

Salare Security has launched one of the most intense Unified Communications Security Boot Camp in the industry. We have combined Online Learning + Self Study + Hands-on Labs to provide the most powerful learning experience possible

Course Description

UC deployments are entering the enterprise at a rapid rate every day. Many industry leaders are considering the advantages of data and telecommunications convergence, but have overlooked the concept of adequate security and vulnerability issues which comes with deployment. Every segment of the market and every technology professional will find themselves in need of a greater understanding of VoIP and the tools to keep the network safe from intruders.

This course consists of 3 hours of Pre Course Webinars that will lay the foundation of Telephony and Cyber Security for the non telephony professional. You will then attend 2 full days of Hands-on Labs at the Illinois Institute of Technology.

What you will receive

- 3 hours of Pre Course Online Webinar training.
- Self Study Kit containing over 1000 pages of critical reading.
- 2 days of hard hitting Hands-on Labs.
- 2 hours of Post Course Online Webinar training.
- Certification of completion to use toward your CPE credits.

What you will learn

- Understand VoIP technology from top-to-bottom.
- Get clear view of the vulnerabilities of IP-based voice service, how they vulnerabilities are exploited and how the vulnerabilities can be mitigated or remediated.
- Conduct you own VoIP security assessment the very next day.

Who should attend

- Data Security Professionals that need to know about voice and how to handle voice security.
- Voice Professionals that need to understand Data Security Issues and how they interact with UC.

Unique critical content

- Auditing and risk assessment for UC – A Guide based on the Internet Security Alliance's UC Security Project's VoIP Threat Risk Analysis.
- UC and covert channels – Special focus on an area of greatly increasing concern to US-CERT – the use of UC transmissions to bypass data network security measures.

Open source VoIP tools

- UCsniff
- Redirectpoison
- Teardown
- Vunneler
- Inviteflood
- Udpflood
- Wireshark
- Cain and Abel
- Rtpflood
- Rtpinsertsound
- Rtpmixsound
- Reghijacker

Event Details

<i>Location</i>	Illinois Institute of Technology (Rice Campus) 201 E. Loop Rd. Wheaton, IL 60189
<i>Pre Course Online Webinar Dates</i>	August 10, 2010 10:30-11:30am CDT August 11, 2010 10:30-11:30am CDT August 12, 2010 10:30-11:30am CDT
<i>Boot Camp Dates</i>	August 16-17, 2010 8:30-4:30pm CDT
<i>Post Course Online Webinar Dates</i>	May 17, 2010 10:30-11:30am CDT May 18, 2010 10:30-11:30am CDT

Cost

Just \$895.00 for 3-days of training and over a 1000 pages of value-packed resources.
*For each paid enrollment by July 15th receive a copy of Hacking VoIP Exposed – By David
Endler and Mark Collier*



**To reserve your seat today
visit training.salaresecurity.com or
call us at 312.994.2336**

Pre Course Online Webinar Details

August 10, 2010 10:30-11:30 CDT

VoIP Technology and Security Boot Camp Introduction

Meet the instructors, learn about the unique integrated content delivery behind the course so you know what to expect and how to be prepared to capture the most value from our webinars, hands on labs, lectures and background literature and tools

August 11, 2010 10:30-11:30 CDT

Foundations of Telephony for the non-Telephony Professional

If your career has brought you to the heights of Data Security and you've now been asked to manage voice in a converge network, this webinar is designed to cover the important topics you need to understand about voice and how voice works on an IP-network.

August 12, 2010 10:30-11:30 CDT

Foundations of Cyber Security for the Telephony Professional

If you have spent your career entrenched in the world of traditional voice communications, and now are being asked to provide a secure, reliable voice server via voice over internet protocol, this webinar is designed to introduce you to the important concepts of data security and how traditional data security can be used in a VoIP network.

Post Course Online Webinar Details:

August 23, 2010 10:30-11:30 CDT

Assessing the Security of a VoIP Network

Get the core knowledge and a list of questions that you need to answer as you begin to assess the security of your very own VoIP system.

August 24, 2010 10:30-11:30 CDT

Implementing Security on a VoIP Network

Understand the major controls that are necessary to properly manage the risks present in a VoIP Network.

Boot Camp Outline

Day 1 – August 16, 2010, 8:30am-4:30pm CDT

First Half Day – Foundation of UC

1. History of Telephony (Lecture)
2. Asterisk IP-PBX (Lab)
 - a. Overview
 - b. Installation
 - c. Step-up
3. Configure X-lite and Twinkle Soft Phones (Lab)
4. Configure and connect Cisco 7940 (Lab)
5. SIP Protocol and VoIP Architectures (Lecture + Lab)

Second Half of Day – Broad UC Security Issues

1. VoIP Security Overview
2. External Attacks on VoIP Systems
 - a. How do VoIP Systems connect with the External World
 - b. How are VoIP Systems Vulnerable to external attack
 - c. Some Example Exploits
 - i. Exposed Cisco Phones (lab)
 - ii. Exposed Snom Phones (lab)
3. Caller ID Spoofing
 - a. How does Caller ID work in the PSTN
 - b. How does Caller ID work with VoIP
 - c. What are vulnerabilities with VoIP Caller ID
 - d. How Does Caller ID Spoofing work
 - i. PSTN
 - ii. VoIP
 - e. The Severity of Caller ID Spoofing ... The Risk Impact
 - f. Exploits using Caller ID Spoofing
 - i. vishing
 - ii. swatting
 - iii. voice mail access
 - iv. credit card activation
 - g. Defending against Caller ID Spoofing
4. Call Redirection
 - a. How Call Redirection Works
 - i. PSTN
 - ii. VoIP
 - b. Vulnerability of VoIP to Caller Redirection
 - c. Severity of Call Redirection ... The Risk Impact
 - d. Exploits Using Call Redirection
 - i. Registration Hijacking
 - ii. ARP Poison Redirect

Day 2 – August 17, 2010, 8:30am-4:00pm CDT

First Half of Day - Major UC System Components

1. VLANs
 - a. VLAN Overview
 - b. VLAN Exploits (Non-lab based)
2. TFTP Servers
 - a. Overview of TFTP and its use with VoIP Systems
 - b. Install and Configure a TFTP Server
 - c. Register Cisco IP Phone with TFTP Server
3. Use UCsniff/VoIPhopper to spoof the Cisco IP Phone
4. Session Border Controllers and VoIP Aware Firewalls
5. Overview of Firewall Evolution
6. SBC Functions

Second Half of Day - IP PBX features and Attacks of the IP-PBX and User Agents

1. IP-PBXs
 - a. Major Functions
 - i. Registrar
 - ii. Location Server
 - iii. Proxy
 - iv. Other Functions
 - b. Voice Mail
 - c. Conference Services
 - d. Configure voice mail on Asterisk
 - e. Configure Conference Services on Asterisk
2. DOS attacks on IP-PBX
 - a. INVITE Flood
 - b. REGISTER Flood
3. DOS attacks on Phones
 - a. SIP Bye
4. VoIP Media
 - a. Overview of RTP/SRTP, Media Gateways, Codecs, UDP issues
 - b. Media Exploits
 - i. Sound injection
 - ii. Sound Mixing
 - iii. Vunneling
 - iv. SPIT