ISACA Serving IT Governance Professionals SC Midlands Chapter

Off-Line

CHAPTER 54 NOVEMBER 2008

**November 20th Meeting – Registration Is Still Available

Black Hat Discussion and Demo, Noah Schiffman – Speaker Bio on page 2.

The meeting will last from 10:00 AM to 3:30 PM and will provide 4 CPE credit hours. Sign-in is at 9:30 AM. The discussion will extend to whenever, meaning that the speaker will stay for as long as needed.

Meeting Logistics

You may now pay online with a credit card! Go to http://www.scisaca.org/events.htm. The cost for the event is $120 and comes with 4 CPEs and lunch. Lunch will be provided by Shealy's. Pre-registration and payment is required for this meeting and the **deadline** is **Thursday**, **November 13th**. If you choose to pay online, please email a completed registration form to pbrock@scana.com. If you prefer to pay by check, please make the check payable to "SC Midlands Chapter of ISACA" and mail to *SC Midlands Chapter of ISACA c/o Phil Brock, 1426 Main Street – MC 067, Columbia, South Carolina, 29201*.

No refunds will be made, but substitutions are permitted.

E-symposium Information

For folks needing CPEs to finish out their required annual CPEs or just to catch up on the latest topics, don't forget that a membership benefit of ISACA International is **free CPEs**. The first time you participate in an ISACA e-Symposium, you will need to register at **http://isaca.brighttalk.com**. The User ID and password requested are specifically for the e-Symposium. The credentials are NOT the same as your ISACA username and password. Please be sure to add each e-symposium that you want to download to your e-symposium registration.

Each recorded topic below provides 3 CPEs:

- ✓ Improve the Audit, Minimize the Risk
- ✓ Risk and Compliance - Audit Fatigue
- ✓ Application Security: Attack and Response
- ✓ Security and Compliance Unite
- ✓ Security, Privacy and Trust
- ✓ Data Protection/Data Security
- ✓ Assessing IT GRC Maturity
- ✓ PCI Compliance
- ✓ Application Security - The New Perimeter
- ✓ From Information Security to Information Risk Management
- ✓ Making Data Protection Compliant
- ✓ Competencies for Compliance and Data Protection

In This Newsletter:

Important Dates

November Palmetto IIA Meeting – November 11

November Chapter Meeting – November 20th

Deadline Extended for CGEIT:

Grandfather applications by December 31, 2008

January 1 - Register and pay by this date for our January Meeting

January 21st – 23rd: Securing and Auditing Your Web-Enabled Applications, Ken Cutler.

March 19th: Ethical Hacking Discussion and Demo, Kevin Beaver

The Black Hat – Demo and Discussion

November 20th Meeting – Black Hat Discussion and Demo, Noah Schiffman

What you will learn:

- What you ever wanted to know and understand about the hacker mentality.
- General discussion and demo about computer hacking, which include the current methods, trends, and motives.
- A follow-up to Ken Cutler's network security seminar to discuss and demonstrate the true relevance in terms of real world attacks and threats.
- Tales of the experience of being on the other side of security-- the black hat hacker with a lot of the real world scenarios, true stories and actual unique situations.

  You will also have the opportunity to ask questions and to discuss whatever you need to understand your own working environment.

About the Speaker

Noah Schiffman is a former black-hat hacker turned security consultant with 20+ years of industry experience. Coding at an early age, he developed one of the early text/graphic editing applications and started his first software company in 1980, when he was 11 years old.

With the advent of networking technologies, Schiffman soon mastered the art of manipulating telco-switching systems, known as "Phone Phreaking". This soon led to his career as a computer hacker, performing reverse engineering, cryptographic attacks, corporate espionage, digital surveillance and other ethically questionable projects.

Schiffman has worked as a security consultant specializing in vulnerability assessment, pen testing, cryptography, digital forensics, incident response, and defining corporate security policies and strategies. His clients have consisted of Fortune 500 companies and various government agencies. With degrees in cognitive psychology and mechanical engineering, as well as a doctorate in medicine, he has experience in advanced biometric systems, human factors, physical security, authorization and access technologies, and holds several patents. He is a featured writer for Network World, with his "Security Phreak" blog and has authored numerous articles about hacking and security, on topics ranging from kernel mode metamorphic viruses to corporate data loss prevention. In addition to consulting, Schiffman is currently the acting CIO/CSO of a Department of Defense contractor.

Requirements for CGEIT Certification Under the Grandfathering Provision EXTENDED!!

Until December 31, 2008, highly experienced professionals who have had a significant management, advisory and/or assurance role relating to the governance of IT, can apply for certification as a CGEIT without being required to pass the CGEIT examination. To earn the CGEIT designation during this period, applicants are required to:

1. Submit evidence of appropriate work
2. Agree to adhere to the ISACA Code of Professional Ethics
3. Agree to comply with the: CGEIT Continuing Professional Education Policy

For a great overview, watch the CGEIT Certification Presentation.

