CRAFTING AN ADAPTIVE MOBILE SECURITY POSTURE

Vijay Dheap (@dheap)
IBM Security Division

RSA CONFERENCE EUROPE 2013

Session ID: MBS-R07

Session Classification: Intermediate

So Let's Talk!

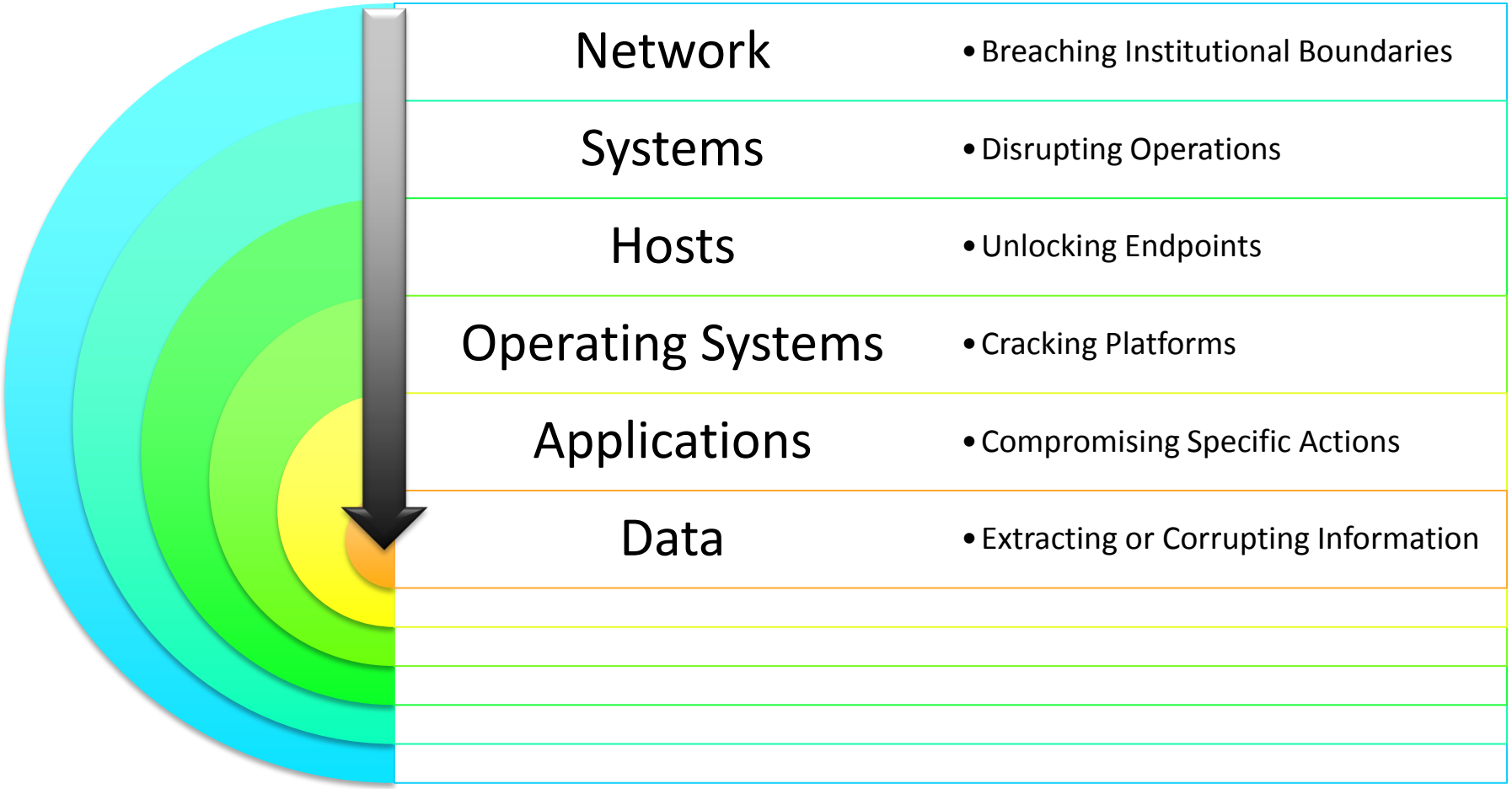
- Motivations for Mobile Security
  - Trends
  - Challenges
- What does Mobile Security Include?
  - Securing the Mobile Device
  - Protecting Mobile Access & Managing Users
  - Mobile App Security
- Looking Ahead…
  - Assessing Your Mobile Security Posture
  - Bold Prediction

So Tell Me Again Why We Need Mobile Security?

