Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

Teaching IP Encryption and Decryption Using the OPNET Modeling and Simulation Tool

Jungwoo Ryoo, *Penn State Altoona* and Tae Hwan Oh, *Southern Methodist University*

Abstract – Combining theoretical instruction with meaningful hands-on exercises is often challenging due to the lack of resources such as laboratory facilities and equipment. To overcome this problem, the use of a simulation/virtualization technology such as the OPNET simulation tool can be considered. In this paper, we discuss how one can use the OPNET simulation tool to effectively teach IP encryption and decryption concepts such as ones found in IP Security (IPSec).

Index terms – encryption, decryption, IPSec, education, OPNET, simulation, and virtualization

I. Introduction

It is non-trivia to teach a sophisticated network security technology like IPSec to non-computer science majors in the first two years of their degree program. This statement is even truer for the institutions that do not currently have network equipment readily available for student hands-on exercises. Therefore, instructors often focus on the theoretical aspect of the technology and do not cover all the technical details necessary for the students to apply their theoretical learning to real-life problems. An ideal situation would be having an opportunity to reinforce lessons in theories by providing full-blown lab sessions with access to adequate equipment for each student. This is, however, not the reality for a significant number of educators bearing the brunt of teaching security at the college level, and therefore students sometimes end up being deprived of opportunities to truly internalize what they learn.

We believe that this problem can be alleviated by introducing an alternative based on simulation and virtualization. The OPNET simulation tool [1,2,3,4,5] allows individual students to be exposed to a wide range of virtual network equipment (such as various types of hosts, switches, routers, etc.) with the fraction of cost required to purchase and maintain their real-life counterparts. For educational purposes, the virtual network components made available by the tool are sometimes even more effective than the physical devices they simulate since the tool can visualize certain logical networking abstractions that do not actually exist in networking hardware found in real life. For example, the Open Systems Interconnect (OSI) seven layer reference model or Transmission Control Protocol/Internet Protocol (TCP/IP) reference model is difficult for students to associate with a hardware unit like desktop or laptop computers. In the OPNET simulation tool students can easily see all the layers of the reference models and data flows including the addition and deletion of headers and trailers when a packet is moving through the different network layers made visible by double clicking on a picture icon representing a host.

Therefore, this paper shows how an instructor can use the OPNET simulation tool to effectively teach a particular network security technology such as IPSec and provides reasoning for why our approach makes sense.

II. IP Encryption and Decryption Concepts

A. IPSec

Packets sent over the Internet usually have no protection against malicious attempts to intercept them. Once intercepted, the confidentiality and integrity of the data within the packets may be compromised. Therefore, an unintended user can now read the data (breach of confidentiality) and change the data (breach of integrity) without the knowledge of the sender and the intended receiver of the data. In addition, one can no longer guarantee that the data received was sent by a claimed sender (i.e., the claimed sender can be repudiated).

IPSec is a technology developed to ensure the integrity, confidentiality, and non-repudiation of data sent over a public network such as the Internet [6]. Students often have difficulties in understanding the concept of IPSec because the technology is built on many existing networking technologies and has many complex facets of its own. For example, IPSec operates in the network layer of the TCP/IP reference model [7]. Additional headers and trailers are added to encapsulate either the data field of a packer or the entire packet. To understand the idea of encapsulating a packet or its data field, one must be knowledgeable about how each TCP/IP layer adds a

