intel

Intel European Research & Innovation Conference 2013

incorporating Research@Intel Europe

Nice, France
October 22 & 23

Mobile Security and Privacy

Alexandra Dmitrienko
Cyberphysical Mobile Systems Security Group
Fraunhofer SIT, Darmstadt
Center for Advanced Security Research in Darmstadt (CASED)

Fraunhofer SIT

TECHNISCHE UNIVERSITÄT DARMSTADT

CASED

Smartphone is Your Best Freind !

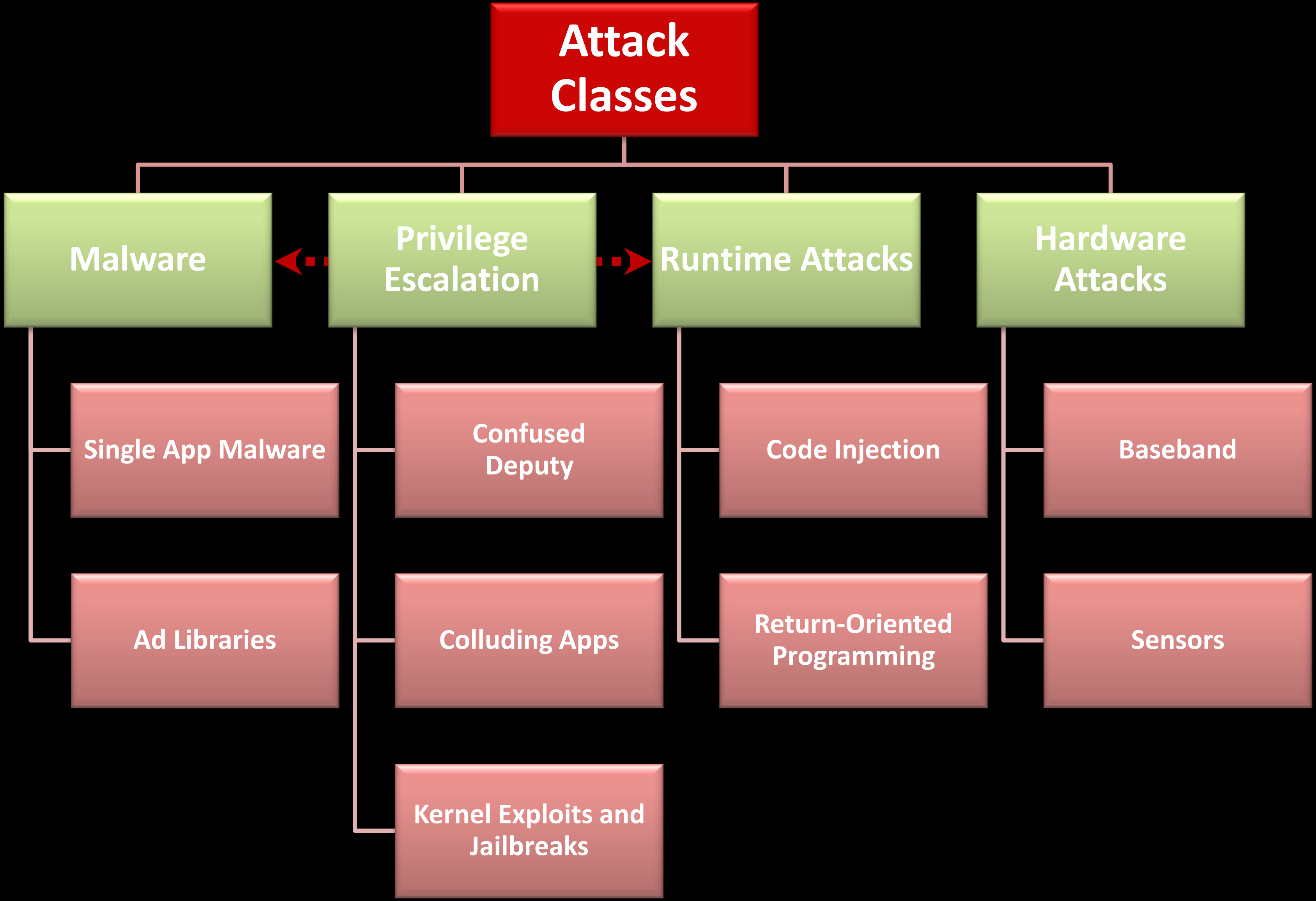
Nomophobia:
New Epidemic of Smartphone Addiction

An App for Every Wish….

Large Attack Surface

- Millions of Apps available today
- Developed by thousands of different developers

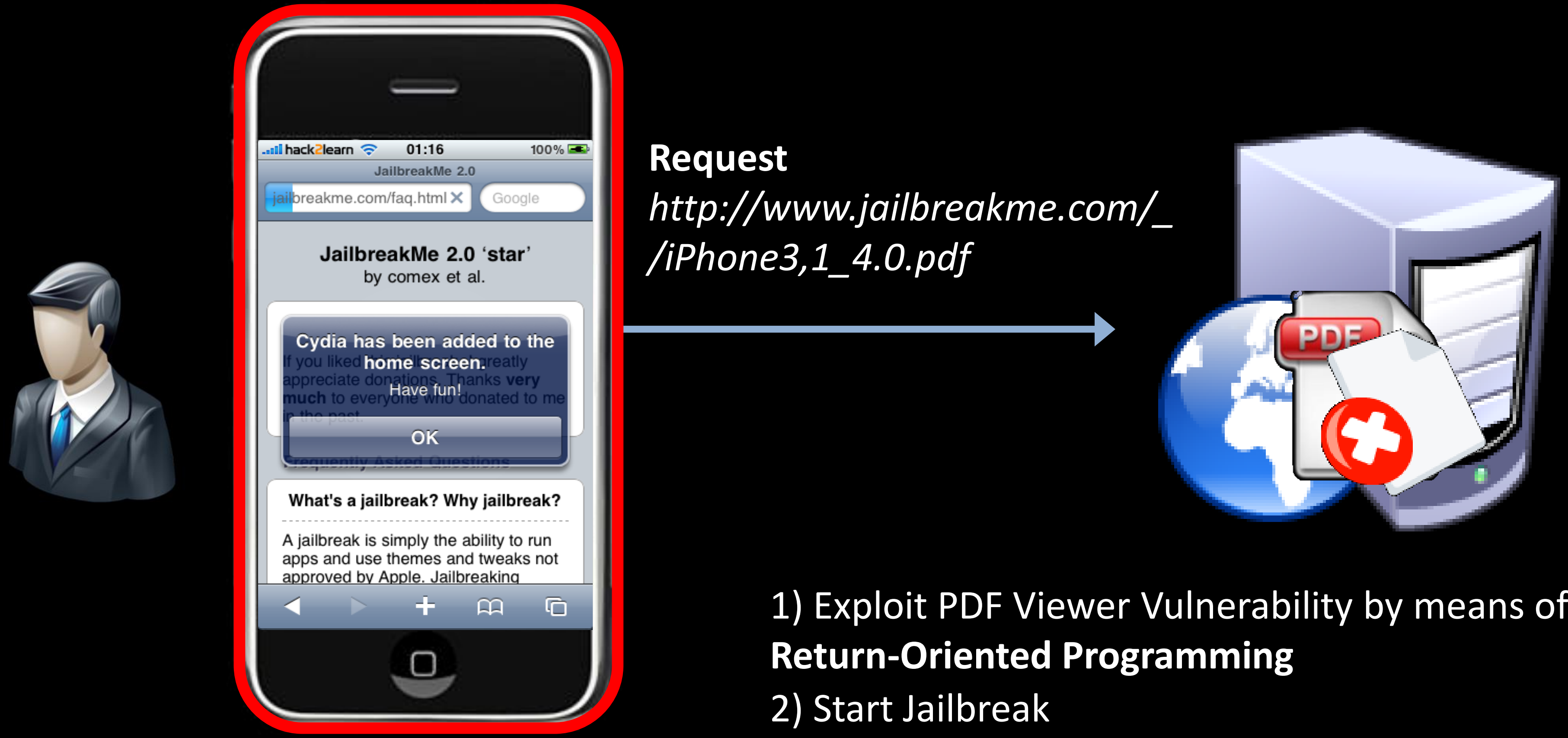
Attack and Threat Classification



Let‘s Start with Some Attacks

Apple iPhone Jailbreak

Disable signature verification and escalate privileges to root



JailbreakMe 2.0 'star'
by comex et al.