#RSAC

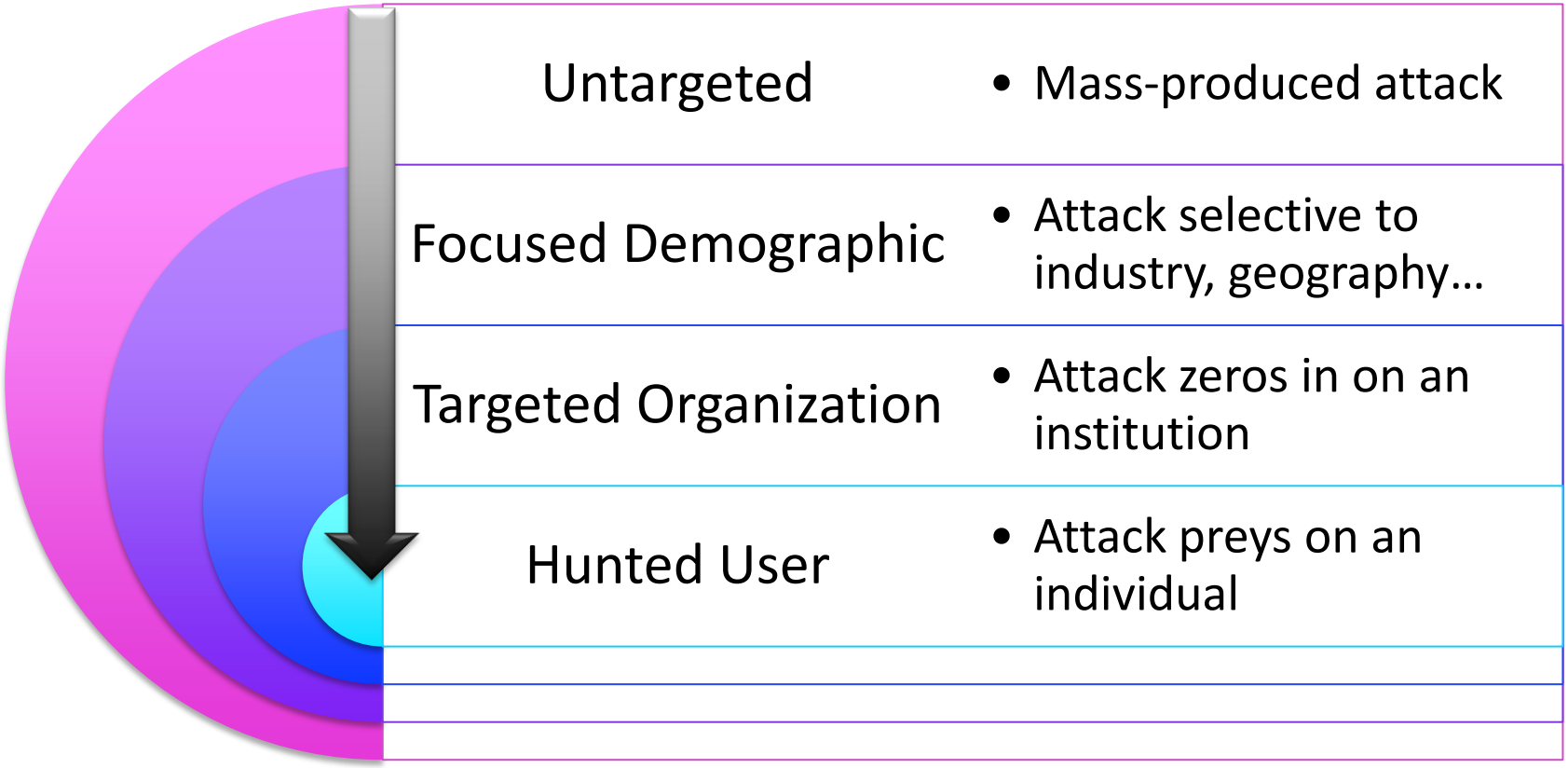
RSA CONFERENCE EUROPE 2013

Firstly How are Threats Evolving?



