移动应用 安全为先

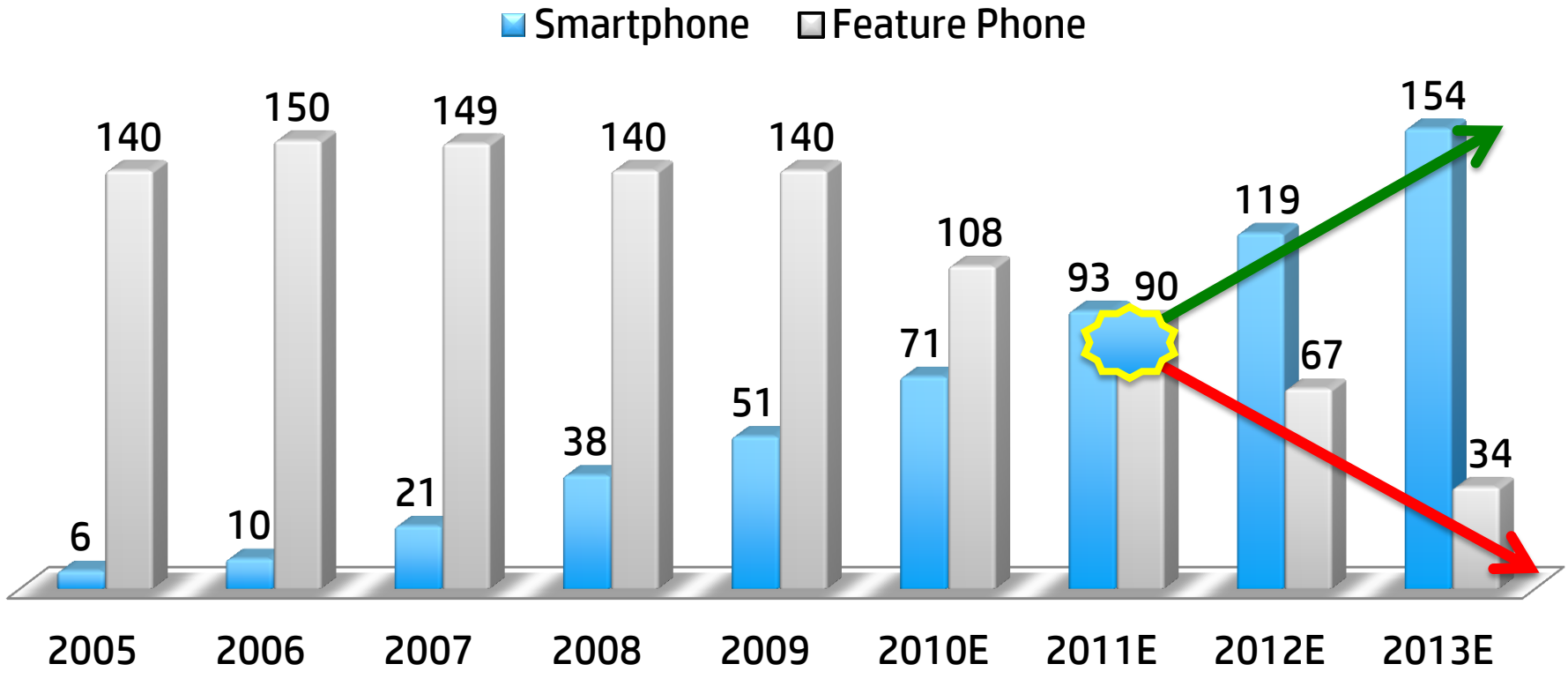
姚翔
北亚区总经理
企业安全产品部

关注惠普安全官方微博@惠普安全

大纲

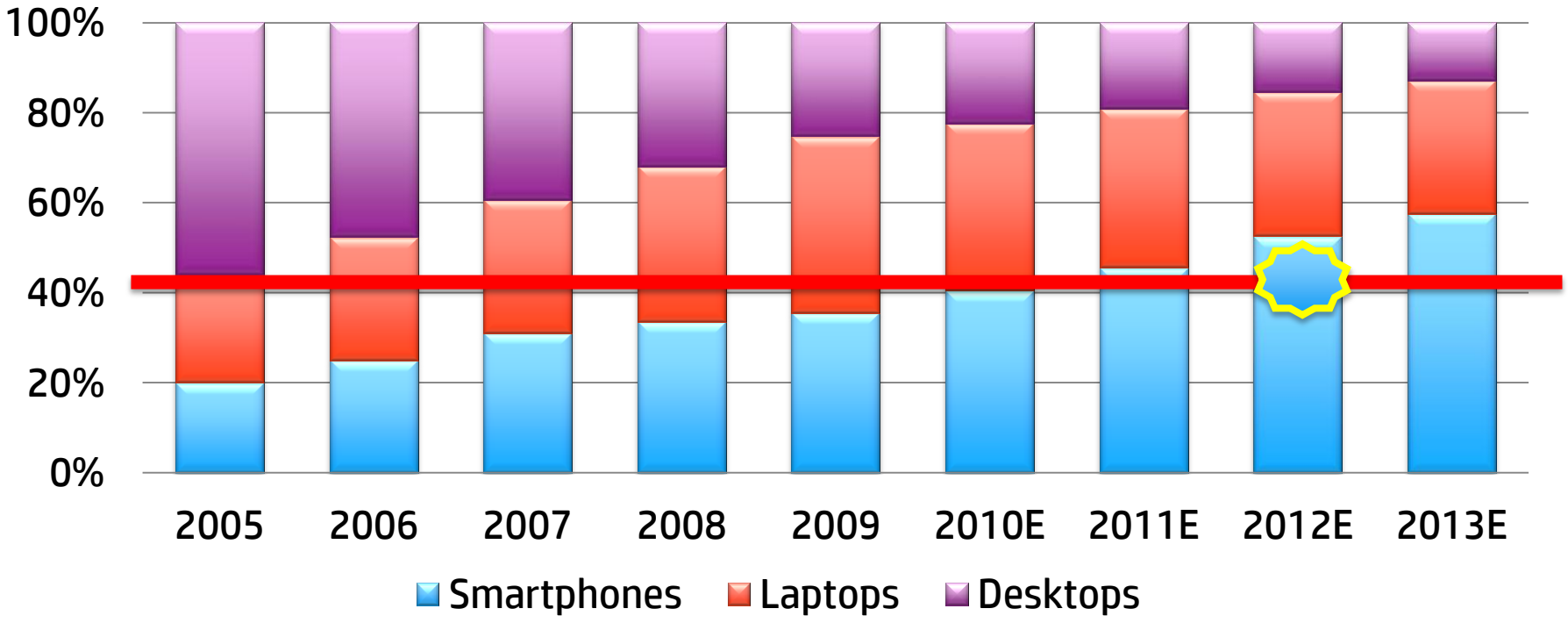
- 移动应用的趋势与威胁
- 移动应用 – **Three Layers**
- 移动应用安全解决思路
- 惠普移动应用安全解决方案
- **HP Fortify SCA**
- **HP WebInspect**
- 惠普移动应用安全解决方案视频
- **Q & A**