Cydia has been added to the home screen.

Have fun!

What's a jailbreak? Why jailbreak?

A jailbreak is simply the ability to run apps and use themes and tweaks not approved by Apple. Jailbreaking

Request

http://www.jailbreakme.com/_ /iPhone3,1_4.0.pdf

1) Exploit PDF Viewer Vulnerability by means of **Return-Oriented Programming**

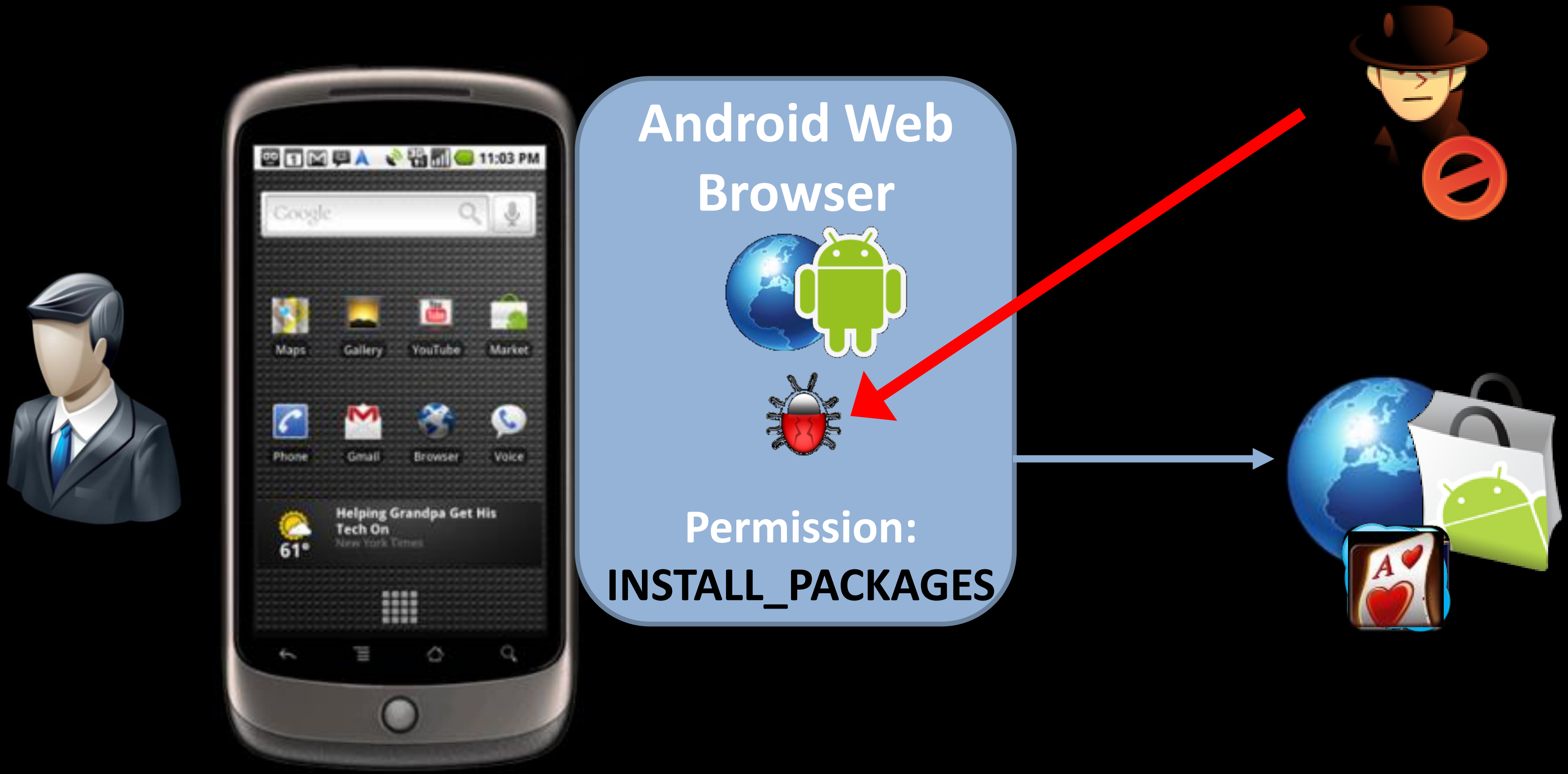
2) Start Jailbreak

3) Download required system files

4) Jailbreak Done

Google Android:

Install arbitrary applications without the users knowledge



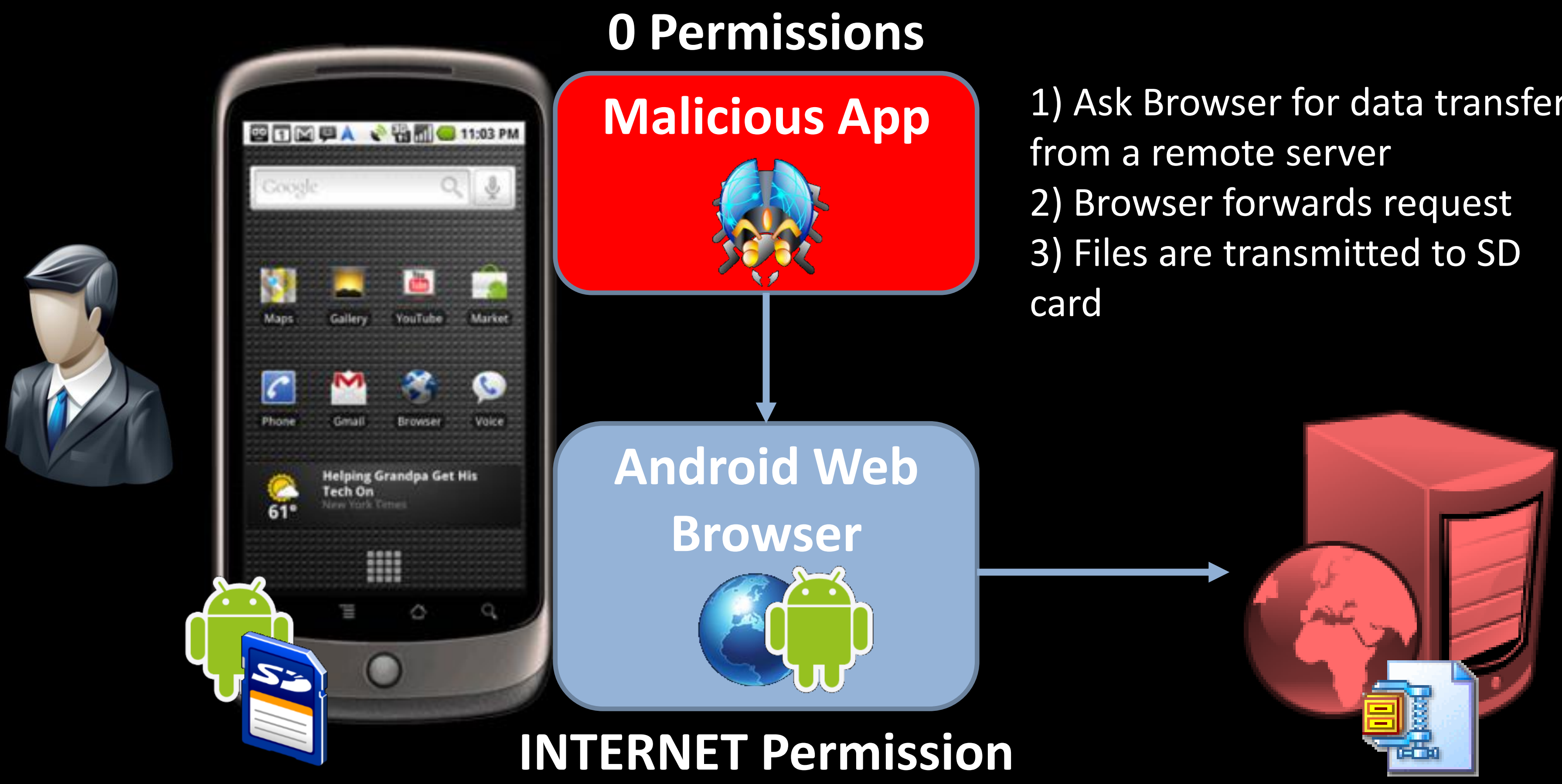
Android Web Browser

Permission: INSTALL_PACKAGES

1) Exploit Bug in web Browser
2) Enforce the installation of various apps

Confused Deputy Attack:

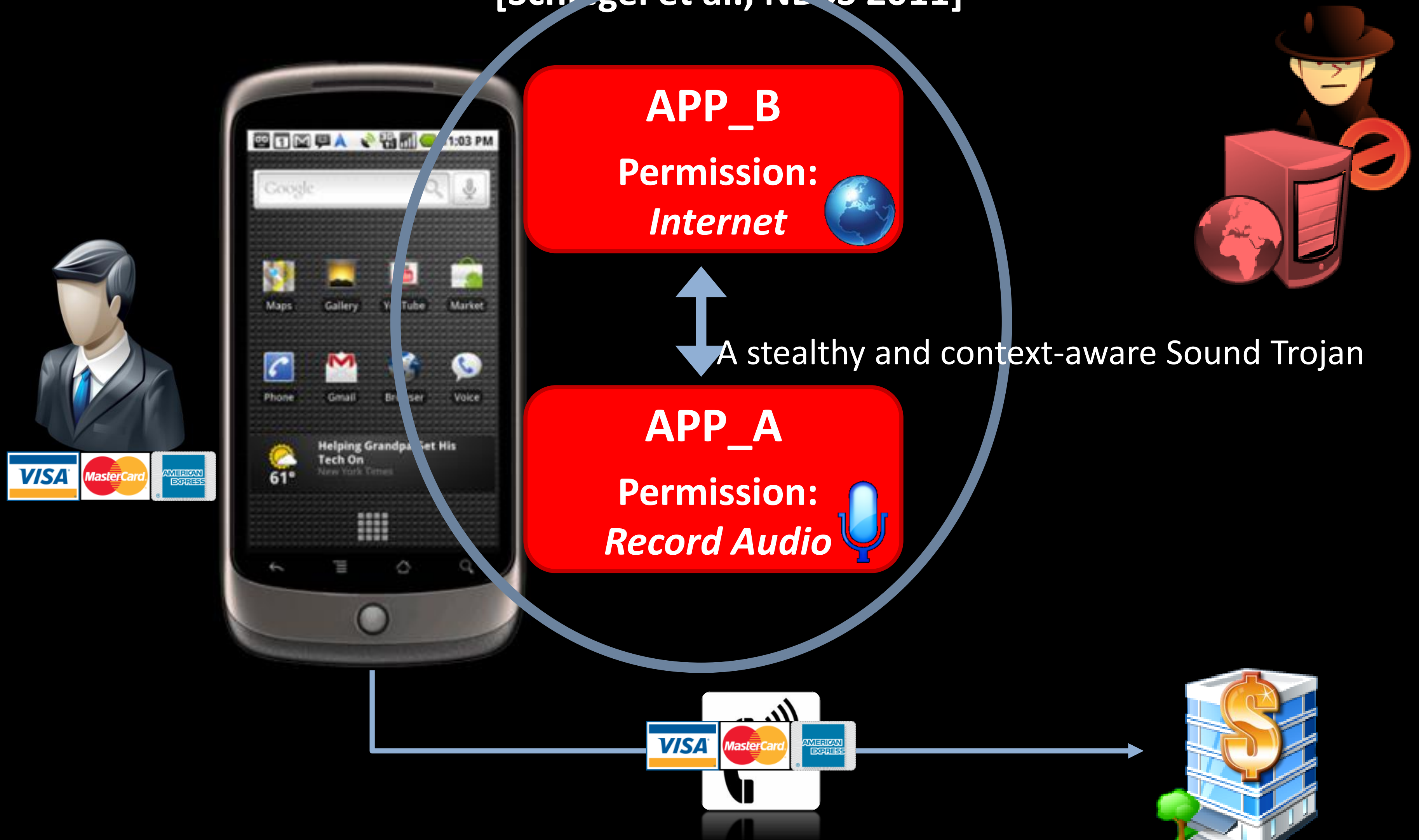
Internet access without INTERNET Permission



1) Ask Browser for data transfer from a remote server
2) Browser forwards request
3) Files are transmitted to SD card

Collusion Attack: Soundcomber

[Schlegel et al., NDSS 2011]



APP_B

Permission: *Internet*

APP_A

Permission: *Record Audio*

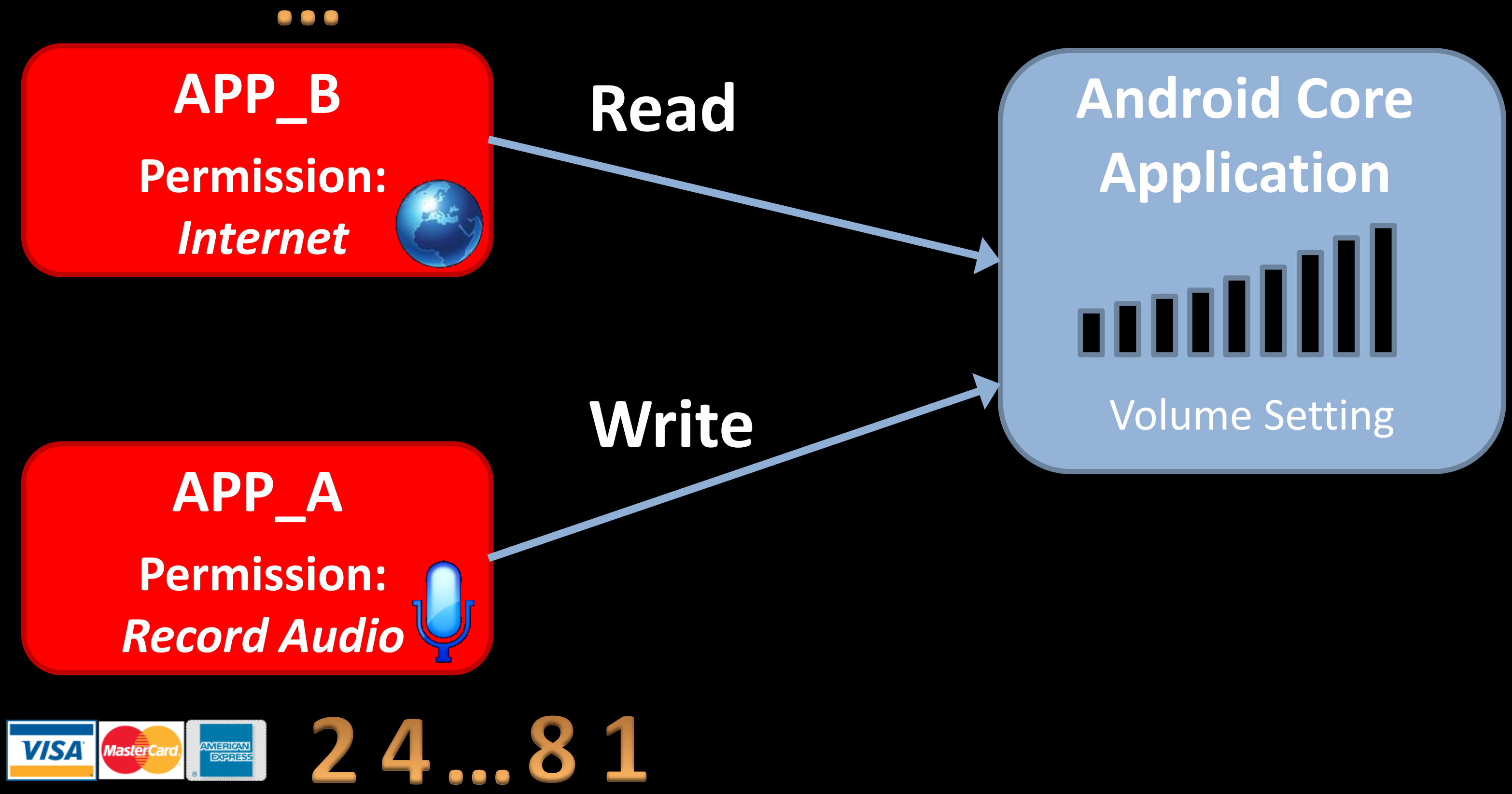
A stealthy and context-aware Sound Trojan

