Software Security Goes Mobile

Jacob West

CTO, Fortify Products

HP Enterprise Security

July 12, 2012

Motivation

Redefining the **phone** and the **computer**

Money: Beyond ringtones and 99¢ games

Landscape

What is mobile?

What **matters**?

Who cares?

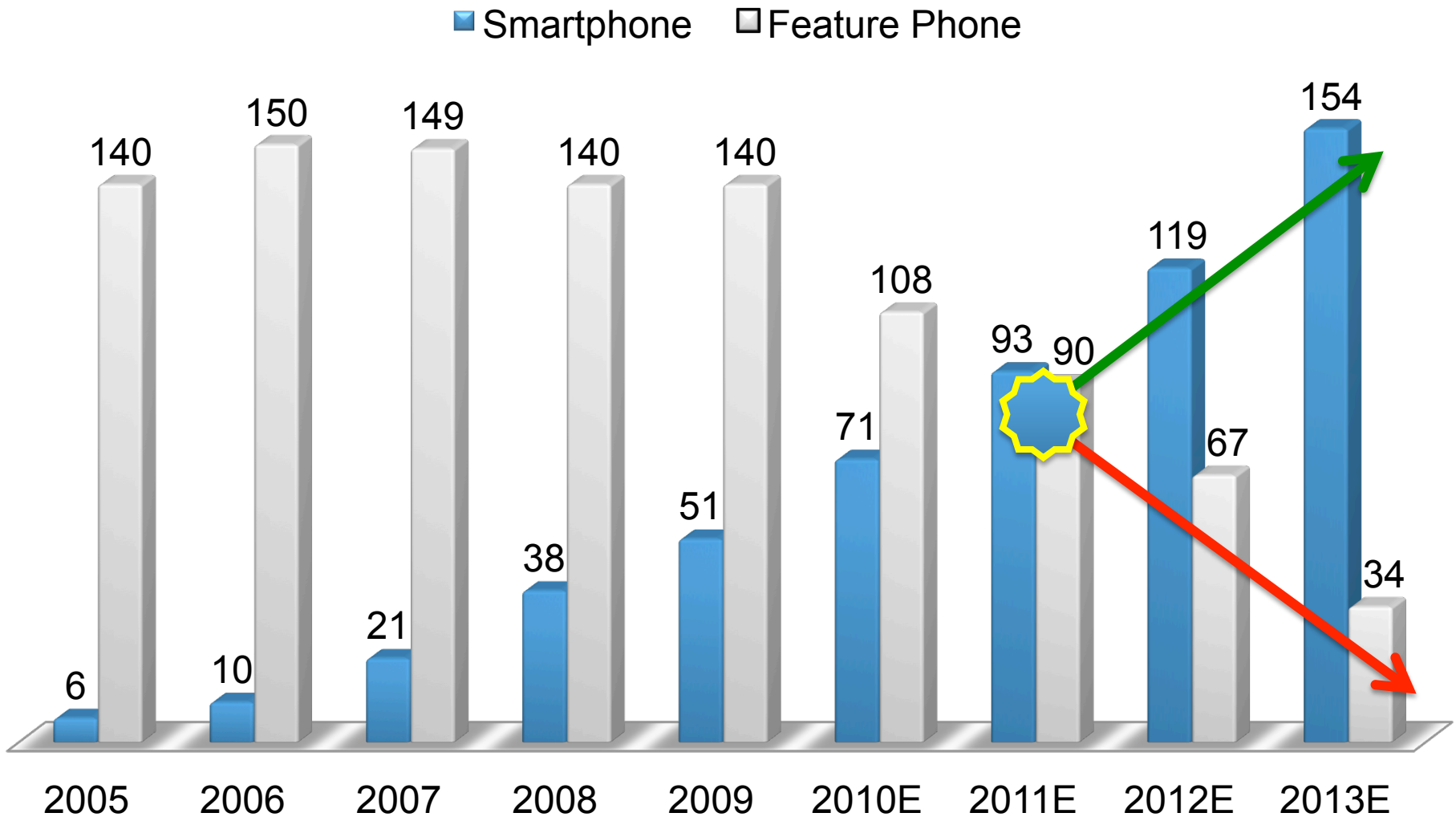
Mobile Threats

Parting Thoughts

Questions you can ask
to begin **improving** your
mobile security today

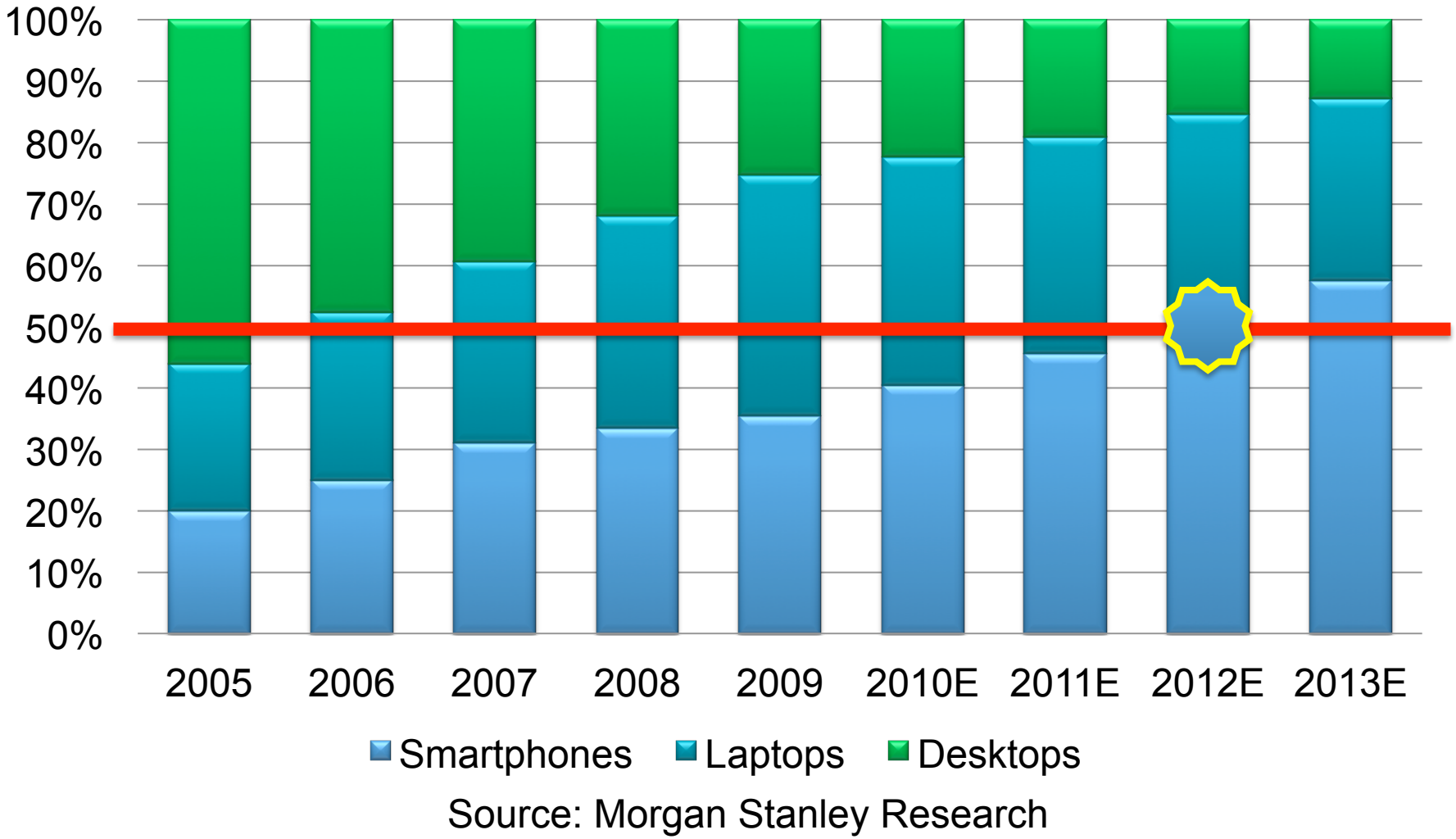
Motivation

Smartphones > Feature Phones



Source: Morgan Stanley Research

Smartphones > PCs



Source: Morgan Stanley Research

Page Vi n the Rise

?

