JavaOne℠

Sun's 2002 Worldwide Java Developer Conference℠

JSR-118 (MIDP v2.0)

Session 2 of 2

Dr. James E. Van Peursem
Specification Lead, JSR-118
Chief Architect, J2ME Platform
Motorola, Inc.

Roger Riggs
Senior Staff Engineer
Sun Microsystems, Inc.

Overall Presentation Goal

Learn about new capabilities being introduced in the next generation of the Mobile Information Device Profile (MIDP v2.0) specification

Learning Objectives

- As a result of this presentation, you will get an overview of the new features being introduced in MIDP 2.0
- In addition, you will get in-depth knowledge about the following new MIDP 2.0 features:
  - Trusted MIDlet Suites for better security
  - Enhanced networking
  - HTTPS
  - Push

Speaker's Qualifications

- Jim Van Peursem is the Specification Lead for JSR-118 and is also a Distinguished Member of Technical Staff at Motorola, Inc.
- Roger Riggs is a Senior Staff Engineer at Sun Microsystems and is Sun's Technical Lead for Wireless for MIDP 1.0 and MIDP 2.0

Presentation Agenda

- MIDP 2.0 overview
- Trusted MIDlet Suites for better security
- Enhanced networking
- HTTPS
- Push
- Q&A

Java™ Specification Request (JSR) 118: MIDP 2.0

- JSR filed April 2001
- Expert group consists of nearly 60 companies including network operators, manufacturers, content developers, technology providers and individuals
- Producing the specification for MIDP 2.0
- MIDP 2.0 is a complete specification that includes new functionality and is backward compatible with MIDP 1.0

MIDP 2.0 New Functionality

- Overview presented today, and detailed discussions contained in a separate session:
  - Application Delivery
  - Enhanced UI
  - Game
  - Sound
- Detailed discussions today:
  - New Security Model through Trusted MIDlets
  - Enhanced Networking
  - HTTPS
  - Push

Application Delivery

- MIDP 2.0 formally includes the Over The Air (OTA) Recommended Practice document associated with MIDP 1.0
- Enhancements were made to this specification to enable reliable delivery of server notifications
- Notifications are enabled for successful application installation as well as deletion

Enhanced UI

- Builds upon the features of LCDUI
  - Custom Item support
  - Layout control
  - Graphics enhancements
  - Miscellaneous improvements
- Backward compatible with MIDP 1.0

Game API

- Provides a rich set of features for developing 2D gaming content
  - Enables native implementation
  - Simplifies game development
- Compatible with LCDUI Graphics classes
- Flexible design

Sound

- Provides rich audio capabilities to MIDlets:
  - Tone Generation (required)
  - Sampled sounds (e.g. wav) (optional)
  - MIDI (optional)
- Structured as a subset of JSR-135 (Multimedia), to gives full upward compatibility

Security and Networking

Roger Riggs
Senior Staff Engineer
Sun Microsystems, Inc.

Example Use Case

- An E-Commerce application to manage a consumer's confidential or financial data
- Registers to store financial data
- Registers to be notified of significant events
- Polls for information or is notified

MIDP 2.0 Security

- Untrusted Applications
  - Sandbox support as in MIDP 1.0
  - Used for any application that can not be trusted
  - Minimum required functionality is specified
- Trusted Applications
  - Permissions are defined for restricted APIs
  - One Protection Domain for each trust level
  - Device makes choice to trust based on policy

Permissions

- Permissions are boolean
  - Granted or denied
  - May be granted by user or denied
- Naming conventions follow package naming
- Extensible to APIs developed independently in other JSRs or as Licensee Open Classes
- Each API defines the permissions that apply

Restricted APIs Define Permissions

Permission	Protocol
javax.microedition.io.Connector.http	http
javax.microedition.io.Connector.https	https
javax.microedition.io.Connector.datagram	datagram
javax.microedition.io.Connector.datagramreceiver	datagram server
javax.microedition.io.Connector.socket	socket
javax.microedition.io.Connector.serversocket	server socket
javax.microedition.io.Connector.ssl	ssl
javax.microedition.io.Connector.comm	comm
javax.microedition.io.PushRegistry.datagram	datagram
javax.microedition.io.PushRegistry.socket	socket

