RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: MBS-R02

Mobile App Security Mandates Identity, Authenticity and Trustworthiness

Christopher Hockings

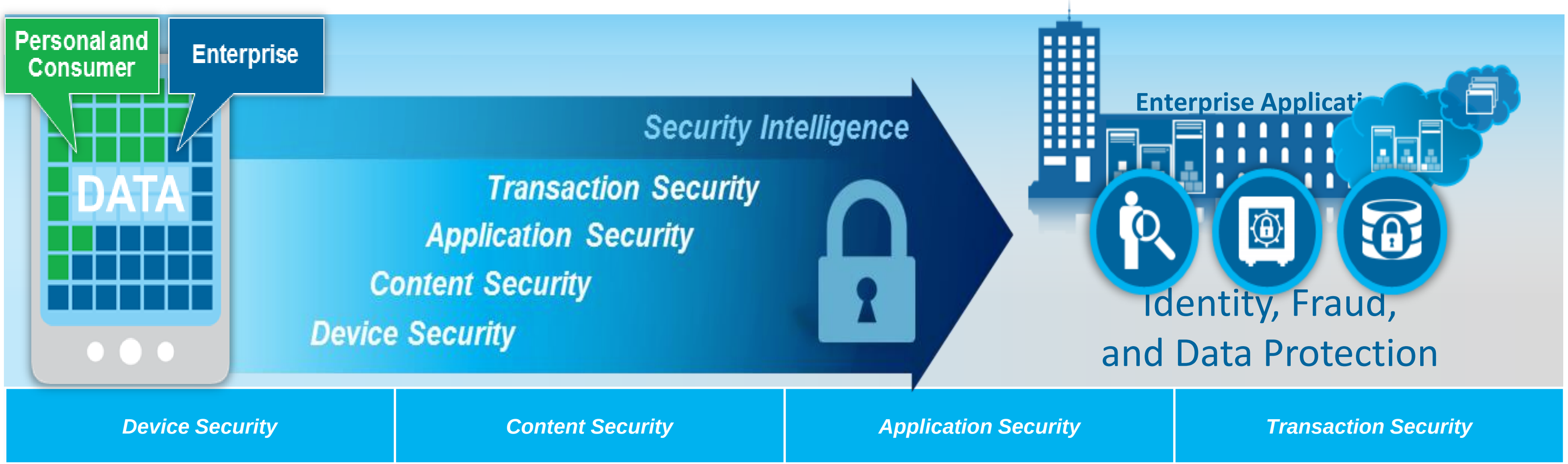
Master Inventor
IBM Security
@chockings

Session Objectives

- Introduce the mobile threat domain
- Discuss traditional internet solution components
- Explain the three focus domains for delivering a secure mobile app
  - Identification of the user
  - Trustworthiness of the device
  - Authenticity of the app code
- Live demonstration of integrated solutions for the focus domains
- Actions for takeaway for your business