智能手机 > 功能手机



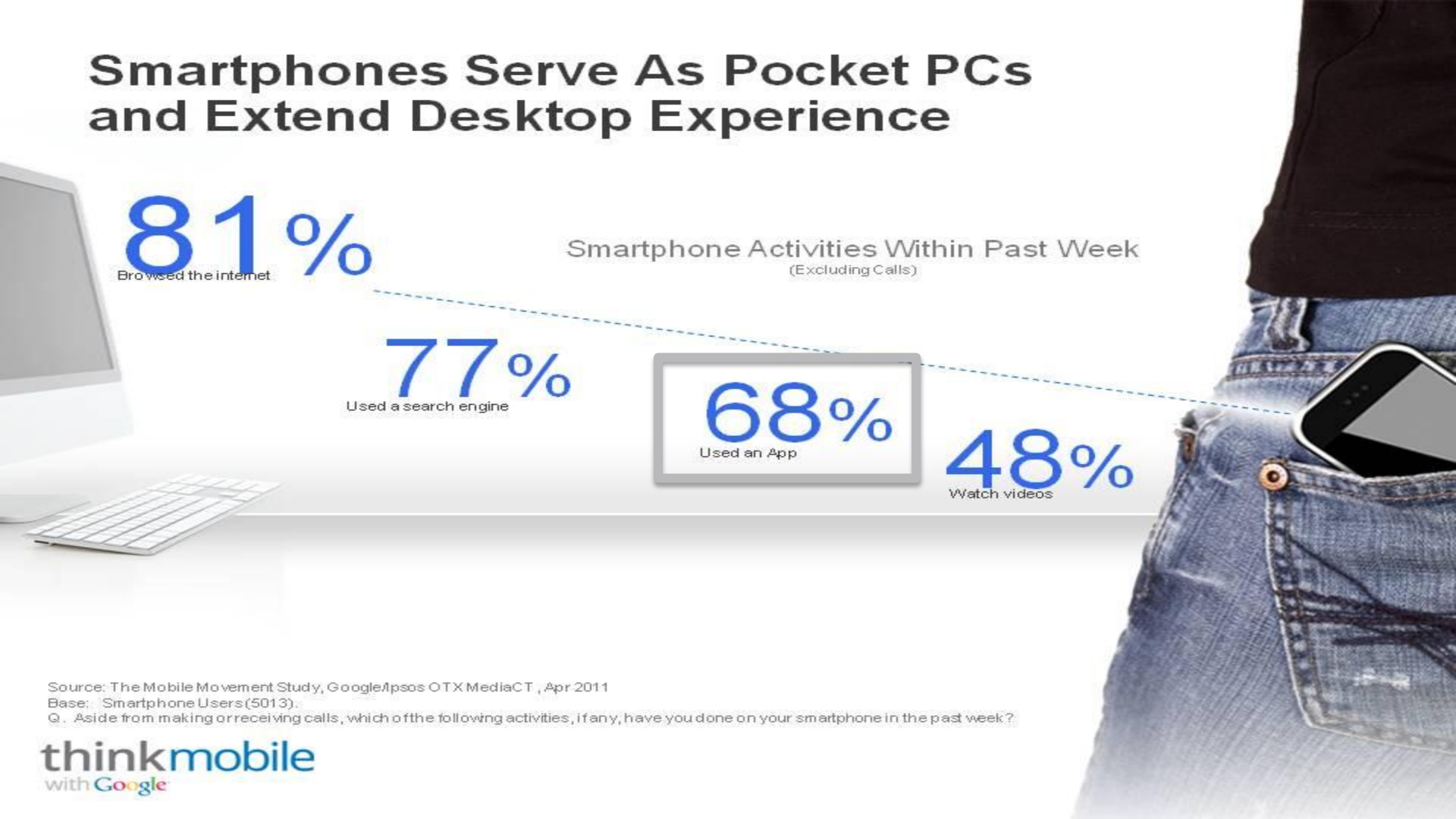
Source: Morgan Stanley Research

智能手机 >PC机



Source: Morgan Stanley Research

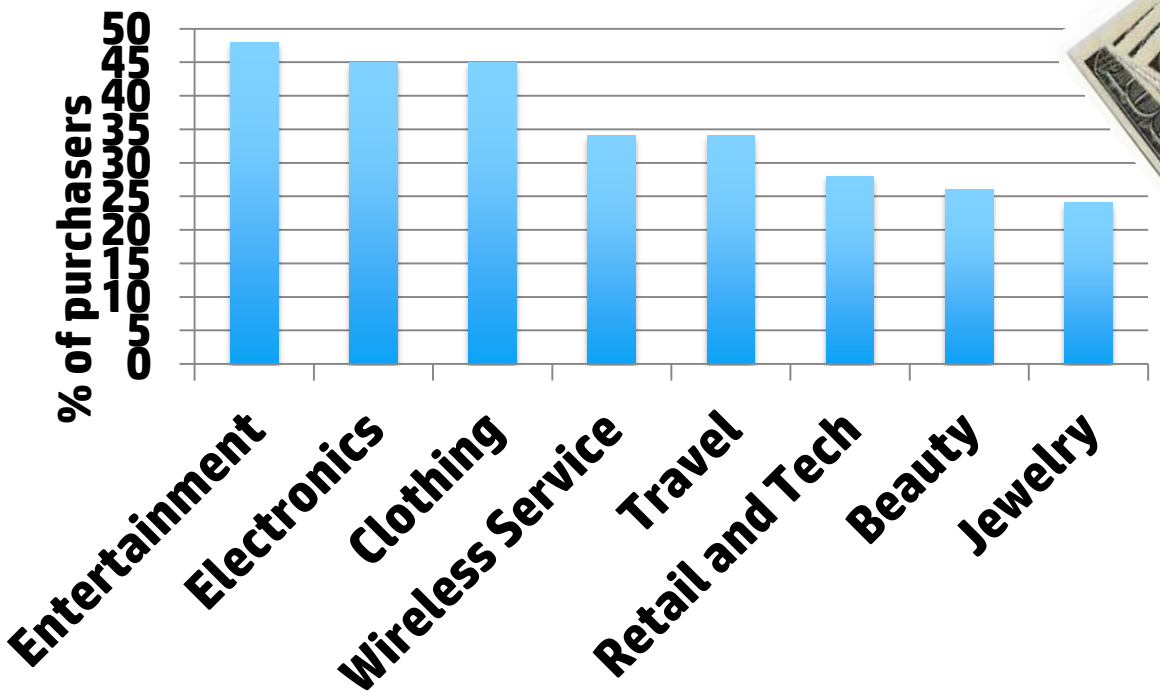
Smartphones Serve As Pocket PCs and Extend Desktop Experience



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

移动支付消费项



$300/year/user

Source: Google The Mobile Movement Study

移动应用的趋势

- <u>惠普趋势分析</u>
- 2015年（约6亿个移动台设备，将有近一个人均移动台设备）
- 2014年移动支付将超过的900亿美元
- 2010年和2015年间，全球移动台数据流量将增加26倍
- 2015年，全球移动台数据流量的三分之二将会是视频(个人移动 TV，Movie)

