FIPS 140-2 Validation of OpenSSL for Android Devices

The leveraging of open source software for timely and cost effective use of COTS products in government

Time Sensitive Requirements

- Rapidly evolving technology and market pressures in the mobile device market result in new smart phone releases almost every month
- The government and DoD markets have unique information requirements
- Many desirable COTS products do not currently use approved cryptography
- The approved products that are available are expensive and lag the market
- The cost and difficulty of negotiating the approval processes means many vendors don't even try
- Some useful prototype products have been developed in-house on late model mobile devices for use by DoD, but formal approvals considerably lag functional utility

The Challenge

- The combination of fast moving technology and slow formal approvals creates an information assurance problem for government agencies
- As a result the renaissance of mobile devices inspired by Android doesn't benefit the government market
- Typical DoD models of building custom hardware and software are being re-evaluated in favor of using COTS mobile device technology
- Formal product IA approvals are needed on a timescale matching the product life cycles

The Promise

- Most mobile devices are based on open source software (OSS): Android for the O/S and OpenSSL for cryptography
- Both of those OSS products are highly portable and actively maintained
- The OSS model can reduce the cost and delays of deploying the latest technology, especially for mobile devices
- OSS has characteristics, especially for mobile devices, that can be leveraged to this end

Background - FIPS 140-2

FIPS 140-2 Validation

- Cryptographic Module Validation Program (CMVP) is a joint U.S. - Canadian program
- Universal procurement requirement in federal government and DoD
- Validation typically takes 6-12 months for previously validated code, 12-18 months if starting from scratch
- Smaller vendors are discouraged from competing in the government market due to cost and perceived difficulty

Background - the Cryptography

OpenSSL

- Full featured cryptographic software widely used in both commercial and open source products
- Open source with a business friendly license
- Basis for the majority of all validated cryptographic software
- Is validated in essentially identical form over and over again by different commercial vendors

The Open Source Validated Cryptographic Module

OpenSSL has been used as the basis for a small series of unique validations

- Most recent such validation was #1051 in 2008
- The “OpenSSL FIPS Object Module” is a core cryptographic module, not the full OpenSSL library and toolkit
- The validation is based on open source code and documentation
- The validated module if available for use by anyone at no cost

The Open Source Validated Cryptographic Module

Benefits

- Can be used directly, or (until 2011) as a model for “private label” validations
- Designed to easily retrofit existing products for FIPS 140-2 compliance
- Supports a wide range of platforms
- Supports global enabling of FIPS mode for all OpenSSL based applications on a device

The Open Source Validated Cryptographic Module

Drawbacks of the current module

- #1051 validation is dated; only compatible with OpenSSL 0.9.8 which is near end-of-life
- Slow POST performance is a real problem for embedded devices
- Lacks cryptography of current interest such as Suite B
- No longer useful as a model for “private label” validations

The Current Initiative - Code

Implement a new OpenSSL FIPS Object Module

- Add new cryptography such as Suite B
- Satisfy new validation requirements
- Improve POST performance
- Remove many revision dependencies

The Current Initiative - Approval

Obtain a FIPS 140-2 Level 1 validation

- Include platforms of immediate interest (three Android based mobile devices)
- Provide the ability to quickly add new platforms (in weeks, not months) via the “change letter” process
- Results will be available for use by government and industry
- Began January 2011, estimated completion February 2012

The Current Initiative - Status

Current Status of FIPS 140-2 Level 1 validation

- "Code freeze" was last week
- Testing of the first Android mobile device is underway
- A total of 30 platforms have already been sponsored by commercial vendors
- "Private label" validations for 10 platforms are waiting on completion of the open source based validation