

Security Management

Information security is a problem that all businesses must deal with. The secure creation, storage and transportation of information is even becoming a legal requirement for many industries. Data privacy and confidentiality issues abound! This COS explains and educates attendees on the issues and techniques associated with managing all aspects of IT Security. It includes an end-to-end view of information security including management issues, OS/400 features, software applications, and networking communications. Newer issues addressed include passing an IT audit and Single sign-on capabilities.

Demystifying SF06 Miami Sessions: Thursday, 9/21/2006

21MH: Mon 8 - 9:15, B122, Miami Conv Ctr

ID:490074

Level:
All

Course:
Security
Management

Speaker:
Patrick S.
Botz
IBM Corporation

Understanding the fundamentals of security is required in order to provide your organization with the level of security it requires. This session defines security and the process required to effectively implement it. The different aspects of the process are described along with the roles and input required to "do" security with reasonable amount of effort and cost.

In this session you will learn:

1. Fundamental security concepts required in order to effectively implement security.
2. The standard security process and how to implement it in your organization.
3. Your role, the roles of others, and where they fit within the security process.
4. The role of a security auditor and how to manage them.

Tips for Writing A Security Policy

22MH: Mon 9:30 - 10:45, B122, Miami Conv Ctr

ID:510076

Level:
Advanced

Course:
Security
Management

Speaker:
Patrick S.
Botz
IBM Corporation

Without a security policy, the chances of implementing an organization's security requirements is impossible. This session describes why a security policy is required and tips for writing a policy.

Compliance - Help! Where do I Start?

23MH: Mon 11 - 12:15, B122, Miami Conv Ctr

ID:510077

Level:
Advanced

Course:
Security
Management

Speaker:
Carol
Woodbury
SkyView Partners,
Inc.

Everywhere you turn the word "compliance" pops up. But what does compliance really mean to your organization? This session will discuss how to determine what laws and regulations your organization must be in compliance with, an indepth review of many of the laws and regulations with which your organization must comply and how to translate these requirements into i5/OS settings.

LDAP, Domino and System i - the Redbook

25MM: Mon 2 - 3:15, B212, Miami Conv Ctr

ID:410033

Level:
Beginner

Course:
Security
Management

Speaker:
John M.
Taylor
COMMON UK

LDAP-enabled directories provide phone and email addresses and help to manage server access, authorize B2B users, find experts via Knowledge Management and share a single sign-on with Enterprise Identity Mapping (EIM). Learn how to integrate and manage OS/400 with Websphere, Domino Directory, Novell and MS Active Directory using IBM's Directory Server and BlueNotes Directory products.

F06 Miami Sessions: Thursday, 9/21/2006

Laying the Foundation of OS/400 and i5/OS Security

25MF: Mon 2 - 4:45, B118, Miami Conv Ctr

ID:490075

Level:
All

Course:
Security
Management

Speaker:
Carol
Woodbury
SkyView Partners,
Inc.

This session will describe the concepts that make-up the foundation of OS/400 and i5/OS Security and explain how to translate these concepts into reality so that you can implement them on your system. Starting from the ground up, we will discuss practical, real-life examples that will help you when you return to the office. We will also discuss tips and techniques for managing security. Whether you are a security novice or expert, this session will provide you with new information.

Real Stories from Developing and Invoking an Incident Response Plan

31MH: Tue 8 - 9:15, B122, Miami Conv Ctr

ID:510065

Level:
Advanced

Course:
Security
Management

Speakers:
Carol
Woodbury
SkyView Partners,
Inc.
Richard
Dolewski
Midrange Computer
Group

A security incident has occurred? Is your organization prepared? Who should be contact? What data should be gather? What method should be used to gather the data? This session will discuss how to develop an incident response plan and how to effectively invoke it. Real-life stories and scenarios will be presented.

After this session you will:
Understand the required components of an incident response plan
Know what data to collect
Understand how to collect the data
Learn from other organizations who have already experienced a security breach

Hardening Your i5/OS Environment

31MB: Tue 8 - 9:15, B114, Miami Conv Ctr

ID:510114

Level:
Intermediate

Course:
Security
Management

Speaker:
John Earl
The PowerTech
Group

The default settings on i5/OS are good enough for a lot of companies. But if you need to harden your OS beyond the factory defaults, this session will provide you with a series of steps you can undertake to ratchet up your environment and reduce the risk of exposure.

This session will cover configuration areas such as:

System Values, Network Settings, Library and Directory Settings, User Profiles, and more.

By the end of this session, attendees will be able to:

1. Recognize i5/OS settings that could be hardened.
2. Understand the risks and benefits of these changes.
3. Create a plan to harden their environment

A Step by Step Approach to Implementing Object Security

35MF: Tue 2 - 3:15, B118, Miami Conv Ctr

ID:402377

Level:
Intermediate

Course:
Security
Management

Speaker:
Carol
Woodbury
SkyView Partners,
Inc.