1) Call Credit Institute

2) Credit Card Number is extracted from the speech

Soundcomber Internals

Exploiting Covert Channels in Android

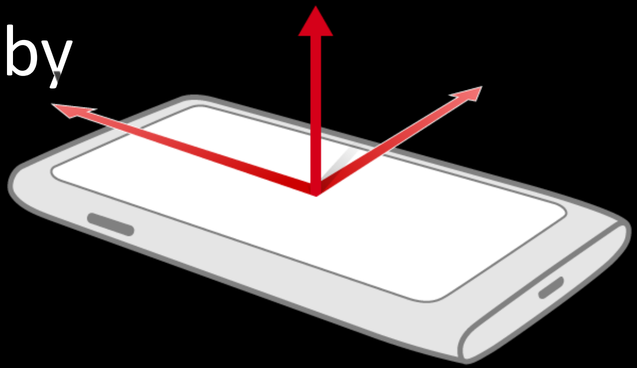


Additional covert channels are vibration, screen lightening, or file locks, see also [Marforio et al., TechReport 2011, ACSAC 2012]

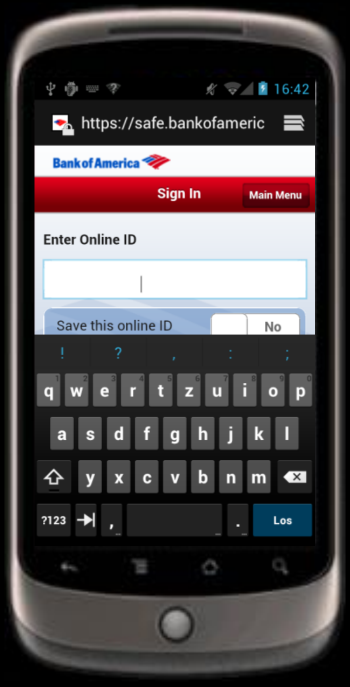
Sensoric Malware: TapLogger / TouchLogger

Infer user's input to virtual keyboard by measuring the accelerometer and gyroscope during typing

[Xu et al., WiSec 2012; Cai et al., HotSec 2011]



