
SAMSUNG
6:01 PM
Tue,
06/21
06:01 PM
Updated 06/21 12:53 PM
20 °C 24° | 18°
Gardena
Partly sunny
AccuWeather.com
Internet
Gallery
Navigation
Music
Applications
Messaging
Contacts
Phone

Mobile **Security**

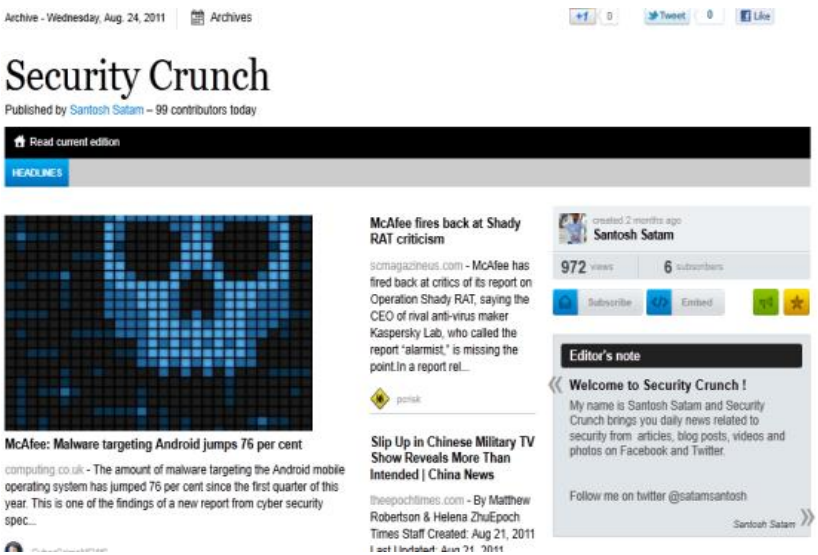
Disclaimer

The following presentation contains information, which is proprietary to MIEL e-Security Pvt. Ltd. and should be treated as strictly private & confidential. This document is being discussed with you solely for your information and may not be reproduced, redistributed or passed on, directly or indirectly, to any other organization or published, in whole or in part, for any purpose without the express written consent of MIEL e-Security Pvt. Ltd.

Presenter's Profile

Santosh Satam
Head-Technical Services
CISA | CISM | CISSP | CSSLP

- Enterprise Security Strategy
- Application & Mobile Security Assessment



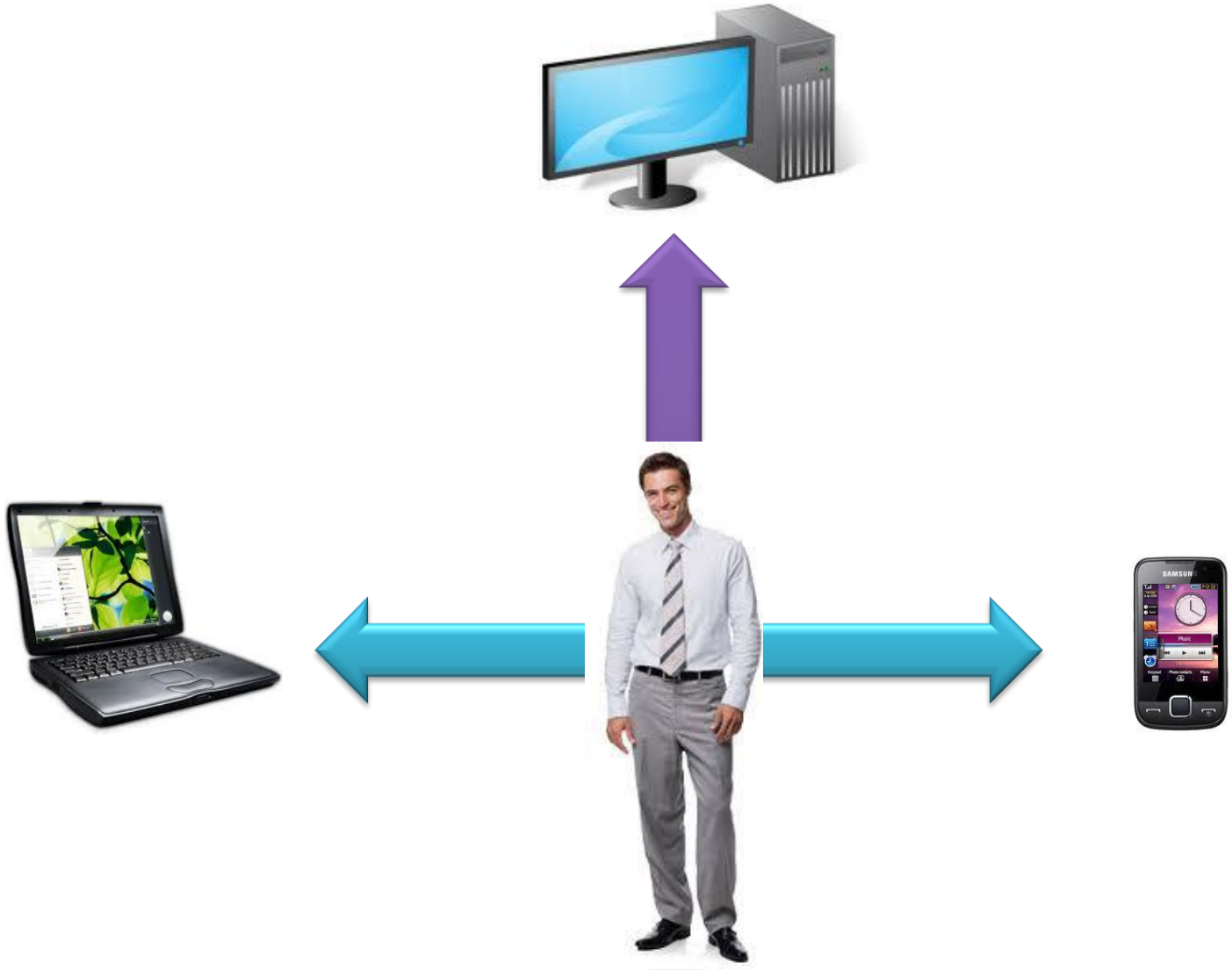
Security Crunch > My Daily Newsletter on Cyber Security