This Trend Continues for Mobile

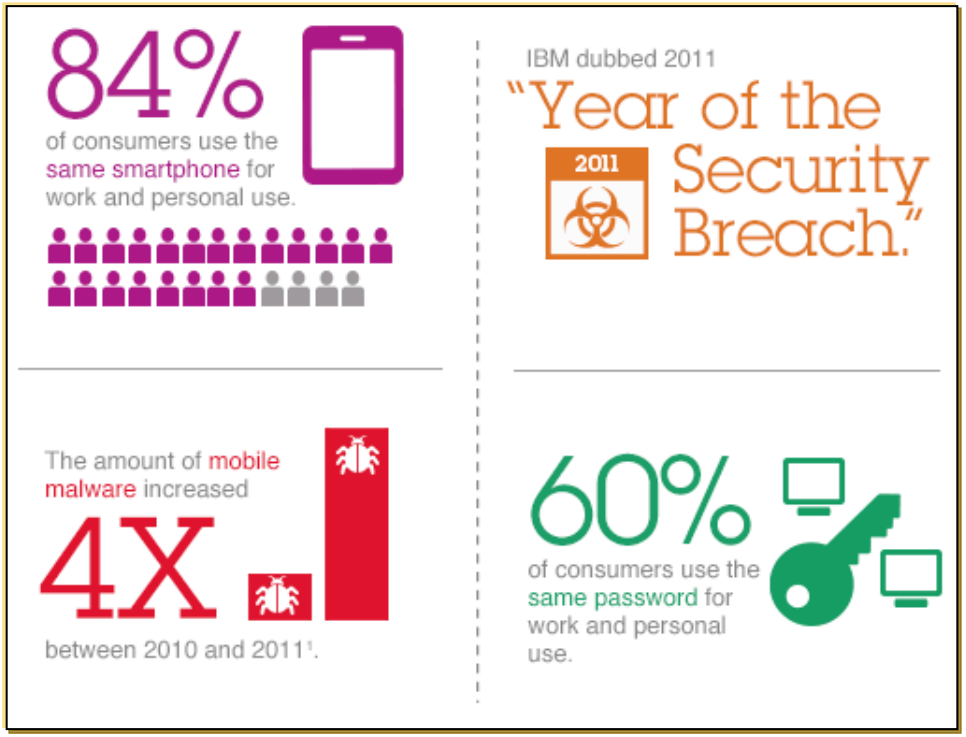
There is More…

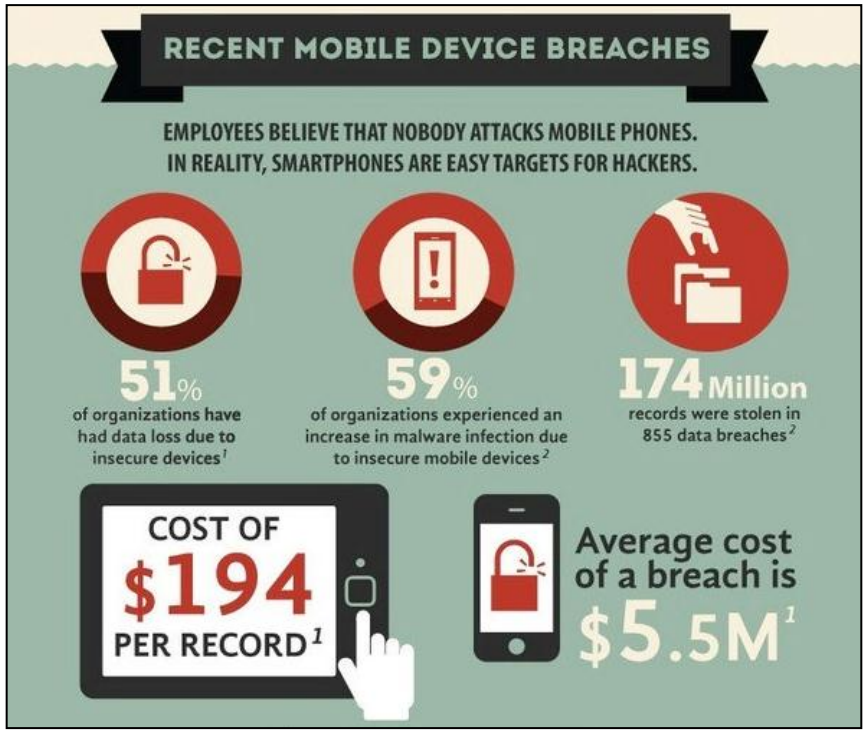


Mobile Facilitates This Trend

Mobile Brings Its Own Challenges

With a cost…





Mobile Security Can Be Unique

Mobile devices are shared more often

- Personal phones and tablets shared with family
- Enterprise tablet shared with co-workers
- Social norms of mobile apps vs. file systems

Mobile devices have multiple personas

- Work tool
- Entertainment device
- Personal organization
- Security profile per persona?

Mobile devices are diverse

.