Given the regulations in effect today, almost every company has a file or application whose access needs to be controlled. In addition, a good security scheme helps provide data availability because accidental errors due to users or processes having too much authority are avoided. The good news is that object level security doesn't have to be that difficult! This session will discuss using object security to protect your data from unwanted access, the steps you go through to determine what access is required, implementation of object security and hints to avoid breaking other processes..

F06 Miami Sessions: Thursday, 9/21/2006

Securing a Wireless LAN

35MD: Tue 2 - 3:15, B116, Miami Conv Ctr

ID:420041

Level:
Intermediate

Course:
Networking

Speaker:
Tom Hadley

Wireless LANs offer a whole new security challenge at the office. This session will review some of the vulnerabilities you face as you move off the wire, and what security solutions you can implement to solve them.

Another challenge we face is combination of wireless LANs and always on connections at home, plus the use of telecommuting by companies large and small. This combination of technologies means that security needs to be a major consideration, not just at home, but for the office access as well. Come explore the potential vulnerabilities that implementing a telecommuting rollout can produce and more importantly find ways to deal with these vulnerabilities.

By the end of this session, attendees will be able to:

1. Understand wireless LAN security options today.
2. Describe the limitations of the existing options.
3. Evaluate emerging solutions to provide better security.

Integrated File System Security

36MN: Tue 3:30 - 4:45, B213, Miami Conv Ctr

ID:440138

Level:
Beginner

Course:
IFS

Speaker:
Timothy Clark
IBM Corporation

Learn a wealth of information about i5/OS Integrated File System (IFS) security. This session covers both fundamental and advanced security topics designed to help you manage and improve the security of your IFS. Topics include blending UNIX, PC, and i5/OS authorities, using security commands, APIs, GUIs and tools, security for created objects, auditing, virus scanning, controlling remote access and more.

Protect Your Application Data With i5/OS Encryption

36ML: Tue 3:30 - 4:45, B211, Miami Conv Ctr

ID:490012

Level:
All

Course:
Security
Management

Speaker:
Jeff Uehling
IBM Corporation

Security reports about data theft and recent legislation requirements have risen the demand for higher security. In many iSeries environments, products and services have been put in place to better control access to the system itself. However, if somebody has gained access to the system, the application data itself is all stored in clear text. Rightful users could then easily manipulate data in or steal data from your database. Sometimes encryption is also recommended when transferring data on tape or as attachments to e-mails. i5/OS provides several options to protect sensitive information on disk by using encryption functions.

In this session, you:

1. Learn the basics of encryption, such as symmetric and asymmetric encryption.
2. Get an overview of the available encryption functions in i5/OS.
3. Get an introduction to key management.
4. Learn based on an API overview flow how to use encryption APIs within i5/OS applications.
5. Learn how to use the DB/2 built-in encryption functions.
6. Get an overview of implementation and migration requirements.

Common Sense Security Auditing

36MF: Tue 3:30 - 4:45, B118, Miami Conv Ctr

ID:500009

Level:
All

Course:
Security
Management

Speaker:
Dan Riehl
The Powertech
Group, Inc.

OS/400 provides a plethora of options when it comes to auditing security-related events. Many of us have shied away from auditing because, from a cursory view, auditing seems only to eat up disk space and generate far more data than a normal human can digest. However, if we take a common sense approach to security auditing, it is possible to eliminate the drawbacks and get the vital information we need to properly manage the system.

By the end of this session, attendees will be able to:

1. Understand security auditing options.
2. Sensibly configure auditing of security related events.
3. Sensibly configure auditing of objects and users.

F06 Miami Sessions: Thursday, 9/21/2006

Securing Your User Profiles Against Abuse

42MA: Wed 9:30 - 10:45, B113, Miami Conv Ctr

ID:500008

Level:
All

Course:
Security
Management

Speaker:
Dan Riehl
The Powertech
Group, Inc.

One of the main security exposures we face is unsecured user profiles. This exposure can be exploited quite easily to violate the strict COBIT and SOX requirement of "separation of duties".

The sessions will explore the methods used to hijack a user profile to gain unlimited power. It will also provide recommendations on eliminating the exposures for a more secure system.

By the end of this session, attendees will be able to:

1. Identify methods to exploit unsecured user profile.
2. Understand how to eliminate the exposures.

Single Sign-On Overview: Don't Synchronize Passwords -- Eliminate them!

46MP: Wed 3:30 - 4:45, B215, Miami Conv Ctr

ID:420089

Level:
Intermediate

Course:
Security
Management

Speaker:
Patrick S.
Botz
IBM Corporation

This is the first session of the Single Sign-on Focused Education Roadmap. This session provides an overview of SSO and some of its many definitions. The session introduces the business case and explains the industry unique, non-disruptive, and password elimination attributes of the IBM eServer approach to SSO.

In this session, the first of the Single Sign-on Focused Education Roadman, you will learn:

1. Different definitions of Single Sign-on.
2. The rationale behind the OS/400 & i5/OS SSO strategy.
3. The technologies involved in the OS/400 & i5/OS strategy.
4. Why the OS/400 & i5/OS approach can be cheaper than other approaches.