½

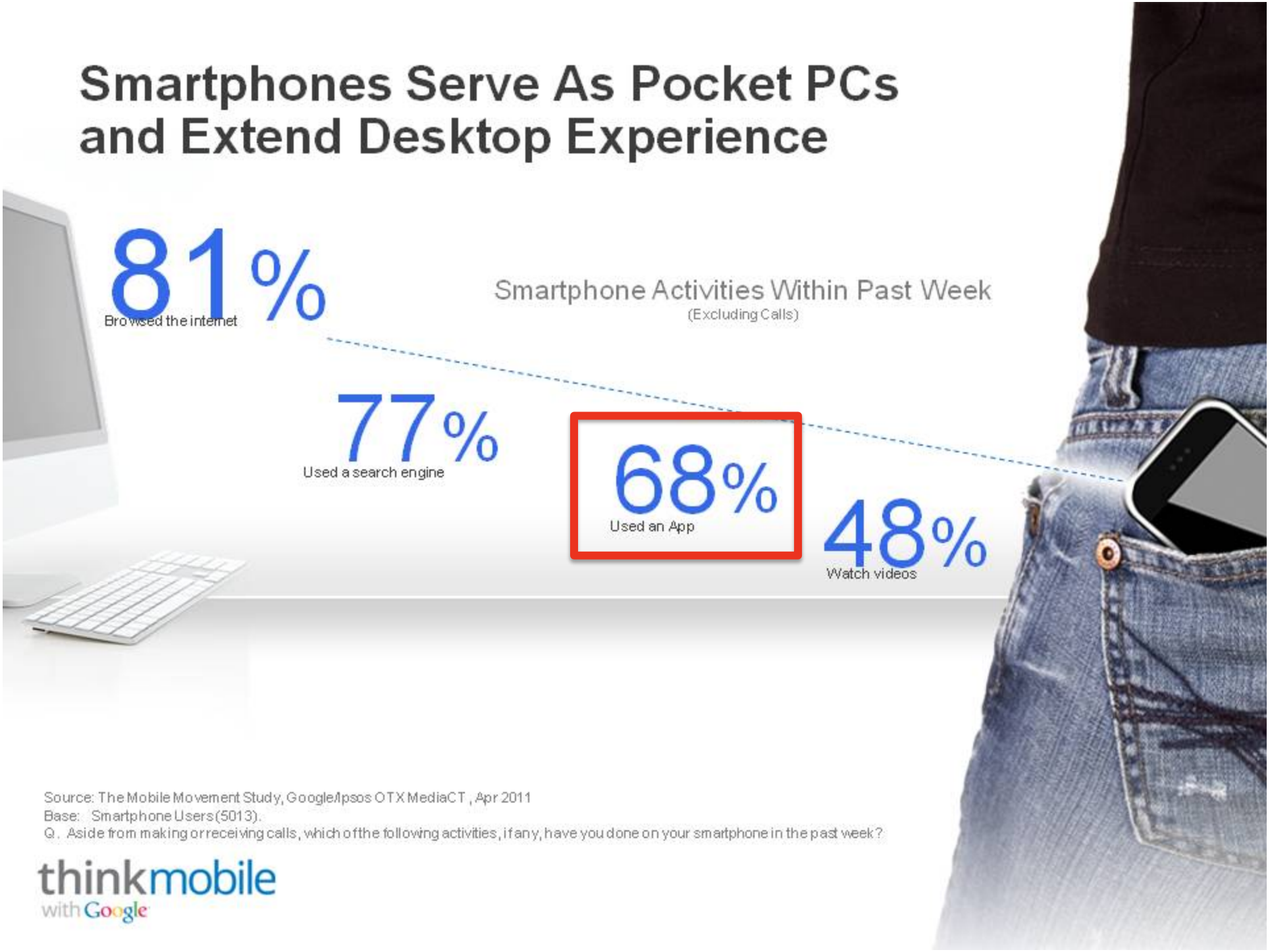
2

3½

6½

Source: Morgan Stanley Research

Smartphones Serve As Pocket PCs and Extend Desktop Experience

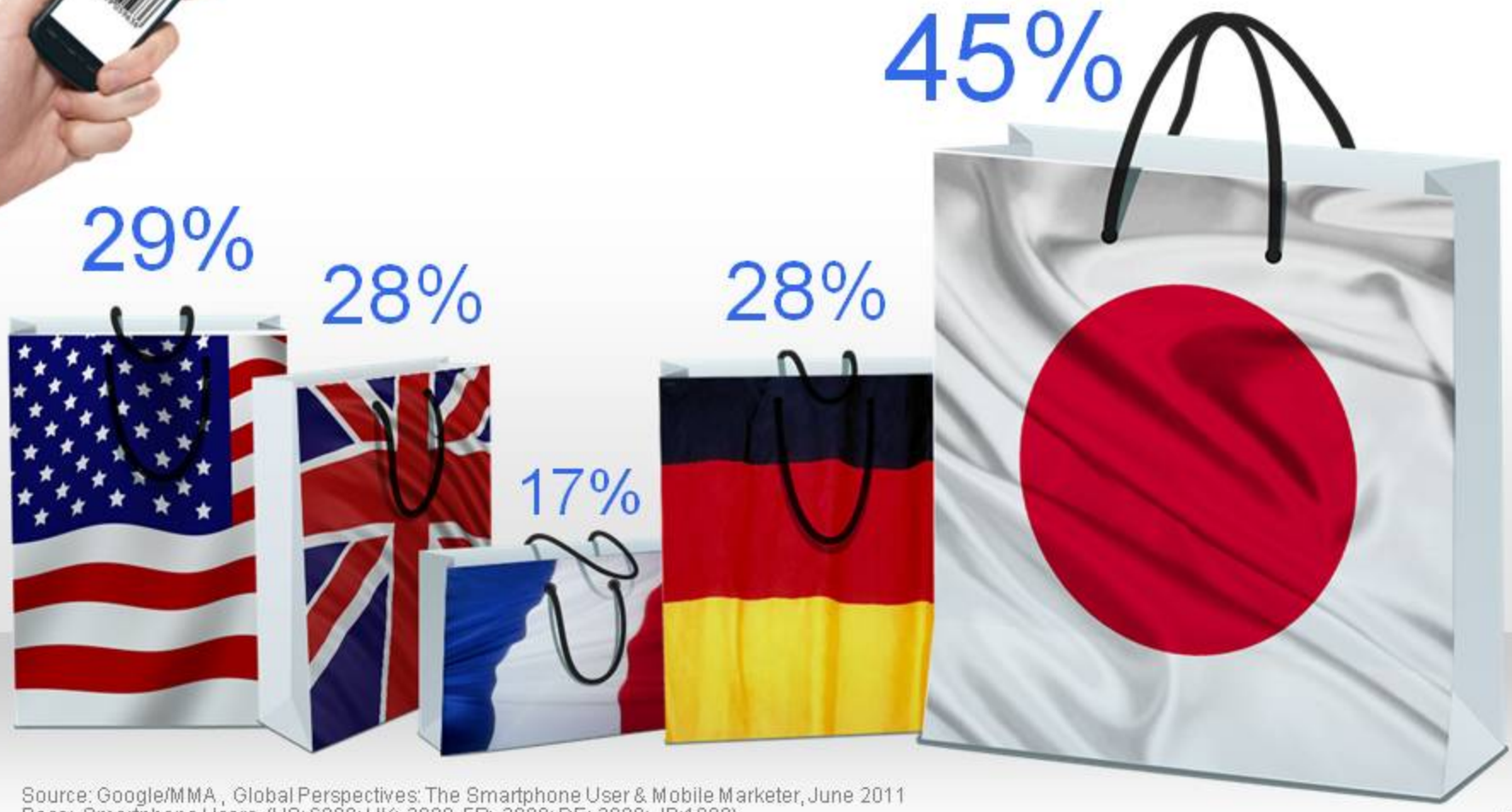


Source: The Mobile Movement Study, Google/Ipsos OTX MediaCT , Apr 2011
Base: Smartphone Users (5013).
Q. Aside from making or receiving calls, which of the following activities, if any, have you done on your smartphone in the past week?