Work Experience

In order to qualify for the CGEIT certification under the grandfathering provision an applicant must provide evidence of management, advisory or oversight experience associated with the governance of the IT-related contribution to an enterprise. Eight (8) years of such experience (there are substitutions available for experience) is required and is defined and described specifically by the CGEIT job practice domains and task statements.

Specifically, an applicant must have:

1. A minimum of one year experience relating to the development and/or maintenance of an IT governance framework (CGEIT domain one (1)) and;
2. Additional broad experience related to any two or more of the remaining domains (CGEIT domains two (2) through six (6))

For further information link to Grandfather in to CGEIT

November 2008 IIA Chapter Meeting - Skills for New Auditors

Mark your calendars for **Tuesday, November 11th** for the next Palmetto Chapter IIA program.

Presenter:

Thomas L. Richardson

Mr. Thomas L. Richardson, CIA was the General Auditor for Santee Cooper, a state-owned electric and water utility. Mr. Richardson's responsibilities included managing and directing the Internal Audit function, which performed financial, operational, compliance and information systems audits. During the course of his 30+ year career with Santee Cooper, Mr. Richardson also served as Supervisor of Plant Accounting and Auditor.

Mr. Richardson was a member of the General Accounting, Finance, and Audit Committee of the American Public Power Association (APPA) and the South Carolina State Internal Auditors Association (SIAA). A charter member of the Coastal Carolina Chapter of the IIA, he served as its first president. He later served two 2-year terms each, as the Mid-Atlantic Region District 4 Representative and Mid-Atlantic Regional Director. In December 2001, he was selected for the IIA's Global Ambassadors Program, which augments field services and chapter operations. He currently serves on the International Academic Relations Committee.

Mr. Richardson attended the University of South Carolina and graduated with a Bachelor of Science degree in Business Administration. After serving a two-year tour of duty in the United States Navy Reserve aboard the USS Seattle AOE-3, he returned to the University of South Carolina, where he received a Master of Accountancy degree. He has been a lecturer and presenter for The Institute of Internal Auditors and the MIS Training Institute for over twenty years.

Location: Seawells - 1125 Rosewood Drive, Columbia, SC 29201

Cost: $22 for members, $25 for non-members

CPE: 1

Date and Time: November 11, 11:00 - 1:00 (Registration starts at 10:30am)

Registration Deadline: November 7th

Contact: Amanda Gantt (Amanda.Gantt@bcbssc.com)

ACL Training in December

Palmetto IIA Chapter is holding two ACL classes in December and will be held at BlueCross BlueShield of SC at 4101 Percival Road. Dates: Dec 1 – 5, 2008. Registration is limited.

ACL 303 Advanced ACL concepts and techniques: Functions and Scripts will be a three day class. The cost is $810 for 25 CPEs.

ACL 252 Using ACL to Detect Fraud is a two day class. The cost is $540 for 16 CPEs.

To register contact Amanda Gantt at Amanda.Gantt@bcbssc.com or register online at http://www.theiia.org/chapters/index.cfm/view.events/cid/108

Securing and Auditing Your Web-Enabled Applications (22 CPEs) taught by MIS Instructor, Ken Cutler

Designing and Ensuring End-to-End Security and Compliance in Today's E-Business Applications

Three Day Event to begin Wednesday, January 21 to Friday, January 23, 2009

Registration and Payment required by January 1, 2009. Class size is limited so sign up soon. No refunds, but substitutions allowed. Register and pay at SC Midlands ISACA Home Breakfast and lunch served onsite and included in cost.

Tuition: $550 (A $2,300 Value!!)

Class Times: 8:30 am until 4:30pm Wednesday and Thursday

8:30 am until 3:00pm on Friday

Location: BlueCross BlueShield of SC

4101 Percival Road

Columbia, SC 29219

Meet in the Lobby at 8:15 for security escort.

You may park in any space outlined in white. Proceed to the Lobby at the center front of the building and obtain a Visitor's Pass. This will require a photo id. BCBS staff will collect you from the lobby and direct you to the classroom. Coffee, juices and a light breakfast will be served in the morning, lunch and a light snack in the afternoon. Contact Sue Rusher at 803-264-7631 with concerns. See attached registration form and directions.

Focus and Features

The recent avalanche of government regulatory initiatives, litigations, and intensified attacks on Web-based applications, along with traditional information asset protection, have significantly raised the stakes on the importance of secure application design, testing, certification/accreditation, and audit. In addition, IT applications have become more complex and frequently rushed to market by commercial IT product and internal developers, increasing the business risks and the challenges to applying and verifying reliable security safeguards.

In this information-packed three-day seminar you will cover key building blocks and significant risks, and systematically sort through the available safeguards in today's complex Web-enabled, multi-tiered applications. You will place special emphasis on a control point definition and transactional analysis approach to application design, security, and auditing within the context of robust but practical enterprise architecture and governance models. Case studies, demonstrations, and checklists will provide reinforcement and enhanced comprehension of complex design, safeguard concepts, and best practices.