十大移动应用未來趋势
2011 GARTNER REPORT

1、地理位置服务

2、社交网络

3、移动搜索

4、移动商务

5、移动支付

6、移动电邮

7、移动视频

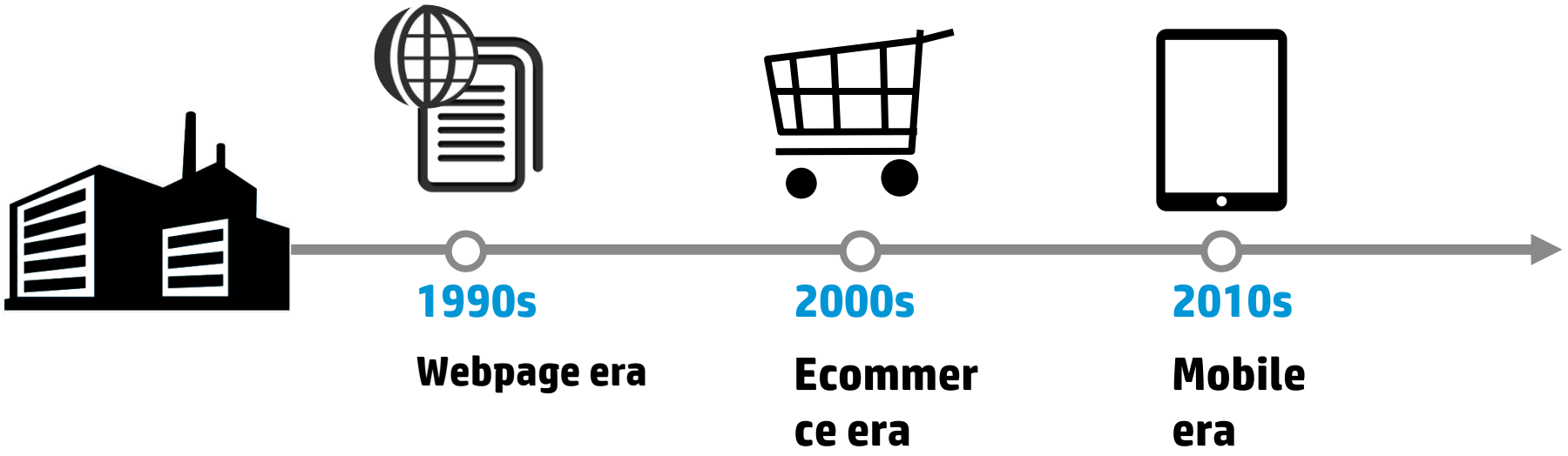
8、情境感知(context-aware)服务

9、移动即时通讯（MIM）

10、目标识别(object recognition)服务

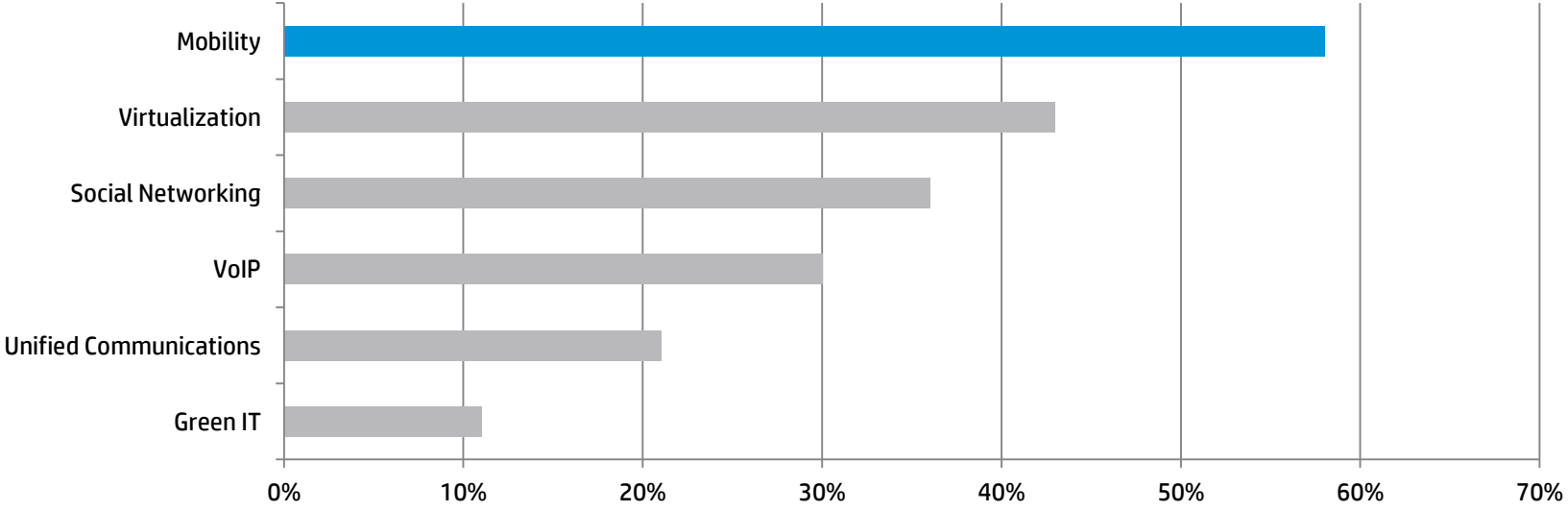
这些移动应用趋势的背后意味着，需要有更多相关移动应用程序的支撑。

现代商业的进化



安全迫在眉睫.....

Which of the following technologies have resulted in an increase in IT security management spending at your organization within past 12 months?

