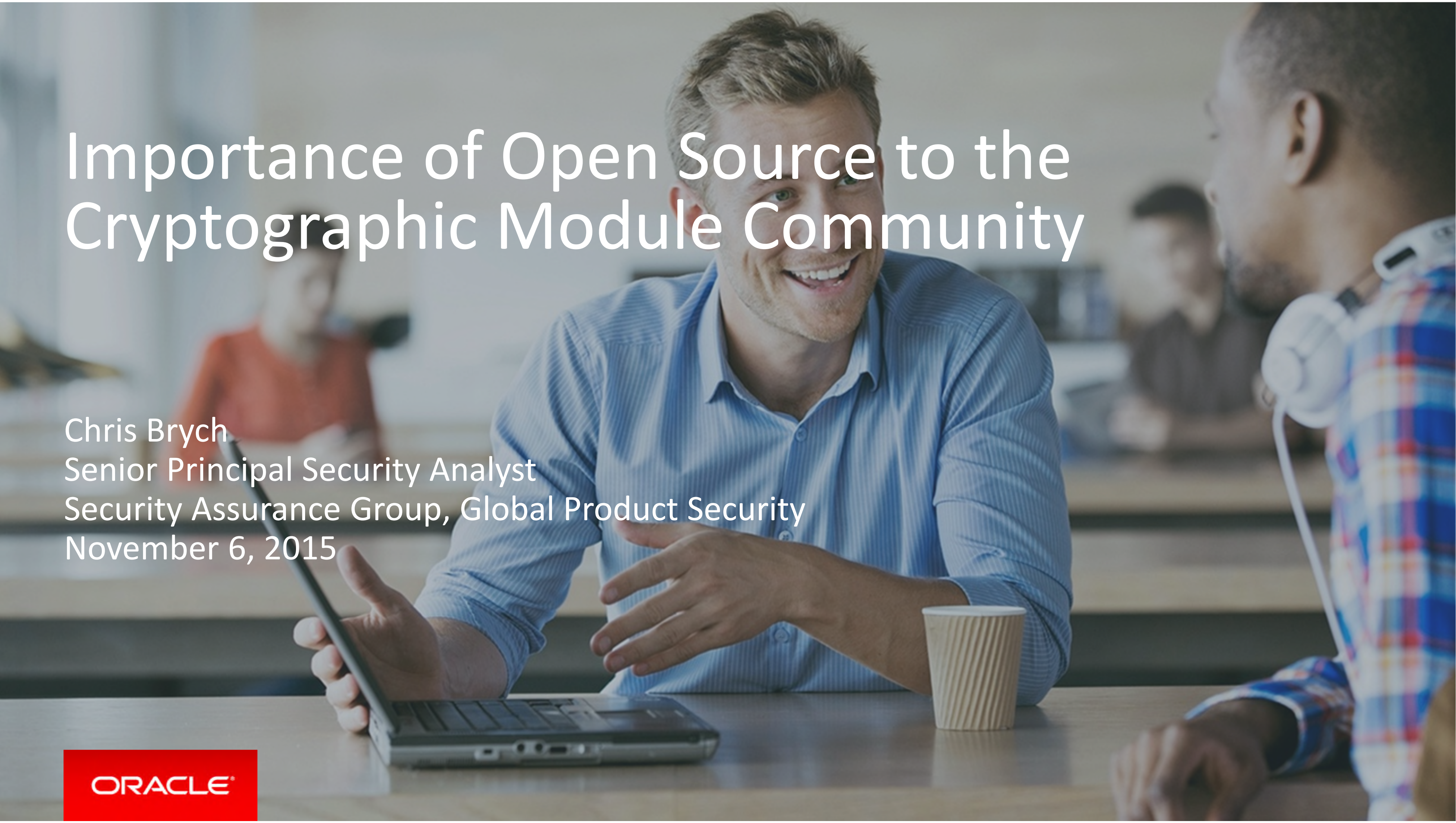


Importance of Open Source to the Cryptographic Module Community

Chris Brych
Senior Principal Security Analyst
Security Assurance Group, Global Product Security
November 6, 2015