- OS immaturity for enterprise mgmt
- BYOD dictates multiple OSs
- Vendor / carrier control dictates multiple OS versions

Mobile devices are used in more locations

- A single location could offer public, private, and cell connections
- Anywhere, anytime
- Increasing reliance on enterprise WiFi


Mobile devices prioritize the user

- Conflicts with user experience not tolerated
- OS architecture puts the user in control
- Difficult to enforce policy, app lists

Structuring Our Thinking…

1. Device Security & Management

Security for endpoint device and data

2. Network, Data, and Access Security

Achieve visibility and adaptive security policies

3. Application Layer Security

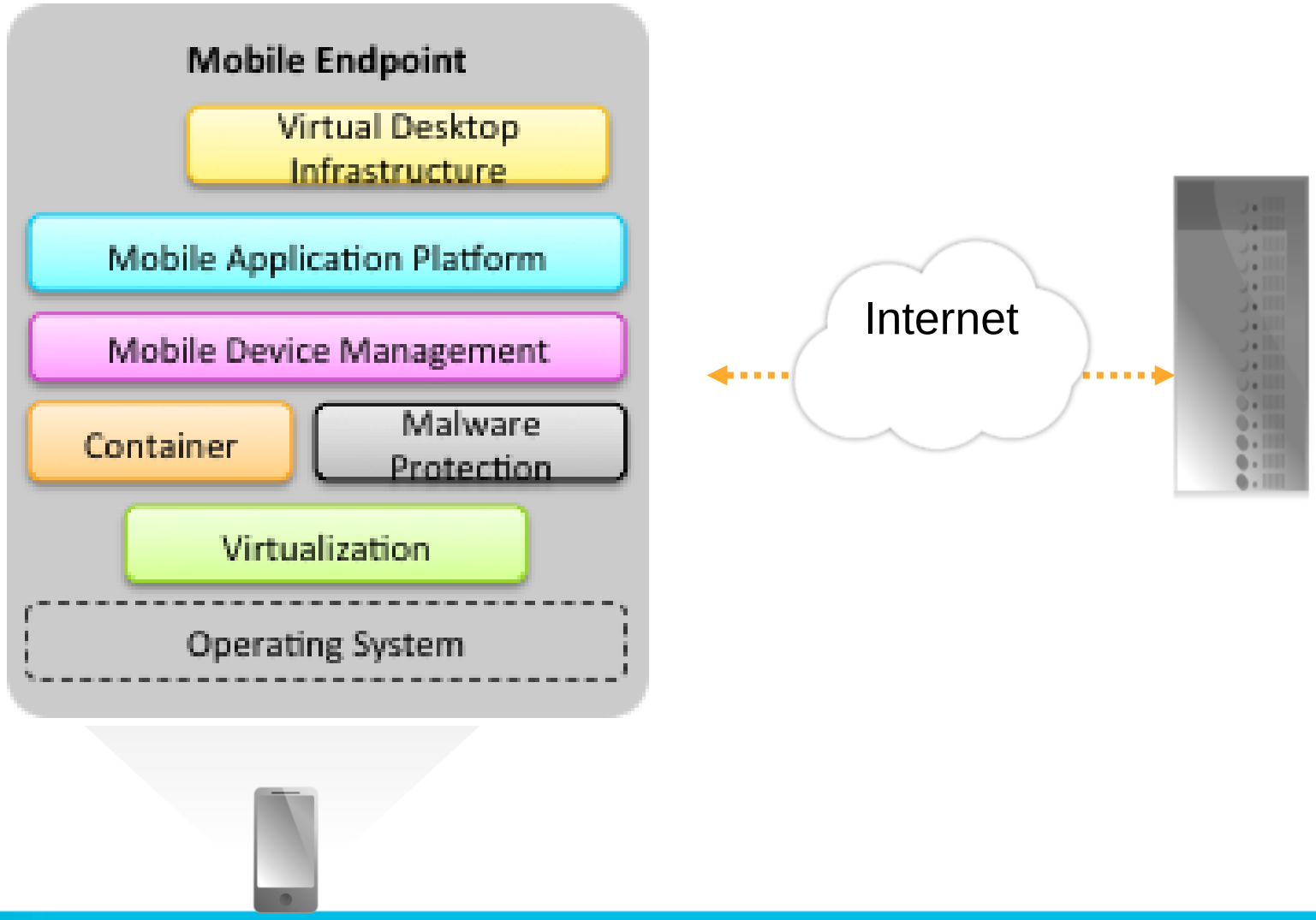
Develop and test applications

How Do We Approach Endpoint Security?

#RSAC

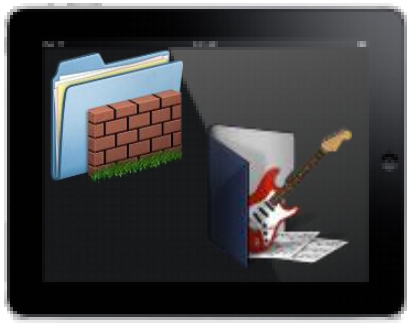
RSA CONFERENCE EUROPE 2013

Device Security: Technical Options



It’s the Data not the Device!