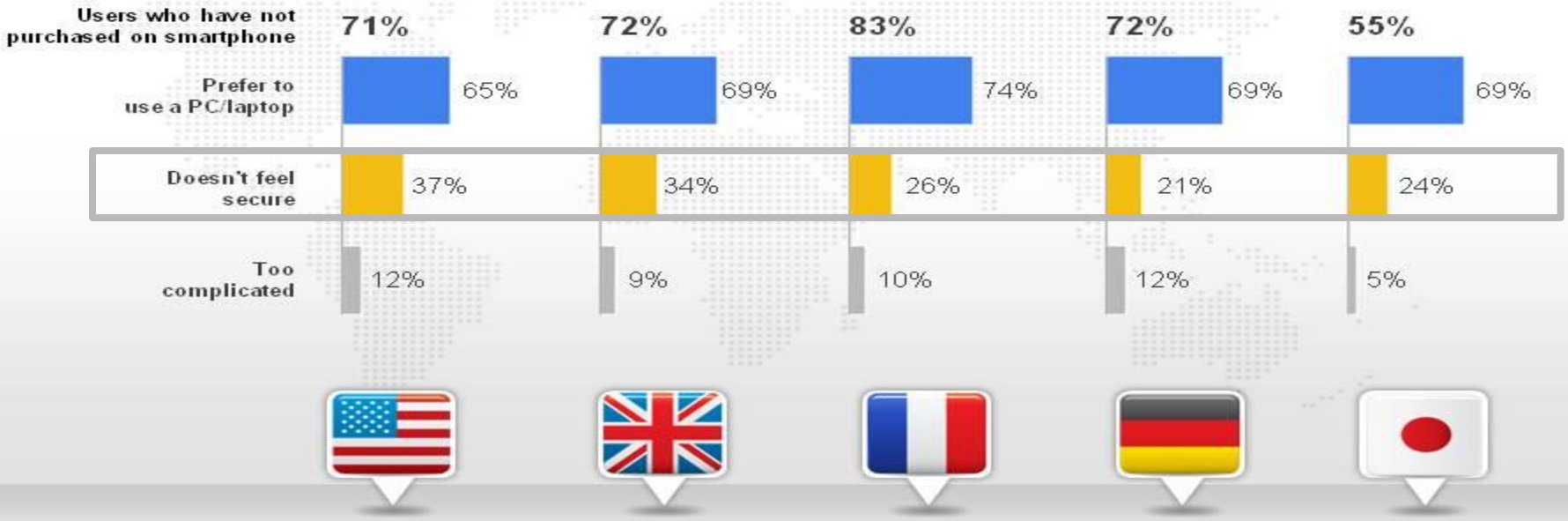


IDC Web Conference, 12 April 2012

Source: IDC Security as a Service Survey n-47

因为安全问题....

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?

恶意软件成企业级市场移动应用最大隐忧

恶意软件成企业级市场移动应用最大隐忧

http://www.enet.com.cn/cio/ 2012年04月05日08：46 来源：新浪-科技频道

【文章摘要】网络安全公司Juniper Networks移动安全主管丹·霍夫曼（Dan Hoffman）表示，应用商店中正“迅速成为感染应用的主要传送机制”。消费者通过在线应用商店为其设备购买相关应用。由于消费者可以自由向其设备上下载应用，所以威胁防范的门槛较低。黑客只是简单的将恶意软件嵌入到有吸引力的游戏和应用中，以诱使用户下载。

越来越多的公司开始允许员工在工作中使用智能机和平板电脑，他们正面临一个新的潜在威胁——嵌入游戏和应用的恶意软件。

网络安全公司Juniper Networks移动安全主管丹·霍夫曼（Dan Hoffman）表示，应用商店中正“迅速成为感染应用的主要传送机制”。消费者通过在线应用商店为其设备购买相关应用。

由于消费者可以自由向其设备上下载应用，所以威胁防范的门槛较低。黑客只是简单的将恶意软件嵌入到有吸引力的游戏和应用中，以诱使用户下载。一旦被嵌入到应用中，恶意软件就会在用户毫不知情的情况下拨打可盈利的电话号码，或者向付费网站发送短信、窃取密码以及其它账户，并追踪用户行踪。