Breadth of Mobile Security Domains

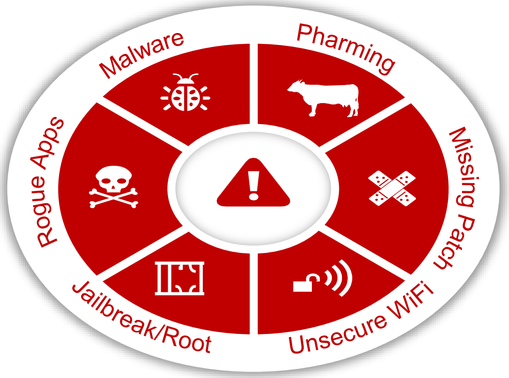
Focus of the session today at this end



Introducing New Mobile Threats

Mobile Banking Fraud Vectors

Compromised and Vulnerable Devices

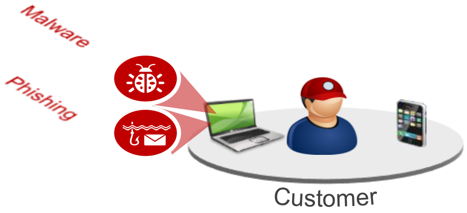


Jailbroken/rooted devices susceptible to suspicious apps, malware

Account Takeover via a Mobile Device

Web-based device ID isn't effective on a mobile device

Cross-Channel Credential Theft

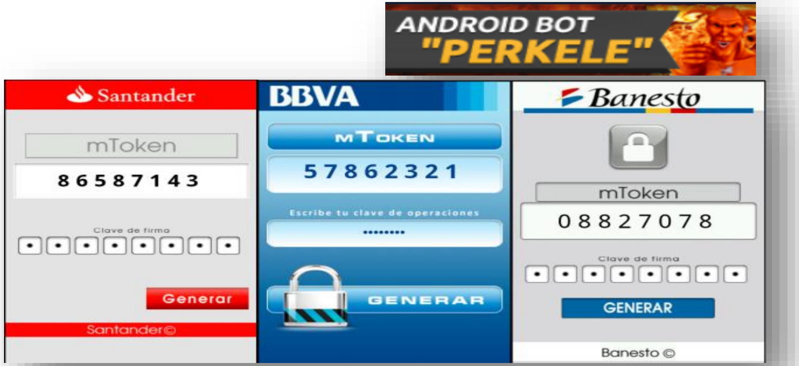


Malware and Phishing credential theft from the desktop enable mobile fraud

Mobile Malware and Suspicious Apps

- SMS Interceptors (only when relevant)
- Device rooters
- Data stealers
- Generic downloaders
- Key-loggers

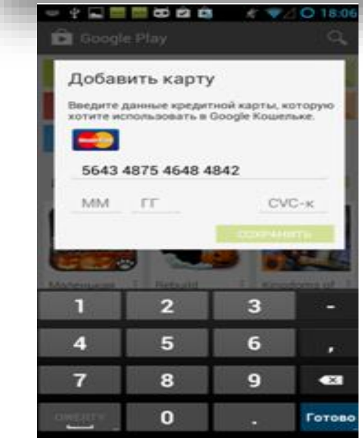
- Android risk is higher due to multiple, not Google-controlled, marketplaces

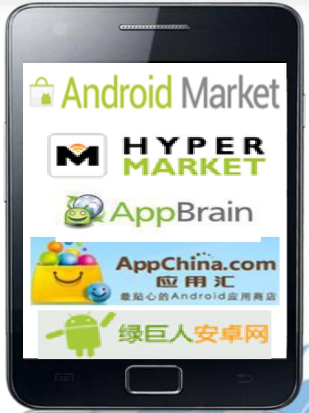

ANDROID BOT "PERKELE"

Santander
mToken
86587143
Clave de firma
Generar
Santander©

BBVA
mToken
57862321
Escribe tu clave de operaciones
••••••••
GENERAR

Banesto
mToken
08827078
Clave de firma
GENERAR
Banesto ©


Google Play
Добавить карту
Введите данные кредитной карты, которую хотите использовать в Google Кошельке.
5643 4875 4648 4842
MM ГГ CVC-к



Mobile App Code is Vulnerable to Attacks

Integrity Risk

(Code Modification or Code Injection Vulnerabilities)

- Application binaries can be **modified**
- **Run-time behavior** of applications can be altered
- **Malicious code** can be injected or hooked into applications