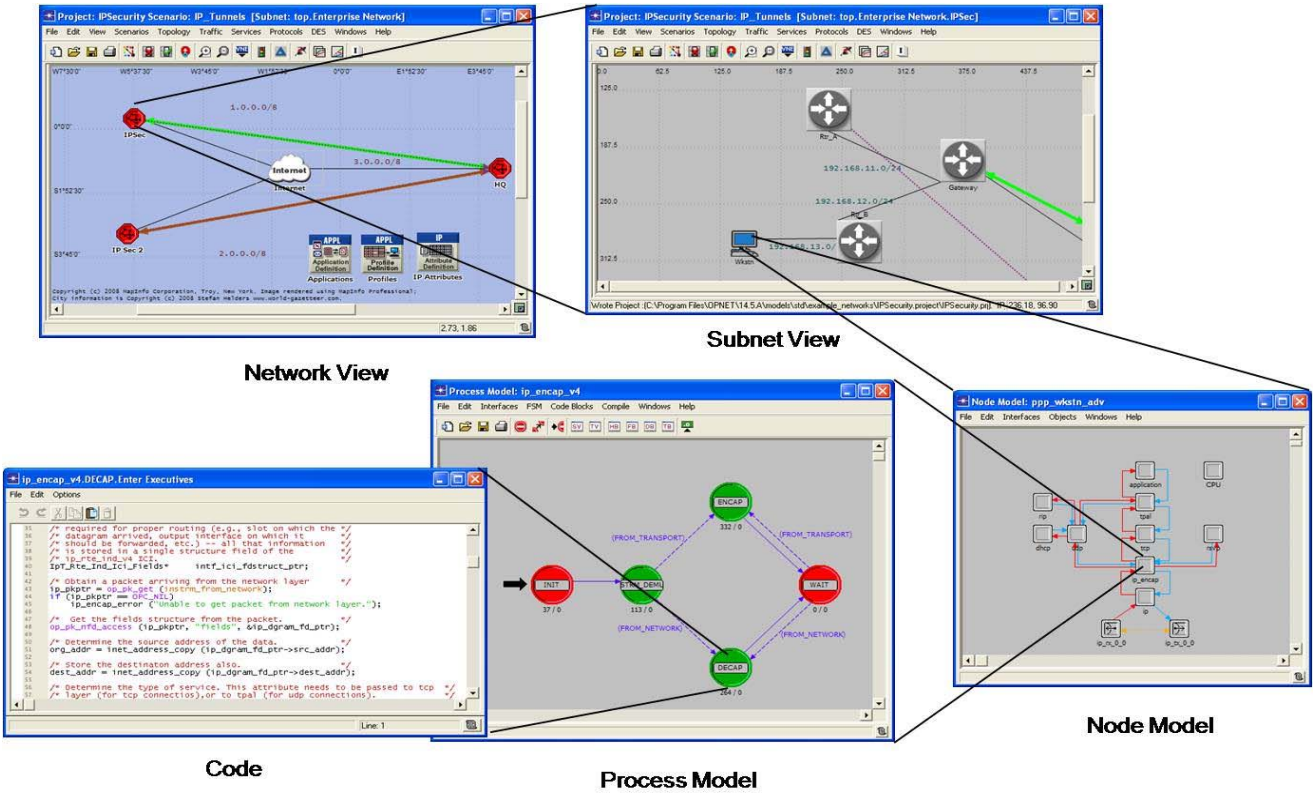
jryoo@psu.edu Information Sciences and Technology; taehwan@engr.smu.edu Department of Computer Science and Engineering

header and/or a trailer (also referred to as encapsulation) and how it removes them to retrieve the necessary data (also referred to as de-capsulation). Additionally, IPSec has different modes of operations such as transport and tunnel modes. The transport mode securely connects two individual hosts and requires VPN software to be installed on both of the hosts. The tunnel mode allows two gateways to be securely connected so that hosts behind each gateway can exchange messages without having to install the VPN software. There are also two different types of IPSec headers. One of them is called Encapsulating Security Payload (ESP), and the other is called Authentication Header (AH). ESP is the most common IPSec header type and ensures message-by-message authentication, integrity, and confidentiality. AH is a less rigorous form of header that only provides authentication and integrity check support. Whether using ESP or AH as its header and trailer, an IPSec mode (either transport or tunnel) needs to make a decision on what specific mechanisms it would use to implement ESP and AH between two hosts or gateways. This initialization step before an IPSec connection is established is referred to as Security Association (SA). To prevent any security compromises when SA is in progress, IPSec adopts the Internet Key Exchange Standard (IKE). The default key exchange algorithm used for IKE and SA is the Diffie-Hellman Key Agreement. DES-CBC is used during the actual data exchange process. The default message-by-message authentication and integrity check algorithm for IPSec is a hashing method called key-Hashed Message Authentication Codes (HMAC).

B. Learning Objectives

Based on the description of IPSec provided in the previous section, one can develop the following learning objectives. Students are expected to learn:

1. the core functionality of each layer in the TCP/IP reference model (particularly, in terms of encapsulation and de-capsulation using headers and trailers within or beyond a Local Area Network),
2. the two IPSec modes: transport and tunnel modes, and their differences,
3. what is involved in properly configuring hosts or gateways for the IPSec transport and tunnel modes,
4. the differences between two IPSec header/trailer types, ESP and AH,
5. the concept of SA, and
6. the major security protocols used in IPSec (including IKE, Diffie-Hellman, DES-CBC, and HMAC).



III. OPNET Simulation Tool

OPNET Modeler is a leading industry and academic solution for modeling and simulating communications networks, devices, and protocols with many features and flexibility. This tool uses an object-oriented modeling approach and provides simulated functionalities and graphical representations of real-life network components. By providing specialized editors, elaborate analysis tools, and off-the-shelf models, it allows highly sophisticated analyses of production networks for enhancing their performance. Because of its open design, new protocols and related approaches can easily be incorporated, simulated, and tested.