thinkmobile with Google

Mobile is an Emerging Point of Purchase

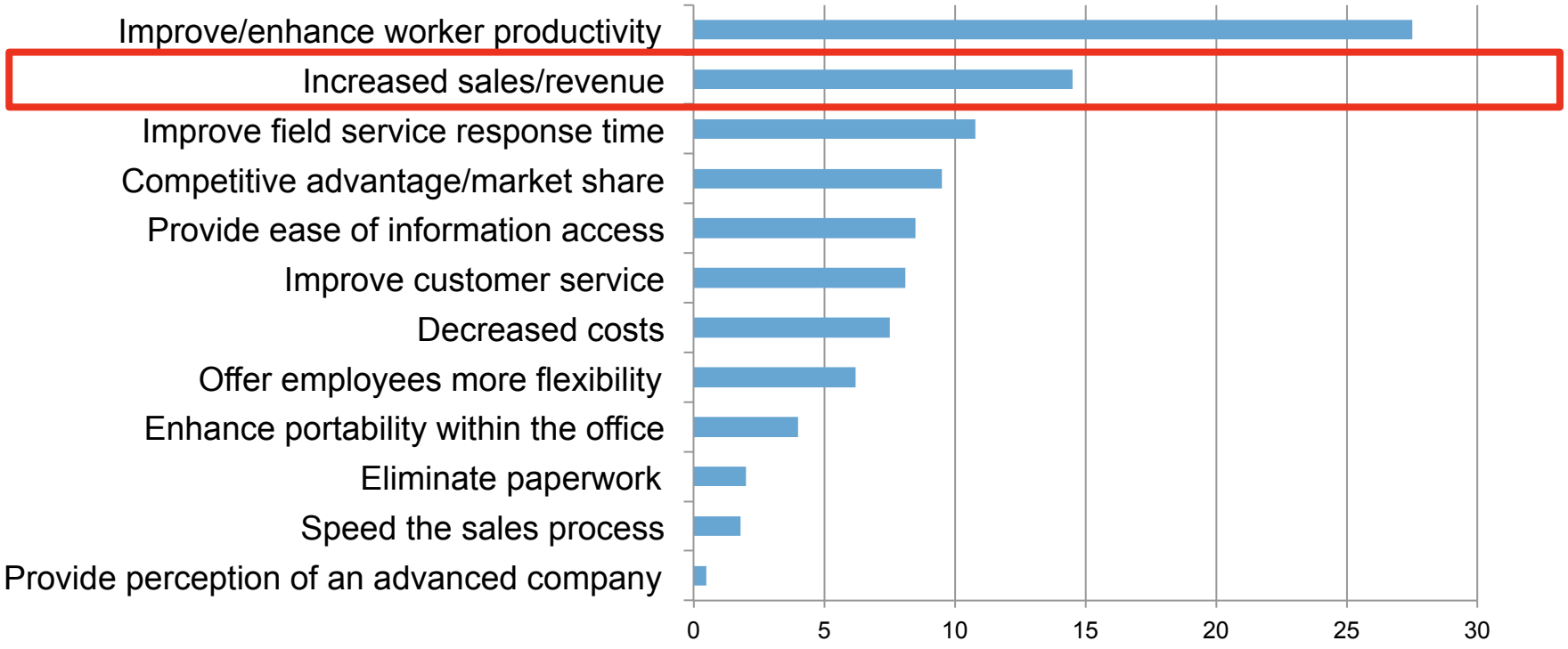
Have Purchased on Smartphone



Source: Google/MMA , Global Perspectives: The Smartphone User & Mobile Marketer, June 2011
Base: Smartphone Users (US: 6000; UK: 2000, FR: 2000; DE: 2000; JP:1000).
Q. Have you ever purchased a product or service over the Internet on your smartphone?

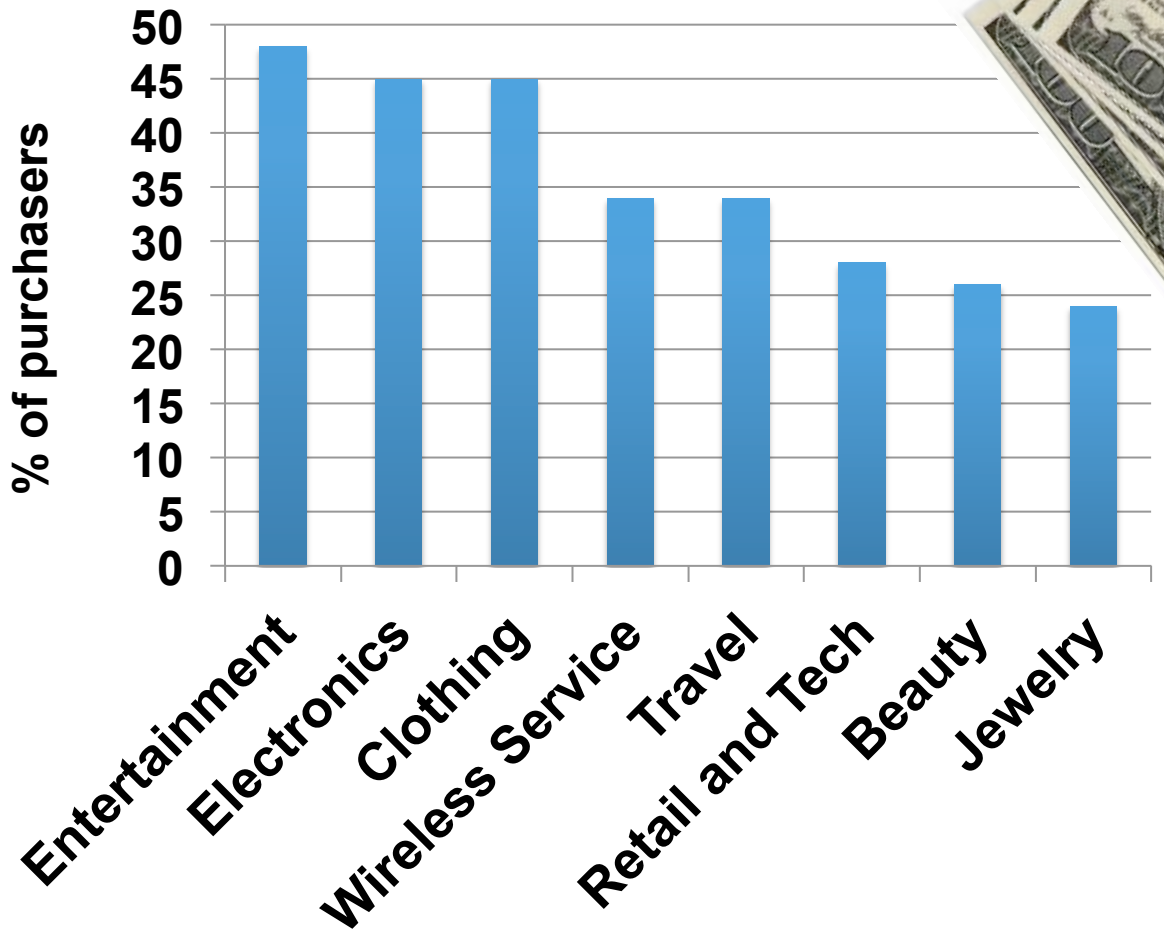
Mobile Opportunities

Please select the most important benefit that your organization ultimately expects to gain from current or future mobile solutions deployments (whether or not you are currently receiving those benefits)



N = 600, Source: IDC's Mobile Enterprise Software Survey (2011)

