

# TC-Native for Undertow

Using TC-Native library for Undertow's TLS encryption

Workshop R&D

Jocelyn Thode & Simon Brulhart



# Summary

- Undertow
- Tomcat native
- SSL/TLS protocol
- OpenSSL
- SSL encryption with Undertow
- Project Goals
- Motivation
- Conclusion

# Undertow

Undertow is a flexible performant web server integrated into **Wildfly Application Server**

It supports :

- Websockets
- Servlet 3.1

In 2014, it replaced JBoss Web Server as the Web Server for **Wildfly Application Server**

# Tomcat Native

“An optional component for use with Apache Tomcat”

- Better performance and compatibility with OS
- Access to sockets through Apache Portable Runtime (APR)
- Access to OpenSSL through APR
- Access to OpenSSL through JNI

# SSL/TLS Protocol

- Provides security when communicating over a computer network
- Makes use of public/private key pair encryption to exchange a symmetric key
- Widely used on the web
- Java implementation is **Java Secure Socket Extension (JSSE)**

# OpenSSL

- Open source implementation of SSL/TLS protocol
- Written in C
- Works on almost all platforms
- Many vulnerabilities (POODLE, Heartbleed, etc.)

# SSL Encryption with Undertow

- Undertow is using **JSSE** for SSL/TLS
- Some work done to use OpenSSL via **JSSE** API

# Project Goals (1)

Modify Tomcat Native

This means :

- Study Tomcat Native, Undertow and the current OpenSSL experiments for Undertow
- Remove APR code used to load OpenSSL in Tomcat Native
- Abstracts Tomcat Native so that it can also be used in Undertow instead of JSSE
- Run benchmarks to measure performance



# Project Goals (2)

<TODO DIAGRAM>



# Motivations (1)

- APR has a lot of C code and is hard to maintain
- Undertow is using JSSE which performs poorly
- OpenSSL is efficient, active and cross-platform

Using Undertow directly with OpenSSL should perform better and be easier to maintain

# Motivations (2)

MAYBE ADD DIAGRAM THROUGHPUT DIFFERENT CONNECTORS

# Conclusion

The main challenges of this project will be :

- Understand the different projects and how they work together
- Adapt Tomcat Native and Undertow to work with OpenSSL

# Questions

