ISC 2015 中国互联网安全大会

360互联网安全中心

ISC 2015

数据驱动安全

2015 中国互联网安全大会 China Internet Security Conference

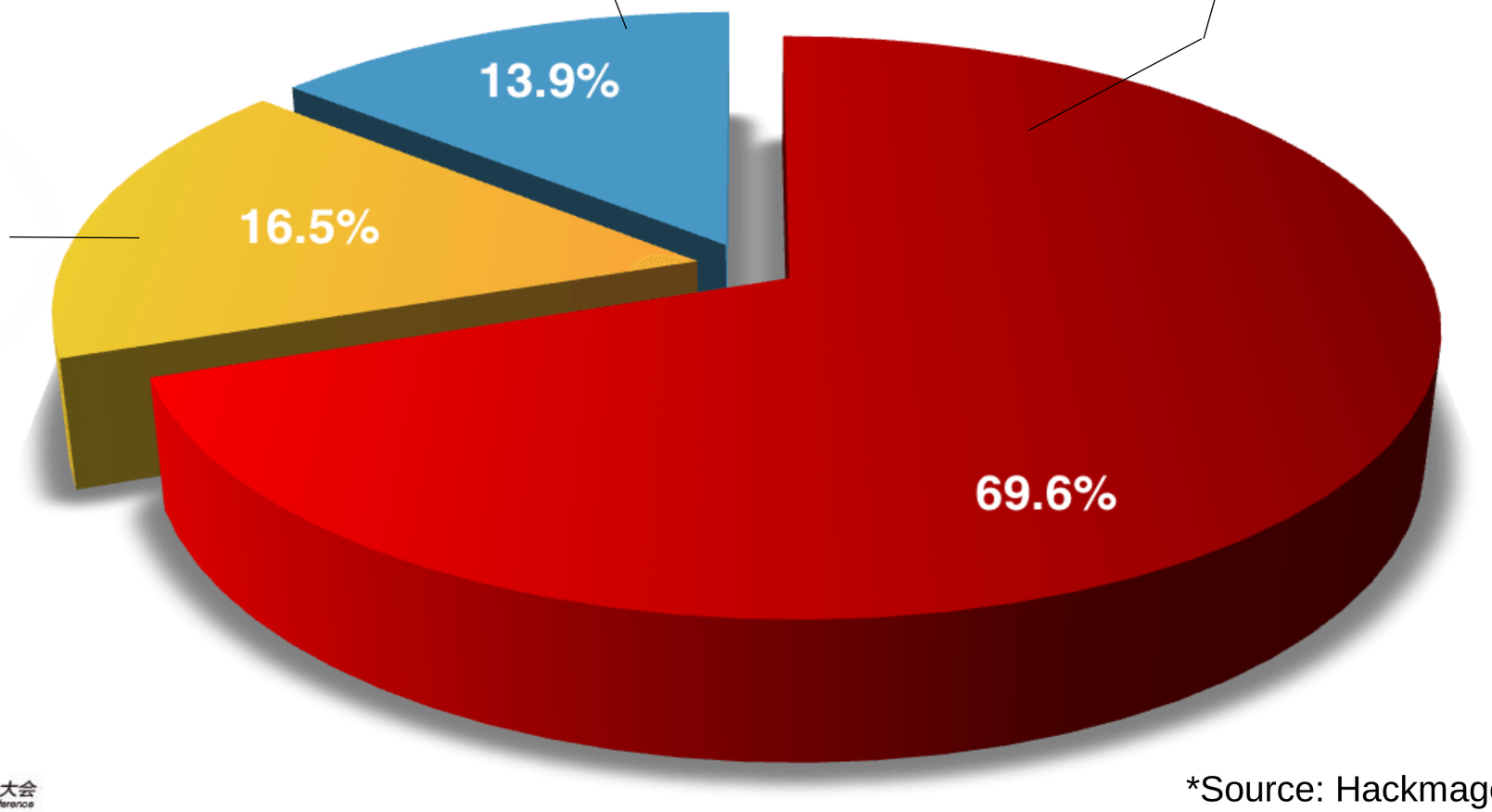
Smartphones: The Hacker's Ultimate Intelligence Gathering Tools