Other Interests: Running Marathon

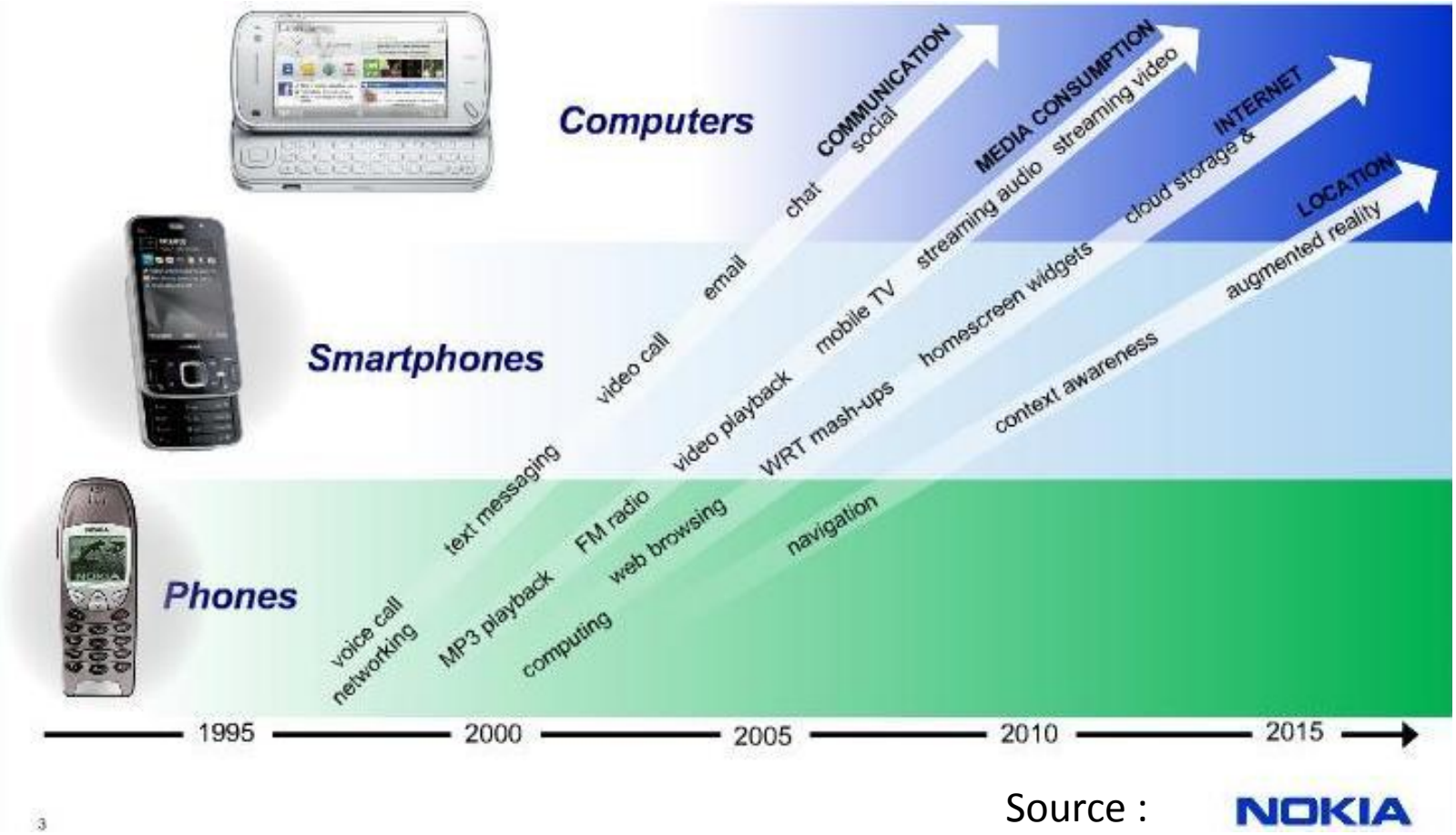
Agenda

- **I**ntroduction
  - **T**rends and Threats
    - **M**obile Threatscape
      - **E**nterprise Challenges
        - **R**ecommendations
          - **C**onclusion