企业所忌惮的是，恶意软件可以会被用来访问已经下载到个人设备上的公司数据。霍夫曼称，Android设备成为去年恶意软件攻击的主要目标，因为该机型统治了智能机市场。

目前还不清楚苹果设备上是否会出现类似威胁，因为苹果的系统是封闭的，不允许外部安全厂商独立追踪苹果设备威胁。

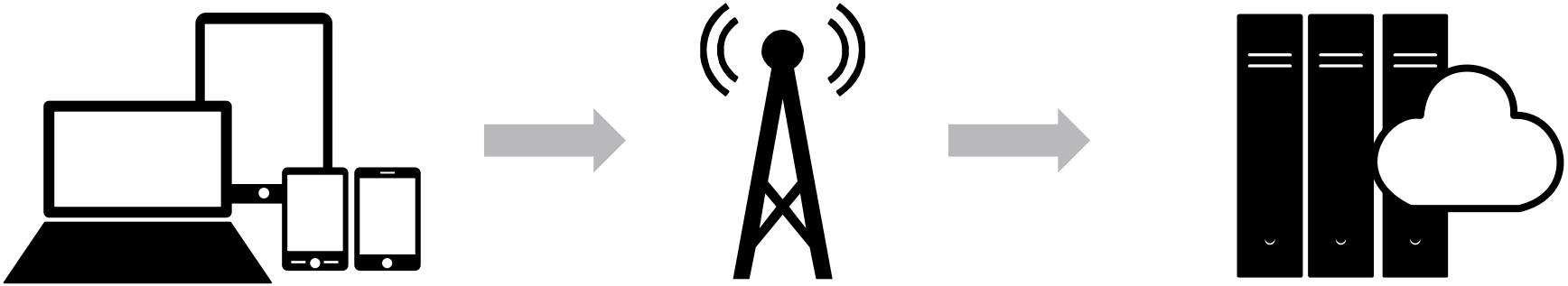
智能手机会暴露你的隐私

Your smartphone knows you better than you know yourself

- Pins & passwords
- Contacts
- Call history
- Messages
- Social networking
- Visited web sites
- Mobile banking
- Personal videos
- Family photos
- Documents

… and cyber attackers are after your personal records

来自三个层面的威胁



Client

- Insecure storage of credentials
- Improper use of configuration files
- Use of insecure development libraries

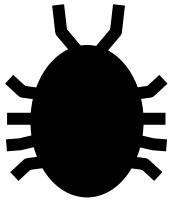
Network

- Insecure data transfer during installation or execution of the application
- Insecure transmission of data across the network.

Server

- Authentication
- Session Management
- Cross-site Scripting
- SQL Injection
- Command Injection

典型的移动互联安全威胁有:

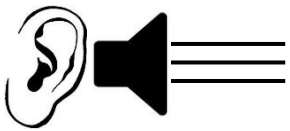


Malware

Spyware, viruses, trojans, and worms

Loss and Theft

Data lost due to misplaced or stolen mobile devices

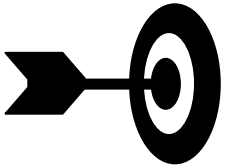


Data Communication Interception

Eavesdropping on communications, including emails, texts, voice calls, etc., originating from or being sent to a mobile device

Exploitation and Misconduct

The inappropriate use of a mobile device for personal amusement or monetary gain

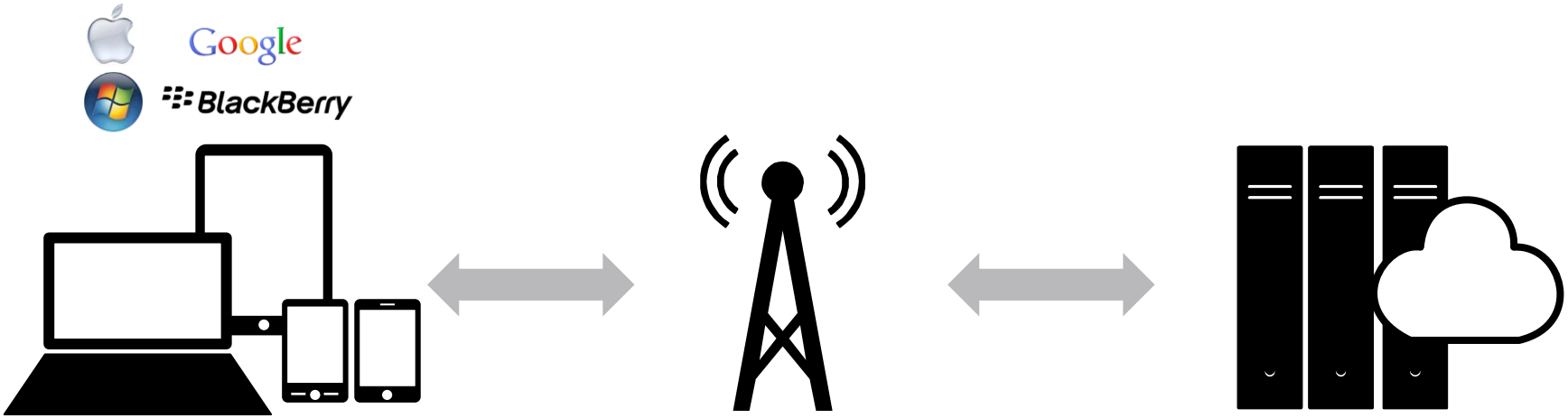


Direct Attacks

Short message service (SMS) and browser exploits

The solution

What is mobile?