Avi Rosen
CEO and Co-Founder, Kaymera Technologies

CYBER ATTACK BY MOTIVATION

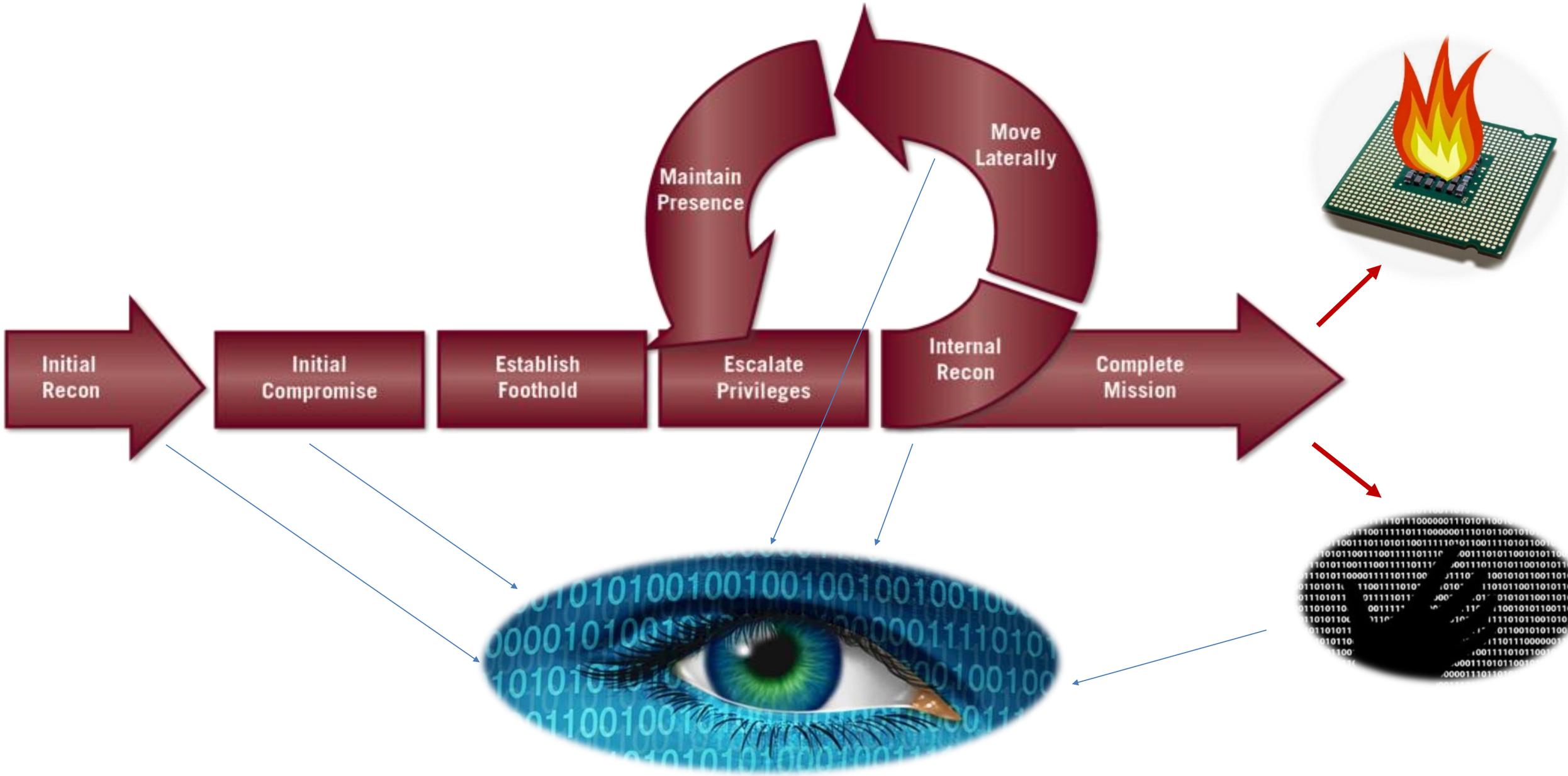
August 2015*

100% growth M/M

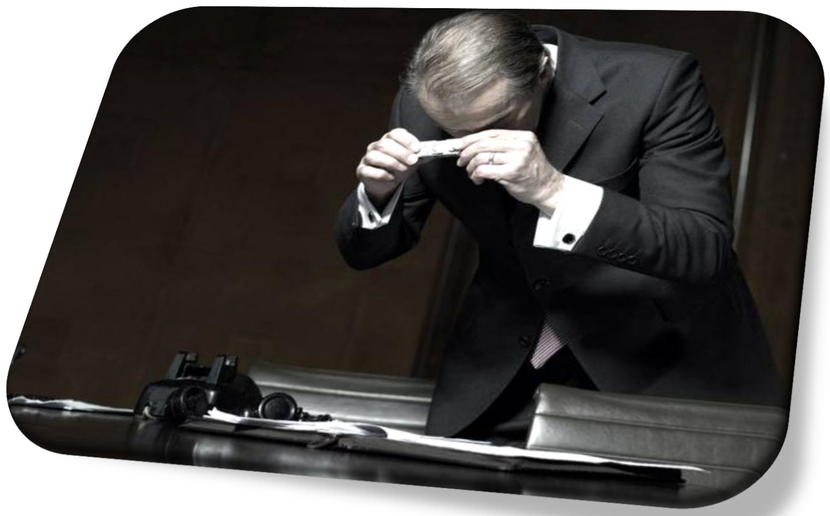


