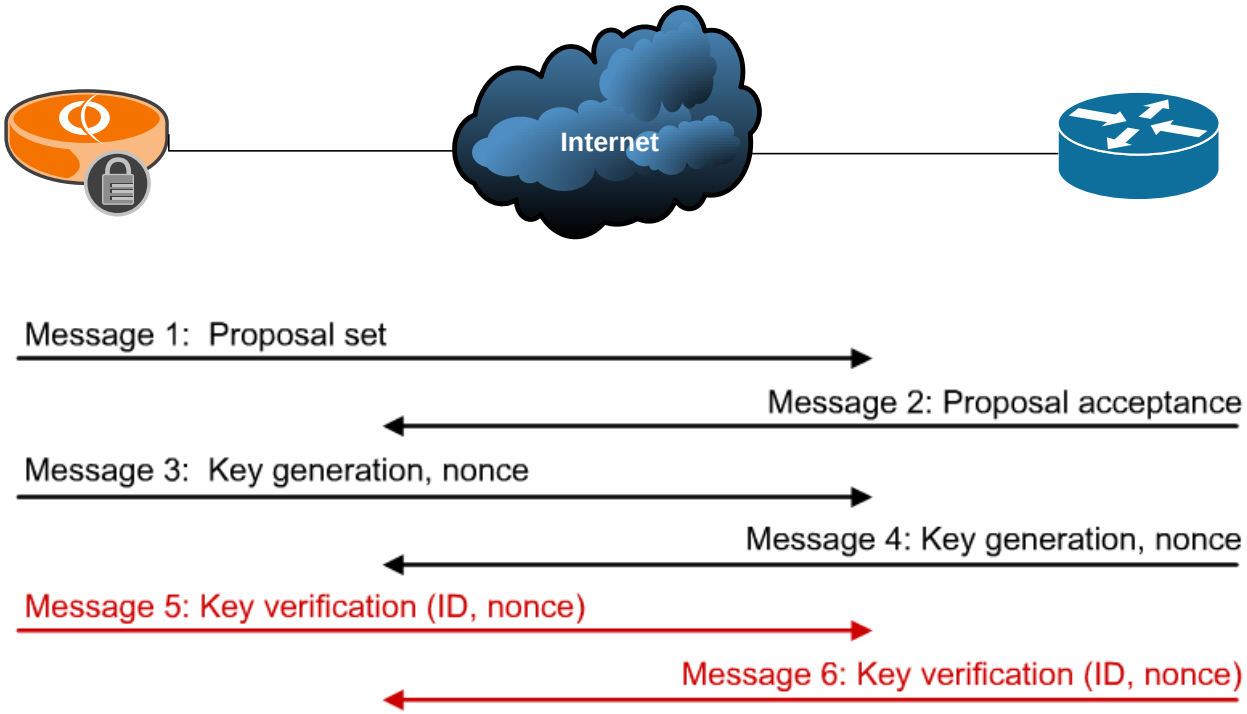
I have used ESP, which encrypts the data and protect it from being accessed or modified by unauthorized parties, and IKE, which provides a secure method for key exchange to negotiate, create, and manage security associations.

3.1. IPsec Phase 1 and Phase 2

IKE (Internet Key Exchange): It is a negotiation protocol of IPsec protocol suite which allows devices as they communicate across the world to negotiate on what policies they want to agree upon.

IKE Phase 1: It establishes an ISAKMP Security Association to provide secure encrypted connection between two tunnel peers. Its purpose is to verify tunnel peer identity and negotiate encryption to establish an encrypted connection for Phase 2 exchanges.
To establish an ISAKMP Security Association, the two peers must comply with all of the following:

- The encryption algorithm
- Key exchange: Diffie Hellman
- Authentication Method
- Hashing
- The authentication material



When a peer begins tunnel negotiation it sends a message that contains a proposal of encryption and authentication method that it can support. If one of the proposals matches at the peer, it responds with the proposal acceptance message.

Message 3 and Message 4 are Diffie-Hellman's key exchange (asymmetric encryption). If this key exchange is successful it establishes a secure foundation for each peer to calculate the symmetric keys.