Data Separation



- BYOD trend: Personal devices being employed for business use
- Need to balance control, security and management of enterprise data on dual/multi-use mobile devices without infringing on user privacy
- Separation of enterprise data (mobile apps, email, and mobile browser) affords greater precision in mandating and enforcing security policy

Data Leakage Prevention

- Data flow on a mobile device needs to be controlled to prevent data leakage or loss
  - Enterprise data may flow from enterprise apps to non-enterprise apps to view content (i.e. email attachments)
  - User may consciously move enterprise data to personal apps (i.e. DropBox, Gmail)
  - User or malware may move enterprise data to secondary storage or over a network (i.e SD card, Bluetooth)

How Do We Protect the Data?

	Description	Strengths	Weaknesses
Mobile Device Mgmt +Mobile App Platform (optional)	MDM will provide security and management features for the device and enterprise apps. Mobile App Platform will provide a secure run-time for each app and enforce development best practices	• Lightweight footprint on the device • Maintains user experience of the device • Enterprise apps enforce separation • Adaptable to OS containerization services	• Cannot guarantee data separation enforced by third-party apps • Limited data leakage prevention • Limited differentiation
Secure Container	Explicit data separation by segregating enterprise apps in a secure zone on the device. Provides a separate email client and browser for business use	• Data separation and data leakage prevention • Granular management of just the secure zone not the whole device	• Negative impact on user experience • Forces third party apps to employ SDK • Loses value if OS delivers containerization • Most solutions don't support native iOS apps
Virtual Desktop Infrastructure	Allows employees to access enterprise data, applications without ever transferring content to the mobile device – all applications run on the server	• Data separation and data leakage problems don't arise • Only requires a secure connection	• Negative impact on user experience: network latency, most apps don't support touch interface • Network overhead
Virtualization	Transforms a mobile device into a personal device and a business device. Mobile users will employ a separate OS stack to access enterprise apps and data	• Data separation achieved • Enterprise can standardize on a secure OS • Complete control	• Cannot support iPhones and iPads • Still requires MDM for the business virtual image to prevent data leakage (i.e. prevent installing of unsanctioned apps) • User may have two distinct user experiences to learn

Mobile Users…
Protecting Them and their Access

#RSAC

RSA CONFERENCE EUROPE 2013

Why Mobile User Security?

Mobile users prioritize user experience and make device decisions based on their preferences

Mobile devices are shared and can have multiple personas

Imposing access security controls and methods that are unsuited for mobile can either lead to non-compliance or non-participation

Authenticating and authorizing just the user OR just the device might not provide necessary levels of controls on data and apps

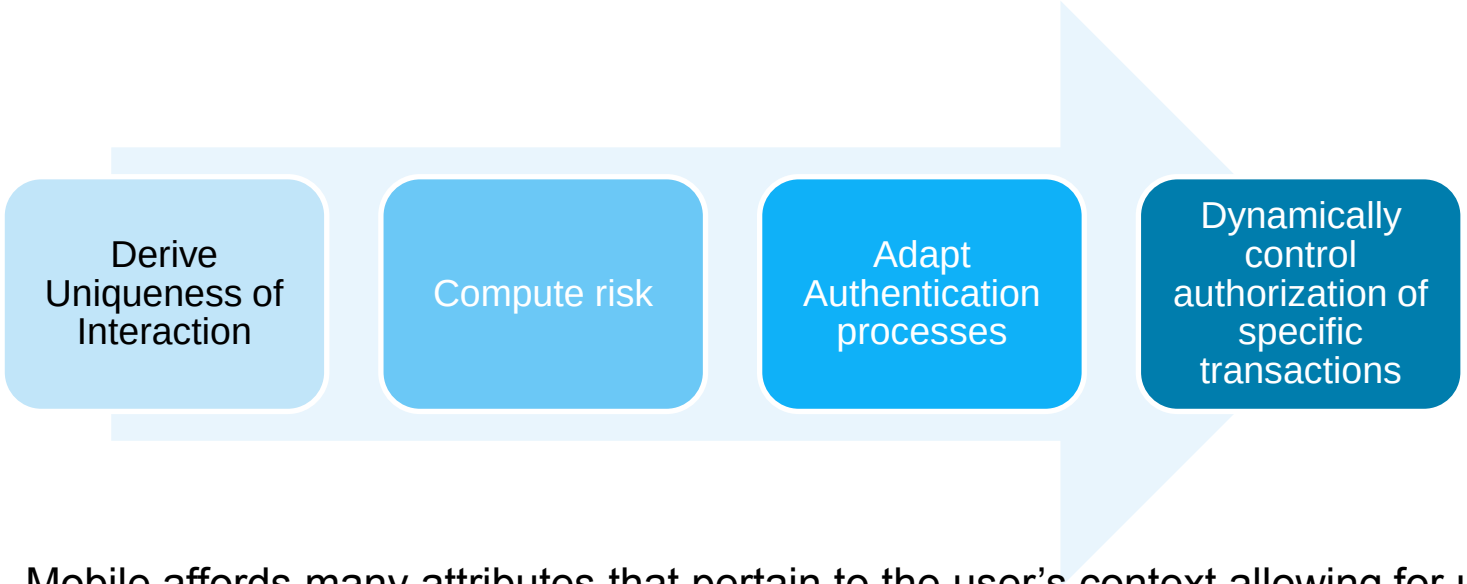
Mobile devices are most often used outside the corporate network and consumers may employ a wide variety of networks to access their accounts