*Source: Hackmageddon, September 10th, 2015

COMMON ATTACK LIFECYCLE



INTELLIGENCE GATHERING EVOLUTION



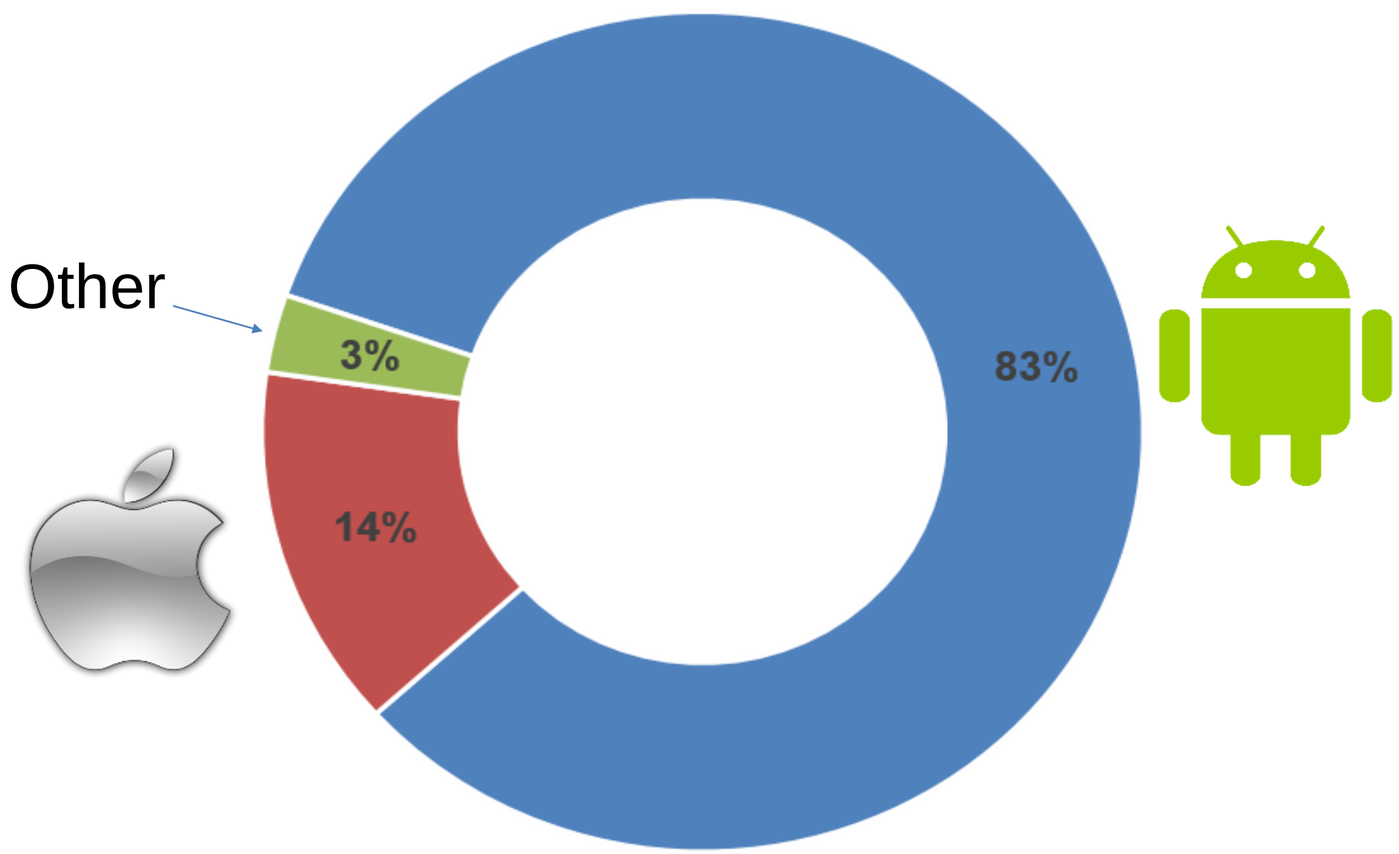
Why Smartphones?