Protection Domains

- One Protection Domain ⇔ One MIDlet Suite
- Allowed Permissions
  - Granted if trust is verified
- User Permissions
  - Granted with explicit user approval
  - User may grant
    - Blanket—valid until user revokes
    - Session—valid for a single invocation
    - Oneshot—valid for a single use of an API

Security Policy

- On Device Policy
  - Protection Domains for each source of trust
  - Off-line and no-bandwidth security checks
  - Configured in advance
- Security policy is device and market specific
  - Variations in purpose of device
  - Variations in security requirements in markets

Trusted Signed Applications

- A mechanism for trust based on PKI
- Application Descriptor includes
  - Signature of the MIDlet Suite JAR
  - Manifest attributes is secured in JAR
  - Certificate(s) needed to verify signature
  - Permissions requested by the application
- JAR Signature
  - PKCS #1 Version 2.0 using private key
  - Corresponding public key is in certificate
  - Root public key (certificate) on the device

Over The Air Signed Applications

- Installation
  - Verify integrity of JAR using signature
  - Verify certificates to a protection domain
  - Verify requested permissions are valid
- Invocation
  - Some permissions may be granted by protection domain via root certificate
  - Some permissions may be granted by user as prompted for requested permissions

Security Summary

- Untrusted applications for widest distribution
- Permission and Protection Domain Model
- Per API definitions of required permissions
- Per MIDlet Suite requests for Permissions
- On device trust decisions and enforcement
- Policy is configured to match device and market requirements

MIDP-NG Networking Enhancements

- New network and device I/O handlers
- Secure Networking
- Push Application Support

New Protocol Handlers

- The new handlers follow the CLDC Generic Connection Framework
  - Allows for optional implementation with minimal footprint impact
- The new I/O functions are protected as privileged operations

Networking APIs

- SocketConnection—TCP/IP socket
- ServerSocketConnection—TCP/IP Server socket
- UDPDatagramConnection—UDP Datagram
- API features
  - Socket options control buffer sizes and special delays—for example, linger on close
  - Provide access to local and remote IP address and port information
  - Added system assignment of dynamic port address
- APIs are specified—not all devices must implement

Secure Networking APIs

- HTTPSConnection
  - Secure HTTP over SSL 3.1 or TLS 1.0 or WTLS
- SecureConnection
  - Secure socket connection using SSL or TLS
- SecurityInfo
  - Access to server certificate
  - Verification of encryption algorithm
- Certificate
  - Access to server identity and parameters
- CertificateException
  - Exceptions for certificate and connection setup errors

Serial Communications APIs

- comm:<port identifier>[<optional parameters>]

	Default value
– baudrate	platform dependent
– bitsperchar	8
– stopbits	1
– parity	none
– blocking	on
– autocts	on
– autorts	on

- System property to list available ports
  - Naming convention to distinguish IR versus serial cable accessed ports. For example, IR0, COM1, etc.

MIDlet Invocation

- Application registers expected inbound connections
  - Application Descriptor file or
  - PushRegistry to register or unregister
- Registration includes
  - Inbound connection datagram://:12345
  - MIDlet name example.ChatDemo
  - Source Filter 129.148.70.142
- Application Management Software support for specific protocols is implementation specific
- Alarm function allows one-shot startup at a specific time

MIDlet is Invoked for A New Connection

- On notification the MIDlet is launched to handle the inbound I/O operation
  - The listConnections() method is available for the MIDlet to check for connections already registered within the MIDlet suite, or
  - For connections that have a pending inbound connection
- The MIDlet handles all I/O as normal
  - For example, open(), read(), close(), etc.
  - After the MIDlet exits, the AMS resumes listening
- Application can be rejected at installation
  - If proper credentials don't include push permissions
  - If the connection is already allocated to another installed application

Summary

- MIDP 2.0 is backward compatible with MIDP 1.0
- MIDlets developed for MIDP 1.0 will work on MIDP 2.0 devices
- Significant new functionality is being specified in MIDP 2.0

If You Only Remember One Thing…

The new MIDP specification offers significant new capabilities that enables a wide range of new content. Take advantage of these new capabilities!

Review the details at:

http://jcp.org/aboutJava/communityprocess/review/jsr118/

Q&A

JavaOne℠

Sun's 2002 Worldwide Java Developer Conference™

BEYOND BOUNDARIES

Session 3006