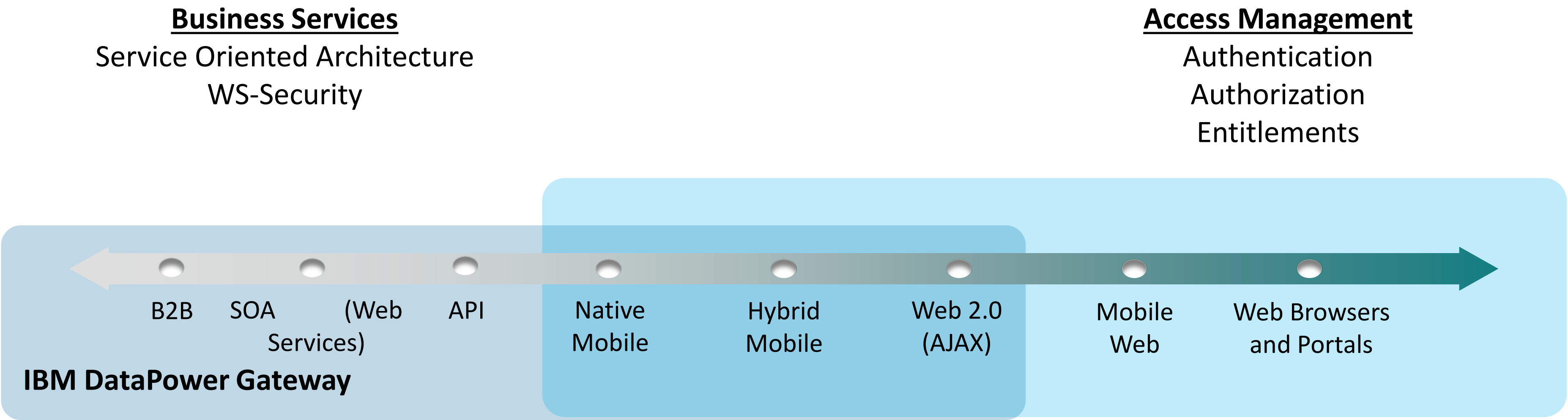
Confidentiality Risk

(Reverse Engineering or Code Analysis Vulnerabilities)

- **Sensitive information** can be exposed
- Applications can be reverse-engineered back to the **source code**
- Code can be lifted and **reused or repackaged**

Market State and Transformation Challenges

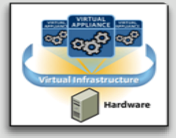
Traditional Solutions are Adapting to APIs



- AJAX has emerged to address (1) complexity of SOA implementations; and (2) corruption of browser HTTP/HTML

