Web API Misuse Detection in JavaScript Web Applications

SungGyeong Bae
KAIST
imai0917@kaist.ac.kr

Hyunghun Cho
Samsung Electronics
hyunghun.cho@samsung.com

Sukyoung Ryu
KAIST
sryu.cs@kaist.ac.kr

Introduction
Web applications are prevalent thanks to the dynamic nature of JavaScript. However, because of the extreme freedom of JavaScript developers, it is very difficult to define and detect errors in JavaScript web applications. To mitigate the problem, various platform vendors provide Web APIs[1] in Web IDL for JavaScript developers. We present a technique to statically analyze Web APIs and JavaScript web applications that use Web APIs and to detect possible misuses in them.

JavaScript[2]
• Scripting language
• Prototype-based object-oriented language
• Functional language
• Dynamic language
• Implicit type conversion

Web IDL[3]
• Web Interface Description Language
• Web IDL specifies interfaces and types
• Web IDL has rich types (dictionary, enumeration, callback, …)

Methodology
Extend SAFE(Scalable Analysis Framework for ECMAScript)[4, 5]
• Web IDL parser to parse Web APIs
• Platform object that implements every interface defined in Web APIs
• Mock-up objects that model Web IDL types
• Callback function invocation that models Web API functions
• Web API misuse detection by using analysis results

Reference