Information **A**ge and **You**



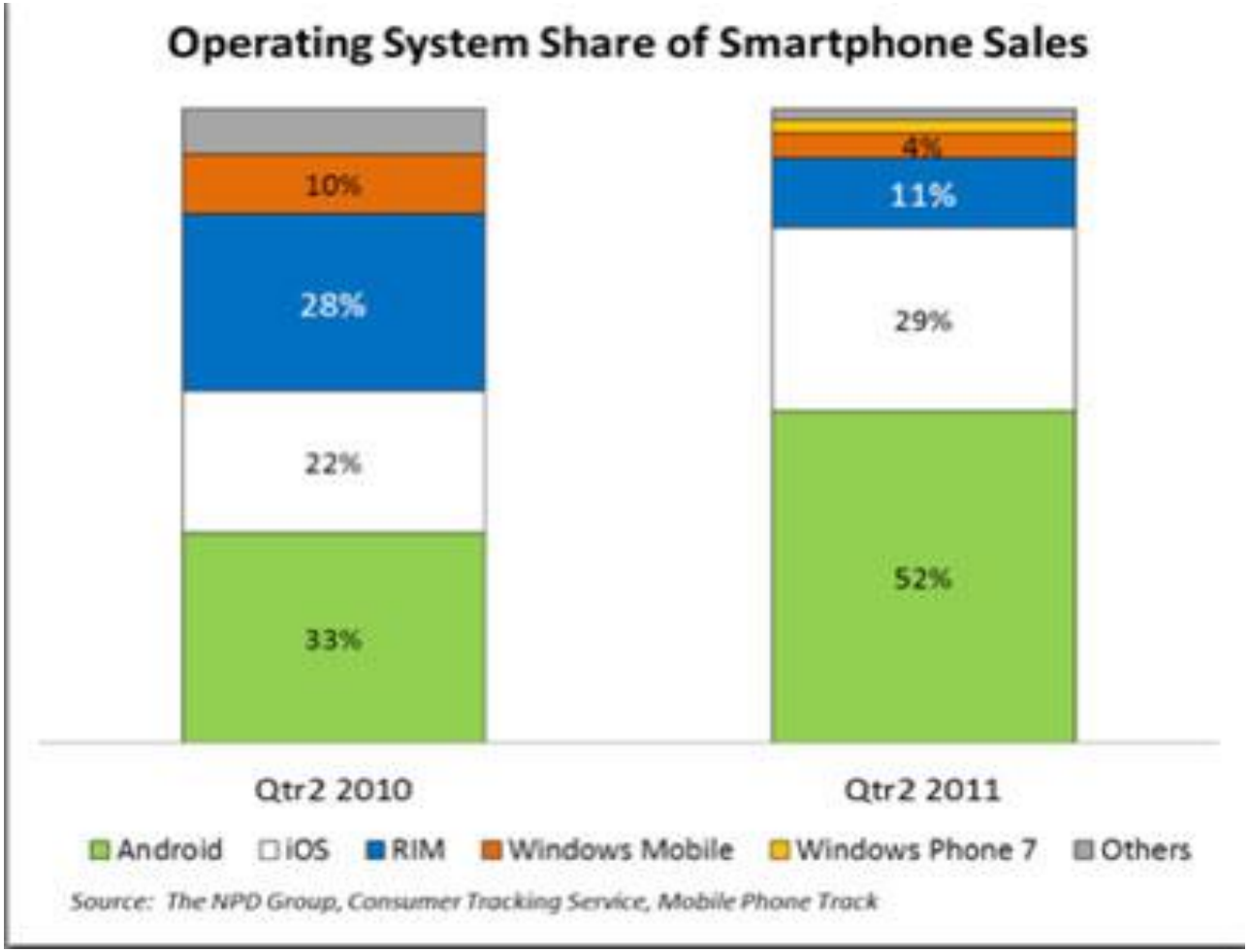
*E*volution of **M**obile **U**se **C**ases



Source : NOKIA

Mobiles are becoming a first class citizen in enterprises

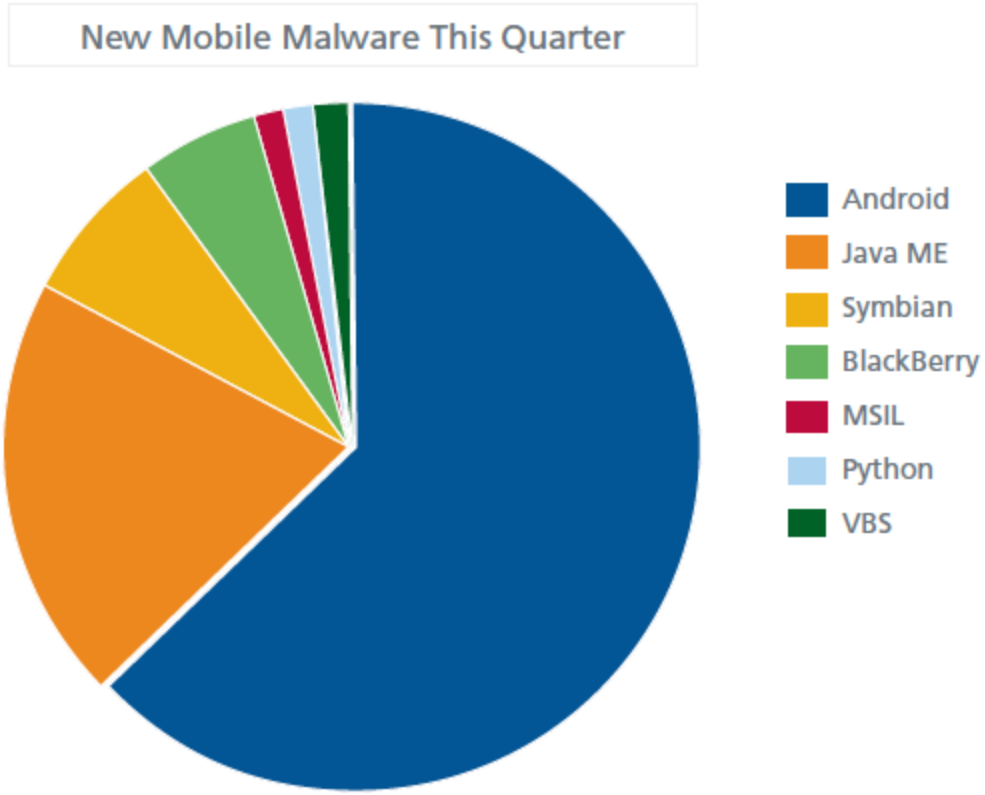
Mobile Trends



Evolution of Mobile Phones

- Now evolved to powerful machines with almost all capabilities as out laptops
- **Always on, always with you**
- Constantly evolving and becoming more powerful
- Security not kept pace with this growth, remains afterthought

Mobile Threats



Source: McAfee Quarterly Report 2011

Lots of security incidents reported..