Devices **Connection** **Servers**

移动应用 – Three Layers

1. Server

移动应用 – Three Layers

2. Network

移动应用 – Three Layers

3. Client

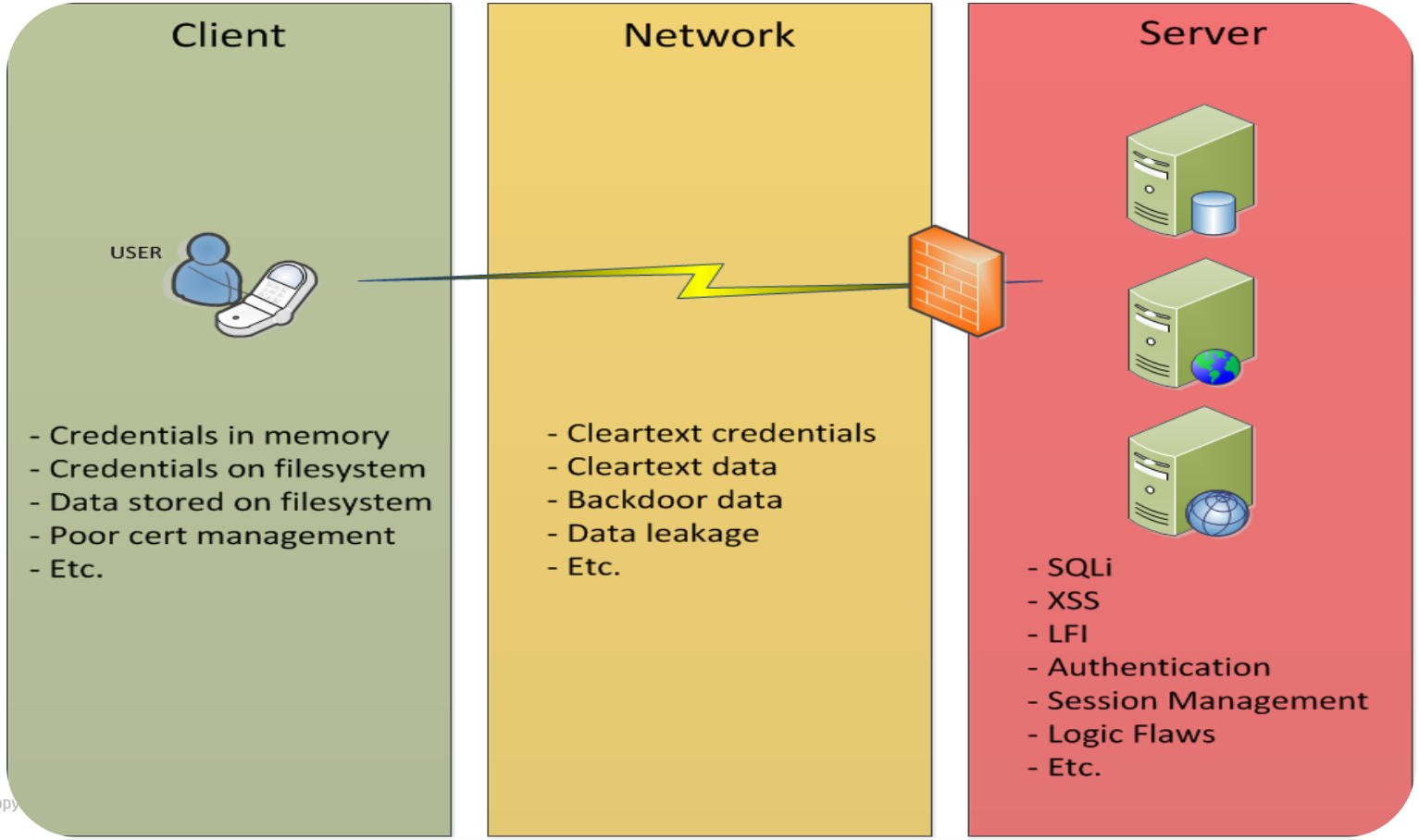
移动应用 – Three Layers

1. Server

2. Network

3. Client

移动应用安全方案 - Security Thinking



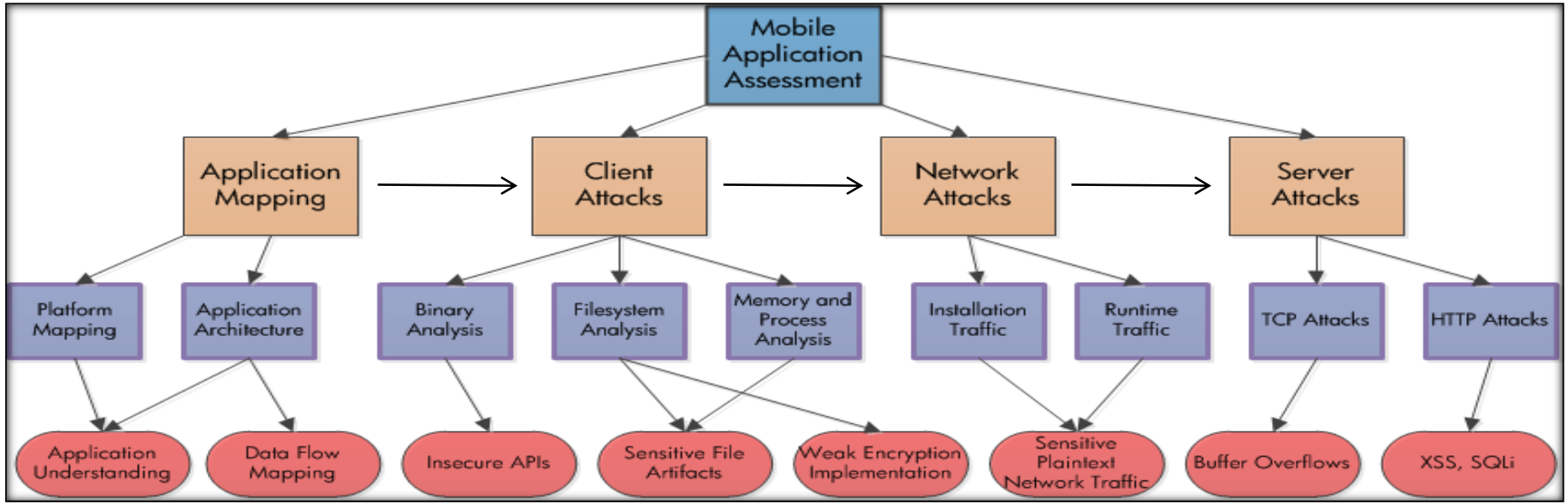
移动应用安全方案 – 基本检查表

Methodology Section	Check / Vulnerability Examples
Client (Static and Dynamic)	• Dropped files on the filesystem • Poor use of APIs • Certificate issues • Credentials stored on device • Data stored on device
Network (Dynamic)	• Insecure transmission of credentials • Improper transmission of application data • Reliance on the client for security • Checks for sensitive obfuscated data
