INSIDE PRODUCTS
Thinking Inside the Box

Nalini Elkins

SSL and AT-TLS Implementation and Diagnostics (Web Based)

Are you implementing secure sockets for z/OS TCP/IP? What options are available? What is the difference between Secure Sockets Layer (SSL) and Application Transparent Transport Layer Security (AT-TLS)? What implementation pitfalls will you run into? Would you like to have some hands-on experience before you get started? Would you like to see trace packets using such protocols?

In class, we will start by demystifying the security and cryptography terminology: x-509 certificates, RSA, public key / private key encryption, and much more. Please see the class details for more topics.

Then, we will show a live demonstration of configuring a z/OS system with AT-TLS and SSL. This needs Policy Agent and the z/OS Network Configuration tool. We will also create our own certificates. We will bring up AT-TLS and SSL applications and as always trace many, many packets. We want to understand what a good SSL handshake looks like and a failing handshake. We will discuss the components of handshake timing? Then, we will take a look at packet decryption. How in the world can we do this? What are our options – what are the risks?

Nalini Elkins, an experienced TCP/IP network performance expert, with many years in network management and working with IBM, will teach you practical TCP/IP diagnostic skills. You will learn how to identify protocol and performance problems, whether originating from TCP/IP system setup, application problems or hardware failures.

Audience

This 1 day (two 4 hour sessions) web based course is designed for systems programmers who are responsible for troubleshooting, performance measurement, security, analysis, or tuning of their installation's TCP/IP network, socket applications and TCP/IP stack. You will leave class knowing how to implement and troubleshoot the TCP/IP security protocols. Most importantly, you will have an understanding of the protocols and how they interrelate to transport data. You can then find and eliminate potential trouble spots or problems in your own TCP/IP stack, network or socket applications.

INSIDE PRODUCTS
Thinking Inside the Box

Class Overview

This intensive seminar is designed to provide the attendee with an understanding of how to implement and troubleshoot security protocols and functions on z/OS such as SSL and AT-TLS. The seminar will provide live experience with configuration of policy agent, AT-TLS and SSL. You will learn how to analyze traces, profile and setup parameters for the security protocols. The strength of this course comes not only from theoretical information learned but from hands-on labs and exercises.

Prerequisite

A basic understanding of z/OS, TCP/IP, and networks is assumed. For best results, you may wish to take our Trace Reading and Diagnostics on z/OS course first. It will provide you with a clear understanding of the core Internet protocols and IPv4.

Seminar Dates and Location and Prices

For dates and locations and prices, please contact sales@insidethestack.com or call our office at 831-659-8360. Seminars are regularly offered in the USA, Europe, and Australia.

For More Information…

For more information on this or other seminars, including prices and locations, please contact:

Inside Products, Inc.
36-A Upper Circle
Carmel Valley CA 93924

Phone: 831-659-8360
Fax: 408-228-8019

Email: bill.jouris@insidethestack.com or
Email: training@insidethestack.com

Instructor: Nalini Elkins

Nalini Elkins, of Inside Products, Inc., (www.insidethestack.com), is a recognized leader in the field of computer performance measurement and analysis. In addition to being an experienced software product designer, developer, and planner, she is a formidable businesswoman. She has been the founder and co-founder of two start-ups in the high-tech arena.

During her career Nalini served in groups responsible for network performance design, analysis, troubleshooting, and systems programming. The classes Nalini produces and instructs, and the products she develops are designed with the needs of systems programmers as a key requirement. Nalini has an excellent understanding for the needs of system programmers because she was in their shoes for many years.

Nalini has also developed an expert system for diagnosing network hardware problems. The marketing rights for this product were sold to Boole & Babbage (which was later taken over by BMC). Nalini then joined Boole to further develop and support this product. After some time at Boole, Nalini joined some other Boole employees in co-founding a new company – Applied Expert Systems.

As Technical Co-founder, Nalini helped to design and develop a number of products in the SNA and TCP/IP network management area. These products included expert systems for SNA diagnostics, web performance diagnostics, TCP/IP routing diagnosis and TCP/IP network management. She was the Chief Developer of the product IBM first marketed as NetView Performance Monitor for TCP/IP.

Nalini now has her own company, **Inside Products, Inc.** (www.insidethestack.com), which designs, develops and markets TCP/IP network management software. The products are Inside the Stack TCP/IP monitor, TCP Problem Finder and TCP Response Time Monitor. Inside Products also provides consulting to resolve network problems such as FTP throughput, socket application performance and TCP/IP tuning. In fact, the Inside Products Network Health Check can be purchased via IBM. Please contact the IBM Network Traffic Analysis group at 1-800-876-8801. Of course, you may also contact Inside Products to purchase our consulting or Health Check services. Inside Products has international distributors in Australia, Germany, Switzerland, the United Kingdom, Belgium, Netherlands, Luxemburg and Brazil.

Nalini has published numerous articles in publications such as zJournal, Technical Support, Xephon's TCP/IP Update, and Enterprise Systems Journal. Nalini is also a regular speaker at SHARE, both national and regional Computer Measurement Groups (CMGs), and variety of international conferences.

Nalini can be contacted directly at Nalini_Elkins@Insidethestack.com

Seminar Outline

The following is a high level outline for this seminar. Since the seminar is constantly being updated, actual seminar content and flow may vary slightly from this outline.

Introduction to Cryptography

- DES, 3DES, AES,
- Asymmetric encryption / symmetric encryptionm
- Certificate authority
- Diffie-Hellman key exchange / groups
- Message authentication code (MAC)
- Message digest algorithm 5 (MD5)
- Rivest Shamir Adleman (RSA)
- Secure hash algorithm 1 (SHA1)
- Hashed message authentication codes (HMAC, HMAC MD5, HMAC_SHA)
- X.500 distinguished name
- X.509 digital certificate

SSL / AT-TLS Implementation

- Live demo: implementation of Policy Agent
- Live demo: implementation and use of z/OS Configuration Assistant
- Live demo: implementation of SSL on z/OS
- Live demo: implementation of AT-TLS on z/OS
- Live demo: RACF authorizations
- Live demo: Creation of certificates and storing in RACF

SSL / AT-TLS Diagnostics

- Secure Sockets Layer (SSL) / Transport Layer Security (TSL) protocols
- SSL handshake and performance implications
- SSL certificates
- Server and client authentication
- Sockets API for SSL
- Lab: Read traces with SSL / AT-TLS used
- How does SSL work with HTTP?