MOBILE MISHAPS IN THE NEWS

Zeus malware variant begins targetting BlackBerry users

by **Lee Mathews** on March 7, 2011 at 09:00 AM

FILED UNDER: security, blackberry

It's been widely reported that the world's millions of smartphones are the next juicy target for malware creators, and we're beginning to see the shift. Trojanized apps recently infiltrated the Android Market and now Trend Micro is reporting that a Zeus trojan variant has begun infecting BlackBerry devices.

The trojan installs silently and then notifies its administrators that the compromised device is ready to receive instructions. Trend notes that an infected BlackBerry can be forced to block calls and phone numbers, add administrator accounts, turn the device on or off, and forward, delete, and display SMS messages.

While BlackBerry devices seem to be the primary target, Zeus variants have also been spotted on Symbian and Windows Mobile phones.

As is the case with desktop malware, vigilance and knowledge is the best defense: don't install untrusted apps and don't visit links you're unsure of on your mobile device.

source : trendmicro

26 trojanized apps pulled from Android Market

Posted on 01.06.2011

26 applications containing a variation of the DroidDream Trojan have been found on the official Android Market and are believed to have been downloaded by at least 30,000 users.

Lookout researchers believe that they were created and uploaded by the same developers who were behind the original DroidDream onslaught back in March.

It seems that the stripped down Trojan code has been added to legitimate apps and the apps were consequently uploaded and made available via six developer accounts.

According to F-Secure researchers, the grafted code is triggered only after the infected phone receives a text message:

After that, it contacts remote servers and sends out information such as the phone model, its IMEI, IMSI, Software Development Kit's version, and more.

source : netsecurity.org

Google issues hacking alert to 260,000 smartphone users who downloaded virus-infected apps

By DAILY MAIL REPORTER
Last updated at 8:51 AM on 10th March 2011

Comments (23) | Add to My Stories

Google yesterday admitted that up to 260,000 smartphones have been hacked after handset users unwittingly downloaded virus-infected apps.

The threat came to light last week when the technology giant was forced to withdraw at least 50 apps from its official Android Market.

Google operated a 'killswitch' and remotely removed all of the affected apps from peoples' phones.

Infected: Google has admitted that up to 260,000 smartphones have been hacked after handset users unwittingly downloaded virus-infected apps

First mobile phone worm reported

Cabir spreads through Symbian and Bluetooth.

By Paul Roberts, IDG News Service | Published: 00:00, 15 June 04

Like Be the first of your friends to like this.

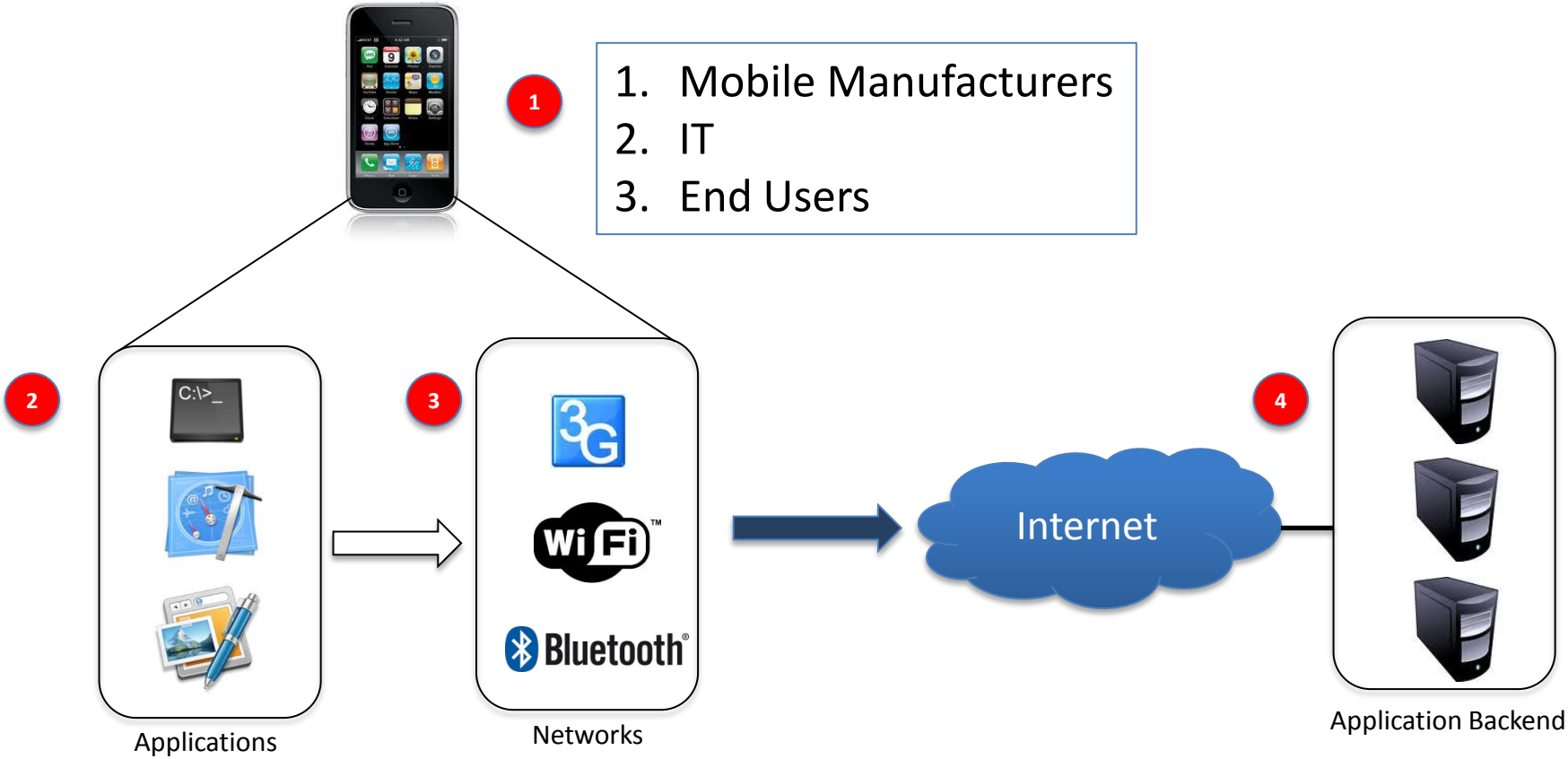
Anti-virus company Kaspersky Labs says it has discovered the first-ever computer virus capable of spreading over mobile phone networks.