QUESTION:

HOW MANY SMARTPHONES SHIPPED SO FAR IN 2015 WORLDWIDE?

~1.12 Billion Smartphones*

WW Statistics, ~340M devices per quarter, 13.8% growth Y/Y



*Source: IDC

QUESTION:

HOW MANY BABIES BORN SO FAR IN 2015 WORLDWIDE?

~104 Million Babies*

2015 world population growth: 61M

“New People” to “New Smartphones” ratio:

1:11

*Source: worldmeters

SMARTPHONES – THE ULTIMATE INTELLIGENCE GATHERING TOOLS

Extremely rich data environment

- **Voice Communication**
  - Real time, History
- **Text Communication**
  - eMail, SMS, Instant messaging
- **Files**
  - Attachments, Cloud storage, Generated on device, Application related data
- **Online Accounts**
  - Access, Data, Account information
- **Multi dimensional social connection map**
  - Phone numbers, eMail addresses, Social networks, Groups and categories, Communication patterns

SMARTPHONES – THE ULTIMATE INTELLIGENCE GATHERING TOOLS

Powerful surveillance tool

- **Microphone**
  - Room tap, Live environment feed
- **Camera**
  - Video, Environment snapshots
- **GPS**
  - Highly accurate location tracking, always carried in subject's pocket
- **Network**
  - Always online and connected, Simplifies exfiltration, Bi-directional communication
- **Storage**
  - Large, Exfiltration on demand

