CRII: SaTC: A Language-based Approach to Hybrid Mobile App Security

(NSF CNS #1566321)

Meera Sridhar
University of North Carolina Charlotte

Background and Motivation

More than 70 Hybrid app frameworks available

Combines the best of both the worlds (Native and Web)

Reduced development cost across multiple platforms

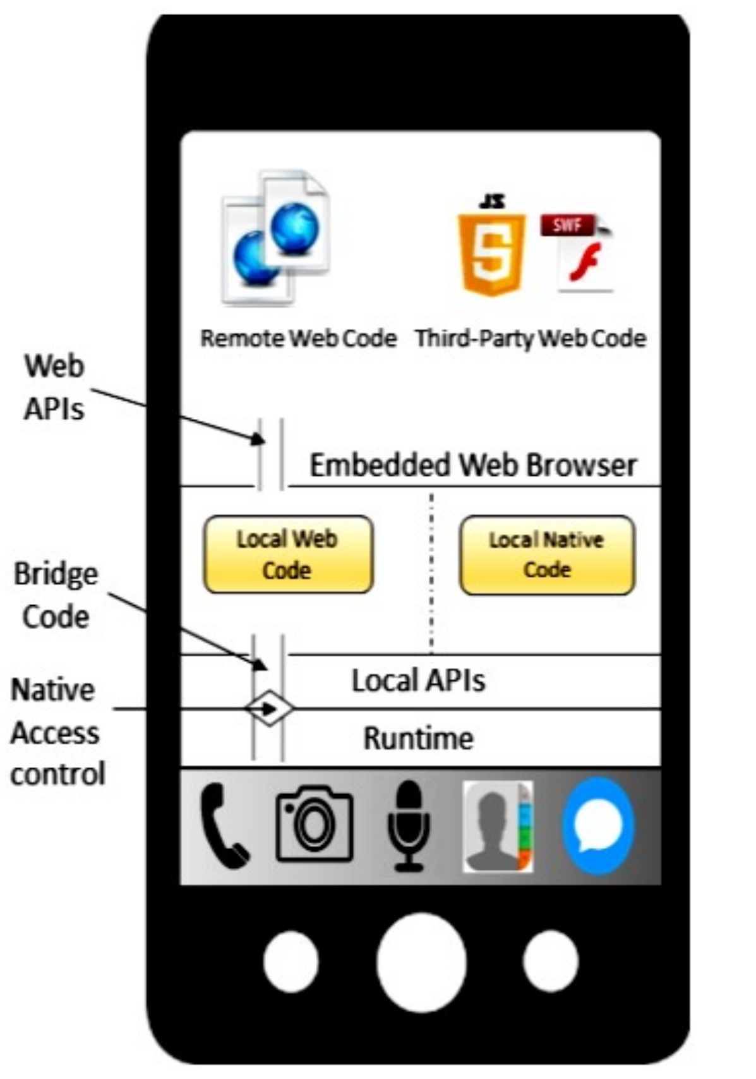


Diagram follows the format of: [Georgiev et al.,WWW,2015]