Cabir is a network worm that infects phones running Symbian. No infections have been reported though and Cabir may be a proof of concept worm from an international group of virus writers known as 29a that is credited with the release of recent virus "Rugrat" that targets Windows 64-bit operating systems, the Moscow-based company said.

Cabir spreads between mobile phones using a specially formatted Symbian operating system distribution (or SIS) file disguised as a security management utility. When the infected file is launched, the mobile phone's screen displays the word "Caribe" and the worm modifies the Symbian operating system so that Cabir is started each time the phone is turned on.

LET’S GO EXPLORING MOBILE SECURITY !

Stakeholders in Mobile Security



1. Application Developers
2. End Users

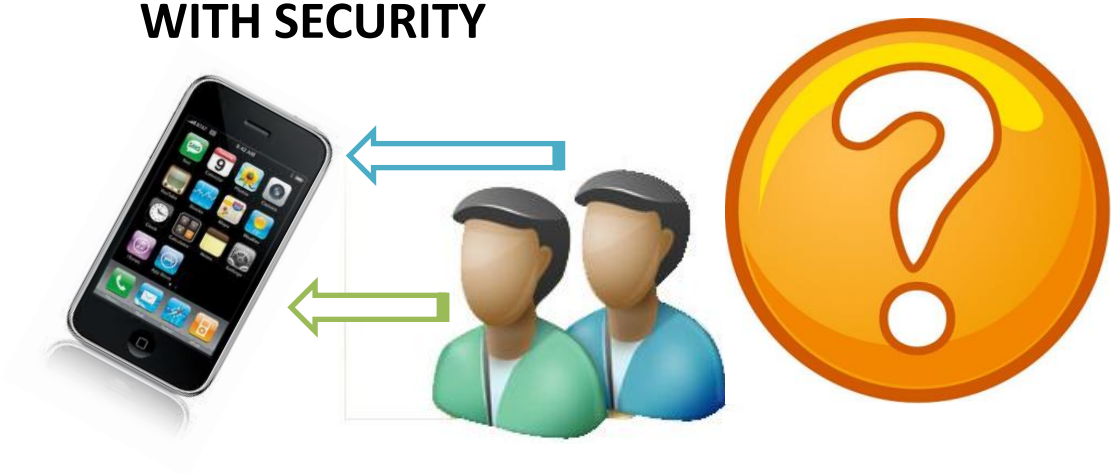
1. Mobile Operators
2. IT
3. End Users

1. Application Developers
2. IT

Mobile **security-specific issues..**

- **SECURE DATA STORAGE**(on Disk)