LAB: Security Auditing On a Shoe-String Budget

43LB: Wed 11 - 12:15, A201, Miami Conv Ctr

ID:430151

Level:
Intermediate

Course:
Security
Management

Speakers:
Jeff Uehling
IBM Corporation
Patrick S.
Botz
IBM Corporation

This lab is for people who want to know more about the security audit journal and how to extract data from it. In this lab you will learn techniques for moving security audit data to outfiles, running queries, and developing simple programs to analyze the data. The lab includes a scavenger hunt to detect suspicious activity.

New, at Spring Common, 2006, a task that shows you how to create your journal and add application level auditing to your i5 application.

If you ever had questions about the data in the security audit journal, but were afraid to ask, this is the lab for you!

By the end of this lab, you will be able to:

1. Create and populate outfiles with security audit data.
2. Analyze security audit data.
3. Build audit support into your own application.

Secure Your iSeries Web Applications

51MC: Thu 8 - 9:15, B115, Miami Conv Ctr

ID:480084

Level:
All

Course:
Security
Management

Speaker:
Jim Mason
Cape Cod Bay
Systems

This session is a must if you are deploying iSeries Internet applications! Beyond the high level overviews of security standards, products and architectures, this session outlines specific scenarios for integrating security tools and resources to meet your Internet security needs.

By addressing the security challenges for a scenario, you'll learn to apply the 'security service layers' available in your e-business environment including iSeries security, TCP network security, HTTP security, J2EE and WebSphere security, Java security, application level security. The scenarios will highlight some of available the options in these layers including portal environments, SSO and directory solutions that integrate multiple platforms well.

You'll learn how to create an e-business security plan workbook to build your own security plans that can be implemented by your team or outside resources as needed.

The solution models reviewed are adapted to work affordably in both large shops and small ones.

F06 Miami Sessions: Thursday, 9/21/2006

What's New in Security

52MC: Thu 9:30 - 10:45, B115, Miami Conv Ctr

ID:500052

Level:
Intermediate

Course:
Security
Management

Speaker:
Jeff Uehling
IBM Corporation

This presentation will cover recent security enhancements, V5R3 and beyond. The presentation will give an overview of all the recently added security functions in i5OS.

You Can Do What With Service Tools? An Overview

53MC: Thu 11 - 12:15, B115, Miami Conv Ctr

ID:420158

Level:
Advanced

Course:
Security
Management

Speaker:
Mark S.
Waterbury
Industrial Strength
Software

The Start System Service Tools (STRSST) and Dedicated Service Tools (DST) have been around forever in OS/400. Major changes were made to security and new function added over the last several releases. If you want to learn about how you can use the service tools and more importantly how you can prevent others from using the service tools without your knowledge, then this is the session to attend.

Personal Identity - Protect it or Lose it

55MC: Thu 2 - 3:15, B115, Miami Conv Ctr

ID:470051

Level:
All

Course:
Security
Management

Speaker:
Jim Rostis
National
Forwarding Co.,
Inc.

Personal ID Theft Is The Fastest Growing Crime In The U.S. And Around The World. This session will discuss the following: (1) What is your PI? at work and at home. (2) How to protect your PI, put your guard up now. (3) How does PI theft occur in the workplace and at home. (4) What to do if you are a victim.

By the end of this session, attendees will be able to:

1. ID your PI.
2. Protect your PI.
3. Learn what to do if you are a victim.

Conducting a Successful DR Test

56MK: Thu 3:30 - 4:45, B210, Miami Conv Ctr

 **GOLD**
ID:430037

Level:
Intermediate

Course:
High Availability
Resilience

Speaker:
Richard
Dolewski
Midrange Computer
Group

Disaster Recovery Planning is an integral part of any effective business strategy. Testing your plan is essential. Listen and learn from over 100 recovery tests and simulations performed to see how to do it right. Testing makes perfect.

By the end of this session, attendees will be able to:

1. Develop testing objectives.
2. Understand what makes a successful DR test.

Configuring OS/400 Single Sign-on

56MC: Thu 3:30 - 4:45, B115, Miami Conv Ctr

ID:440135

Level:
Advanced

Course:
Security
Management

Speaker:
Patrick S.
Botz
IBM Corporation

IBM announced single sign-on (SSO) support for OS/400 in V5R2. Based on Kerberos authentication and IBM's Enterprise Identity Mapping technology, SSO can make using and administering OS/400 much less trouble than ever before. This session shows you which interfaces are enabled for SSO and what you need to do to configure them. While OS/400 SSO is available for any environment that supports Kerberos, this session will use a Windows 2000 domain as the configuration scenario.

After attending this session you will be able to:

1. Configure OS/400 for Kerberos.
2. Configure EIM for your network.
3. Identify all interfaces currently enabled for SSO.
4. Configure the enabled SSO interfaces.