Who Should Attend

Information Security Managers and Analysts; IT Managers, Auditors, and Architects; Security Architects; Application Certification Specialists, Consultants, Architects and Developers

Agenda: What You Will Learn

1. Web Application Architectures

- client/server and middleware security for multi-tiered applications
- contemporary application building blocks
- **w**eb application control points
- middleware and security application program interfaces (APIs)
- hypertext transfer protocol (HTTP) and uniform resource locator (URL) essentials
- HTTP state management: cookies, hidden fields, view state, query strings
- LDAP directory services
- locating control points and mapping associated sources of security services in complex, multi-tiered applications

2. Web (HTTP) Server Security and Audit

- web server configuration: operational and security features
    - web server configuration best practices
    - user authentication and web-based single sign-on
    - access control and server lockdown procedures
    - session encryption: Secure Sockets Layer (SSL)
    - web server security audit logs and intrusion detection systems
- comparing and contrasting security features for prominent web servers: Apache, Microsoft IIS, Sun Java System Web Server (iPlanet/NetScape)
- perils and protections for remote Web application development: Frontpage, WebDAV, Expression Web, SharePoint
- application firewalls and intrusion prevention systems
- tools, techniques, and checklists for securing and auditing Web servers

3. Security in Web Application Software Design

- sorting out the Web application environment building blocks and tools
- common vulnerabilities and attacks on Web applications: brute force attacks, privilege escalation, cross-site scripting, SQL injection, buffer overflow
- server-side web page scripting security: SSI, CGI, ASP, ASP.NET, PHP, JSP
- mobile code security: Java, ActiveX, VBScript, JavaScript, AJAX
- best practices for input validation and error handling
- software testing and assurance tools and techniques
- tools, techniques, and checklists for secure application design

4. Web Application Servers

- roles, architecture, and security control points for XML-oriented development environments and associated Web application servers
- assessing available security services and associated design best practices for the two prevailing Web application server environments:
    - Microsoft .NET Framework and associated ASP.NET components
    - Java 2 Enterprise Edition (J2EE): Sun/Glassfish, Red Hat JBoss, IBM WebSphere, Oracle Application Server (OAS), BEA WebLogic
- demystifying web services and Service Oriented Architectures (SOAs)
- tools and techniques for securing and auditing Web application servers and web services

5. Relational Database Management System (RDBMS) Security and Audit

- RDBMS and Structured Query Language (SQL) terminology, architecture, and features
- security risks associated RDBMS systems
- comparing security and audit features for major RDBMS products: IBM DB2, Oracle, Microsoft SQL Server, Sybase
    - connection and authentication for RDBMS systems
    - user accounts and password management
    - permissions, roles
    - database object protection methods: access control, encryption
    - database audit logging options
    - transaction logs and other database availability controls
    - built-in audit tools: tables, stored procedures
    - tools, techniques, and checklists for securing and auditing RDBMS systems

Serving IT Governance Professionals

SC Midlands Chapter

REGISTRATION FORM

November Meeting:
Black Hat Discussion and Demo 4 CPEs

Location:	Dates:
Harbison State Park	Thursday, November 20, 2008
5500 Broad River Road	Doors Open: 9:30 AM
Columbia, SC 29210	Morning Demo/ Discussion: 10:00 AM – 12:00 PM
803-896-8890	Lunch: 12:00 PM – 1:30 PM
	Afternoon Demo/ Discussion: 1:30 PM – 3:30 PM

Registration

Registration and payment is required for the seminar and is requested by Thursday, November 13, 2008. Checks should be made out to SC Midlands ISACA Chapter. Please complete this registration form and mail with check to:

Phil Brock, Chapter Secretary, 1426 Main Street – MC 067, Columbia, South Carolina, 29201.

ISACA Member	**$120**
ISACA Student Member	**$60**

Pre-registration and payment is required for this meeting. Monies need to be received by Thursday, November 13, 2008. No refunds will be made, but substitutions are permitted. If you would like to pay by credit card, please go to our chapter website at http://www.scisaca.org/events.htm If you pay online, please email your registration form to Phil Brock at mailto:pbrock@scana.com

NAME:

COMPANY:

E-MAIL:

PHONE:

Directions to Harbison Environmental Education Facility:

The center is located in the Harbison Forest off Broad River Road between Piney Grove Rd and Harbison Blvd.

Entrance to Harbison State Forest

- From I-26, take the Harbison Blvd exit. Turn left on the exit ramp toward Lowe's and follow Harbison Blvd to Broad River Rd
- Turn right onto Broad River Rd. The entrance to Harbison State Forest (pictured) will be on the left.
- As you enter Harbison Forest, bear left onto the gravel road.

- Turn right at the sign for the facility (pictured).