http://devfiles.myopera.com/articles/9472/device-gamma.png



16:42

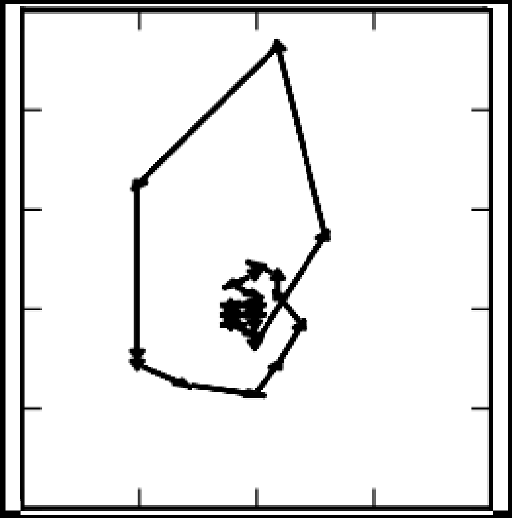
https://safe.bankofameric

Bank of America

Sign In | Main Menu

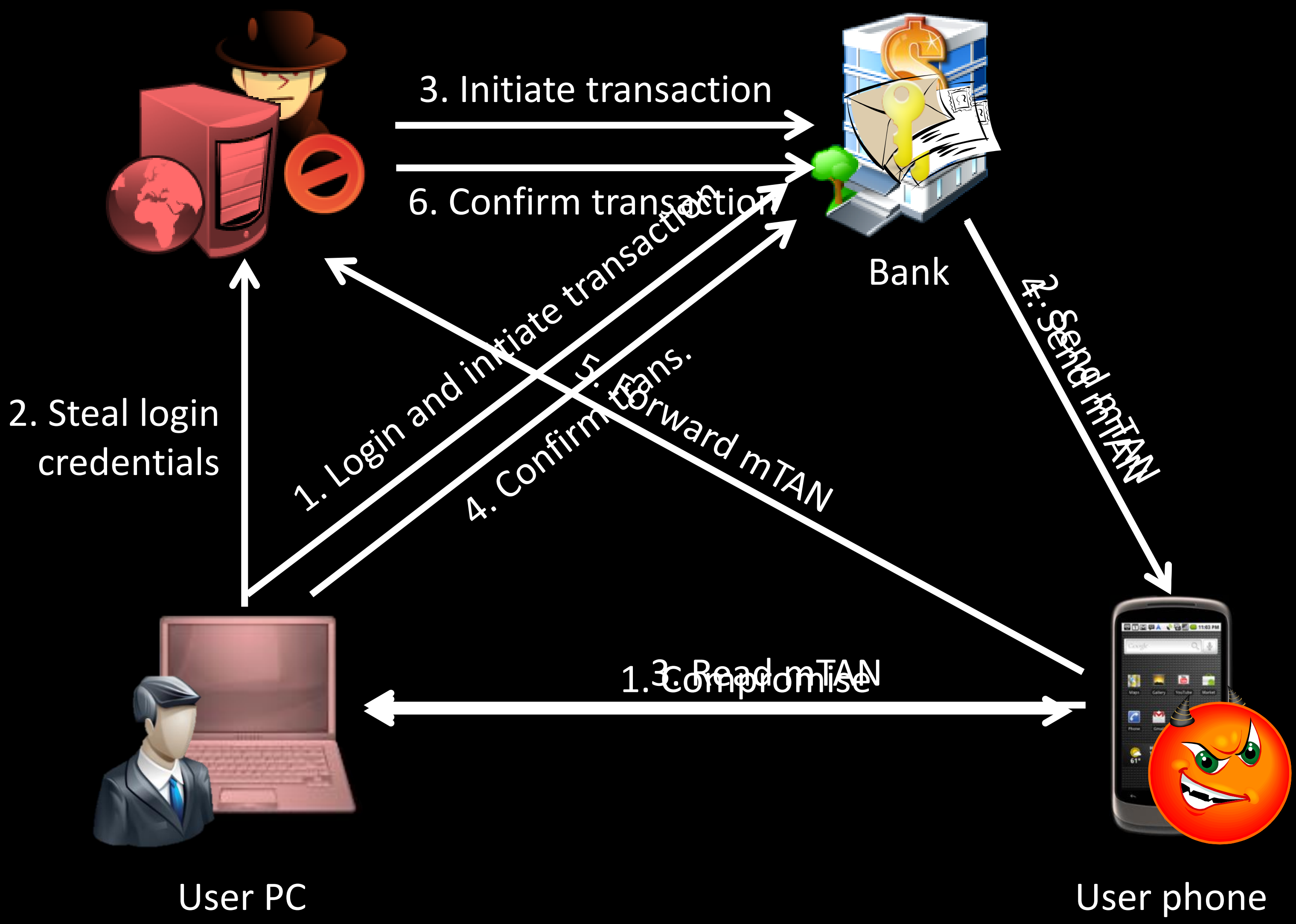
Enter Online ID

Save this online ID | No

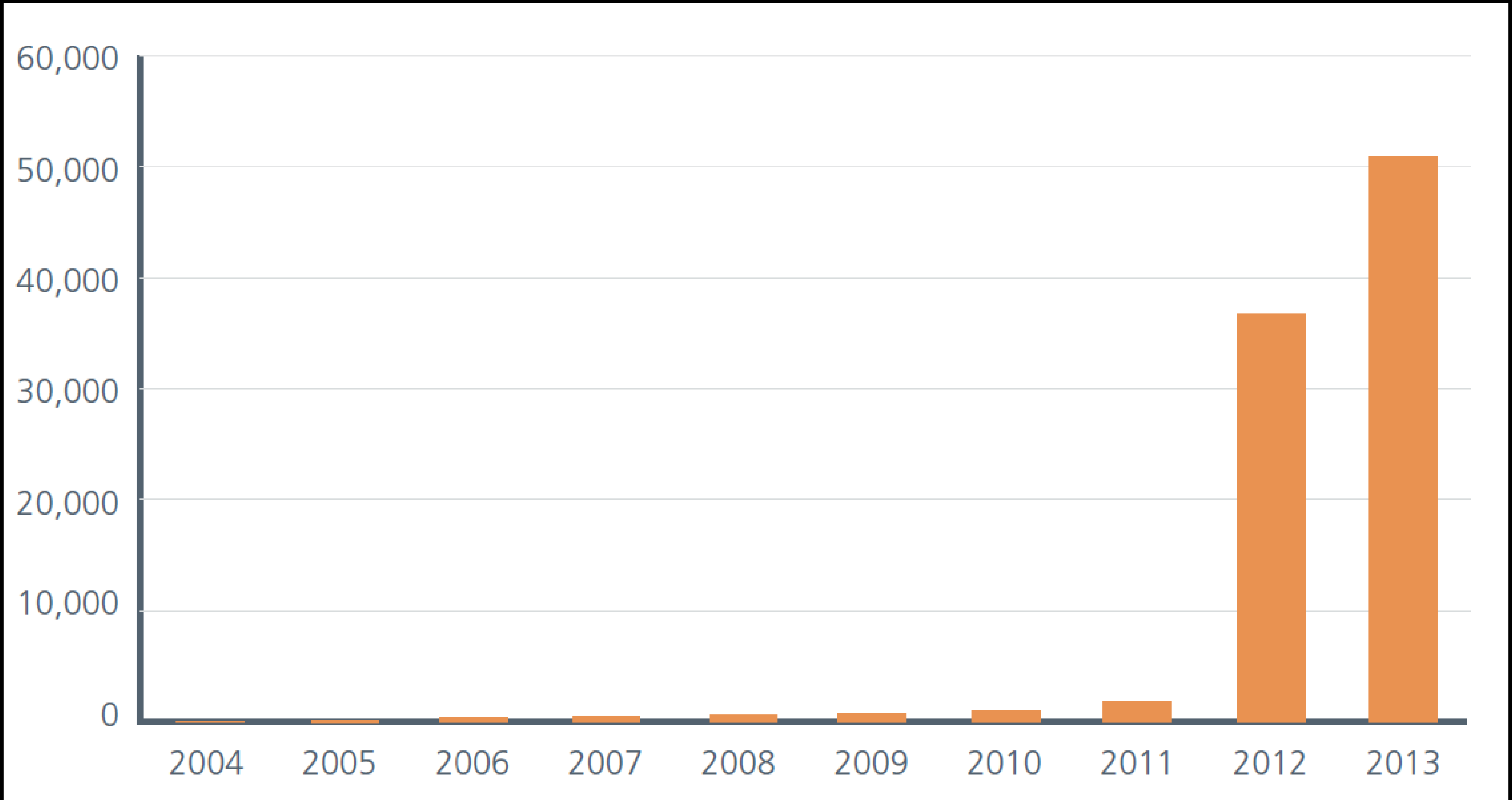


S A F E

Breaking Two-Factor Authentication: Mobile TAN (mTAN)

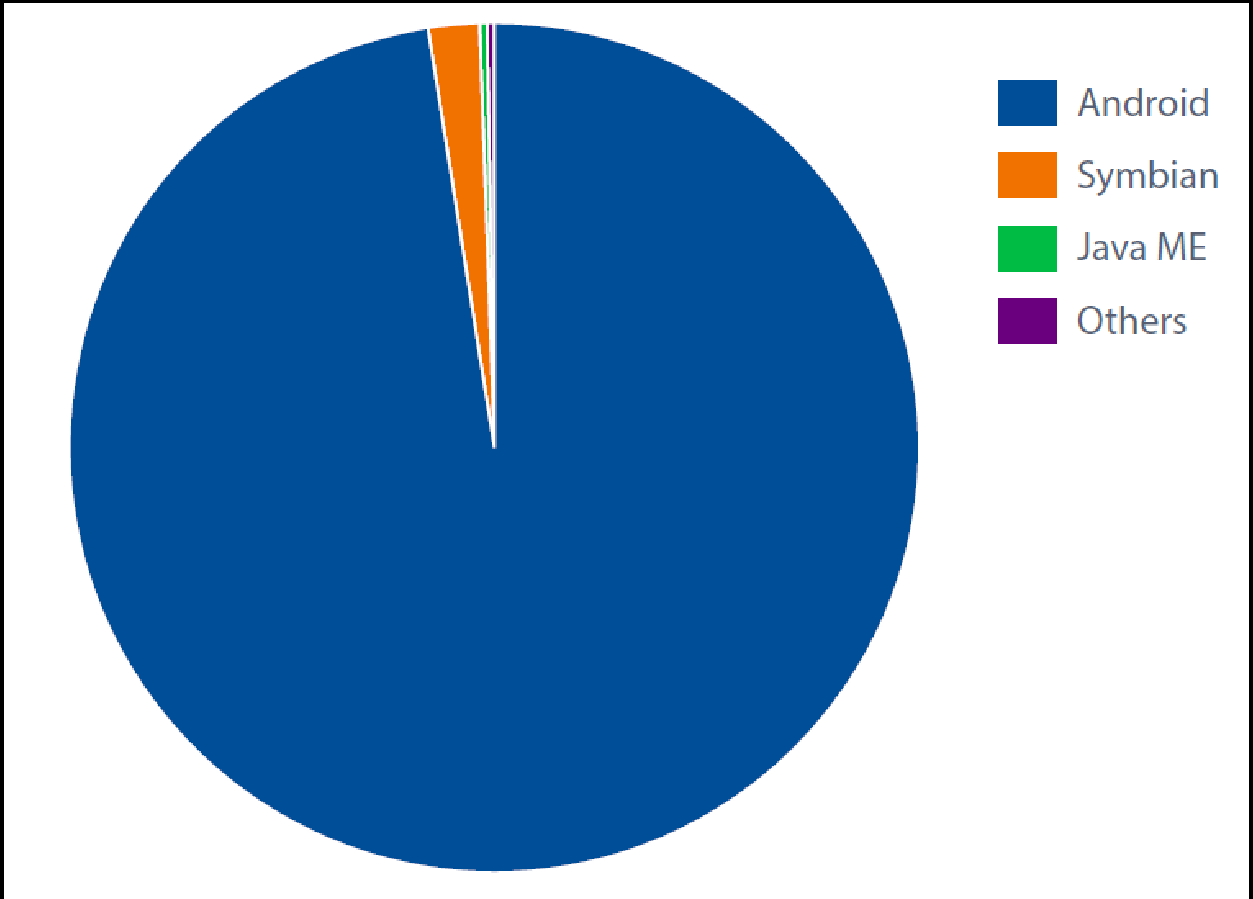


Malware Statistics: Total Mobile Malware Samples



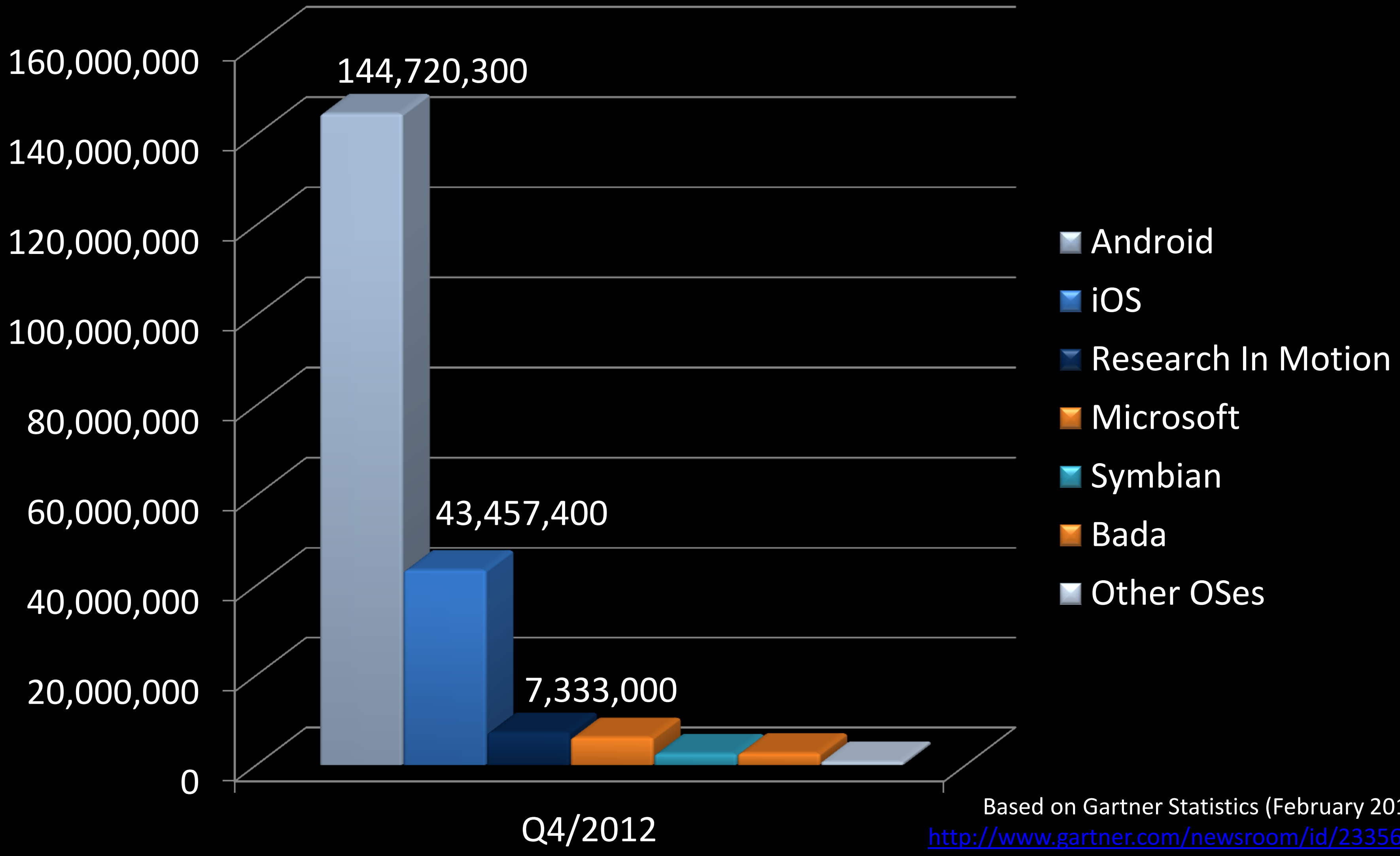
McAfee Labs, “McAfee threats report: First quarter 2013"