Mobile Purchasers

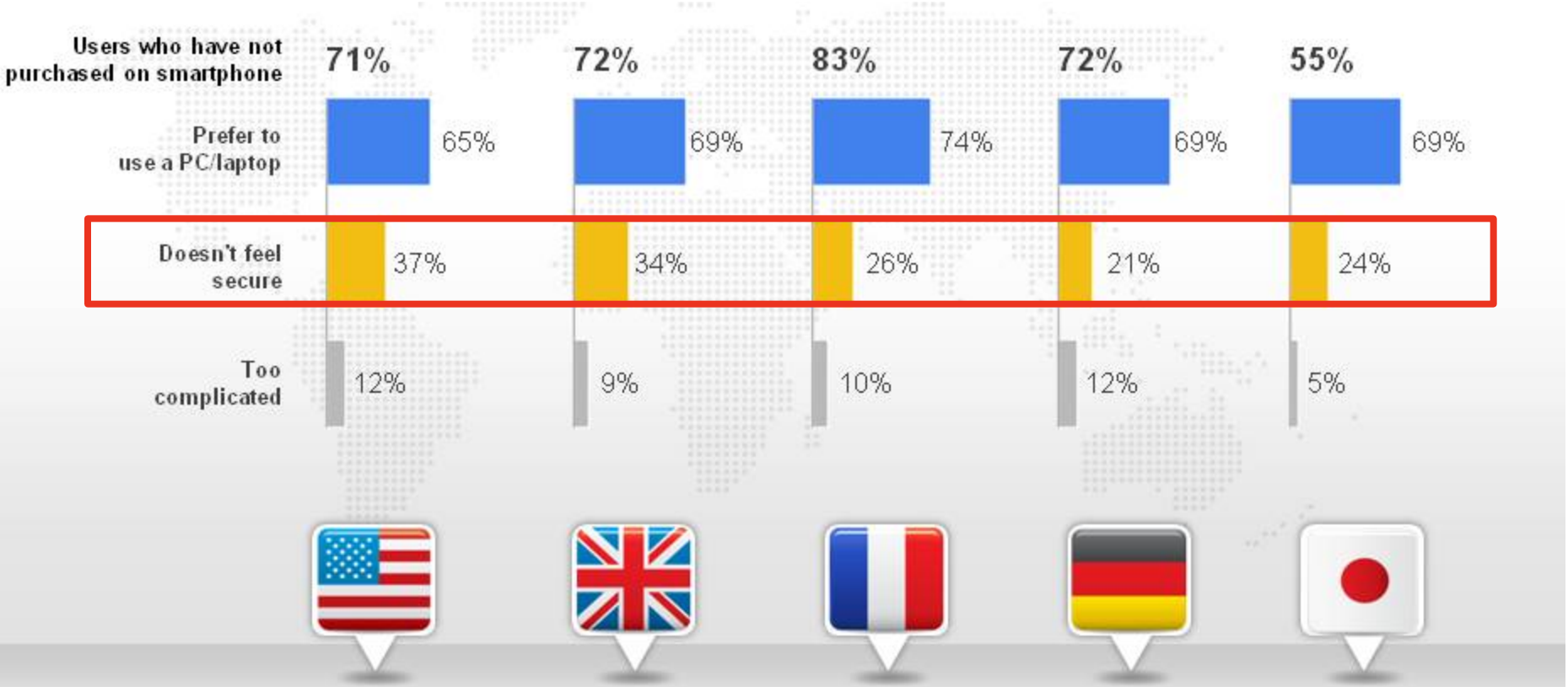


$300/year per user

Source: Google The Mobile Movement Study

Why Mobile Users Don't Buy

- Security is #2 reason to avoid purchases



Source: Google/MMA , Global Perspectives: The Smartphone User & Mobile Marketer, June 2011
Base: Smartphone Users (US: 6000; UK: 2000, FR: 2000; DE: 2000; JP:1000).
Base: Smartphone Users Who Have Not Made a Purchase on Device (US: 4444; UK: 1559, FR: 1653; DE: 1442; JP: 554).
Q. Why have you not made a purchase using your smartphone?

Mobile Landscape

What *is* Mobile?