The nonce value is a random number that a peer uses to verify the calculated keys in Message 5 and 6. In these messages the peer encrypts their ID and nonce value using the calculated symmetric keys. Each peer then decrypts and compares the received data with what it has stored to verify that the keys were computed correctly. These messages are encrypted which is represented by the red color.

IKE Phase 2: IKE Phase 2 is used to negotiate security association for data exchange. Security Associations specifies which encryption keys and authentication methods to use for specific source/destination address pairs. This is where we generate second set of symmetric encryption keys. These will be the keys that will be used for the tunnel itself that is why IKE Phase 2 is also called IPsec negotiation.

Message 1: Proposal set, proxy ID, SPI for →, (key gen)

Message 2: Proposal acceptance, SPI for ←, (keygen)

Message 3: Acknowledgement

After the completion of Phase 1, the peers have a secured connection and can begin Phase 2 negotiations.

The tunnel initiator sends a message containing with Phase 2 proposals it can run, the proxy ID which defines the source and destination subnets being tunneled and the Security Parameter Index to use for this direction of traffic. The responder replies with the proposal that is accepted and the security association for traffic in this direction.

The third message is simply an acknowledgement for the proper exchange of information and the two tunnel peers can now forward end-user data.

Encryption Algorithms: The encryption algorithms are used to scramble the data before sending it across the internet then descrambling it on the receiving device.

- Data Encryption Standard (DES): It was created by IBM in 1977. Now a days it is considered insecure because it can be broken with modern computer equipments in a reasonable amount of time. It uses a 56 bit key.
- 3DES: It uses three DES keys on top of each other to create a single 168 bit key.
- Advanced Encryption Standard (AES): AES is a newer and more efficient algorithm. It is a single key algorithm which operates on 128-, 192-, and 256-bit key.

Key Exchange- Diffie Hellman Groups: It is used to allow secure transfer of symmetric keys (and help generate symmetric keys). It uses 768- (Group 1), 1024- (Group 2), 1536- (Group 5) and up to 8192 bits for encryption.

Authentication Method: Pre-shared key, or pre-shared secret is used to generate a hash such that each VPN endpoint can authenticate the other. It is configured on both tunnel peers, which is supposed to be identical.

Hashing: It ensures correct data transmission.

- MD5 - 128 bit HASH
- SHA1 – 160 bit HASH

4. Virtual Routing and Forwarding (VRF)

Network routers include an IP technology called VRF which allows multiple instances of a routing table to exist on the same router and work simultaneously. It segments network paths without using multiple devices which eventually increases router functionality. Network Security is also alleviated because the traffic is automatically segregated.

VRF acts like a logical router which is totally independent from any other router in the same physical box and has its own:

- Interfaces and IP subnets
- Routing Protocols
- Routing and Forwarding Table

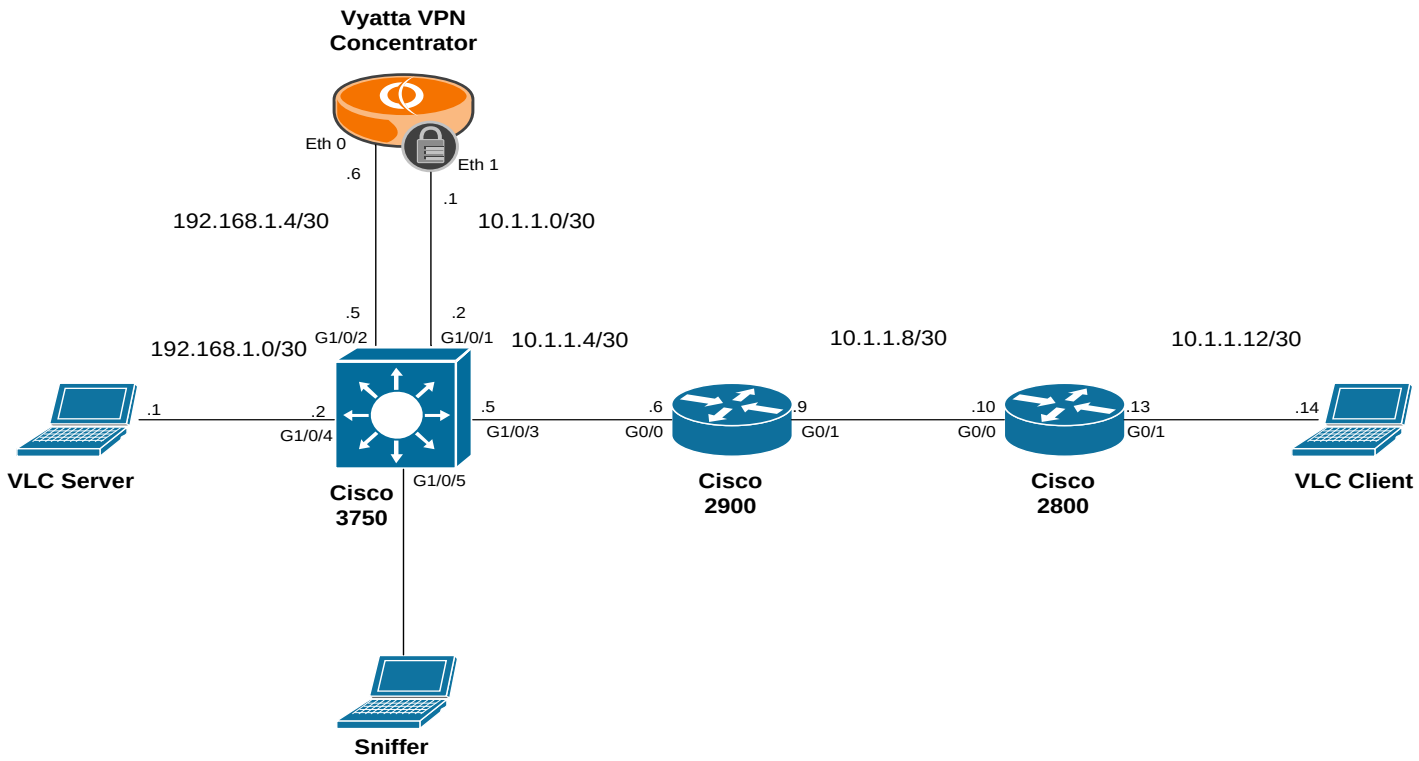
5. Methodology

I have created different test scenarios to find out the possible factors that may affect latency and transmission overhead. My testing is based on the following scenarios:

- VLC server and client, unencrypted video.
- VLC server and client, encrypted video.
- IPsec encryption at the concentrator.

5.1. Testbed Architecture

This testbed is designed to measure the encryption latency and the additional network load introduced by VPN concentrator (encryption) on streaming video.



The testbed consists of the following network elements:

- VLC is used for the server and client sides of the testbed.
- A layer 3 network switch using Virtual Routing and Forwarding (Cisco 3750).
- Cisco 2900 router.
- Cisco 2800 router.
- Open source Vyatta VPN concentrator (installed on SunFire V20Z blade server) which establishes Site-to-site VPN with Cisco 2800 router.
- Wireshark packet analyzer is used to capture packets, running on a computer attached to a mirror port on the switch.

Policies in use

IKE Phase 1 negotiation criteria:

- Encryption algorithm: AES-256 (Health care standard)
- Hashing: SHA-1 (Md5 proven to be insecure)
- Authentication: pre-shared
- Key exchange: Diffie-Hellman Group 2
- Lifetime: 86,400 seconds

IPSec (IKE Phase 2) negotiation criteria:

- Encryption algorithm: esp-aes 256
- Authentication: esp-sha-hmac

Tunnel Parameter:

- Pre-shared key: letmein

5.2. Experimental Data

Video-clips of three different types were used as they differ significantly from the others in terms of quantities and proportion of frame types.

- an interview video,
- an entertainment video, and
- a sport video.

5.3. Measurement Method

Experiment session consisted of streaming each video type – interview, soccer, and entertainment from the VLC video server to VLC client for each testbed:

- Without Encryption
- With Encryption

5.3.1. Encryption Latency Measurement

I have compared the time difference between the frame sent out to the concentrator (G 1/0/2) and the frame received from the concentrator (G1/0/1) for each testbed (with and without encryption).