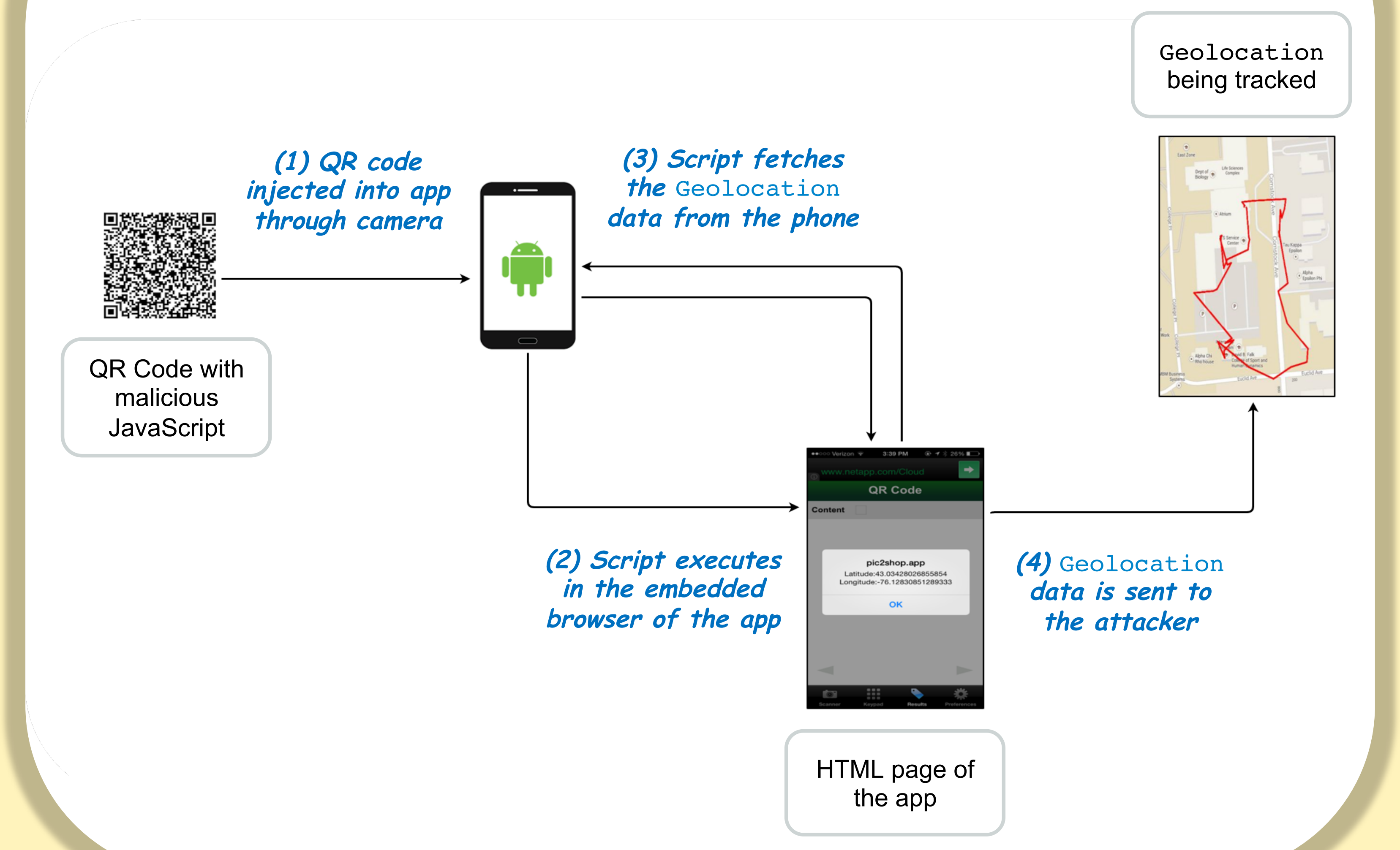
65% Enterprise IT Decision makers prefer hybrid mobile app

REACT NATIVE Facebook's JavaScript library promotes developing using Hybrid frameworks