SMARTPHONE USER'S EXTREME BEHAVIOR CHARACTERISTICS

On average smartphone users have **27 apps** on their phones

On average users spend **81 minutes daily** on mobile apps

66% check their favourite app at least **once** a day

44% check their favourite app **several times** a day

Smartphone users are "super users" especially when it comes to apps

COMMON INTELLIGENCE GATHERING TECHNIQUES

Interception of Voice and Data Communication

Physical Extraction of Data

Trojan Attacks

Location tracking

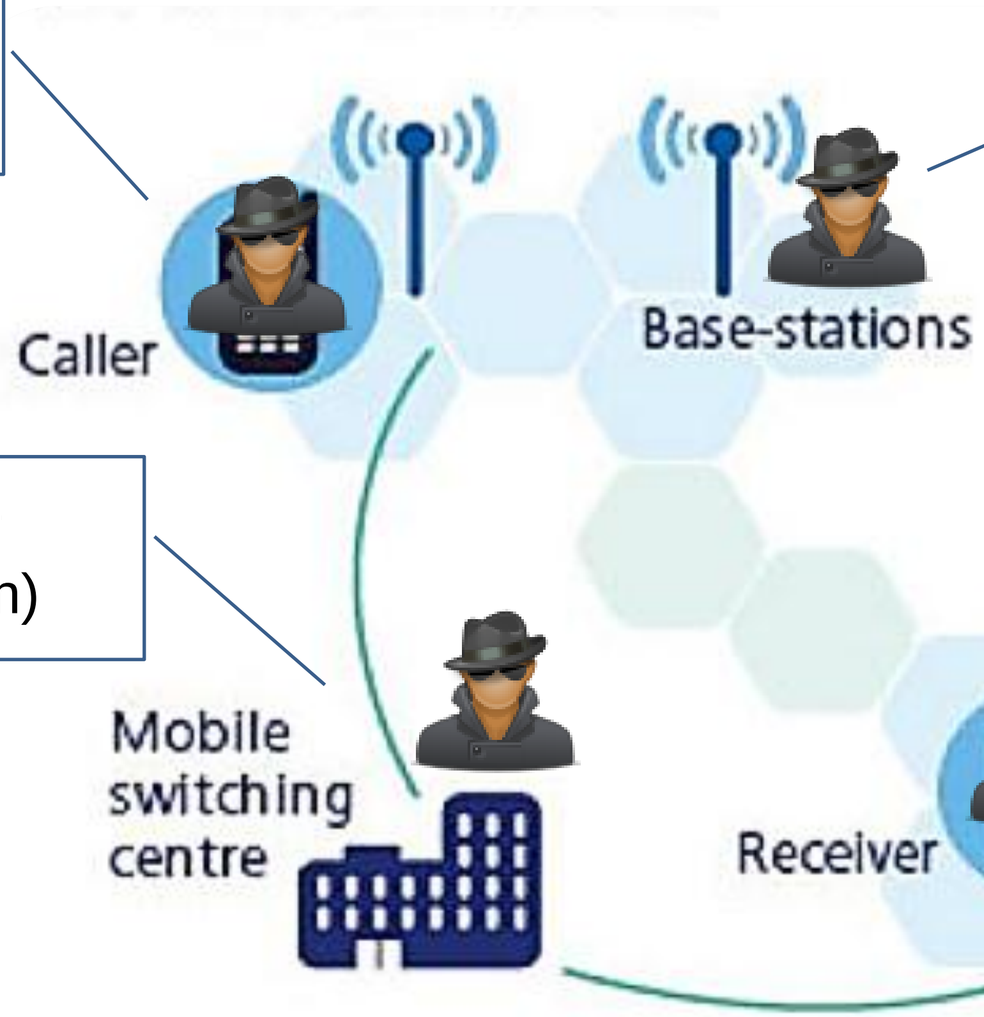
Exploiting applications' permission structure

Exploiting human behavior

COMMUNICATION INTERCEPTION

On the device
(Trojan horse)

Man In the middle
(Rogue BTS/AP)



Network operator
(Lawful Interception)

On the device
(Trojan horse)

Remote Control System

Operations | System | Monitor 2

1

All operations ▶ Swordfish ▶ John Doe ▶ Laptop (1) ▶ Configurations ▶ Config

2

Build | Save | Export | Import | Templates | Advanced Config

3

Calls (Phone, Skype, MSN) ON

Contacts & Calendar OFF

Messages (Mail, SMS, Chat) OFF

Visited Websites OFF

4

Accessed Files ON

☑ Documents ☐ Images

Keylog, Mouse & Password OFF

Screenshots ON

Grab a screens

Position ON

Save target's p

ANDRORAT APK BINDER
FIRST EVER ANDROID RAT APP BINDER + BUILDER
CLICK HERE!