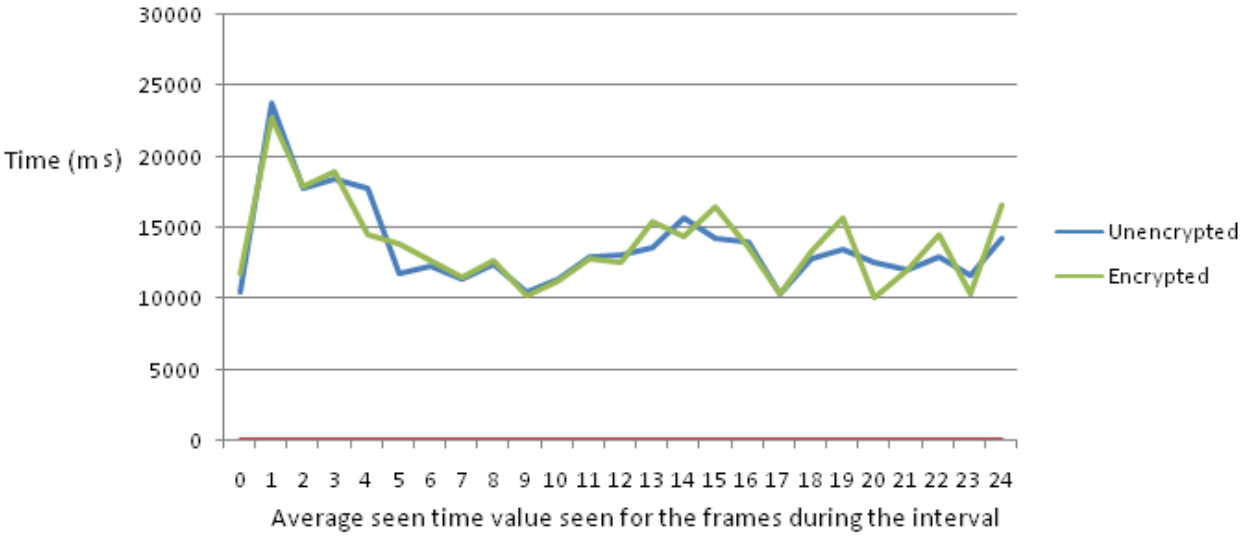
A wireshark filter is used to measure the time difference between the inbound and outbound frame: frame.time_delta_displayed

5.3.2. Additional Traffic Calculation

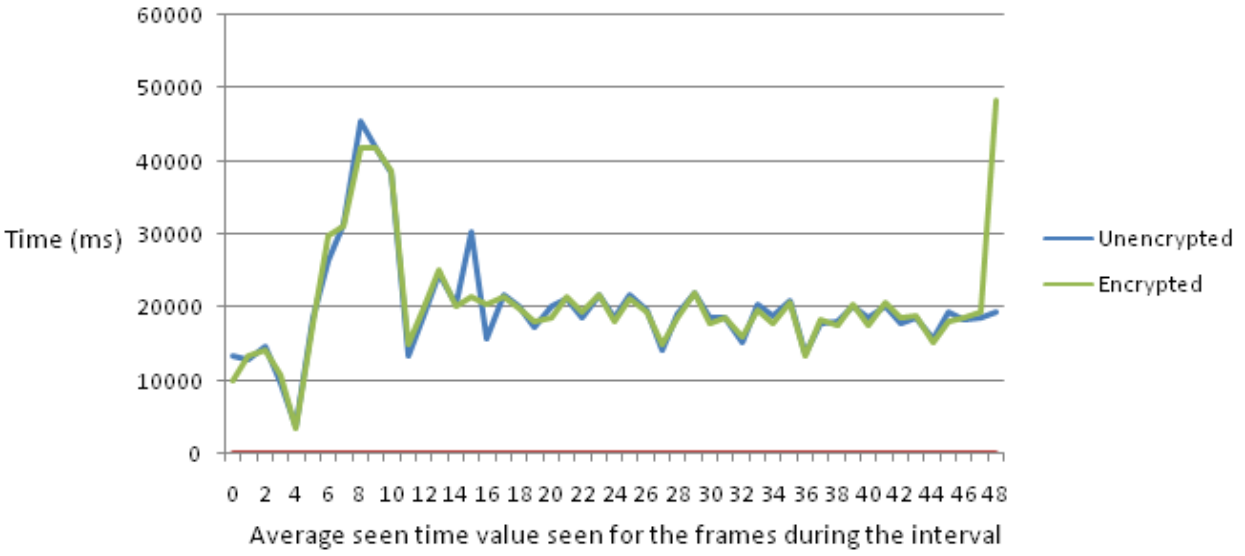
It is calculated by looking into the frame length before encryption and after encryption. Additional overhead is introduced in the form of bytes to the frame after encryption.