Today’s Speaker

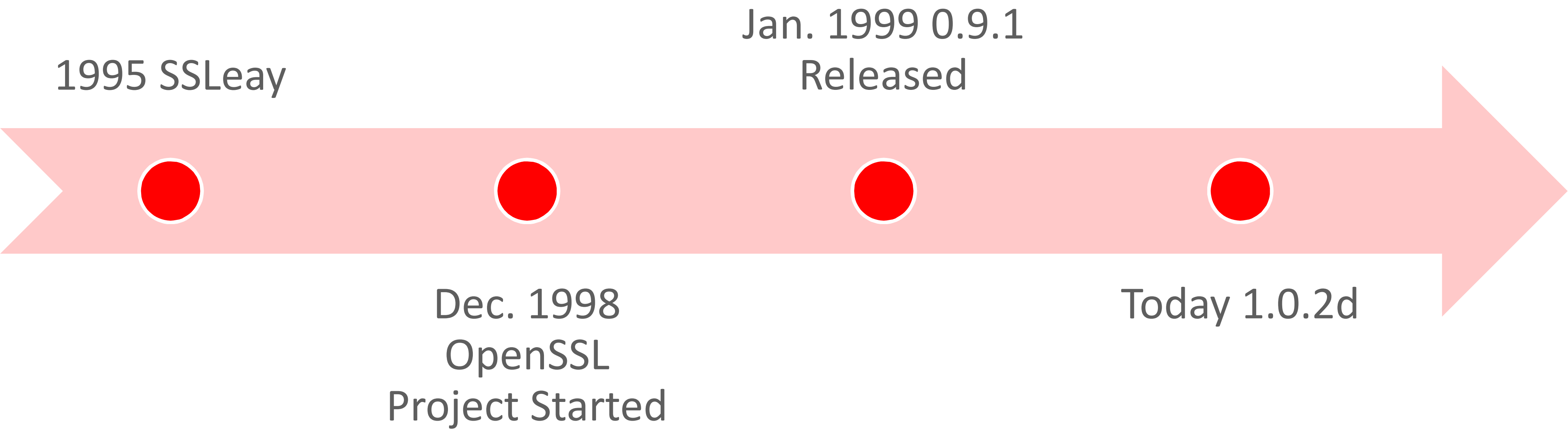
- Previous Speaker at ICMC and ICCC
- Over 15 Years Experience Working With FIPS 140 on Lab and Vendor side
- Sits on Oracle’s Crypto Review Board
- Worked With OSSI on First Open Source FIPS Certification

Chris Brych

Program Agenda

1. History of the OpenSSL and FIPS Object Module Project
2. Why Use OpenSSL FIPS Object Module
3. Advantages and Disadvantages of Using FIPS Object Module
4. Current Life Cycle of OpenSSL Distributions
5. The Future of OpenSSL and FIPS Object Module

History of the OpenSSL Project



1995 SSLeay

Dec. 1998 OpenSSL Project Started

Jan. 1999 0.9.1 Released

Today 1.0.2d

OpenSSL Project Today

15 People Globally Who Upkeep the Code

- Most of those are volunteers

Currently 2 Full-Time Paid Employees With Plans to Hire 2 More

No Direct Source of Funding

- Some private contributions
- Some donations

7,098,576 Web Servers Use OpenSSL (0.9.7 – 1.0.2)

- Does not include other application uses of OpenSSL

History of the FIPS Object Module Project

2003 Steve Marquess, Working for US DoD, Embarked on a FIPS 140 Project to Validate a Cryptographic Toolkit Derived from an OpenSSL Distribution

- Motivation was exorbitant licensing fees from 3rd party toolkit vendors
- Needed a cost effective solution

Fork Created in OpenSSL Distribution to Isolate FIPS Crypto Code Only

1. Required in order to create a means to replicate a build process of FIPS Object Module that was repeatable every time the fipscanister.o was built
2. Hash calculated over the fipscanister.o and verifying it with a hash published in the FIPS Security Policy Document guaranteed that the same code that was validated could be used to build the FOM
3. Contiguous boundary created in memory that allowed for integrity checking

History of the FIPS Object Module Project

Strategy Allowed for Maintenance of OpenSSL Distributions Without Affecting the FIPS Validation Status

- As long as the crypto code in the forked distribution didn’t change, the FOM could be rebuilt and linked into new distributions of full OpenSSL distributions (interoperable)

2006, First OpenSSL FIPS Object Module Validated

- Based on 0.9.7e distribution

Still a Lot of Work Required to Make it More Secure

Cryptographic Module Community Saw Value and Started Picking up this Code and Make Contributions to Make it More Secure

History of the FIPS Object Module Project

As OpenSSL Evolved From 0.9.7 to 0.9.8 to 1.0.0 to 1.0.1 to 1.0.2, FIPS Support Included