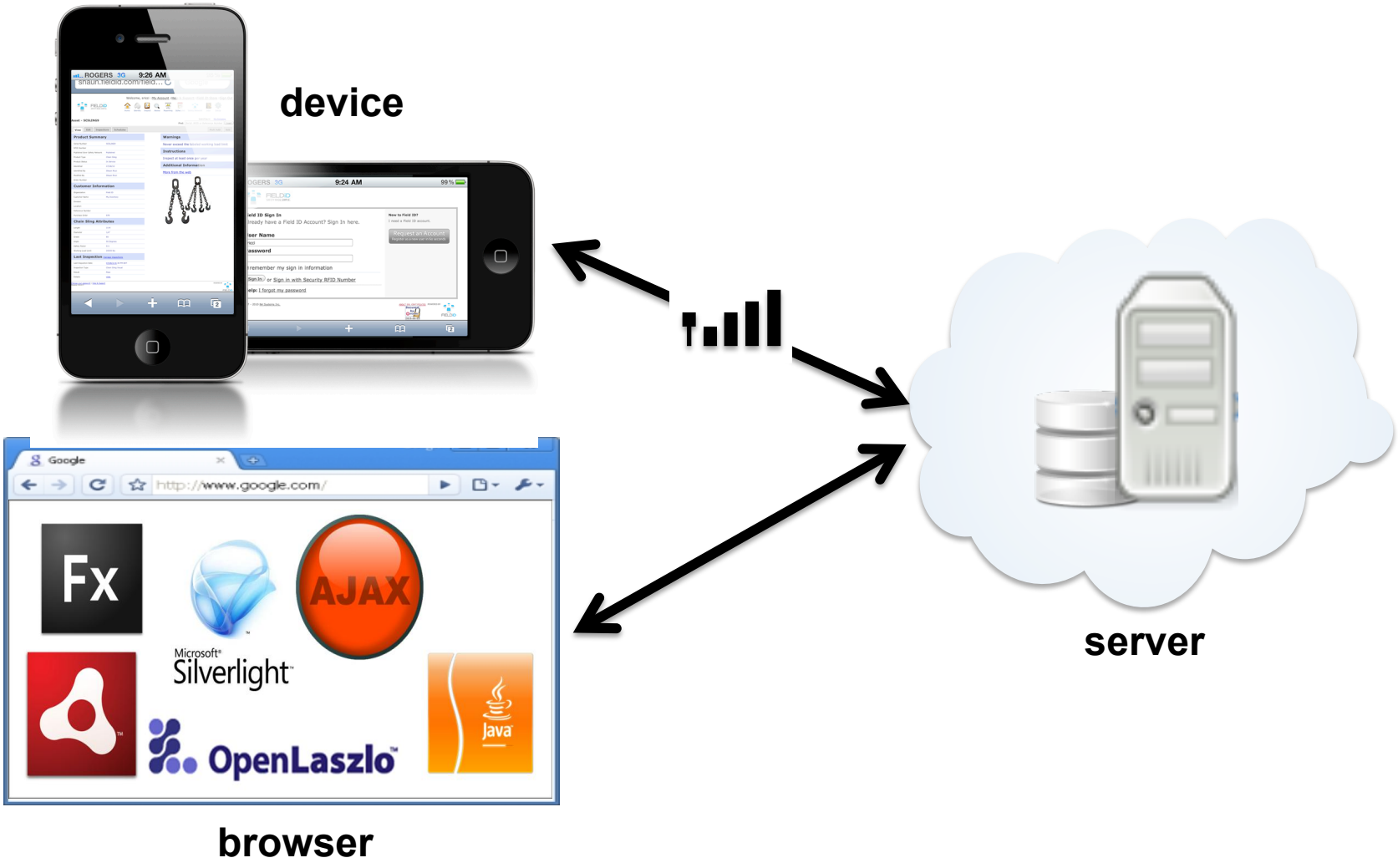
device

connection

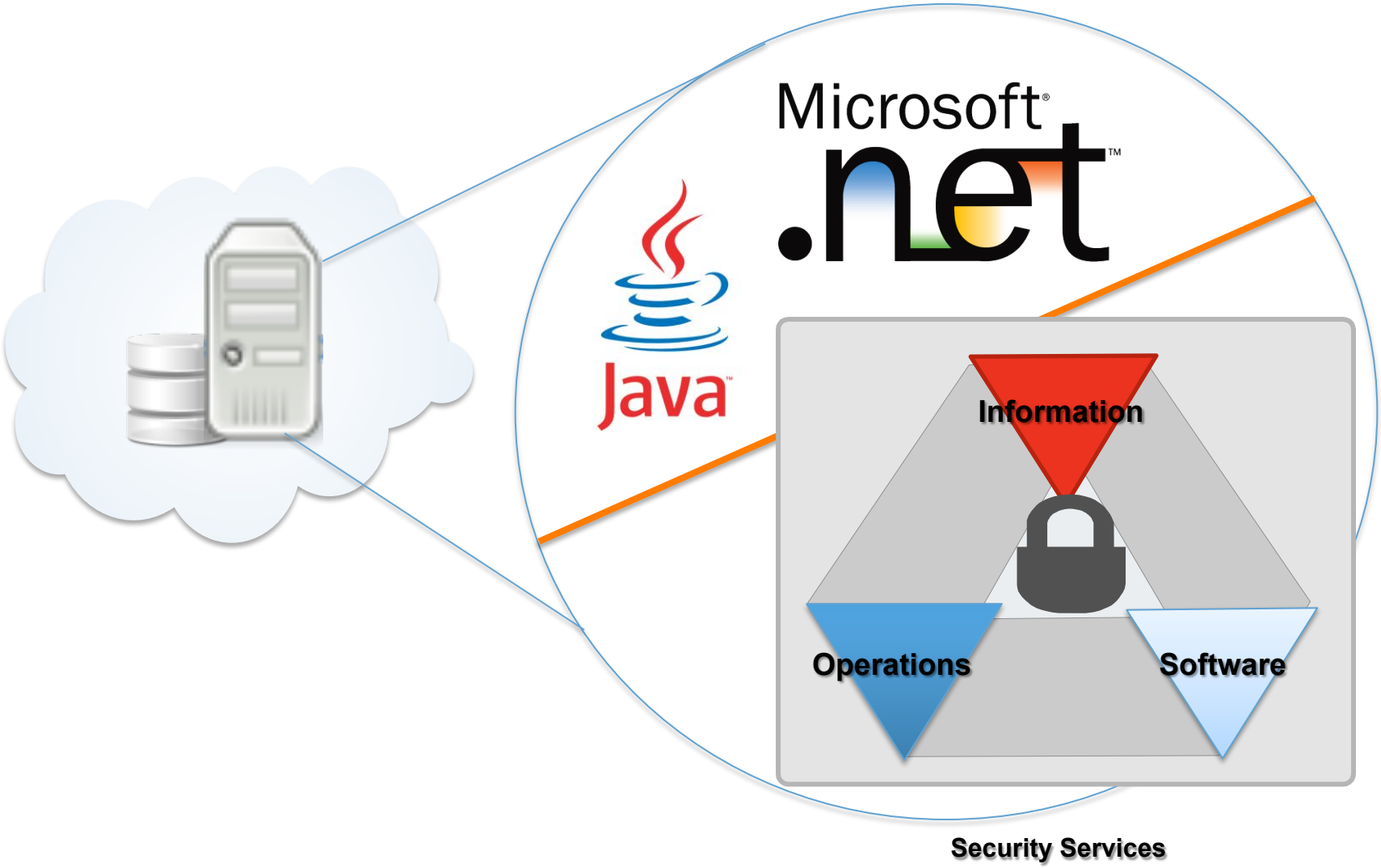
server

os

Familiar Model



Same Ol' Server



Client-Side Persistence

- Local data persistence
- Similar to HTML 5
- Invisible to users and always available

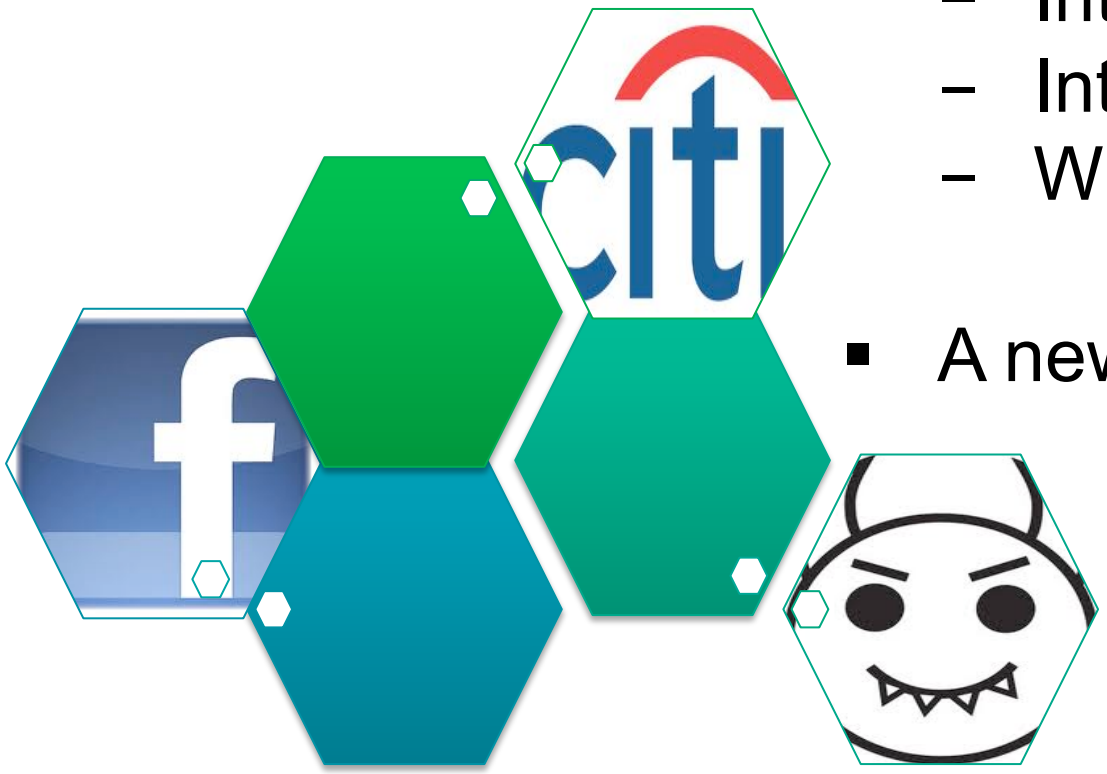
Mobile OS

Google

BlackBerry

- Benefit of hindsight
- Security features
  - Read-only stack
  - Data encryption
  - Permissions
- Confusing
  - Wait, permissions?

Can’t We All Get Along?



- Formal communication
  - Inter-application
  - Intra-application
  - With the OS
- A new trust boundary

What Matters?