6. Results

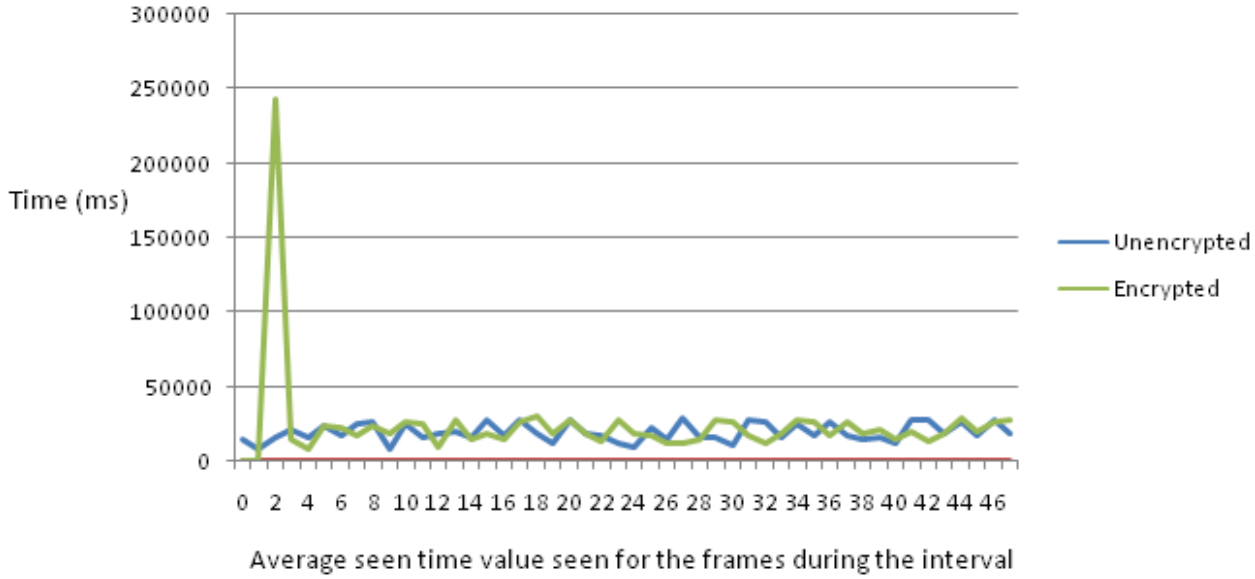
The following figures compares the propagation time for encrypted and unencrypted videos in the VPN concentrator. It shows the results for all three different types of videos.