The *network editor* graphically represents the topology of a communications network that contains nodes and links between them. The *node editor* shows the internal architecture of each node by displaying the data flow between different functional network layers called modules. These modules perform different network functions within each node. A module can send or receive data to or from other modules. The *process editor* allows users to specify the behaviors of a module and uses finite state machines to describe its protocol details. Figure 1 shows different OPNET views provided by the network editor, the node editor, and the process editor.

IV. Use of the OPNET Simulation Tool for Accomplishing the IPSec Learning Objectives

A. The TCP/IP Reference Model

As shown in Figure 2, the node editor supported by OPNET shows all the TCP/IP layers. One or more rectangles in the node editor represent layers in the TCP/IP reference model. The editor is activated when a user double clicks on a node in the network editor. Before covering the IPSec topic, the students are asked to experiment with the node editor. Benefits of doing this is that students get familiar with the layer concept that is crucial for understanding IPSec in general. The first thing they usually observe is a pair of arrows going in and out of each node. The arrows in red indicate an incoming traffic. The box at the very bottom is a symbol used for the physical layer consisting of media (such as network interface cards or fiber optics cables) carrying electronic signals in their raw form. The boxes above the physical layer, labeled as MAC/ARP represent the data link layer. The transition from electronic signals to bits representing frames is visible by clicking on the red arrow going out of the MAC/ARP rectangle. Students can inspect all the details of the frame such as headers and trailers as shown in Figure 3. Considering that the idea of layers is a highly abstract concept, having access to tangible layers and traffics going through them greatly enhances students' learning especially by making them visible and manipulable. When students inspect the details (the red arrows) of data coming in and going out to the next layer (network layer, labeled as IP in the rectangle), they realize that the headers and trailers of the frames have now been removed, and an IP packet has been exposed. Through these exercises students can easily understand the de-capsulation concept (i.e., removing headers and trailers of a certain layer for processing in the next layer). Encapsulation can be explained in the same manner by tracing the blue arrows.

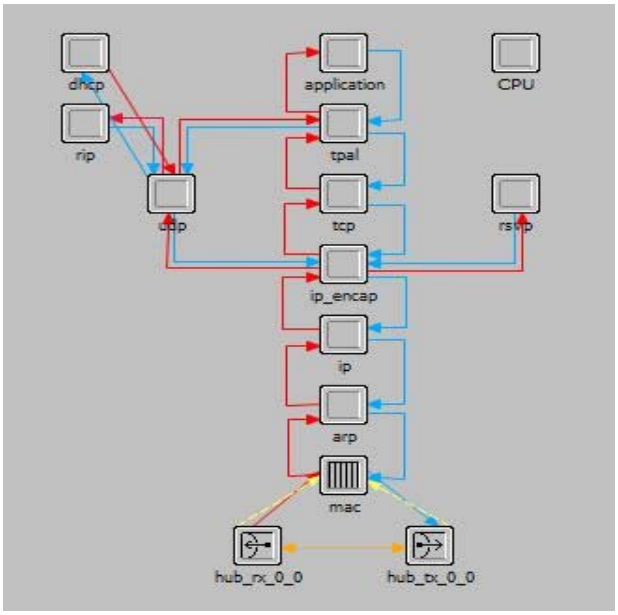
B. The IPSec Modes and Headers

As discussed in the previous section, the main differences in the two IPSec modes can be summarized as:

- The network topology: for the tunnel mode, the tunnel is created in between two gateways while a secure channel is created for any two communicating hosts for the transport mode.
- The difference between packet encapsulation and de-capsulation: in the transport mode, only the data part of each packet is encapsulated (as shown in Figure 3) exposing the plain IP header to a potential attack while in the tunnel mode, the entire IP packet is encapsulated by the IPSec headers and trailers.

These differences are clearly visible when students use the network editor and the node editor (see Figure 1).

Figure 2: The Node Editor



C. IPSec Configurations

After a brief introduction (a couple of introductory classes on OPNET), teams of students are asked to create their own VPNs using IPSec.