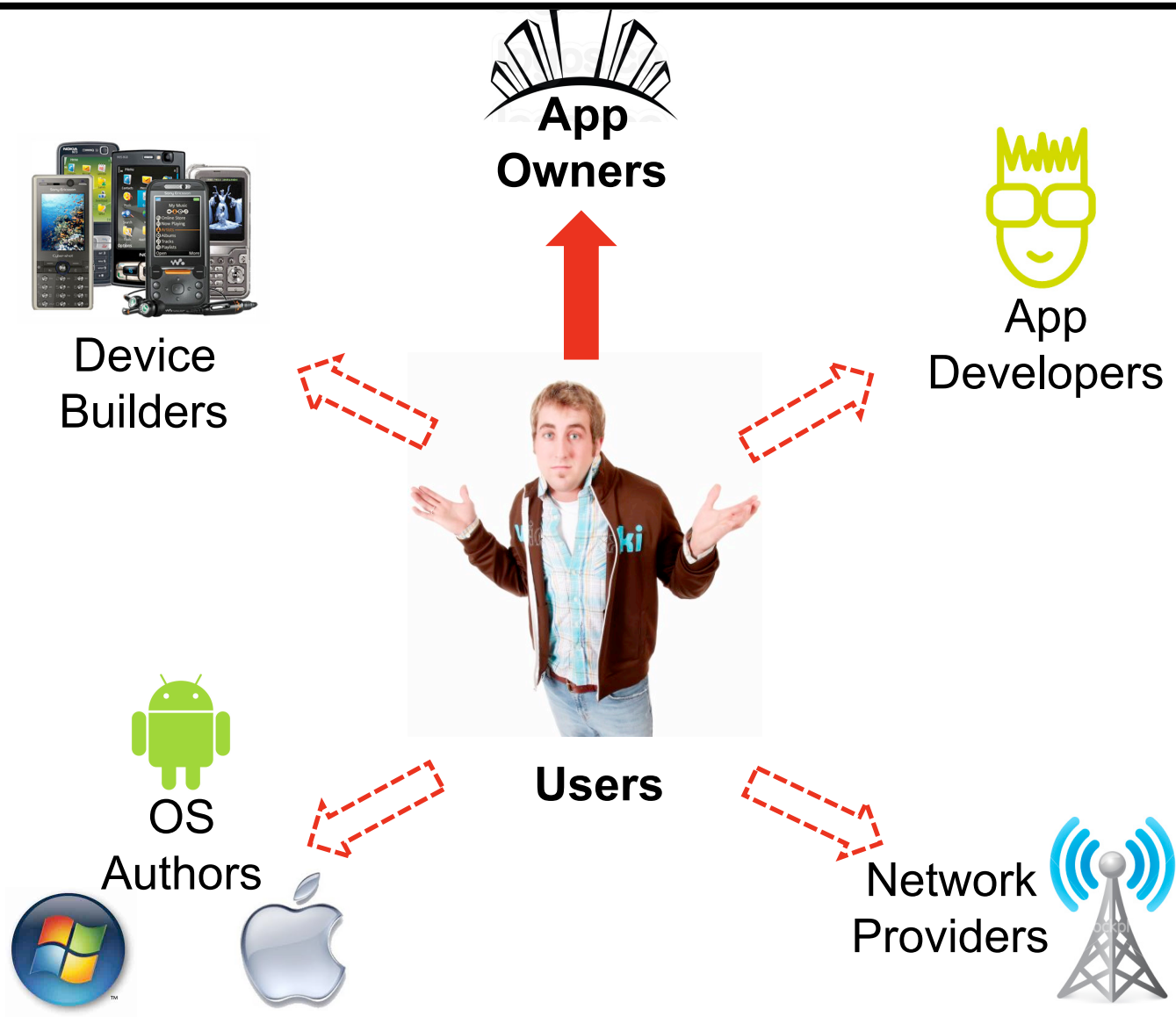
Old

- Handling sensitive user and app data
- Environment and configuration
- Standbys like XSS and SQL injection

New

- Local storage (e.g. SD card)
- Communication (SMS, MMS, GPS)
- Security features (Privileges, crypto)

Who Cares?


App Owners
Device Builders
App Developers
Users
OS Authors
Network Providers

Mobile Threats

Google Android Vulnerabilities

1	**Intent Hijacking**
2	**Intent Spoofing**
3	Sticky Broadcast Tampering
4	Insecure Storage
5	Insecure Network Communication
6	SQL Injection
7	**Promiscuous Privileges**

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

Description: Malicious app intercepts an intent bound for another app to compromise data or alter behavior

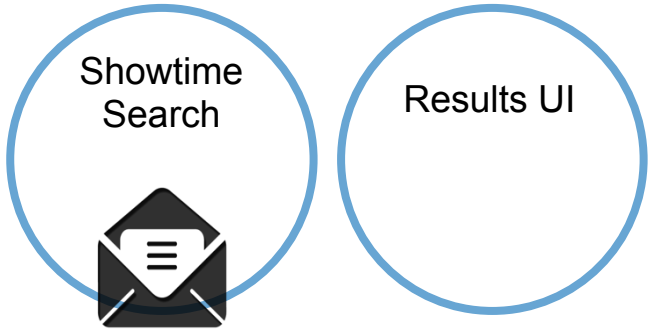
Cause: Implicit intents (do not require strong permissions to receive)

Fix: **Explicit intents and receiver permissions**

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

IMDb App

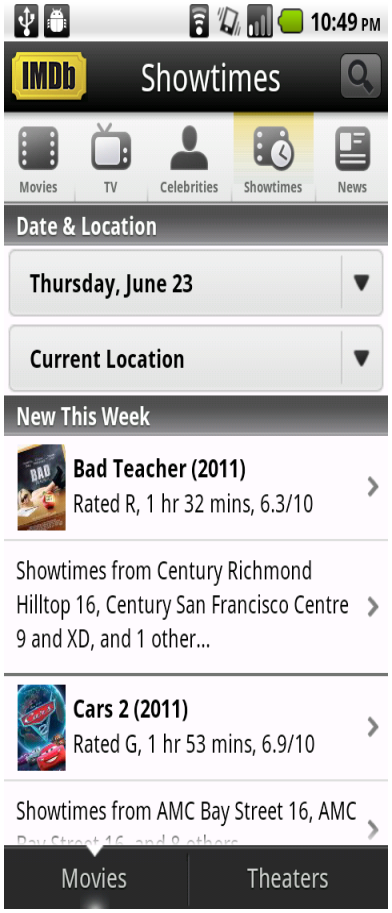


Implicit Intent
Action: *willUpdateShowtimes*

Handles Actions:
willUpdateShowtimes,
showtimesNoLocationError

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges



Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

IMDb App

Showtime Search

Implicit Intent
Action: *willUpdateShowtimes*

Results UI

Handles Actions:
willUpdateShowtimes,
showtimesNoLocationError

Eavesdropping App

Malicious Receiver

Handles Actions:
willUpdateShowtimes,
showtimesNoLocationError

Google Android Vulnerabilities

Intent Hijacking	**Intent Spoofing**	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

Description: Malicious app spoofs a legitimate intent to inject data or alter behavior

Cause: Public components (necessary to receive implicit intents)

Fix: **Explicit intents and receiver permissions**
Sensitive operations in private components

Google Android Vulnerabilities

Intent Hijacking	**Intent Spoofing**	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

Spoofing App

Action: *showtimesNoLocationError*

IMDb App

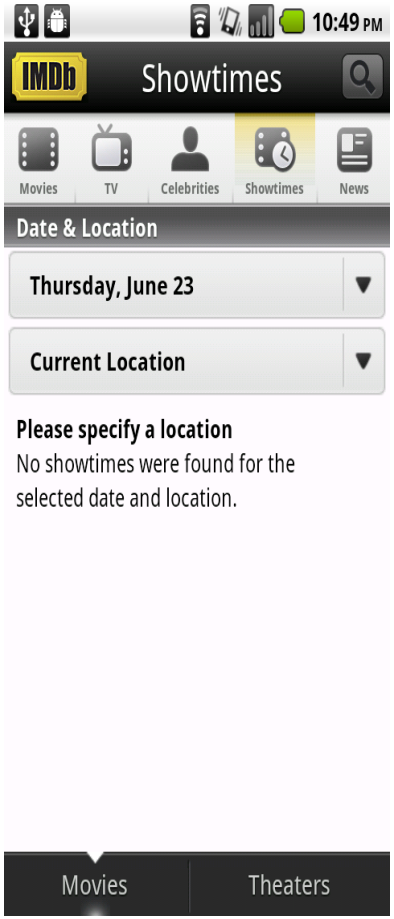
Showtime Search

Results UI

Handles Actions:
willUpdateShowtimes,
showtimesNoLocationError

Google Android Vulnerabilities

Intent Hijacking	**Intent Spoofing**	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges



Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	**Sticky Broadcast Tampering**	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