Malware Statistics: Total Mobile Malware per Platform



McAfee Labs, “McAfee threats report: First quarter 2013"

Worldwide Smartphone Sales to End Users by Operating System Sold Units Q4/2012



Based on Gartner Statistics (February 2013)
http://www.gartner.com/newsroom/id/2335616

Academic research:
Android is a main target

Why Most Research is Done on Android?

1. Market Dominantor

2. Almost Open Source

Security Extensions and Tools

Detecting and Preventing Private Data Leakage

TaintDroid
[Enck et al., USENIX OSDI 2010]

TISSA
[Zhou et al., TRUST 2011]

AppFence
[Hornyack et al., ACM CCS 2011]

Application Hardening and Context-Based Policies

SAINT
[Ongtang et al., ACSAC 2009]

CRePE
[Conti et al., ISC 2010]

AppGuard
[Backes et al., TR 2012]

Mr Hide/Dr Android
[Jeon et al., ACM SPSM 2012]

Aurasium
[Xu et al., USENIX Sec. 2012]

In-App Ad Library Malware

AdRisk
[Grace et al., WISec 2012]

AdDroid
[Pearce et al., AsiaCCS 2012]

AdSplit
[Dietz et al., USENIX Sec. 2012]

Security Aspects of App Stores

DroidRanger
[Zhou et al., NDSS 2012]

DroidMOSS
[Zhou et al., CODASPY 2012]

Meteor
[Barrera et al., IEEE MoST 2012]

More Security Extensions and Tools

Malware Detection

Kirin
[Enck et al., ACM CCS 2009]

Apex
[Naumann et al., AsiaCCS 2010]

Paranoid
[Portokalidis et al., ACSAC 2010]

Airmid
[Nadji et al., ACSAC 2011]

DroidScope
[Yan et al., USENIX Sec. 2012]

DRM Policies and Domain Isolation

Porscha
[Ongtang et al., ACSAC 2010]

TrustDroid
[Bugiel et al., ACM SPSM 2011]

Privilege Escalation (Application-Level)

Confused Deputy

- **IPC Inspection**
  [Felt et al., USENIX Sec. 2012]
- **QUIRE**
  [Dietz et al., USENIX Sec. 2012]
- **XManDroid**
  [Bugiel et al., NDSS 2012]
- **SORBET**
  [Fragkaki et al., TR 2012]

Colluding Apps

- **XManDroid**
  [Bugiel et al., NDSS 2012]
- **FlaskDroid**
  [Bugiel et al., USENIX 2013]

Privilege Escalation (Kernel-Level)

Android SELinux
[Shabtai et al., IEEE S&P Magazine 2010]

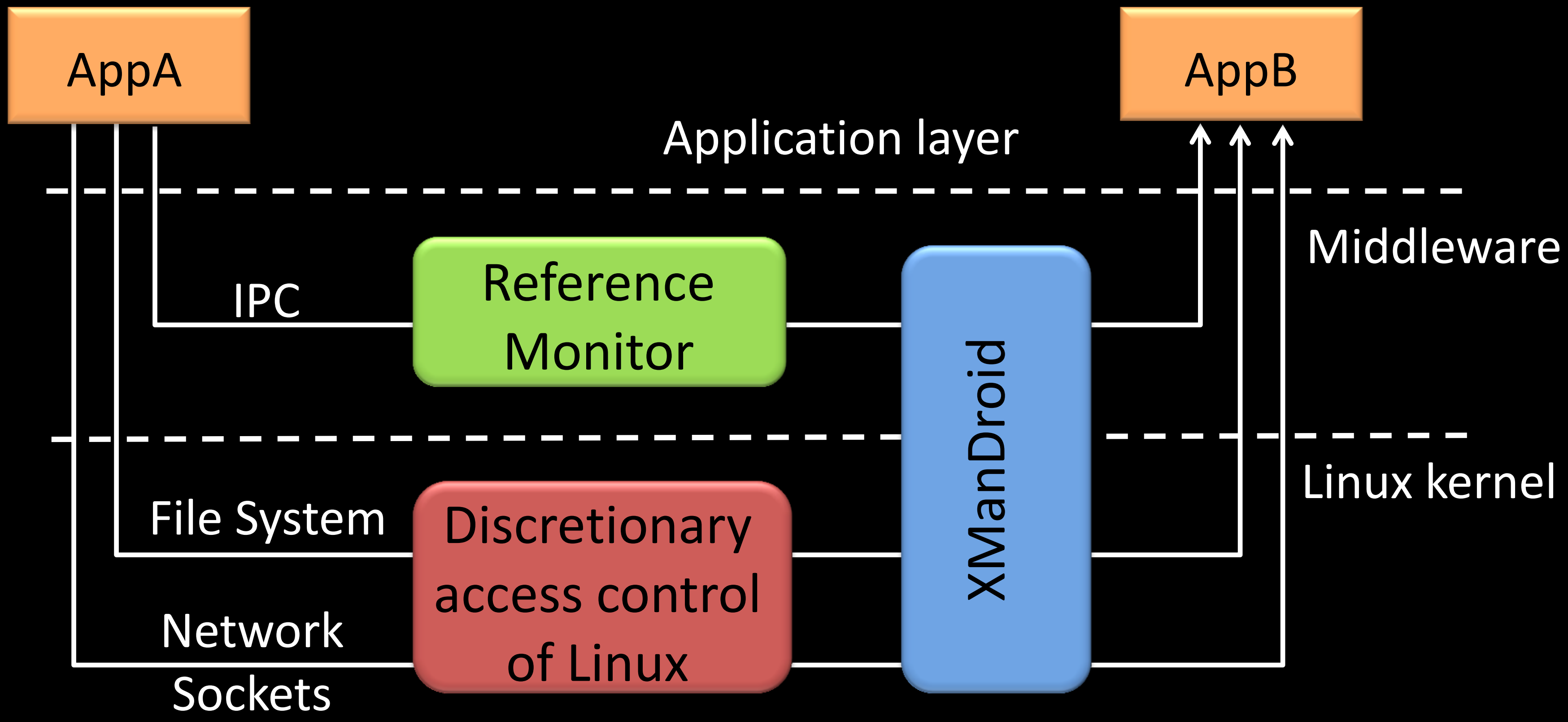
SEAndroid
[Smalley et al., NDSS 2012]

L4Android
[Lange et al., ACM SPSM 2011]