The context in which mobile devices can change dramatically from one session to the next

The integrity of the user's transactions or communication can be compromised while they are interacting with mobile apps

The context can significantly influence the risk of the interaction and without proper consideration can lead to data loss or leakage

Context Influences Risk



- Mobile affords many attributes that pertain to the user's context allowing for unique identification of a specific interaction (i.e. location, network, time, device properties etc)
- Risk of the unique interaction can be computed based on established policies
- The risk score can be utilized to select the authentication processes best suited for that interaction
- The risk score can also be employed to control authorization for specific transactions during that interaction and deliver education to the user on security best practices in context

What Are the Core Requirements?

Authentication, Authorization, Accounting (AAA)	➢ Centralized AAA simplifies app logic thereby improving the risk profile of an app ➢ Flexibilty and support for mobile friendly authentication schemes – OAuth, OTP, Biometrics etc. ➢ Gradient trust levels requires strong/multifactor authentication which also improves user experience and in context bartering of security value ➢ Provides oversight of access for threat determination
Single Sign-On	➢ Preserve and improve user experience ➢ Streamline credentials management ➢ Translation and transformation of credentials based on demands of back-end APIs
Session Management	➢ Counter man-in-the-middle attacks ➢ Validate the integrity of the transaction ➢ Preserve and improve user experience
Federated Identity	➢ Employ third party Identity providers to enhance user experience ➢ Resolve the identity of an entity managed by another administrative domain ➢ Enforce authorization entitlements of the entity to resources

Emerging Requirements…

App-Level VPN	➢ Prevent malicious payloads from other apps on the same device to taint app-level communications ➢ Employ app appropriate encryption for data in motion
Context Gathering (includes device fingerprinting)	➢ Resolve the identity of the entity engaging in the interaction by correlating device, user and app ➢ Capture variables that can influence risk of a mobile interaction
Risk-Based Policy Engine for Management & Enforcement	➢ Standardize risk calculation from context variables across your enterprise ➢ Empower app owners to employ risk to influence business logic in their app through app policy definition and enforcement ➢ Enable IT to define global risk policies to establish a security baseline for all apps
Mobile App (Message-Level) Firewall	➢ Inhibit malicious content or code to be appended to app messages ➢ Identify rogue apps ➢ Mitigate threat from invalid inputs (i.e. SQL injection)
Mobile Network Threat Protection	➢ Counter the threat DDOS attacks by mobile botnets ➢ Identify and neutralize network borne attacks ➢ Detect suspicious activity across multiple sessions ➢ Prevent mobile malware for infecting back-end APIs or systems