Server (Static and Dynamic)	• SQL Injection vulnerabilities • XSS vulnerabilities • Authentication and Session management issues • All standard web assessment vulnerabilities

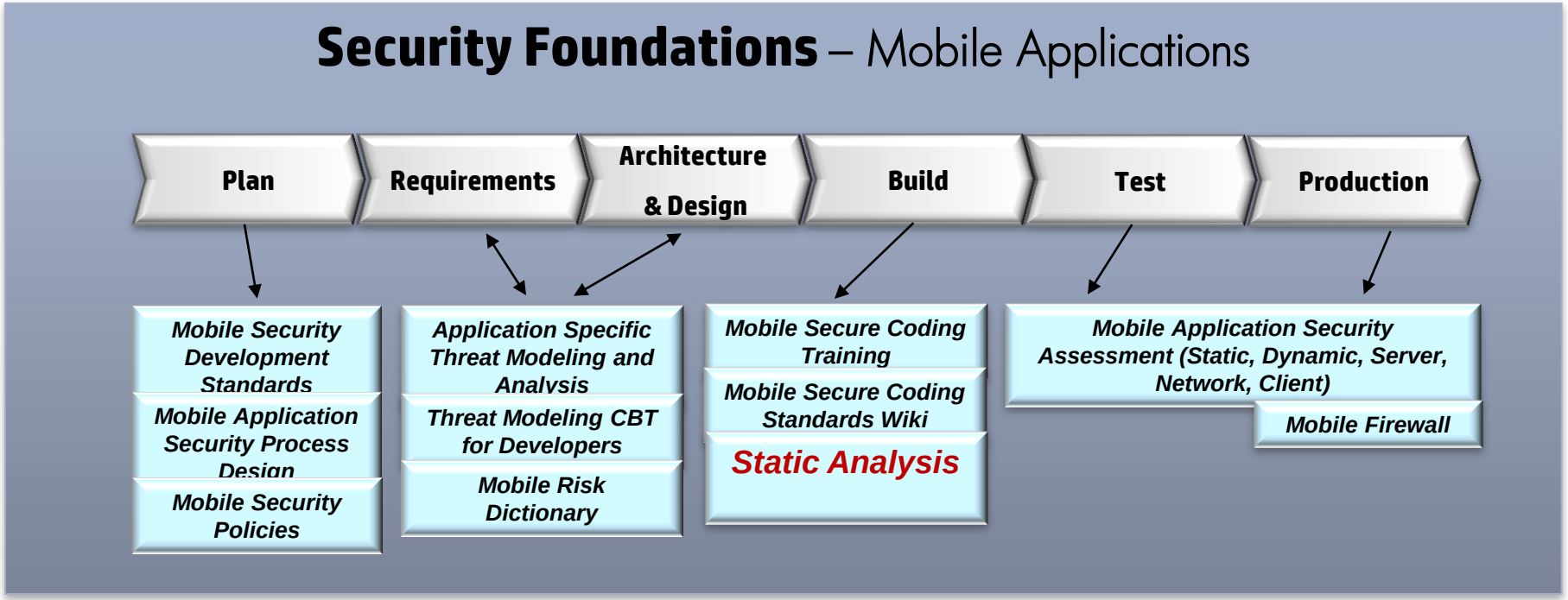
清晰的思路 (Clear Thinking)

- **Know** where you are using credentials
- **Know** what sensitive data is in pl
- **Track** these through the device, and backend
- **Test** those all components and their running paths

移动应用安全设计 - Security Thinking



移动应用安全开发流程整合 – Security Jobs



BETTER TOGETHER

ArcSight

FORTIFY

TippingPoint

ENTERPRISE SECURITY

hp

谢谢！