Broad Range of Security Expectations

1. Web Application Firewall

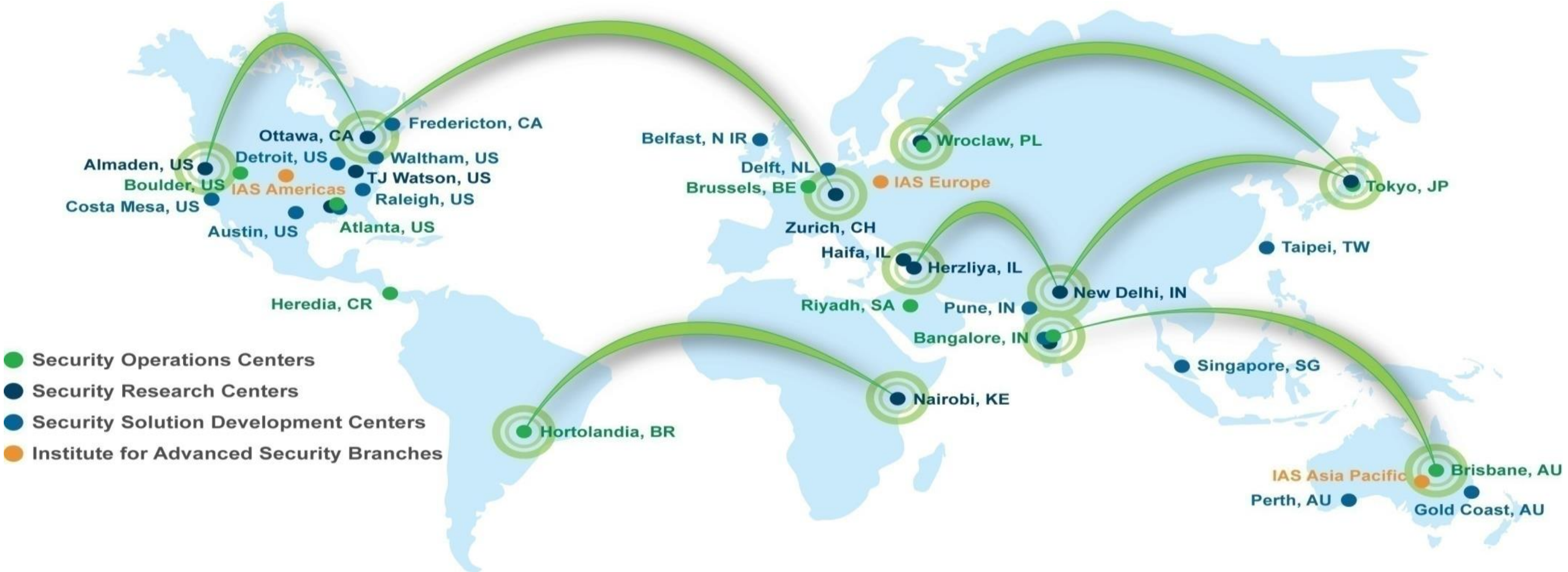


2. XML Schema Validation and Scoped Access Control

3. Context Based Authorization and Authentication

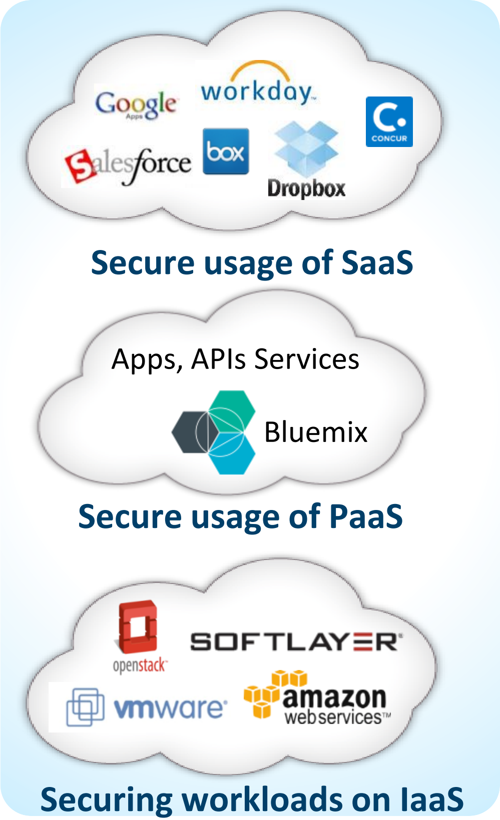
4. Device based Threat Detection

Global Collaboration is Required



- **Global network to provide intelligence to respond to Present Threats**

Deployable to Cloud Infrastructure



Secure usage of SaaS

Apps, APIs Services

Bluemix

Secure usage of PaaS

Securing workloads on IaaS

- Continuous deployment
- Elastically scalable
- Turn-key solutions
- Low Maintenance cost
- API and Mobile ready