1. Step One: Creation of a Network Topology

Creating a network topology is the first task in this exercise. Students are given a concrete scenario that specifies the number of hosts involved, the types of hosts (desktop, laptop, PDA, etc.) and connections among them

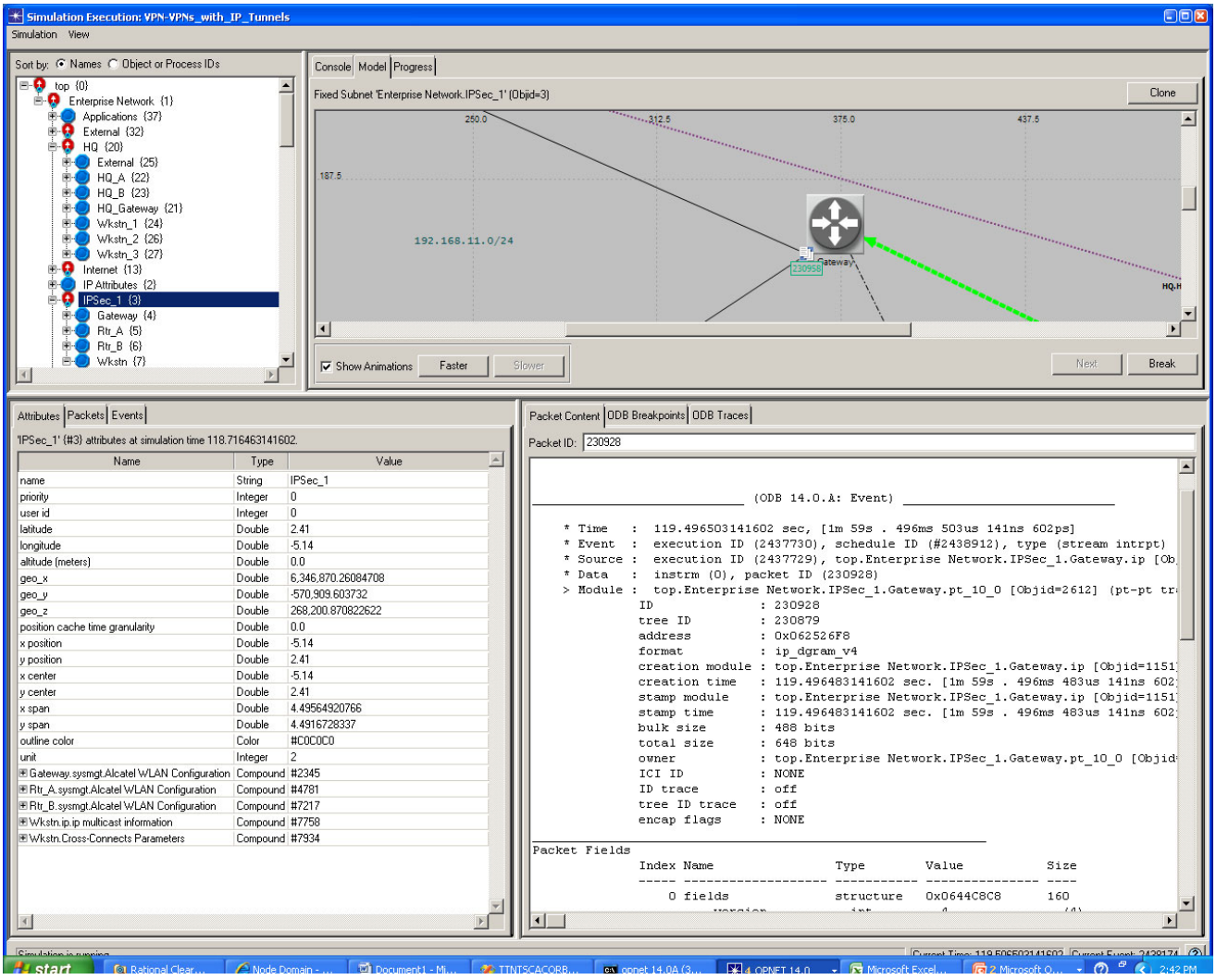
(wireless or wire-line), how the hosts are connected to each other, etc. They are then expected to implement their network topology using the network editor (Figure 1).

Figure 3: Frame Details View

2. Step Two: VPN Configuration

After the network topology is complete, this hands-on exercise asks the students to actually configure their own VPN. The VPN scenario given here is that of a tunnel mode. A number of VPN parameters need to be set in order for the VPN to function properly. Some of these parameters include:

- Tunnel Interface:Tunnel 0: This part of the configuration decides the interface of a gateway through which a VPN tunnel will be created and requires entries such as name, status (active or inactive), operational status (on or off), address (IP address of the gateway), and subnet mask.
- Tunnel Interface:Tunnel 0: Tunnel Information: This decides the destination IP of the tunnel.
- Tunnel Interface:Tunnel 0: Tunnel Mode: A number of tunnel options are available including



IPSec, IPv6, GRE, IP-IP, etc.