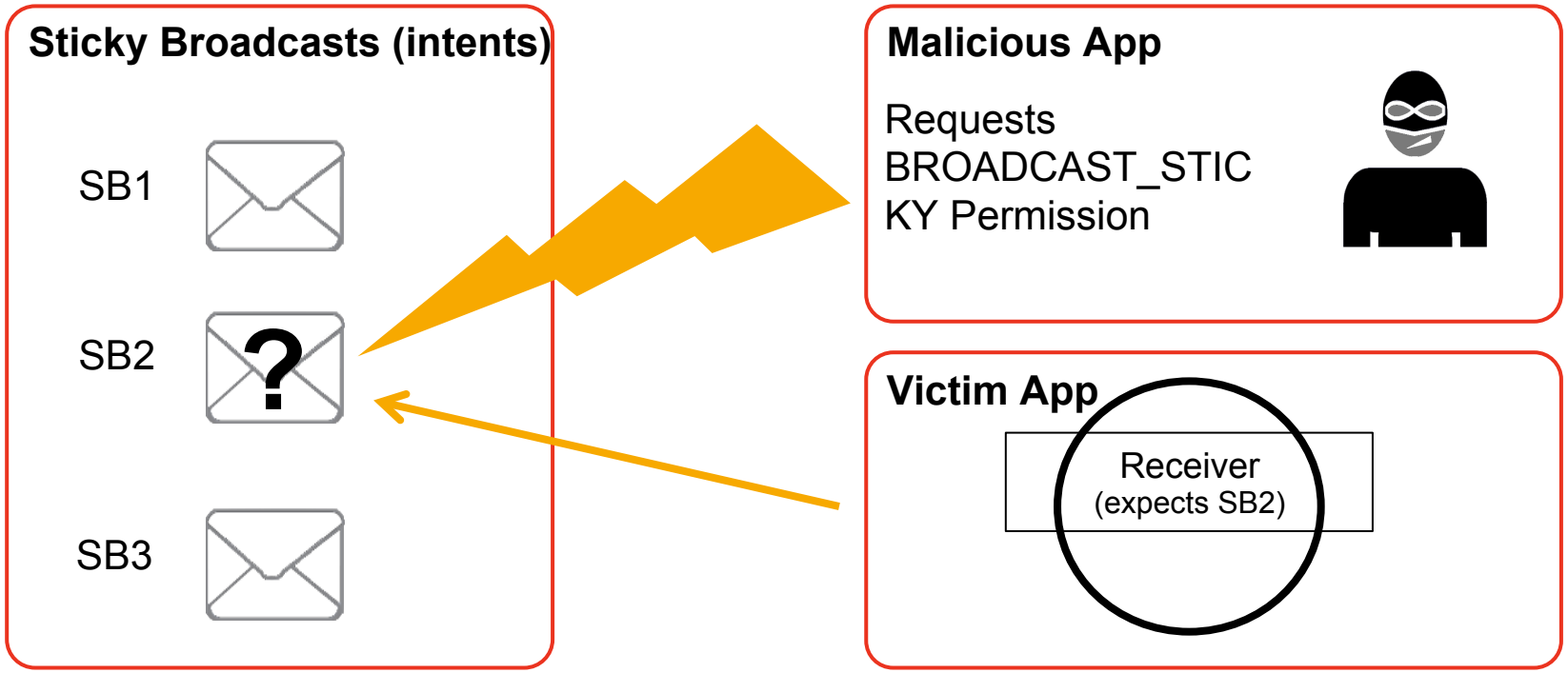
Description: Persistent intents can be accessed and removed by malicious apps

Cause: BROADCAST_STICKY allows to full access to any sticky broadcasts

Fix: **Explicit, non-sticky broadcasts and receiver permissions**

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	**Sticky Broadcast Tampering**	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges



Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	**Insecure Storage**	Insecure Network Communication	SQL Injection	Promiscuous Privileges

Description: Local storage visible to attackers and can compromise sensitive data

Cause: Local files are world-readable and persist

Fix: **Use SQLite or internal storage for private data**

Encrypt the data (keep keys off the SD)

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	**Insecure Storage**	Insecure Network Communication	SQL Injection	Promiscuous Privileges

- Kindle app saves e-books (.mbp and .prc) in a folder on the SD card
  - Depending on DRM, accessible to other apps
  - Saves covers of books (privacy violation)
  - Folder is retained after uninstall of app

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

Description: Unencrypted channels can be intercepted by attackers sniffing network