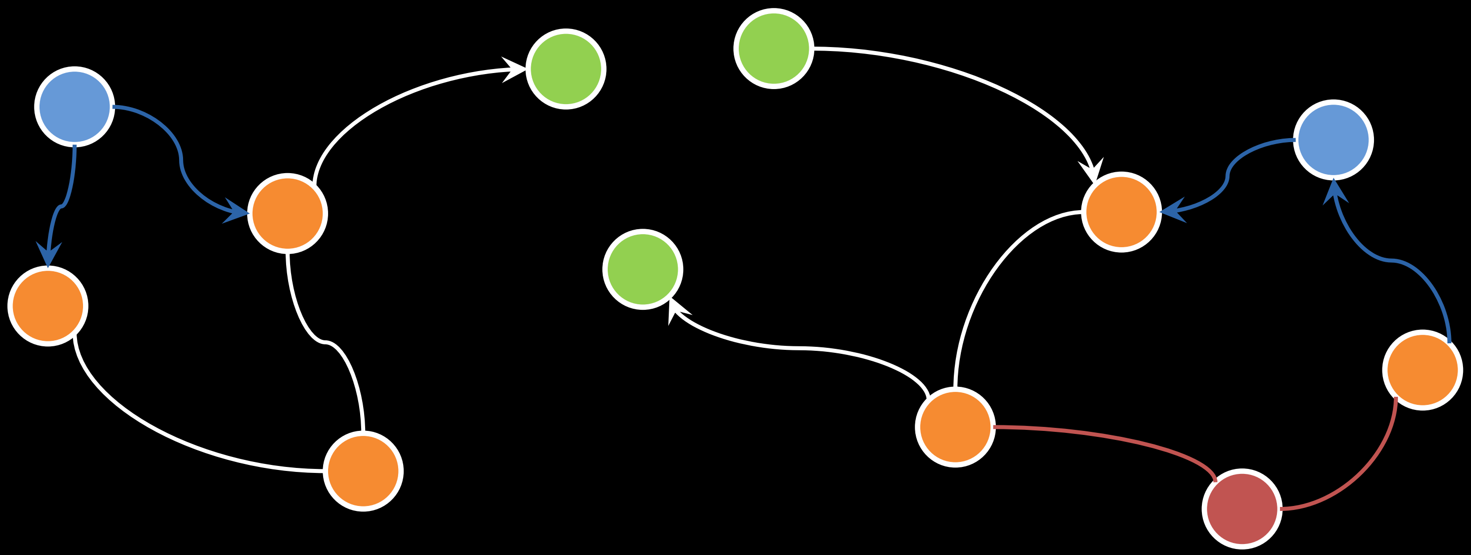
XManDroid: Mitigation of Confused Deputy Attacks and Colluding Apps

XManDroid: High-level Idea

- Monitors all communication channels between apps
- Validates if the requested communication link complies to a system-centric security policy



XManDroid: Graph-based System Representation



🟢 System Components

🟠 Application sandboxes

🔵 Files

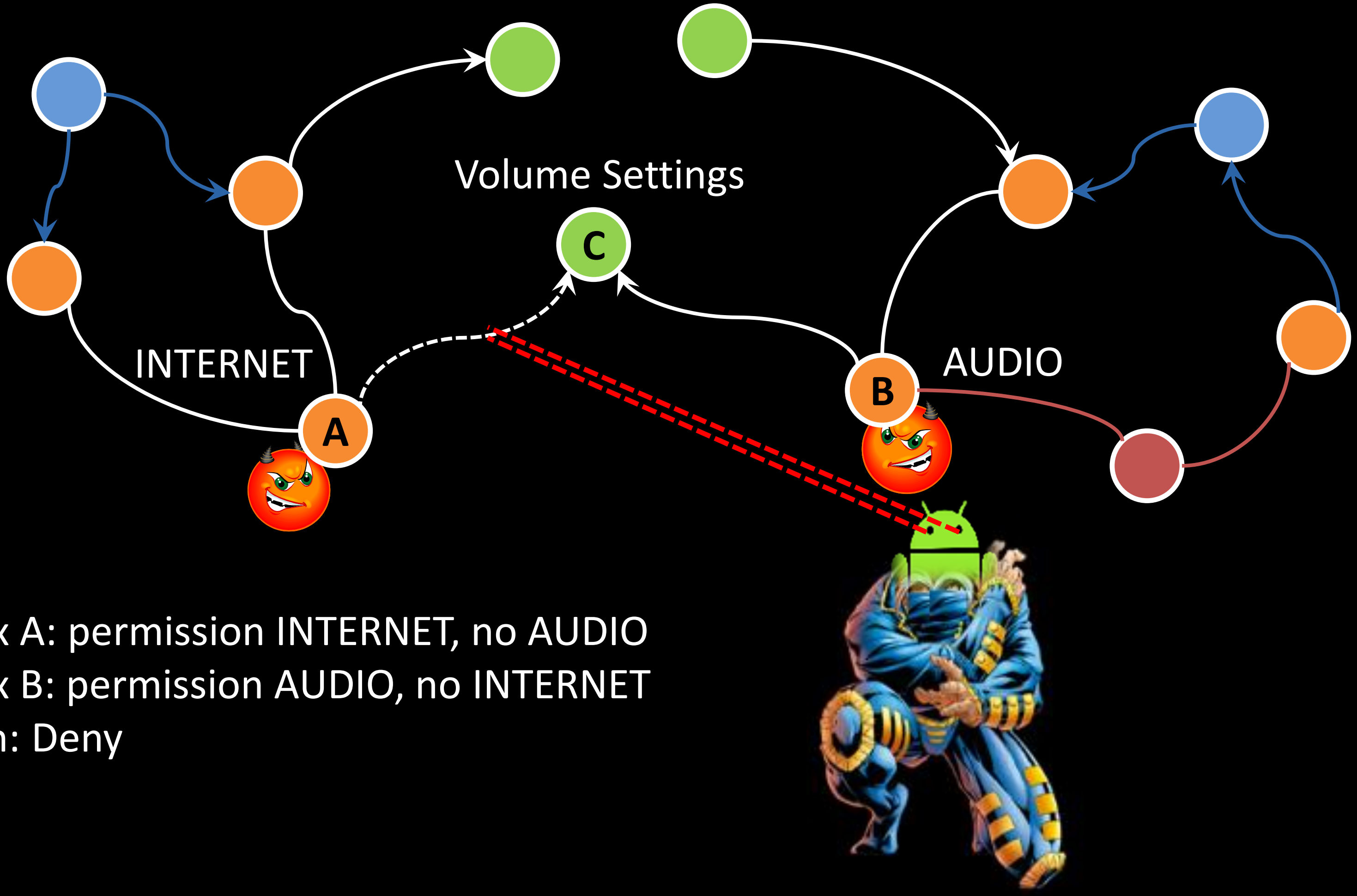
🔴 Internet sockets

— IPC calls

— Access to files

— Socket connections

XManDroid against Soundcomber



Policy Rule:

- Sandbox A: permission INTERNET, no AUDIO
- Sandbox B: permission AUDIO, no INTERNET
- Decision: Deny