- **MULTIPLE USER SUPPORT WITH SECURITY**



- **STRONG AUTHENTICATION WITH POOR KEYBOARDS**

Mobile **security-specific issues..**

- **CONSTRAINED BROWSING ENVIRONMENT**

- **INFORMATION DISCLOSURE**

Mobile **security-specific issues..**

- **LOCATION/PRIVACY SECURITY**

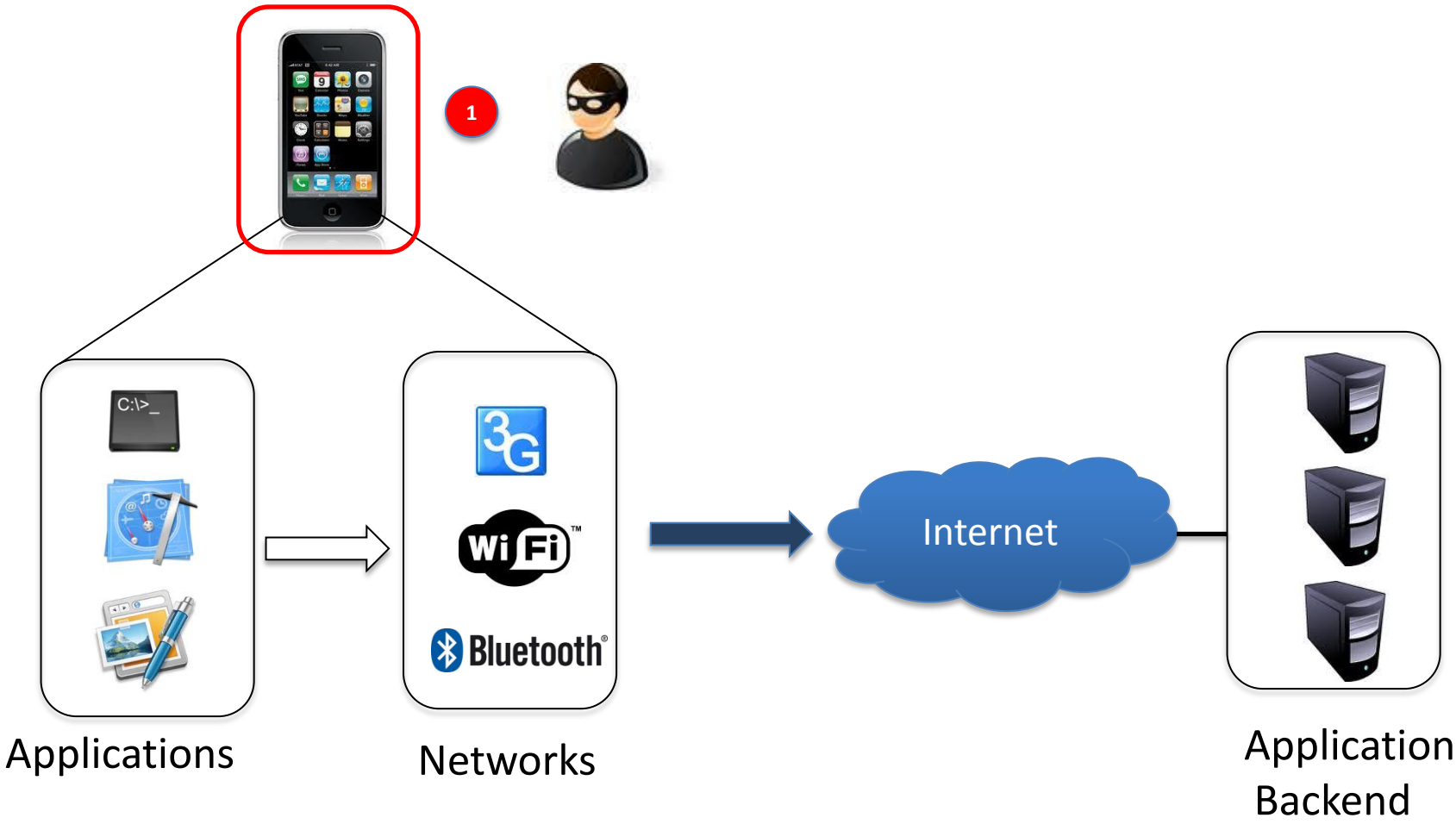
- **MULTIFACTOR AUTHENTICATION**

- **DIFFICULT PATCHING / UPDATE PROCESS**

Diving deeper..

UNDERSTANDING THE THREATS

Mobile Threatscape



Mobile **S**ecurity **A**ssessment

1

Mobile Platform Security Audit

Mobile Platform Security

Threats

- **Diverse Platforms** vulnerable to security problems (Android, iOS, Blackberry, Windows Phone)
- **Operating System security vulnerabilities**
  - Viruses and Worms – is there an Anti Virus?
  - Break-in over Wi-Fi and Internet – is there a Firewall?
  - Is there a Patch Management?
  - Is there a provision to regularly upgrade the OS?
- What happens if the phone is **stolen** ?
- What happens if data is intentionally or accidently **deleted**? Is there a **backup and restoration** mechanism?

Android **P**latform **S**ecurity

- Created by Google and the Open Handset Alliance
- **Linux** based
- Java programmable
- Each Application : a new user (UID)
- Android applications are considered “equal”

Android Platform Security

- **Permissions** - help provide data security
- Android's permission model allows user's to make **bad but informed choices**
- A confused user can't make good choices.

Android Platform Security

- Possible for 2 applications to Share the same User ID
- Be run within the same process and VM Sandbox
- Must be signed with the same certificate
- An application can allow for World Readable and Writeable mode
- This allows any application on the system to read / write the host applications files

Android Platform Security

- Android Market is **the sick man of the app world**
- It's an open market
- Google's Android Market has 90,000+ apps
- Recently Google has removed 26 malicious apps.

iOS Platform Security

- Processor – ARM 6 or 7 depending on model
- Runs iOS
- Derived from Mac OSX
- FreeBSD
- 2 primary users
  - Mobile
  - Root

Platform Security

- There are around **5,00,000+ apps** for iOS platform
- Code Signing applied to all applications
- Appstore applications signed by Apple
- All applications run as user "mobile"
- Chroot used to restrict apps from each other
- Applications are also encrypted when stored
- Runtime decryption before execution

Platform Security

- Jailbreaking is the process of getting "root" access to the phone. This allows running custom software / firmware on the phone

- Unlocking refers to bypass controls which bind the phone to a carrier. This opens it for use with any carrier.

BlackBerry Mobile Platform Security

- Proprietary OS created by RIM
- Provides multi-tasking support
- Currently version 7
- Written in C++
- OS supports devices unique to the BB – trackball, trackwheel, touchscreen and touchpad
- Runs on ARM 7, 9 and ARM 11 processors

BlackBerry Mobile Platform Security

- As vulnerable as other phones, Still less in number
- Difficult to infect as no popular public appstore
- Most applications are loaded over the air by the network managers
- Offers strong suite of security features which include:
  - End-to-end Encryption
  - RSA SecurID Two-Factor Authentication
  - HTTPS Secure Data Access
  - Strong IT Policy Enforcement and Management
  - Built in Firewall

BlackBerry Application Attacks

- Browser a key part of Blackberry
- Based on the open source Webkit
- Webkit known to be vulnerable
- First public exploit on BB demoed at Pwn2Own 2011
- ARM based exploit code

Microsoft Windows Phone

- Microsoft's Mobile OS
- Windows Phone 7 was developed from scratch
- Currently in version 7.5 *(called Mango)*
- Not to be confused with **Windows 8 OS** (One OS for Desktops, Laptops, and Tablets.)