Mobile: Realization of Strategy

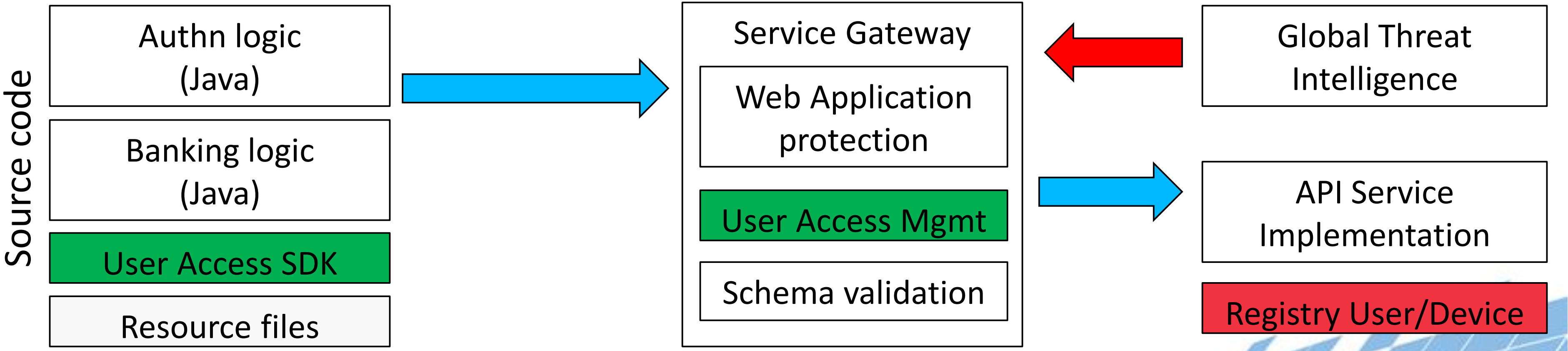
Identity the user on their device

Check Platform Trustworthiness

Ensure App is Legitimate

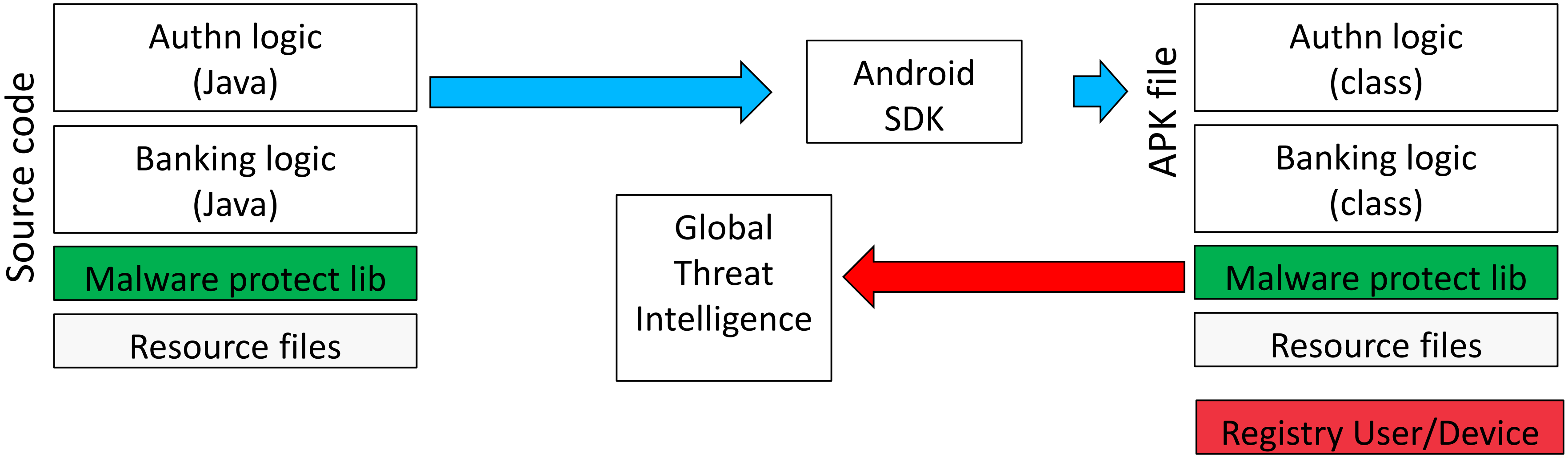
Identity the user on their device

- Adopt Multi-factor authentication solutions
  - E.g. U/P Conversion to token/PIN number, Integrated One-Time-Password flow
- Ensure Device is bound to authenticating User at run-time
- Authorization considers combination of App, Device and User



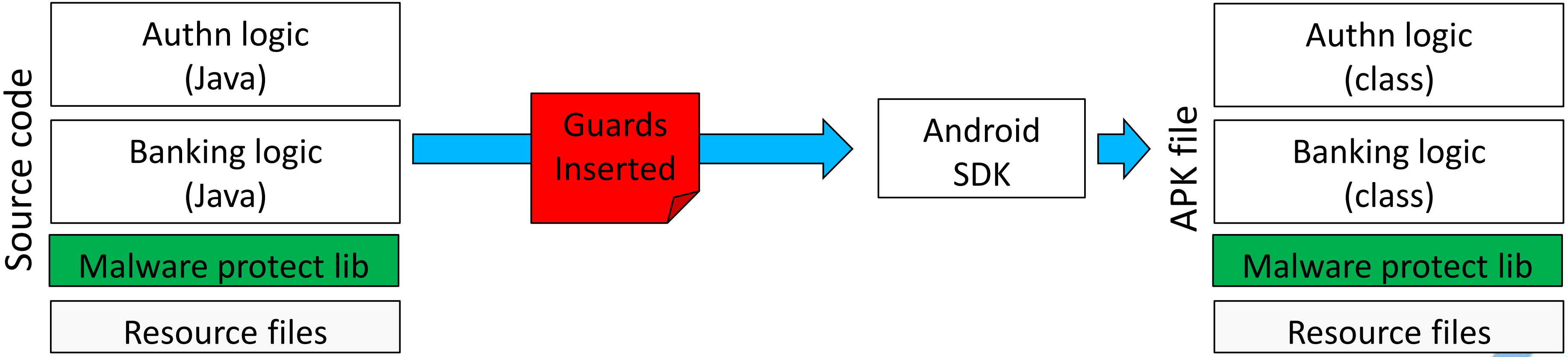
Checking Platform Trustworthiness

- Device Malware infected or jail broken, installed Apps trustworthy
- Has User account has been subject to successful account phishing?



