geekcruises.com®
EDUCATION THAT TAKES YOU PLACES

August 6 –13, 2005

A Seven-Night Alaskan Adventure

Security Surf™

You may select any combination of seminars so long as you do not select more than 3.5 day's worth of sessions. You may also freely move between the class rooms — even in mid-session!

The conference fee is $695 and includes all seminars and course materials.

Advanced Linux Security (half day)

Speaker: **Brian Hatch**

Description of how you can utilize advanced linux kernel patches such as LIDS, Grsecurity, Systrace, RSBAC, or SELinux to lock down your machine to the point that a root compromise is uneventful.

Dealing with Windows RPC (half day)

Speaker: **Eugene Schultz**

The Remote Procedure Call (RPC) protocol is used in a wide range of operating systems for host-to-host communication that supports distributed application environments. No matter what the operating system, RPC-based services have not exactly been known for their intrinsic security, but there are special security problems in the Windows implementation of RPC. This presentation delves into security-related issues in connection with Windows RPC—specifically how this service works, the particular components and associated calls, and the implications for security. There are many possible control measures that can reduce the dangers of this dangerous protocol, but every one leaves something to be desired. The last part of this presentation covers the cost versus benefit ratio of each potential control measure.

Security Solutions from IBM (half day)

Speaker: **Jeffrey Miller**

This talk will cover the range of IBM security products. We'll talk about IBM Tivoli Access Manager, IBM Tivoli Identity Manager, IBM Tivoli Privacy Manager, IBM Tivoli Risk Manager, among others, and discuss how they fit into an overall secure service oriented enterprise architecture that includes human access, application-to-application communication, and Web services.

Secure Linux Programming (quarter day)

Speaker: **Brian Hatch**

Avoiding vulnerabilities such as race conditions, symlink attacks, buffer overflows, and common methods of securely managing processes that have extra privileges with set*id, chroot, and the most common mistakes with coding for enhanced privileges processes. This would be a longer (and less dizzying) version of my "Linux: The Securable Operating System — every Linux security hook in 60 minutes or less."

Windows CIFS Security (half day)

Speaker: **Eugene Schultz**

The Server Message Block (SMB) protocol has been around for a long time now, but few people understand exactly how this protocol works and what its rather dismal implications for security are. SMB sessions involve a bizarre four-step handshake in which security can be bypassed by any reasonably proficient attacker. Additionally, SMB is vulnerable to a variety of denial of service (DoS) attacks. This presentation focuses on the various versions of Microsoft's SMB implementation, the Common Internet File System (CIFS), focusing on the SMB handshake, the format of the SMB portion of packets, the implications for security in Windows systems, and the many solutions that can be implemented.

Email, File, and Filesystem Encryption (quarter day)

Speaker: **Brian Hatch**

How to use GnuPG (GNU's PGP software). How PGP works, creating and managing private keys, using keyservers, verifying and signing other party's keys, encrypting and decrypting from the command line, integration with other tools (email clients such as Mutt, etc). Symmetric file encryption with GnuPG and/or OpenSSL. How to create and use Linux Cryptographic filesystems (including kernel recompilation if necessary) to provide automatic encryption of all data on a given filesystem.

Benchmarking Intrusion Detection Systems (IDSs) (half day)

Speaker: **Eugene Schultz**

How effective is a given intrusion detection system? In most people's minds, the question is settled on the basis of handwaving or religious arguments. Furthermore, vendors have resisted providing empirical data on the IDSs they sell, further clouding the issue. Although few organizations benchmark the IDSs they use, a number of "quick and dirty" benchmark methods that could provide some empirical data without requiring a considerable amount of resources can be used. Additionally, more thorough (and more valid) methods are available if the time and resources needed are available. This presentation covers methods for IDS benchmarking and the advantages and limitations associated with each.

Escape to the good life. Allow yourself to be pampered. Unwind. Have fun. Enrich your mind. And do it all aboard a luxurious cruise ship.

PRICING AND BOOKING INFORMATION

Course Fees: $695. Only passengers booked through Geek Cruises will be admitted.

Deposit: $400 per person, due at time of booking.

Cabin Type	Cruise Rate
Standard Inside	$ 999 (GS* available)
Better Inside	$1,199 (GS,* available)
Standard Outside	$1,399 (GS,* ♿ available)
Better Outside	$1,499 (GS,* ♿ available)
Outside w/verandah	$1,599 (GS,* ♿ available)
Mini Suites	$1,699 (♿ available)
Superior Suites	$2,199

3rd and/or 4th Person Rate: ages 2 and older, $499; under 2 years old, $399.

Single Occupancy: 150% for Inside and Outside cabins and 200% for Outside with Verandah and above.

Port Charges and Taxes: $262 per person (subject to minor change).

Full payment is due on May 1, 2005 (or, if you book after May 1, at the time of booking).

Foreign Booking Fees and Additional Payment Information: There is a foreign booking charge of $60 per foreign residence ($35 per Canadian residence). There is a $25 charge for returned checks.

Air Add-ons: Airfare from most major cities is available through the cruise line. You can call our office for this pricing. (These rates include transfers to/from the dock/airport.) In most cases, however, you will find better airfares on your own. Online travel sites such as Expedia.com or Travelzoo.com are excellent resources.

Pre- and Post-cruise Hotel Stays: Sightsee Seattle! The hotel will be close to the dock.