Windows phone

Security Model

- Does not support for removable storage.
- No tethered file system access from a PC
- No concept of users and user logon
- Application origin based authentication and authorization
- Elements of Windows Phone Security Model
  - Chambers
  - Capabilities
  - Application Safeguards

Windows phone

Chambers

Principle of isolation and Least Privilege

Trusted Computing Base (TCB)	unrestricted access to the platform Driver and OS level code
Elevated Rights Chamber (ERC)	User mode drivers and services.
Standard Rights Chamber (SRC)	All pre-installed MS and OEM applications
Least Privileged Chamber (LPC)	Default permission set in which all apps from the App Marketplace run

Windows phone

Capabilities

- Capabilities are granted during application installation, and their privileges cannot be elevated at run time
- Capabilities include geographical location information, camera, microphone, networking, and sensors.
- The Least Privileged Chamber (LPC) defines a minimal set of access rights by default. This helps in reducing the attack surface.

Application Safeguards

- Application developers must register with Microsoft
- Stringent check before inclusion in the App store
- All applications are code-signed by VeriSign.
- Applications that are not code-signed cannot run on Windows Phone 7.
- Applications run in a sandboxed process
  - Can interact with the OS in a limited way
  - Execution Manager monitors programs and kills programs with unusual activity

Windows Mobile Malware

JUNE 4, 2010 3:52 PM PDT

Malware found lurking in apps for Windows Mobile

by Elinor Mills

Print E-mail

Recommend Tweet 0 +1 0 Share 58 comments

Scammers are distributing apps for Windows Mobile-based smartphones that have malware hidden inside that makes calls to premium-rate numbers across the globe, racking up expensive bills unbeknownst to the phone's owner, a mobile security firm said on Friday.

The apps--3D Anti-Terrorist game, PDA Poker Art, and Codec pack for Windows Mobile 1.0--are being distributed on as many as nine popular download Web sites, including DoDownload, GearDownload, and Software112, according to John Hering, chief executive and founder of mobile security provider **Lookout**.

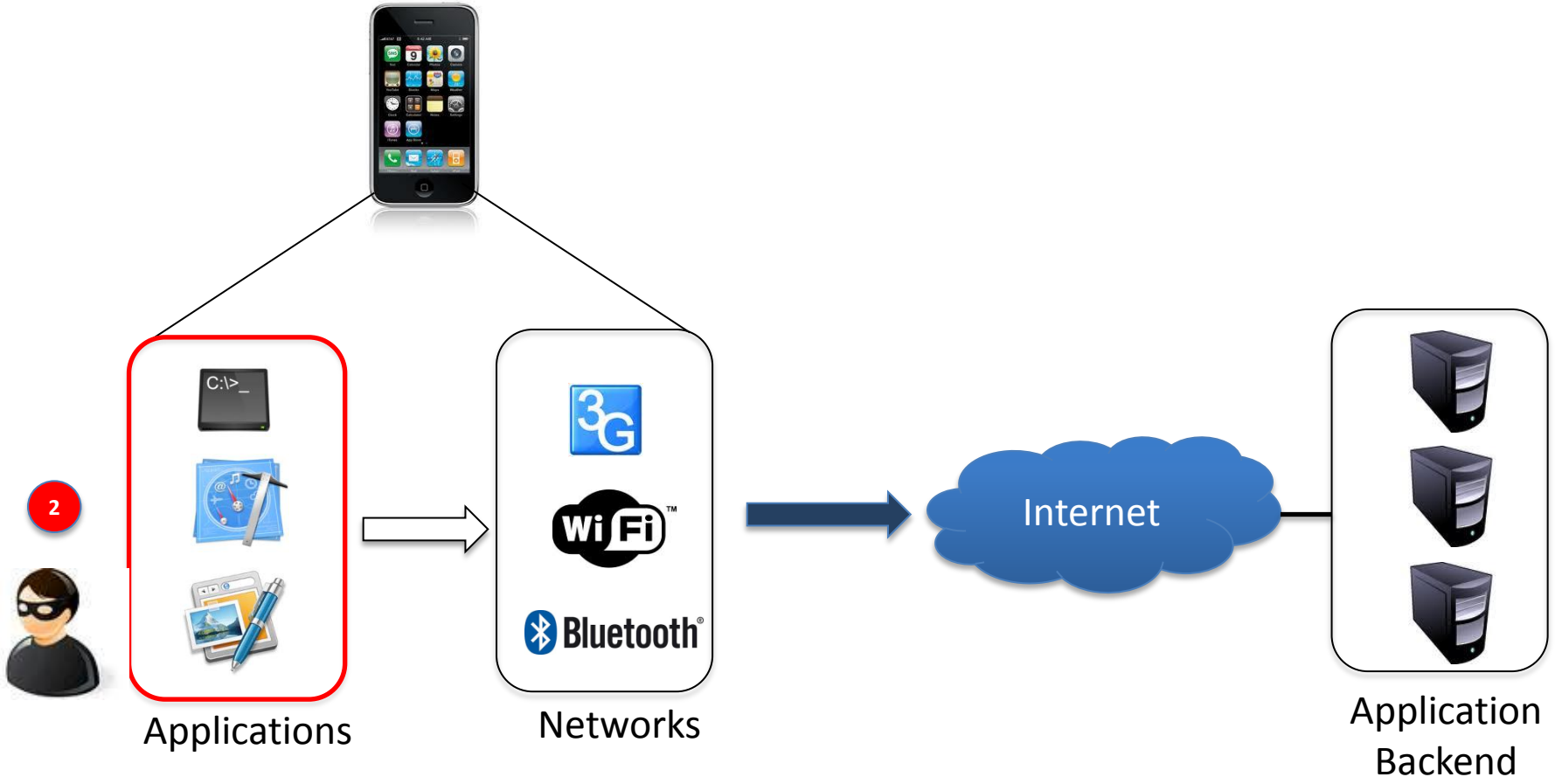
Someone has copied the programs and repackaged them with the malware inside, he said. Once the app is installed the virus wakes up and starts dialing premium-rate numbers like in Somalia and the South Pole, Hering said. He added that victims may not know about the problem until they get their phone bill and see that it's $50 or $100 higher than it should be.