Write Once Run Anywhere

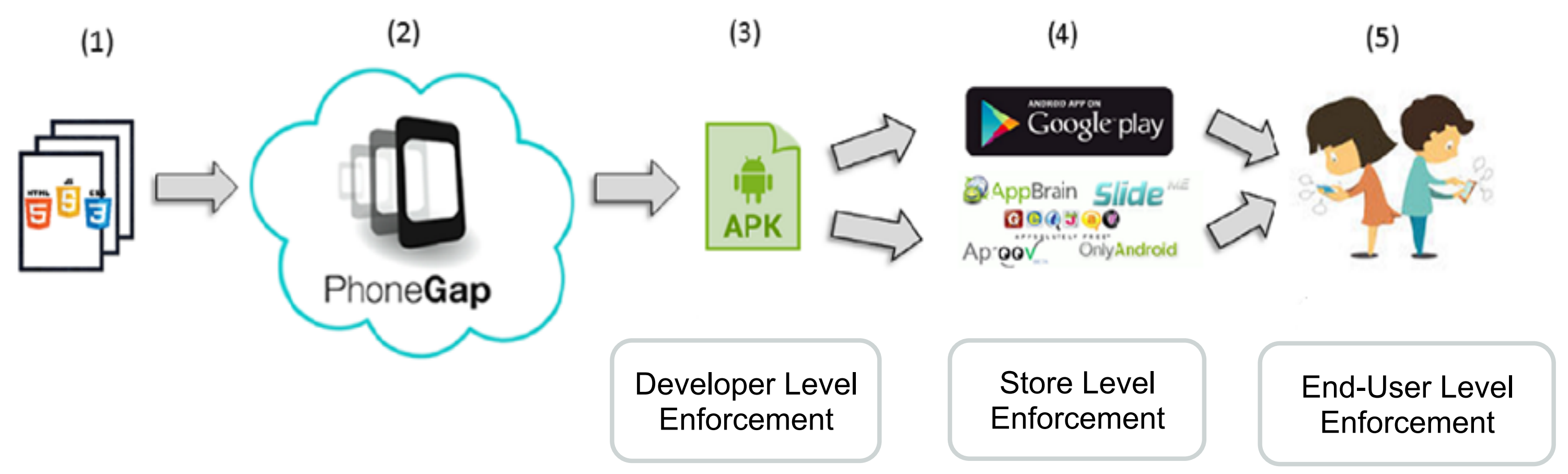
Some famous hybrid apps: Amazon App store, Twitter, Apple app store, Gmail, Instagram, Uber

pic2shop Code Injection Attack [Jin et al.,CCS,2014]