	1 Night	2 Nights	3 Nights
Shared Double	$150	$265	$360
Single Occupancy	$250	$455	$645
3rd Person	$90	$175	$250

(prices are per person)

♿ Physically challenged available

***Guaranteed Share (GS) Fares:** This plan is for passengers who are coming on a Geek Cruise by themselves and wish to share a cabin with another Geek Cruises passenger in an inside or outside cabin only. The prices are the same as the per person double occupancy rates. Share Passengers who smoke are not to do so in the cabin, unless okayed by fellow roommates. We try to match passengers with someone close in age, whenever possible. Note: Holland America will not accept any booking unless a fully completed Reservation Form is accompanied with a per-person deposit:

http://www.geekcruises.com/booking/ss01_booking.htm

Holland America
A TRADITION OF EXCELLENCE

Cryptographic Tunnels with SSH and Stunnel (quarter day)

Speaker: **Brian Hatch**

This talk will provide a quick overview of VPNs with the majority of time spent describing SSH and Stunnel (SSL) tunnels, including how to properly set up unattended logins for ssh, and being your own certificate authority for SSL.

Secure Shell and Network-based Intrusion Detection: Can (or Should) They Co-exist? (half day)

Speaker: **Eugene Schultz**

Secure shell (ssh) provides strong authentication and protection against unauthorized capture of data sent over networks. At the same time, however, by encrypting the data portion of packets, ssh makes network-based intrusion detection considerably more difficult. Attackers also often take over a host, gain a root shell, and then plant a tty sniffer that captures ssh keys/passwords before they traverse the network, thereby defeating the password security that ssh provides. Some organizations have simply given up by banning the use of ssh altogether, even though data sent over networks becomes exposed to snooping. There are, however, better alternatives, one of which is Baysian analysis of connection context—determining the kind of ssh connections that occur between hosts and calculating the probability that a given host is compromised given the probability that others that share ssh connections with it are or are not compromised. A case study will be used to show the kinds of problems associated with using a network intrusion detection system to identify security breaches and how Baysian analysis can help address these problems.

Linux VPNs and Cryptographic Tunnels (quarter day)

Speaker: **Brian Hatch**

There are a plethora of technologies that can be used to protect network communications. VPNs are the most popular buzzword of the day, but are often misconfigured or unnecessary. In this seminar noted author Brian Hatch will provide an overview of several VPN technologies available on the Linux platform, discussing their features, drawbacks, and interoperability with third party hardware and firewalls. He will also discuss other more lightweight options for creating secure communications between hosts that are frequently more efficient and provide better security than full blown VPN connections, such as SSH tunnels and SSL/TLS sessions using Stunnel. Private communication, be it with VPNs or other crypto tunnels, are in today's technology headlights, and this seminar provides technical insight and knowledge that you can use immediately to enhance your projects and secure your network communication.

IBM Tivoli Access Manager (quarter day)

Speaker: **Jeffrey Miller**

Access Manager is an extremely versatile access control enforcer. In this talk we'll look at the various ways Access Manager can secure enterprise applications, discussing its components and architecture. We'll also demo several uses of Access Manager and see how you can programmatically use Access Manager's APIs to talk to its authorization server and administrative policy manager.

Introduction to Application Security Concepts (half day)

Speaker: **Jeffrey Miller**

In this talk we'll introduce the basic concepts of security and how they apply to enterprise systems and applications. We'll start with fundamentals, covering encryption, hashing, digital signature, authentication, and authorization among other concepts. Then we'll apply those to network, system and application security, explaining how the fundamentals are usedby enterprises to protect valuable data. We'll look at how we can use security at the transport layer, such as with SSL, to protect data in transit. We'll see various access control enforcement techniques such as firewalls and reverse proxy security servers. Along the way we'll see how J2EE declarative security makes the job of developing secure applications easier, delegating much of the security responsibility to the application server. Finally we'll briefly introduce security for Web services.

OpenSSL and Stunnel (Quarter Day)

Speaker: **Brian Hatch**

How to use Stunnel to tunnel arbitrary cleartext network connections inside SSL if you control one or more endpoints. How to use Stunnel to allow SSL transmissions for clients and servers when you do not control the source code of the applications. How to build native SSL support into your own applications using OpenSSL. All issues of SSL Certificates, Certificate chains, and becoming your own certificate authorities are discussed as well.

geekcruises.com®
EDUCATION THAT TAKES YOU PLACES

Geek Cruises, Inc.
1430 Parkinson Avenue
Palo Alto, CA 94301
650-327-3692
928-396-2102 fax
215-519-0141 cell
neil@geekcruises.com
CST# 2065380-40

DAY	PORT	ARRIVE	DEPART	CONFERENCE SESSIONS
Saturday, August 6	Seattle, Washington	—	5:00 pm	7:15 pm, Bon Voyage Party
Sunday, August 7	Cruising Queen Charlotte	—	—	8:30 am – Noon, 1:30 pm – 5:00 pm
Monday, August 8	Juneau, Alaska	1:00 pm	8:00 pm	8:30 am – Noon
Tuesday, August 9	Cruising Hubbard Glacier	—	—	8:30 am – 11am, 1:30 pm – 5:00 pm
Wednesday, August 10	Sitka, Alaska	7:00 am	6:00 pm	6:00 pm – 8:00 pm
Thursday, August 11	Ketchikan, Alaska	7:00 am	1:00 pm	1:30 pm – 5:00 pm
Friday, August 12	Victoria, British Columbia	8:00 pm	Midnight	8:30 am – Noon, 1:30 pm – 5:00 pm
Saturday, August 13	Seattle, Washington	7:00 am		