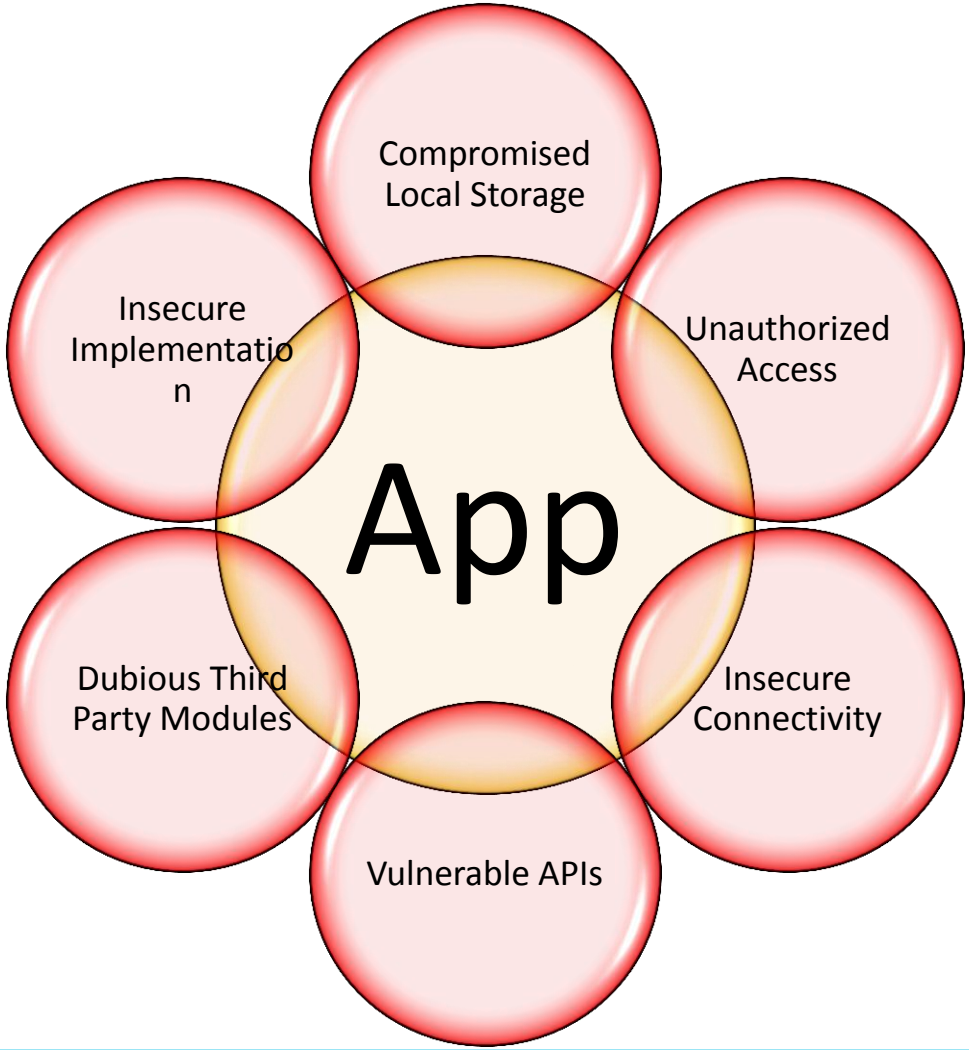
And the Apps?
How do we Defend them?

#RSAC

RSA CONFERENCE EUROPE 2013

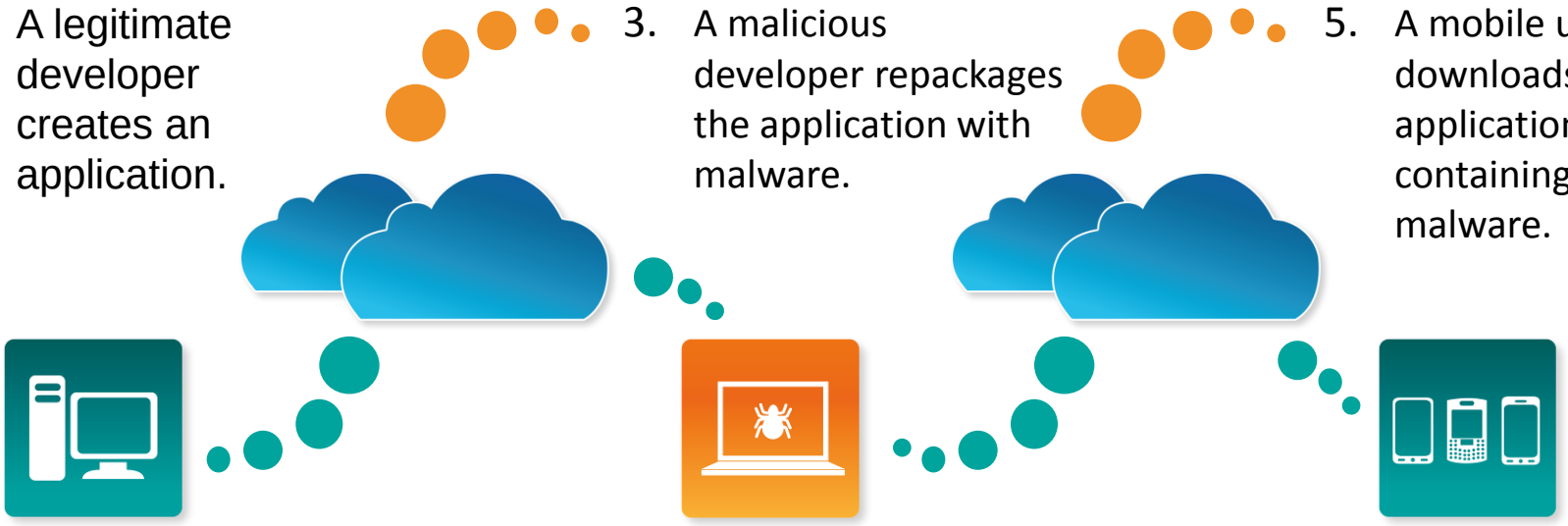
What Are We Defending?