The above configurations need to be made on both gateways involved in the VPN.

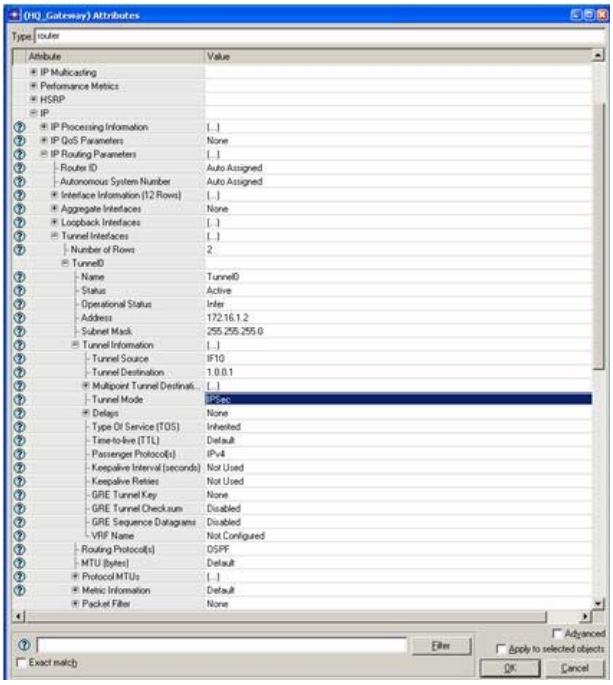
3. Step Three: Observation

After steps 1 and 2 are successfully finished, students are ready to run their simulation and observe interactions between the two VPN gateways as shown in Figures 3 and 4. Students can intercept a snapshot of the data stream and scrutinize it as shown in Figure 5. By using the packet content tab of the simulation execution view, one can view the effect of IPSec to the IP packet structure. Students can actually see IPSec headers and trailers added to the existing packet.

D. Security Association

In addition to the default IPSec options described in the previous section, it is possible to add additional features to the set of existing IPSec features provided OPNET. For example, the Security Association (SA) step that needs to be performed before an IPSec connection is established is not currently supported by the model provided by OPNET. One can however change the model using the process model editor since all the OPNET-provided models are open-source. Although requiring a significant level of expertise in OPNET and a programming language like C++, it is feasible for instructors to modify the existing model and change the code to make the IP stack of the gateways behave the way they want.

Figure 4: VPN Configuration View



E. IPSec Protocols

As in SA, additional security protocols can be added to the default OPNET model for IPSec.

V. Conclusion

This paper has presented an approach using the OPNET modeling tool in teaching students the concept of Encryption and Decryption through IPSec. The advantage of using OPNET over other non-interactive teaching methods relying heavily on diagrams and animations is that students are able to learn better by doing. In a hands-on-oriented setting, students can directly interact with virtual networking devices and instantly observe the consequences of their actions, which is not possible in the diagram or animation-centric approaches. Although proven effective in classroom settings, our approach is still evolving. For instance, we realize that the packet view of the OPNET simulation tool is insufficient to display all the details of the IPSec header/trailer-encapsulated packets. We augment this deficiency by providing a snapshot of real network traffic between two IPSec hosts/gateways captured by a sniffer tool. We are constantly looking for ways to improve the proposed approach by combining the simulation/virtualization technologies with real-life data.

VI. References

[1] OPNET "Understanding IP Model Internals and Interfaces," OPNETWORK 2007, Washington, DC, August 2007.

[2] OPNET "Planning and Analyzing IP Routing and Security in Enterprise Networks," OPNETWORK 2007, Washington, DC, August 2007.

[3] Mohan Krishna Ranganathan and Liam Kilmartin, "Investigations into the Impact of Security Protocols in Session Initiation Protocol (SIP)-based VoIP Networks," OPNETWORK 2001, Washington, DC, August 2002.

[4] Jinhua Guo, Weidong Xiang, and Shengquan Wang, "Reinforce Networking Theory with OPNET Simulation," Journal of Information Technology Education, pp. 215-226, Vol. 6, 2007.

[5] Nanjun Li, "Node-Oriented Modeling and Simulation of IP Networks," 14th Annual IEEE International

Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'07), pp. 123-132, 2007.

[6] Naganand Doraswamy and Dan Harkins, "IPSec: the New Security Standard for the Internet, Intranets, and Virtual Private Networks," Prentice Hall, 1999.

[7] Raymond Panko, "Business Data Networks and Telecommunications," Prentice Hall, 2007.

Figure 5: Capturing the IPSec Data Stream