Ensure App is Legitimate

- Ensure Code has not been compromised through
  - Reverse engineered, Recompiled
- Solutions exist that provide encryption, protection layers added as part of the Software deployment and build process

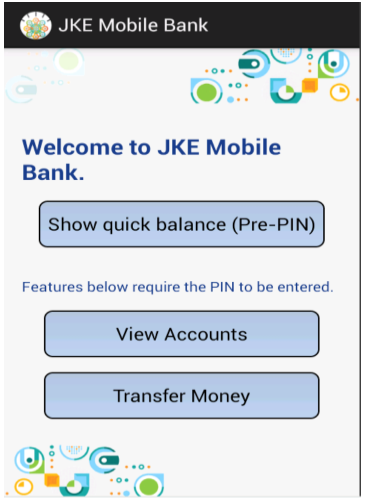


Demonstration:

Native App Banking Use Case with Malware

Demonstration Use Cases

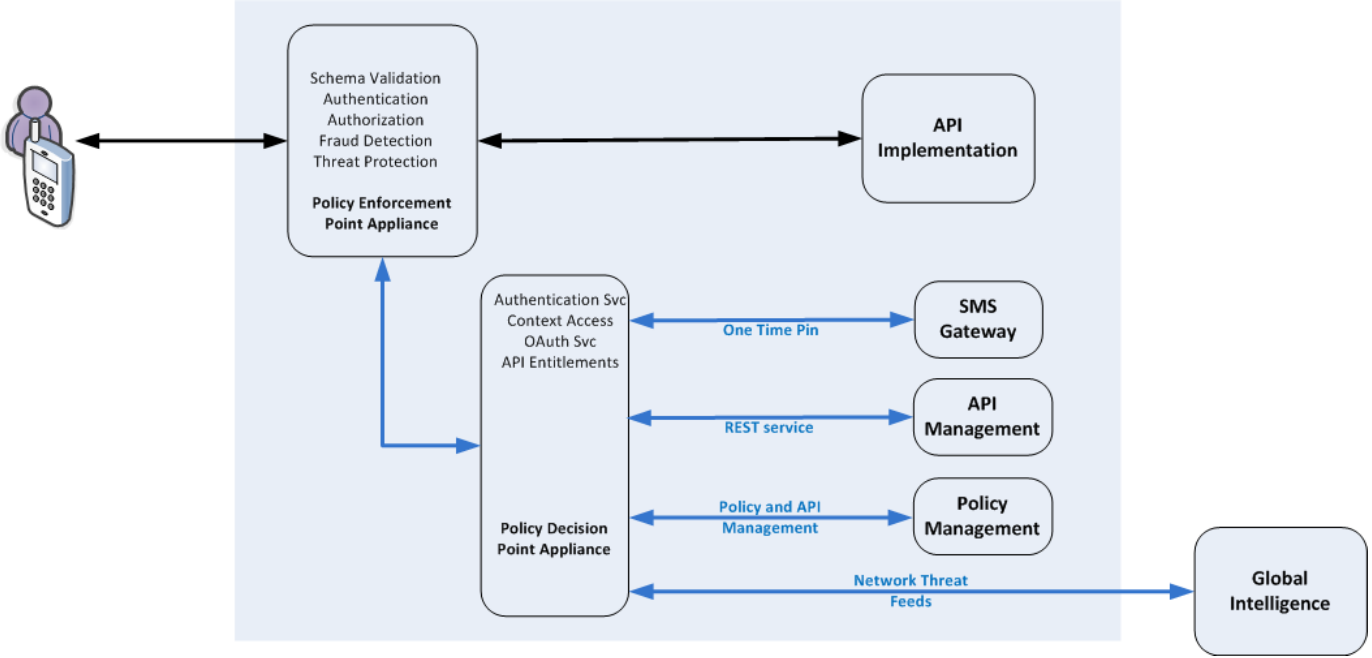
- Android Native Mobile App that demonstrates the end to end security requirements
  - **User registration** and **two factor authentication**
    - username/password = Token+PIN
  - Server side **policy based authorization**
  - Leveraging Access features to support **Native API integration**
  - **Device fingerprinting**
  - API integrated to ensure **App authenticity verification**
- Preventing Fraud by using policy based detection of **Mobile Malware present** on the device


JKE Mobile Bank

Welcome to JKE Mobile Bank.

Features below require the PIN to be entered.

Cloud Deployed Demonstration Environment



- Deployed within IBM Softlayer as a set of virtual appliances

Call to Action

- Does your Security technology and processes contain such controls…
- Are you relying on technology that doesn’t integrate…
- Are your competitor Apps out competing yours…
  - Through non functional aspects such as speed to market, performance
- Do you have a reliable vendor that relies on global intelligence data to make meaningful threat decisions…
- Are your API teams talking to your Security teams…