The Threat Surface Area



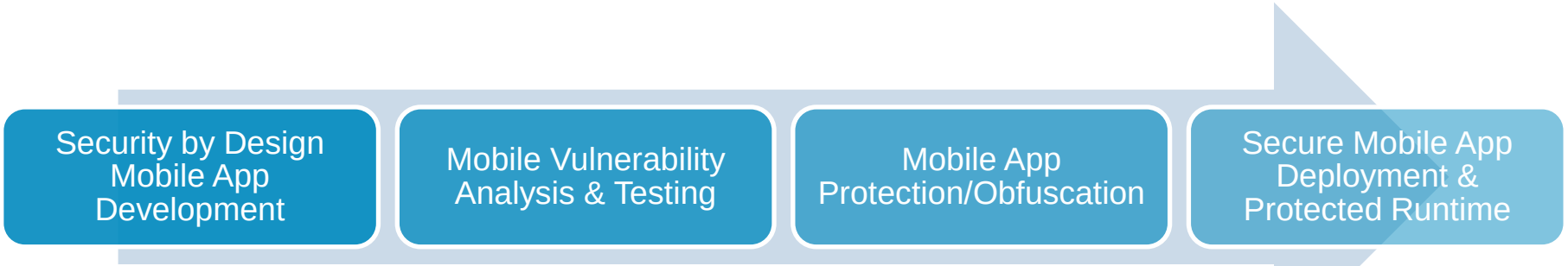
Good Apps Gone Rogue

1. A legitimate developer creates an application.
2. The legitimate developer uploads the application to an application store or website.
3. A malicious developer repackages the application with malware.
4. The malicious developer uploads the repackaged application to an application store where mobile users can download for free.
5. A mobile user downloads the application containing the malware.
6. The malicious developer can control the phone remotely, access the user's sensitive information or even infect enterprise servers.



Source: U.S. Government Accountability Office analysis of studies and security reports. September 2012, "Better implementation of controls for mobile devices should be encouraged"

Designing Security…



Security by Design Mobile App Development	Mobile Vulnerability Analysis & Testing	Mobile App Protection/Obfuscation	Secure Mobile App Deployment & Protected Runtime
Empower developers to seamlessly incorporate core security features into mobile apps	Assist developers to identify vulnerabilities in mobile apps and facilitates organizations' ability to enforce security quality for mobile apps	Enable developers and security engineers to harden and tamper-proof source code and or binary code to protect a mobile app's integrity	Secure the delivery channel for enterprise mobile apps Provide a protected runtime that is able to detect risks and react to threats Provide a context-aware risk based access control for mobile apps

In Conclusion…

#RSAC

RSA CONFERENCE EUROPE 2013

Maturity Model for Mobile Security

Optimized	**Mobile Security Intelligence** Risk Assessments, New Threat Detection, Active Monitoring			
	Integrated management of multiple devices Device Security policy management	Prevent loss or leakage of sensitive information Risk / Context based Access Threat Detection on inbound network traffic	Context / Risk based document collaboration / creating / viewing Enforce restrictions on copy/paste	Multi-factor context aware access and offline access Granular security policy definition and enforcement Enable data sharing based on policy
Proficient	Endpoint Protection with Anti-malware White/black list apps Detection of Jailbreak/rooted devices	Prevent copy and paste of email, calendar, contacts and intranet data Application level VPN	Secure document creation and viewing Document Collaboration with secure file sync / collaboration	App Management – provisioning/updates/disabling Separation of corporate apps from personal apps Application validation
Basic	Update management Device lock / Device wipe Device Registration	Segregated secure access corporate email, calendar, contacts and browser User /device authentication and single sign-on	Connectivity to social networks Secure instant messaging	Enforcing encryption of data within an app App Vulnerability Testing and Certification
	BYOD	**Data Separation**	**Mobile Collaboration**	**Mobile App. Security**

Ah…Now for the Bold Prediction

Mobile computing is becoming increasingly secure, based on technical controls occurring with security professionals and software development

- Separation of Personas & Roles
- Ability to Remotely Wipe Data
- Biocontextual Authentication
- Secure Mobile App Development
- Mobile Enterprise App Platform (MEAP)

Thank you!

Vijay Dheap

IBM Security

@dheap

vdheap@us.ibm.com

www.ibm.com/mobile-security

#RSAC

RSA CONFERENCE EUROPE 2013