TrustDroid (BizzTrust): Dual Persona Phone

Trends: One Phone for Business and Private Tasks

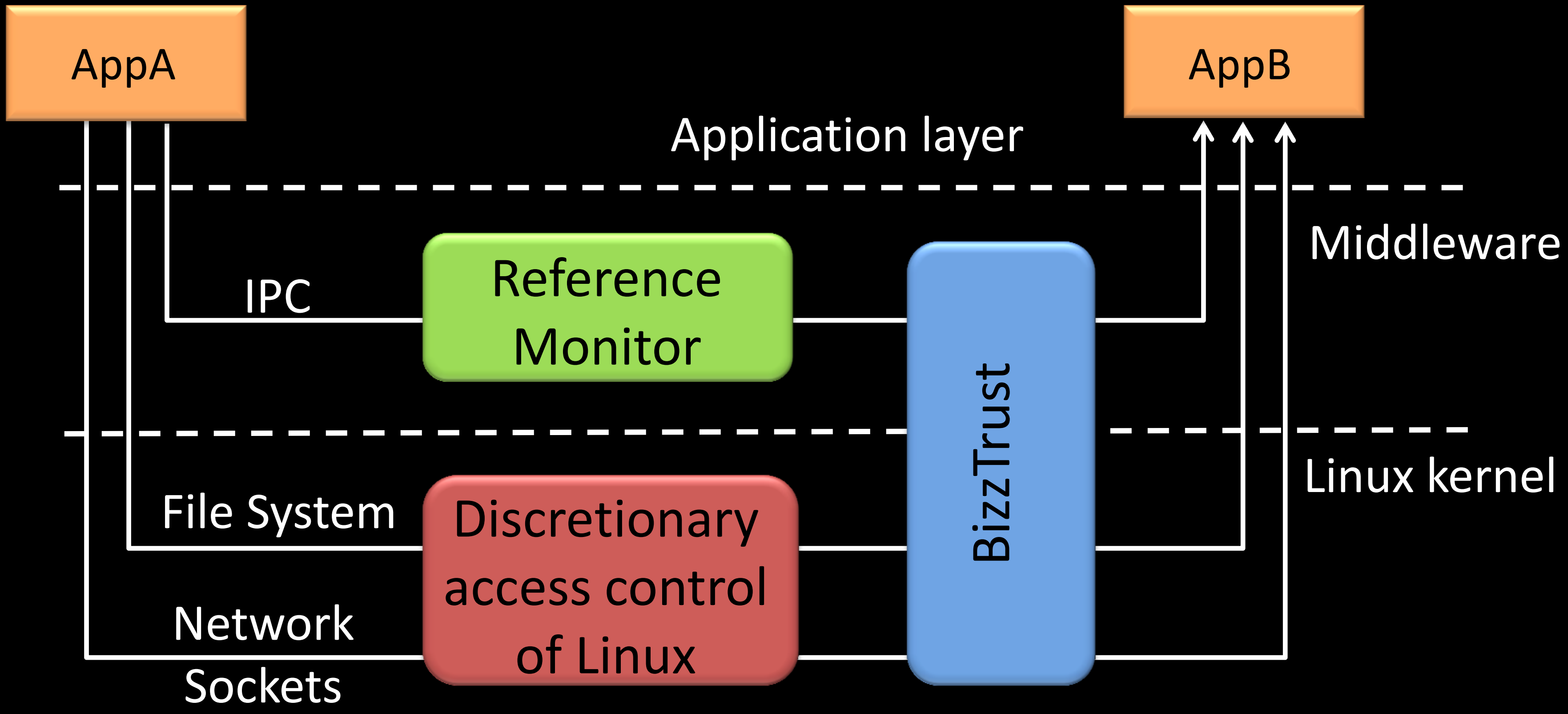
8:32
PRIVATE
BUSINESS
VPN

Private

Business / Work

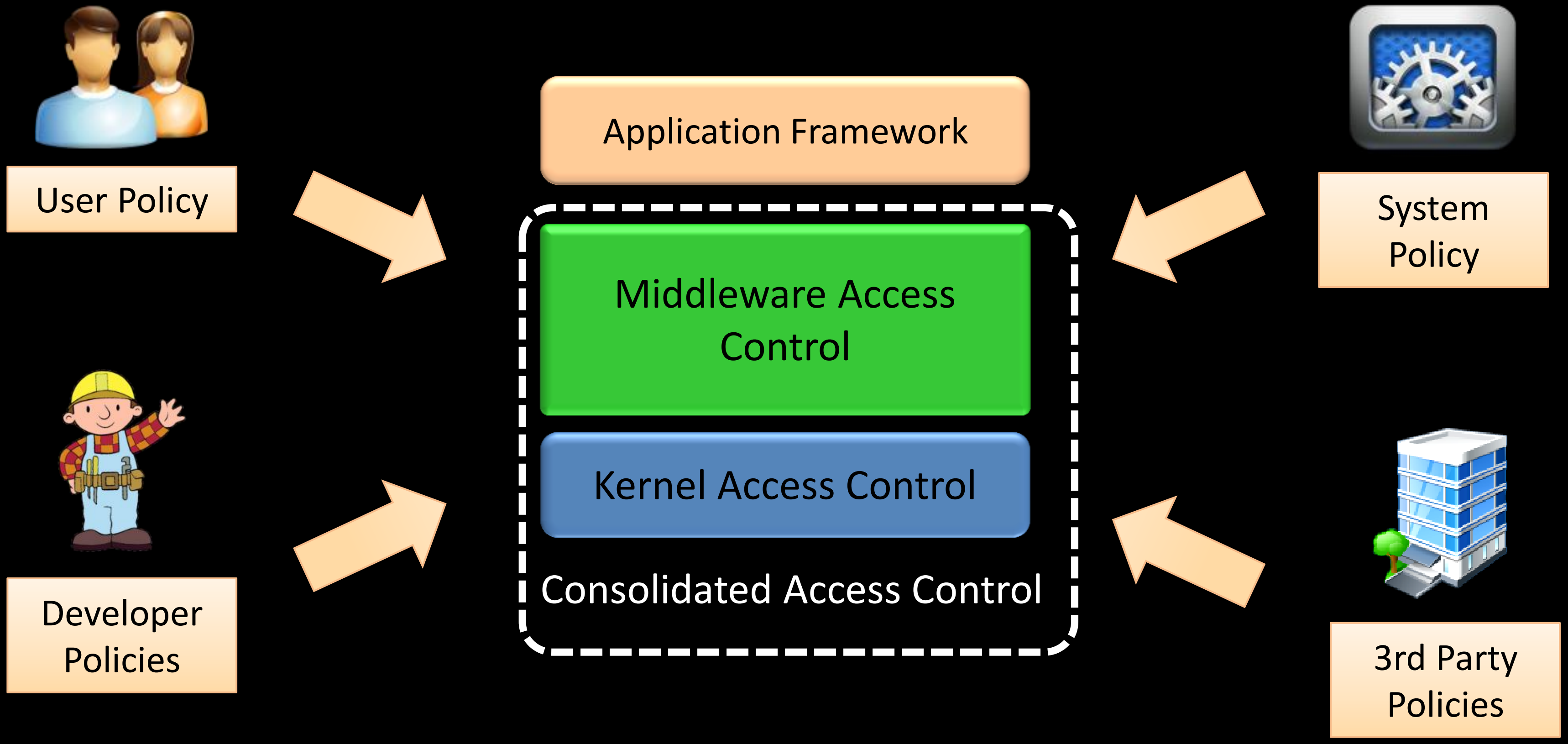
How Does It Work?

- Colors private and corporate apps into different colors
- Controls all communication channels between the apps
- Enforces isolation between apps with different colors



FlaskDroid: A Generic Fine-Grained MAC

FlaskDroid:
Supports Multi Stackholder Policies



User Policy

System Policy

Application Framework

Middleware Access Control

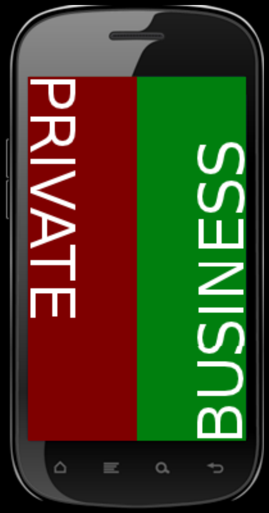
Kernel Access Control

Consolidated Access Control

Developer Policies

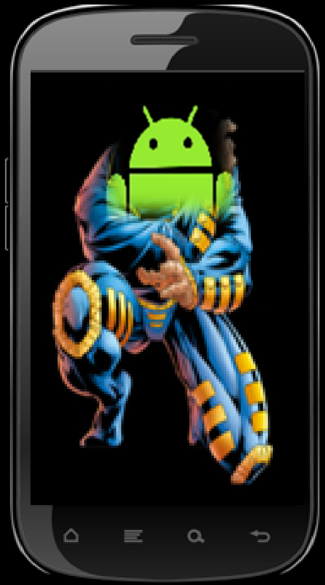
3rd Party Policies

Many Use-Cases

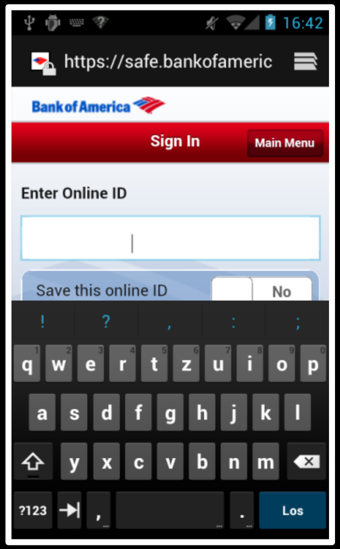


Dual Persona

Phone Booth Mode (lending phone)



XManDroid



Prevent side-channels

Challenge:
The Gap Between Solutions in Theory and Practice

Need More Integration of Research in to Industrial Solutions

Summary

- Smartphones process a lot of privacy-sensitive data
- Large attack surface and rapid grow of malware
- Active academic research particularly on Android to harden overall system
  - Kernel, middleware, applications
- The gap between academic research and industrial solutions

Thank you!

Alexandra Dmitrienko
Alexandra.dmitrienko@trust.cased.de
www.trust.cased.de