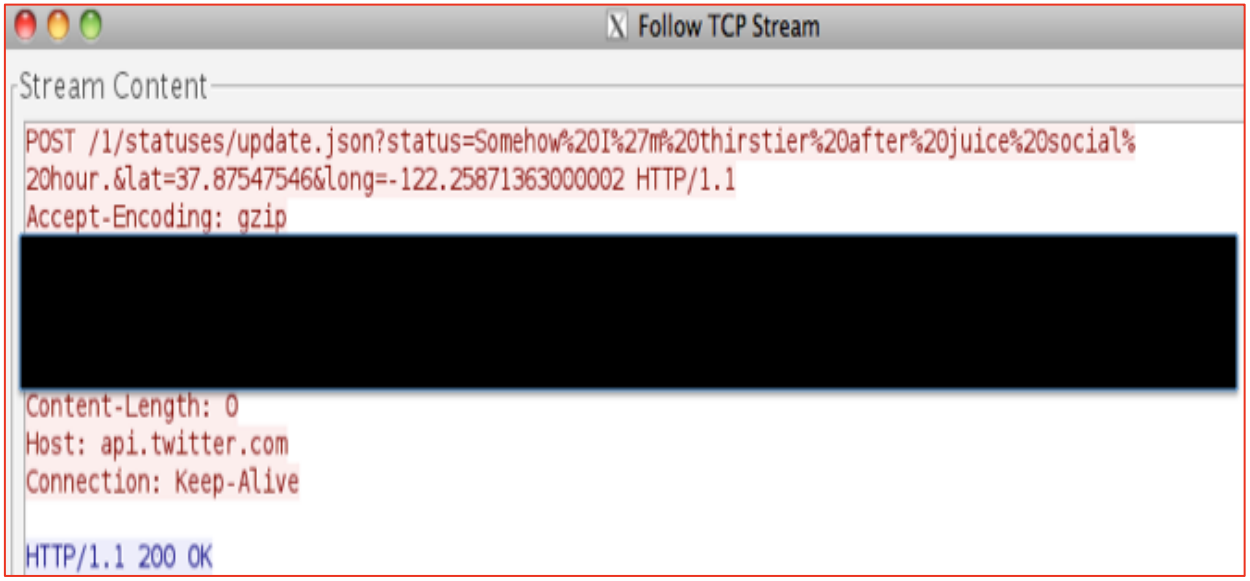
Cause: Non-HTTPS WebView connections

Fix: **Send sensitive data only over encrypted channels**

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

Twitter: Tweets are sent in the clear

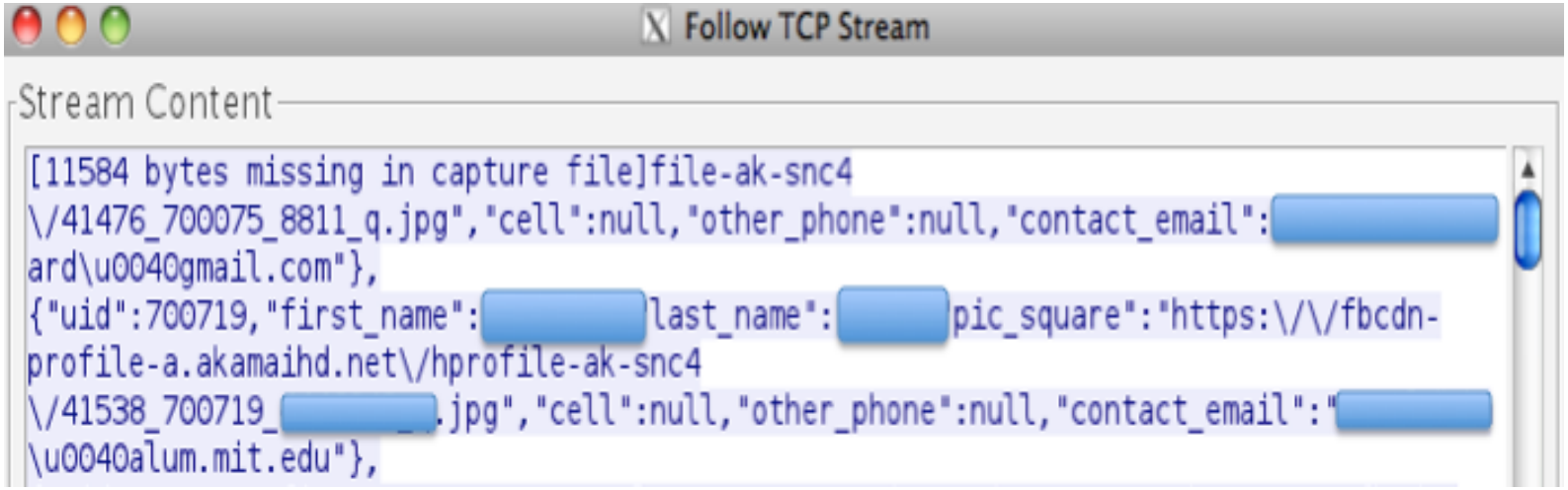


https://freedom-to-tinker.com/blog/dwallach/things-overheard-wifi-my-android-smartphone

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

Facebook: Despite 'fully encrypted' option on the Web, mobile app sends in the clear



Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

Description: Malicious users alter or view (query string injection) database records

Cause: Untrusted data used to construct a SQL query or clause

Fix: **Parameterized queries**

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

```
c = invoicesDB.query(
    Uri.parse(invoices),
    columns,
    "productCategory = '" +
        productCategory + "' and
        customerID = '" + customerID + "'",
    null, null, null,
    "'" + sortColumn + "'",
    null
);
```

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

productCategory = Fax Machines

customerID = 12345678

sortColumn = price

```
Select    * from invoices
where     productCategory = ' Fax Machines'
and  customerID = '12345678'
order by 'price'
```

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

productCategory = Fax Machines' or productCategory = \"

customerID = 12345678

sortColumn = \" order by ‘price

select * from invoices

where productCategory = **'Fax Machines'**

orproductCategory = “ ‘

~~and customerID = ‘~~ **12345678** ~~' order by ‘ "~~

order by 'price'

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

```
c = invoicesDB.query(
    Uri.parse(invoices),
    columns,
    "productCategory = ? and customerID = ?",
    {productCategory, customerID},
    null,
    null,
    "sortColumn = ?",
    sortColumn
);
```

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

Description: Extra permissions permit privilege escalation and desensitizes users

Cause: Deputies,
Artifacts from testing,
Confusion (inaccurate/incomplete resources)

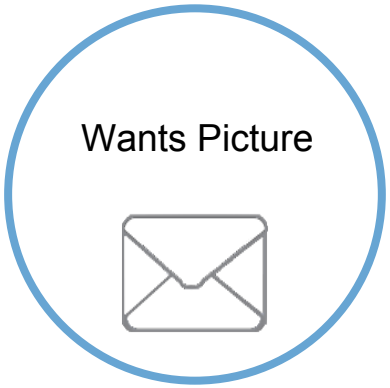
Fix: **Identify unnecessary permissions**

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

User App

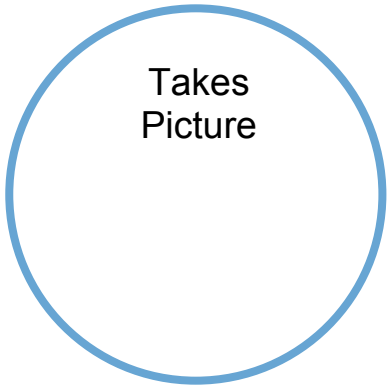
Does NOT need CAMERA permission



Implicit Intent
Action:
IMAGE_CAPTURE

Camera App

Needs CAMERA permission

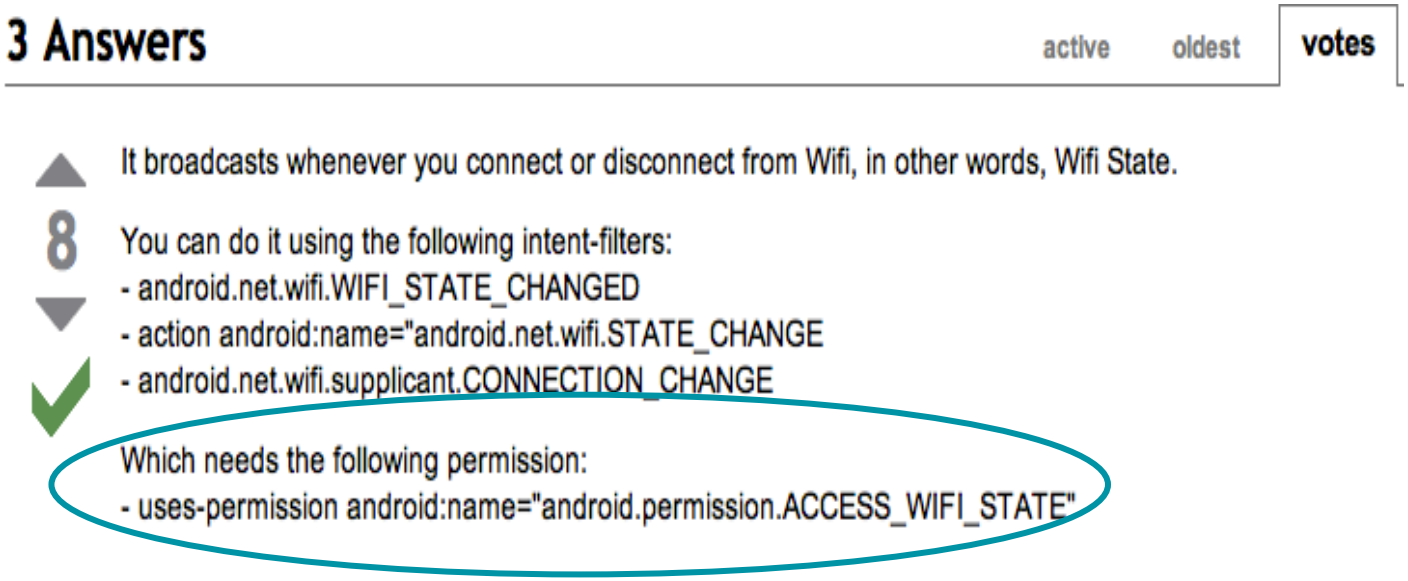


Handles Action:
IMAGE_CAPTURE

Google Android Vulnerabilities

Intent Hijacking	Intent Spoofing	Sticky Broadcast Tampering	Insecure Storage	Insecure Network Communication	SQL Injection	Promiscuous Privileges

- Third hit on Google search



Not true for android.net.wifi.STATE_CHANGE

http://stackoverflow.com/questions/2676044/broadcast-intent-when-network-state-has-changend

Empirical Results: DEFCON ‘11

Vulnerability Type	% of Apps
1. Intent Hijacking	**50%**
2. Intent Spoofing	**40%**
3. Sticky Broadcast Tampering	6%
4. Insecure Storage	28%
5. Insecure Communication	N/A
6. SQL Injection	17%
7. Promiscuous Privileges	**31%**

Bonus: iGoat

- iGoat 1.0 documents 5 vulnerabilities
  - We find 15+
- iGoat 1.2 documents 7 vulnerabilities
  - We find 20+

iGoat

bahhhhhhhhhhhhhhhhhhhhh

Parting Thoughts

What Questions to Ask?

- What do your apps do and for whom?
- What platform(s) do your apps support and how?
- Who develops your apps and where?
- Is there an existing SDL for other development?
- Do you rely on platform providers or app distributors for any security assurance?
- Are mobile apps prompting back-end changes?
- Are your apps appropriately permissioned?

Software Security Goes Mobile

Jacob West

CTO, Fortify Products

HP Enterprise Security

July 12, 2012