Entertainment Video



Interview Video



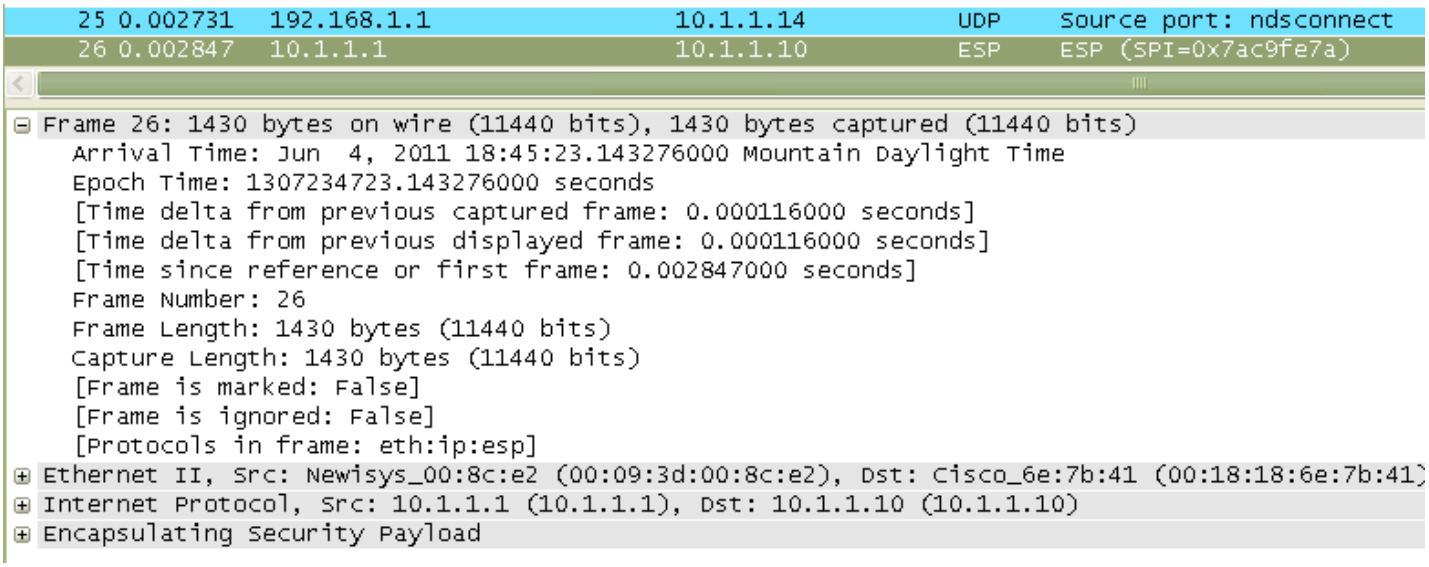
Soccer Video

Additional Network Load Calculation

```
    25 0.002731   192.168.1.1                10.1.1.14                  UDP    Source port: ndsconnect
    26 0.002847   10.1.1.1                   10.1.1.10                  ESP    ESP (SPI=0x7ac9fe7a)

Frame 25: 1370 bytes on wire (10960 bits), 1370 bytes captured (10960 bits)
    Arrival Time: Jun  4, 2011 18:45:23.143160000 Mountain Daylight Time
    Epoch Time: 1307234723.143160000 seconds
    [Time delta from previous captured frame: 0.000112000 seconds]
    [Time delta from previous displayed frame: 0.000112000 seconds]
    [Time since reference or first frame: 0.002731000 seconds]
    Frame Number: 25
    Frame Length: 1370 bytes (10960 bits)
    Capture Length: 1370 bytes (10960 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: Cisco_6e:7b:42 (00:18:18:6e:7b:42), Dst: Newisys_00:8c:e1 (00:09:3d:00:8c:e1)
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 10.1.1.14 (10.1.1.14)
User Datagram Protocol, Src Port: ndsconnect (3890), Dst Port: avt-profile-1 (5004)
```

Frame size before encryption: 1370 bytes



Frame size after encryption: 1430 bytes

Overhead introduced:

1430 bytes (after encryption) – 1370 bytes (before encryption) = 60 bytes per frame

7. Configurations

Vyatta Device

Configuration mode:
set interfaces ethernet eth0 address 192.168.1.6/29
set interfaces ethernet eth0 address 10.1.1.1/29
!
set protocols static route 192.168.1.0/30 next-hop 192.168.1.5
set protocols static route 10.1.1.4/30 next-hop 10.1.1.2
set protocols static route 10.1.1.8/30 next-hop 10.1.1.2
set protocols static route 10.1.1.12/30 next-hop 10.1.1.2
!
commit
save

```
!
set vpn ipsec ipsec-interfaces interface eth1
edit vpn ipsec ike-group IKE1
set lifetime 86400
edit proposal 1
set encryption aes256
set hash sha1
set dh-group 2
top
!
edit vpn ipsec esp-group IKE2
set lifetime 86400
 edit proposal 1
set encryption aes256
set hash sha1
top
!
edit vpn ipsec site-to-site peer 10.1.1.10
set authentication pre-shared-secret letmein
set ike-group IKE1
set local-ip 10.1.1.1
!
edit tunnel 1
set local-subnet 192.168.1.0/29
set remote-subnet 10.1.1.12/30
set esp-group IKE2
!
commit
save
```