5

demot@demo

Fri, Apr 6 13:00:43

ISC 2015 中国互联网安全大会

360互联网安全中心

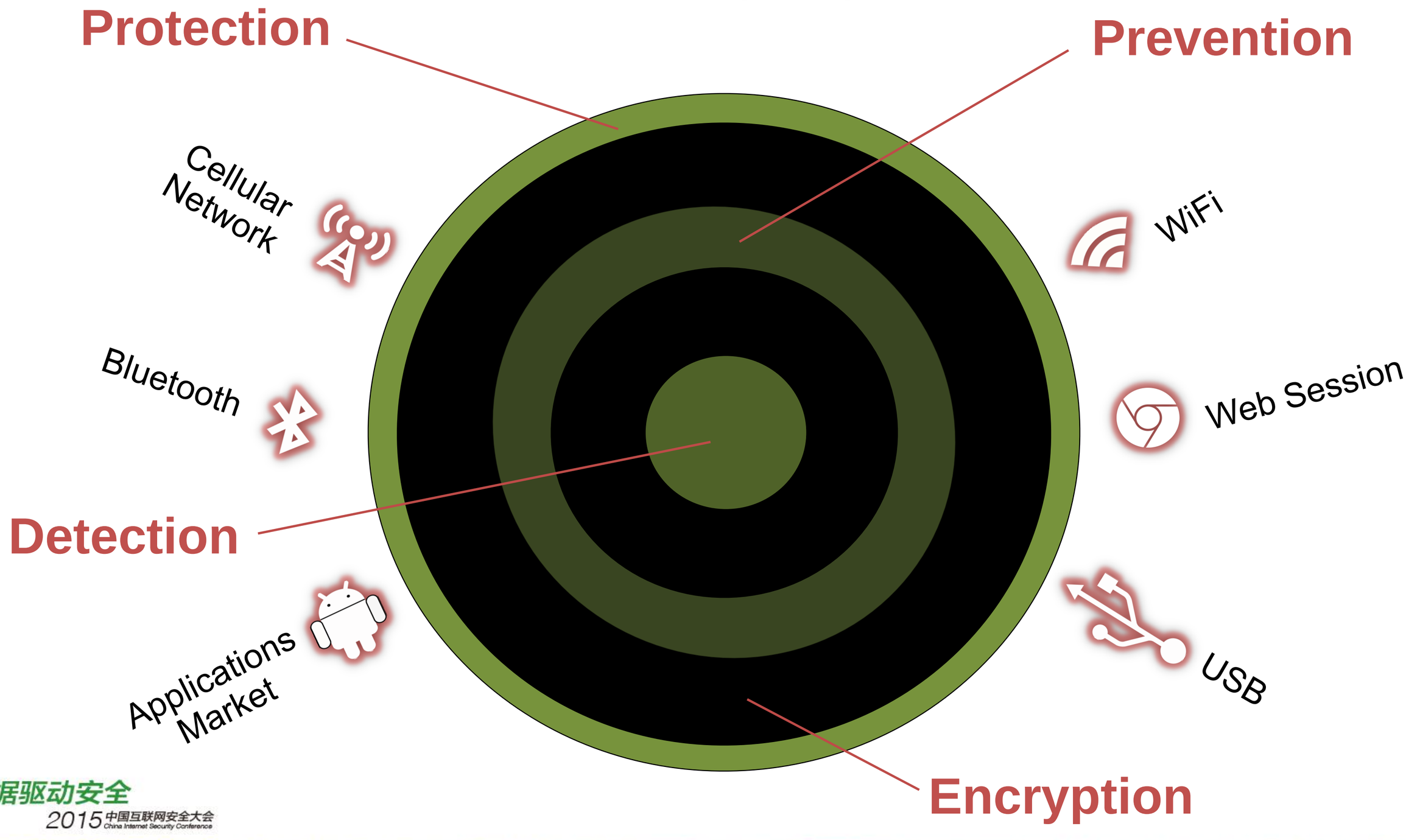
Best Defense Approach

ADJUST TO NEW THREATS

Any solution out there…….

– Need not to rely on the user
  - Too careless, extreme behavior characteristics
  - No security awareness
  - Human factor is the weakest link
– Need to cover **ALL** threats and intelligence gathering techniques
  - Techniques are used in parallel
– Provide usability and functionality
  - Maintain the “Smart” in Smartphone
  - Mobile security by restriction is failing
  - Provide good balance between security and functionality

MULTI-LAYERED PROTECTION APPROACH



Thank you!

avi@Kaymera.com