Do Developers Update Their Library Dependencies?  
An Empirical Study on the Impact of Security Advisories on Library Migration  
Raula Gaikovina Kula1,2, Daniel M. German3, Ali Oun1,4, Takashi Ishio1,2, Katsuro Inoue4  
Nara Institute of Science & Technology1, Osaka University2, University of Victoria3, UAE University4

Motivation
Many software projects today advocate the use of third-party libraries because of its many benefits. Our motivation stems from reports of outdated and vulnerable libraries being widespread in the software industry.

▶ In 2014, Sonatype determined that over 6% of the download requests from the Maven Central repository included known vulnerabilities.

The goal of our study is to investigate (1) whether or not dependencies are being updated and (2) the level of developer awareness to dependency migration opportunities such as fixing security vulnerabilities.

Research Questions
▶ Tracking Library Migration in Practice
  ▶ RQ1: To what extent are developers updating their library dependencies?
  ▶ Developer Responsiveness to Awareness Mechanisms
  ▶ RQ2: What is the response to important awareness mechanisms such as a new release announcement and a security advisory on library updates?
  ▶ RQ3: Why are developers non responsive to a security advisory?

Library Migration & Awareness Mechanisms
▶ Tracking System & Libraries: We define a model of system and library dependency relations. Hence, we formally use the following notations. We define S for a system, and L for a library. L(lib,v) denotes version v of a library lib, and S(sys,w) for version w of a system sys.

▶ Effectiveness of Awareness Mechanisms: We propose a Library Migration Plot (LMP) to visualize impact of awareness mechanisms such as a security advisory.

Conclusions
Although third-party library dependencies is widely practiced, we find that updating is not:
▶ The study provides motivation for our community develop strategies to improve a developer personal perception of third-party updates.
▶ Visual aids such as the Library Migration Plots (LMP) could prove useful awareness and motivation for developers quickly update.
▶ Future work include understanding how developers perceive migration effort and understand responsibilities when using a third-party library dependency.

Replication Dataset
We make available our dataset of 852,322 library dependency migrations at