

Platform Security

Details

Level:	Intermediate
Duration:	2 days
Development language:	C++
Experience:	The class is designed for experienced Symbian OS developers who have a reasonable understanding of OO and C++ in particular. Familiarity with building and developing with an IDE is required. The workshop attendee should be familiar with the operating principles and organisation of Symbian OS to a level provided by training covered in the Symbian OS Essentials and Application Engines courses or have equivalent hands-on experience of developing for Symbian OS for at least 3 months.



The Platform Security course consists of two one-day classes which can also be booked individually:

A design workshop ("Designing for Platform Security course")

A hands-on programming class ("Programming for Platform Security course")

Target audience

People who want just a design overview or have an implementation role:

- Internal Symbian technical consultants/architects;
- Staff with a similar design role in Symbian OS Licensee companies;
- Staff with a similar design role in Symbian Partner companies;
- 3rd party software developers who want an overview of the changes with a view to implementation.

The focus of the workshop is on the overall phone platforms rather than being aimed at developers of any one category of software (UIQ or Series 60).

Description

The first day of the course is an interactive workshop aimed at developers/architects already experienced in Symbian OS but who want to know what is changing in the latest versions of the OS with respect to the implementation of Platform Security. It covers the following areas: platform security concepts and activities that developers need to be aware of during a project's analysis phase and design phase. In the second day of the course more "hands-on" coding exercises aimed at programmers illustrate how to maintain and ensure a secure implementation for different types of Symbian OS components (using the new secure APIs).

On the first day we have approximately 30% interactive sessions and 70% lectures. On the second day we have approximately 30% lectures and 70% programming of coding exercises.

Objectives

The purpose of this course is to help ensure that phones built on Symbian OS v9.1 and onwards are designed and implemented following secure OS principles.

The objective for the course is to help developers redesign insecure architectures, spot security problems and write secure code. On the first day the emphasis is on the design aspects, rather more than the analysis or coding aspects. On the second day the emphasis is on the hands-on aspects.

Upon completing the designing for platform security workshop, participants will be able to:

- Explain to team colleagues why information security is important to phone users and network operators;
- Explain to team colleagues key architectural concepts and goals of Platform Security and be able to apply this to analyzing the design of their own software.

Upon completing the programming for platform security course, participants will be able to:

- Build redesigned code with the modified tool-chain to the new APIs;
- Define a server security policy;
- Define a security policy for data in the new central repository;
- Define a security policy for a publish and subscribe service;
- Re-implement plug-in architectures via ECOM as separate processes;
- Build applications according to the new Application V2 framework;
- Provide embedded document services via application servers.

Tools

You choose your tool chain from the list below:

Metrowerks CodeWarrior C++ IDE
Nokia Carbide.c++ IDE

Exercises and course materials are adapted for the tool chain you choose. The course materials will also introduce the chosen development environment to the candidate.

Platform

You choose your platform from the list below:

Series 60 platform
UIQ platform
Mix of UIQ and Series 60 platform

The course materials and exercises have been adapted to use the Series 60 emulator and SDK's or to use an UIQ environment. If your company did not choose a specific platform yet or needs to target both we can use a mixture of modules which use alternating UIQ or Series 60 platform. Differences between the two platforms will be explained during the module on build tools.

Agenda

Day 1 – Designing for Platform Security

Module 1. Introduction to the course

Explains the setting and requirement for the course and its content.

Module 2. Designing-out insecurity

This module looks at what's involved in redesigning insecure architectures. This module emphasizes the importance of design. The attendee has to be committed to thinking about design problems, rather than being process-driven and thinking purely in terms of implementing APIs.

Unit 2.1 Identify Security Counter-measures

You will be able to select security counter-measures. Topics covered include:

- Identifying threats: explain to others why information security is important to phone users and network operators
- Doing a cost/benefit analysis of counter-measures

Unit 2.2 Understand Platform Security

You will be able to explain to others key architectural concepts and goals of Platform Security. Topics covered include:

- Platform Security concepts – the unit of trust
- Data Caging
- Capabilities

Module 3. Sign your Software

You will be able to describe the need for Symbian Signed. Topics covered include:

- Describe the need for Symbian Signed
- Describe how Symbian Signed handles capabilities
- Overview of the certification process steps inc. developer certificates

Module 4 Secure your design

You will be able to secure your design and be able to apply this to analysing the design of own software. Topics covered include:

- Protection Domains
- Sharing Data
- Securing the architecture of device drivers, servers and plug-ins
- The design process
- Connectivity issues

Day 2 – Programming for Platform Security

Module 1. Introduction & Key concept review

- Explains the setting and requirement for the course and its content
- Recaps very briefly the key concepts of unit of protection, capabilities and data caging

Module 2. Build-up security

You will be able to build, debug and write secure code with the new APIs. Topics covered include:

- Assign capabilities
- Write resilient code
- Identify a trustworthy process

Module 3. Use & write secure servers

You will be able to use and write client-side and write server-side code conforming to the new security APIs. Topics covered include:

- Use IPC v2 APIs
- Police the server security model

Module 4. Share data securely

You will be able to cage your data and share it securely. Topics covered include:

- Cage your data and share securely
- Write a security policy for the new central repository
- Write a security policy for the Publish & Subscribe service

Module 5. Implement ECOM plug-ins

Topics covered include:

- Restructure an ECOM plug-in DLL into an out-of process plug-in

Module 6. Make applications secure

Topics covered include:

- Re-architect an application to the new UI Framework V2 structure without AIF files
- Write an Application Server