- Current Validation Certificate is #1747 and is supported by 1.0.0, 1.0.1 and 1.0.2 distributions

Why Use Open Source Cryptographic Modules

Cost

- Free (subject to license conditions)
- Licensing 3rd party toolkits with FIPS support costly
  - If you have deep pockets it may not be an issue but for small companies it may be an issue

Low Internal Maintenance

- Maintenance is performed by OpenSSL development team
- Engineering can focus on new development features
- New updates can be picked up and easily integrated
- Easily build on existing code base to lower development resources (compared to building new FIPS requirements from scratch)

Why Use Open Source Cryptographic Modules

Transparency in the Acceptance of Open Source

- OpenSSL has been around for quite some time and is widely deployed
  - ~7.1 million web servers use it
  - plus countless routers/switches, software application vendors, and operating systems etc.

- Many vendors stopped doing their own crypto development
  - Why re-invent the wheel when crypto is already available and you don’t have to pay for it

- Large following of organizations/developers contribute to make it better

Disadvantages of Open Source Cryptographic Module

Maintenance Out of Your Control When a Bug is Identified

- Need to rely on OpenSSL to release a fix
- Time not on your side to remediate the bug

May Need to Rely on OpenSSL to Re-certify

- Could have a business impact

One Size May Not Fit All

- Although it does suit most consumers – 80/20 rule applies

Current Life Cycle of OpenSSL Distributions

0.9.8 and 1.0.0 OpenSSL Distributions EOL December 31, 2015

- FIPS Object Module version 1.2.4, Certificate #1051, compatible with 0.9.8 distribution of OpenSSL, no longer supported
- Vendors must migrate to 1.0.1 or 1.0.2 of OpenSSL distributions to have support
- Must upgrade FIPS Object Module to version 2.0.10, Certificate #1747, supported by 1.0.1 and 1.0.2 OpenSSL distributions

Current Life Cycle of OpenSSL Distributions

1.0.1 Distribution of OpenSSL is EOL December 31, 2016

- Vendors must migrate to version 1.0.2 of OpenSSL distribution
- FIPS Object Module, Certificate #1747 is still supported by 1.0.2

Current Life Cycle of OpenSSL Distributions

1.0.2 OpenSSL Distribution is EOL December 31, 2019

- At that time, FIPS Object Module 2.0.10, Certificate #1747 no longer supported

Future of OpenSSL and FIPS Object Module

Future Implications of OpenSSL and FIPS Object Module

- Draft NIST SP 800-131A, r1 published in July, 2015 specifies transition of non-compliant DH, ECDH, and RSA in 2018
- Only FIPS validated key agreement protocols allowed

- FIPS Object Module is not fully compliant with NIST SP 800-56A/B Key Agreement
  - Only Primitives testing for ECDH completed, KDF not tested
  - Diffie-Hellman not tested as part of NIST SP 800-56A key agreement
  - RSA not compliant with NIST SP 800-56B key agreement

- Development required to bring FIPS Object Module in FIPS compliance with NIST SP 800-56A/B and NIST SP 800-131A r1

Future of OpenSSL and FIPS Object Module

Introduction of OpenSSL Distribution Version 1.1

- OpenSSL 1.1 distribution set to be released in April/May 2016
  - Rewrite of the OpenSSL code base to remove legacy code and fix bugs
  - Next generation of OpenSSL
  - API is changing so not backwards compatible with FIPS Object Module 2.0.10

Why is This a Problem?

- “FIPS Object Module and FIPS 140-2 requirements not supported in OpenSSL 1.1 distribution”

Future of OpenSSL and FIPS Object Module

Implications

- Organizations requiring OpenSSL FIPS validated crypto will have limited solutions
  - No known 3rd party FIPS 140-2 validated solutions that support OpenSSL distribution 1.1
- Vendors doing their own modification to OpenSSL
  - Many vendors do not have cryptographic developers on staff to do work
  - Making modifications of a code base containing over 500,000 lines of code very risky
  - Could introduce other vulnerabilities
  - Quality of cryptographic modules to end consumers may differ from vendor to vendor
- Money will not solve the problem
  - OpenSSL organization not interested, at this time, in providing a FIPS solution
  - A few vendors offered to provide funding to support building a FIPS module but OpenSSL organization declined

Future of OpenSSL and FIPS Object Module

How Can the Crypto Module Community Solve This

- Participation in Crypto Module User Forum Technical Committee
- Requires CMVP involvement
- Requires Government involvement

Questions?

Contact Info:

Chris Brych: chris.brych@oracle.com