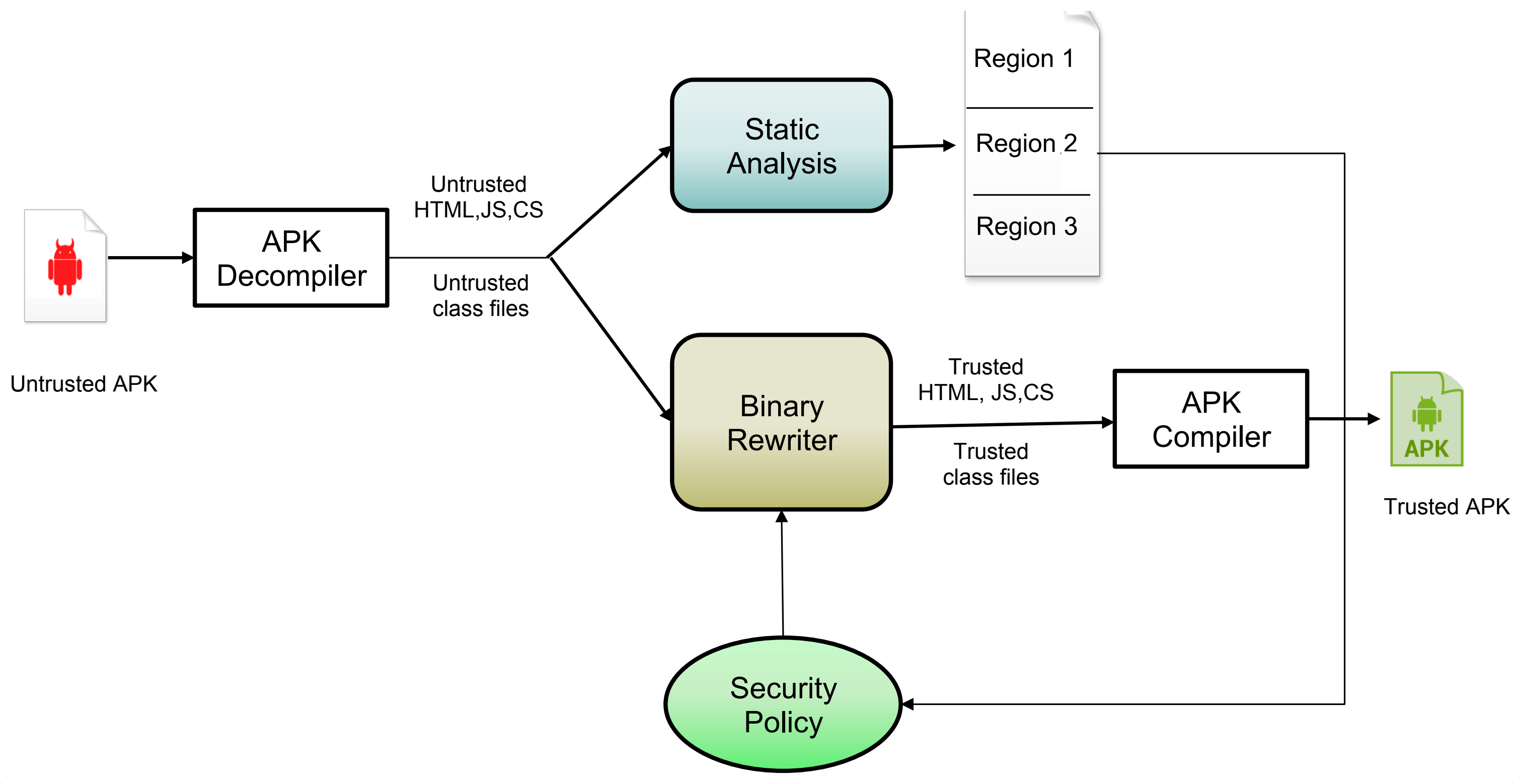

Geolocation being tracked
(1) QR code injected into app through camera
(3) Script fetches the Geolocation data from the phone
QR Code with malicious JavaScript
(2) Script executes in the embedded browser of the app
(4) Geolocation data is sent to the attacker
HTML page of the app
QR Code
Content
pic2shop.app
Latitude:43.03428026855854
Longitude:-76.12830851289333
OK

Approach: Language-based Enforcement through In-lined Reference Monitoring

High Level Enforcement Plan



Technical Implementation Sketch



Scientific Impact

- **Security policies**:
  - Systematic mapping of hybrid attack surface
  - establishing security policy class targeting effective language – based enforcement
  - important research objective: define limitations of security policies enforceable by runtime monitoring
- **Runtime monitoring design and implementation challenges**:
  - effective complete mediation
  - effective tamper-proofing of monitoring system in complex, cross-platform environment
- **Infer fine-grained permissions-regions for pages in the app**:
  - design a static-analysis algorithm
  - permissions regions will:
    - improve bridge access granularity
    - serve as security policy models for integration into monitoring framework

Broader Impact

- **Mobile app security a pressing social responsibility**:
  - 2 billion smartphone users globally today, including children!
  - Proposed research will mitigate a class of dangerous vulnerabilities in smartphones today.
- **Case studies, practical examples, research experience**:
  - graduate-level courses, research seminar on hybrid app security.
  - MS, Certificates in Cyber-Security at UNCC.
  - curricula specifically targeted for the Women in Computing initiative at UNCC
- **University-Industry collaborations in mobile security research:**
  - PI active member of NSF/UCRC UNCC in Charlotte Metropolitan area
  - members include major financial institutions
  - Charlotte also home to major energy, healthcare industries

Related Work

Detecting/Mitigating Code Injection Attacks
- Code-injection attacks in hybrid apps introduced; new channels e.g., barcode scanner, messages, NFC [Jin et al.,CCS,2014]
- New code-injection channel; malicious script injected using HTML5 text box input type paired with `document.getElementById(”TagID”).value`. [Chen et al.,TRUSTCOM,2015]
- new code-injection type; JS encoded in human-unreadable format [Xiao et al.,CBD,2015]
- mitigate code injection attacks by generating behavior state machines of the app [Xiao et al.,CBD,2015]

Access Control and Permission-based solutions
- page-level access control [Shehab & AlJarrah,MobileDeli,2014], frame level access control [Jin et al.,ISC,2015], context-aware permission control system [Singh,RAID,2013]
- RestrictedPath browser & system level enforcement; sees if app deviates from intended path [Pooryousef & Amini,ISCISC,2016]

Information Leaks
- Static analysis of inter-communication between Java & JS to determine programming errors [Lee et al.,ASE,2016]

Detecting Over-privilege
- MinPerm extracts and compares required and requested permissions from hybrid app APKs [Mao et al.,Journal of High Speed Networks,2016]

Please contact PI Sridhar at msridhar@uncc.edu for more information.

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
Jan. 9 – 11th 2017,
Arlington, VA

UNC CHARLOTTE