Layer 3 Switch (Cisco 3750)

```
hostname Switch
!
ip routing
!
ip vrf LAN
!
```

```
ip vrf WAN
!
interface GigabitEthernet1/0/1
 no switchport
 ip vrf forwarding WAN
 ip address 10.1.1.2 255.255.255.252
!
interface GigabitEthernet1/0/2
 no switchport
 ip vrf forwarding LAN
 ip address 192.168.1.5 255.255.255.252
!
interface GigabitEthernet1/0/3
 no switchport
 ip vrf forwarding WAN
 ip address 10.1.1.5 255.255.255.252
!
interface GigabitEthernet1/0/4
 no switchport
 ip vrf forwarding LAN
 ip address 192.168.1.2 255.255.255.252
 no keepalive
!
interface GigabitEthernet1/0/5
 switchport mode access
!

ip classless
ip route vrf LAN 10.1.1.0 255.255.255.252 192.168.1.6
ip route vrf LAN 10.1.1.4 255.255.255.252 192.168.1.6
ip route vrf LAN 10.1.1.8 255.255.255.252 192.168.1.6
ip route vrf LAN 10.1.1.12 255.255.255.252 192.168.1.6
ip route vrf WAN 10.1.1.8 255.255.255.252 10.1.1.6
ip route vrf WAN 10.1.1.12 255.255.255.252 10.1.1.6
ip route vrf WAN 192.168.1.0 255.255.255.252 10.1.1.1
ip route vrf WAN 192.168.1.4 255.255.255.252 10.1.1.1
ip http server
!
monitor session 2 source interface Gi1/0/1 rx
monitor session 2 source interface Gi1/0/2 tx
monitor session 2 destination interface Gi1/0/5
```

Cisco 2900

```
hostname 2900
!
interface GigabitEthernet0/0
 ip address 10.1.1.6 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.1.1.9 255.255.255.252
 duplex auto
 speed auto
!
ip route 10.1.1.0 255.255.255.252 10.1.1.5
ip route 10.1.1.12 255.255.255.252 10.1.1.10
ip route 192.168.1.0 255.255.255.252 10.1.1.5
ip route 192.168.1.4 255.255.255.252 10.1.1.5
```

Cisco 2800

```
hostname 2800
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key letmein address 10.1.1.1
!
crypto ipsec transform-set NRC esp-aes 256 esp-sha-hmac
!
crypto map S2S-VPN 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set NRC
 match address S2S-VPN-TRAFFIC
!
interface GigabitEthernet0/0
 ip address 10.1.1.10 255.255.255.252
 duplex auto
 speed auto
 crypto map S2S-VPN
!
```

```
interface GigabitEthernet0/1
 ip address 10.1.1.13 255.255.255.252
 duplex auto
 speed auto
!
ip route 10.1.1.0 255.255.255.252 10.1.1.9
ip route 10.1.1.4 255.255.255.252 10.1.1.9
ip route 192.168.1.0 255.255.255.252 10.1.1.9
ip route 192.168.1.4 255.255.255.252 10.1.1.9
!
ip access-list extended S2S-VPN-TRAFFIC
permit ip 10.1.1.12 0.0.0.3 192.168.1.0 0.0.0.7
```

8. Conclusion

This project documented the efforts to characterize the impacts of encryption on streaming video.

This experimental approach was evaluated by measuring the encryption latency at Vyatta concentrator, and the additional network traffic introduced by encryption. It was observed that the packet transfer delay was significantly increased due to encryption as it traverses through the concentrator.

This project involves the new AES-256 encryption algorithm which is expected to be standardized by most of the health care organizations.

9. References

1. Characterizing the Impacts of VPN Security Models on Streaming Video
2. http://en.wikipedia.org/wiki/Virtual_private_network
3. www.cs.huji.ac.il/~sans/students_lectures/description-yoad.ppt
4. http://www.howstuffworks.com/vpn.htm
5. Vyatta_VPNRef_R6.2_v01
6. http://www.firstdigest.com/2009/08/cisco-the-basics-about-vrf-implementation/
7. http://en.wikipedia.org/wiki/VRF
8. http://en.wikipedia.org/wiki/IPsec
9. Vyatta VPN Overview (video tutorial)
10. Vyatta Site-to-site VPN using IPsec (video tutorial)