Source: http://news.cnet.com/8301-27080_3-20006882-245.html

Secure Practices Recommendations

- Turn-off GPS / Bluetooth when not in use.
- Do not leave your phone unattended
- Make sure that the OS and firmware is updated
- Use anti-virus software and keep the definition file up to date
- Password protect your device and change this regularly

Mobile Threatscape



Mobile **S**ecurity **A**ssessment

2

Mobile Application Security Audit

1

Mobile Platform Security Audit

Mobile Application Security

Applications

Threats

- Malware and Trojan applications
- Security vulnerabilities in code
- Client Application security
- Bypass Enterprise policies
  - Difficult to apply Enterprise security policy
- Acts like a Backdoor into the Enterprise

What if ? There’s a..

MALWARE IN MY MOBILE !!

Malware that **m**ails **s**ecrets!

Unaware user

Attacker

Downloads App

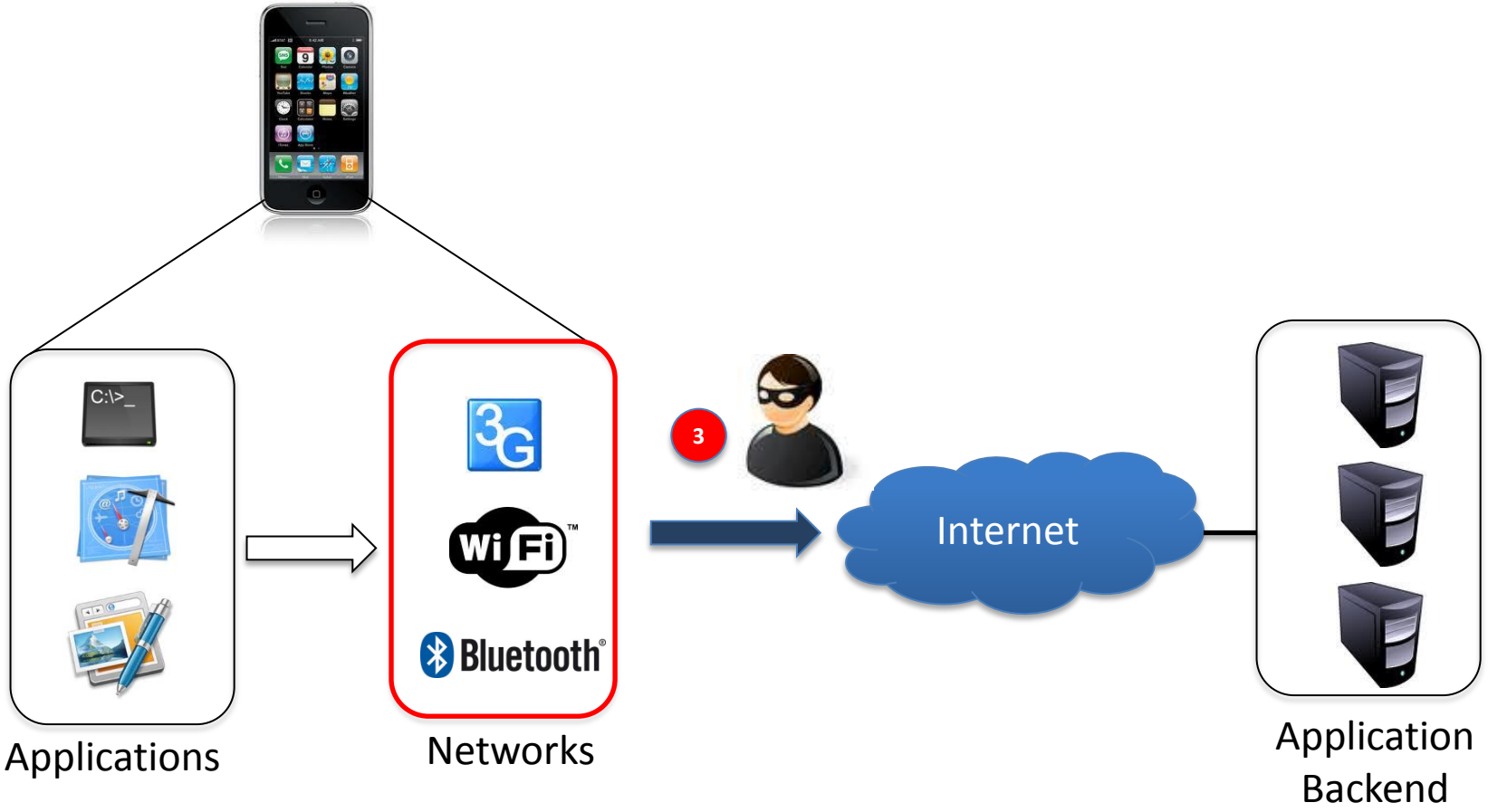
Hidden Trojan

Mails all secrets to attacker / Tracks Location

Secure Practices Recommendations

- Address security in the mobile application development process
- Download apps from trustworthy sources
- Scrutinize permission requirements of applications before installation
- Use mobile security apps for data protection

Mobile Threatscape



Mobile **S**ecurity **A**ssessment

3

Mobile Network Security Audit

2

Mobile Application Security Audit

1

Mobile Platform Security Audit

Network Access Security

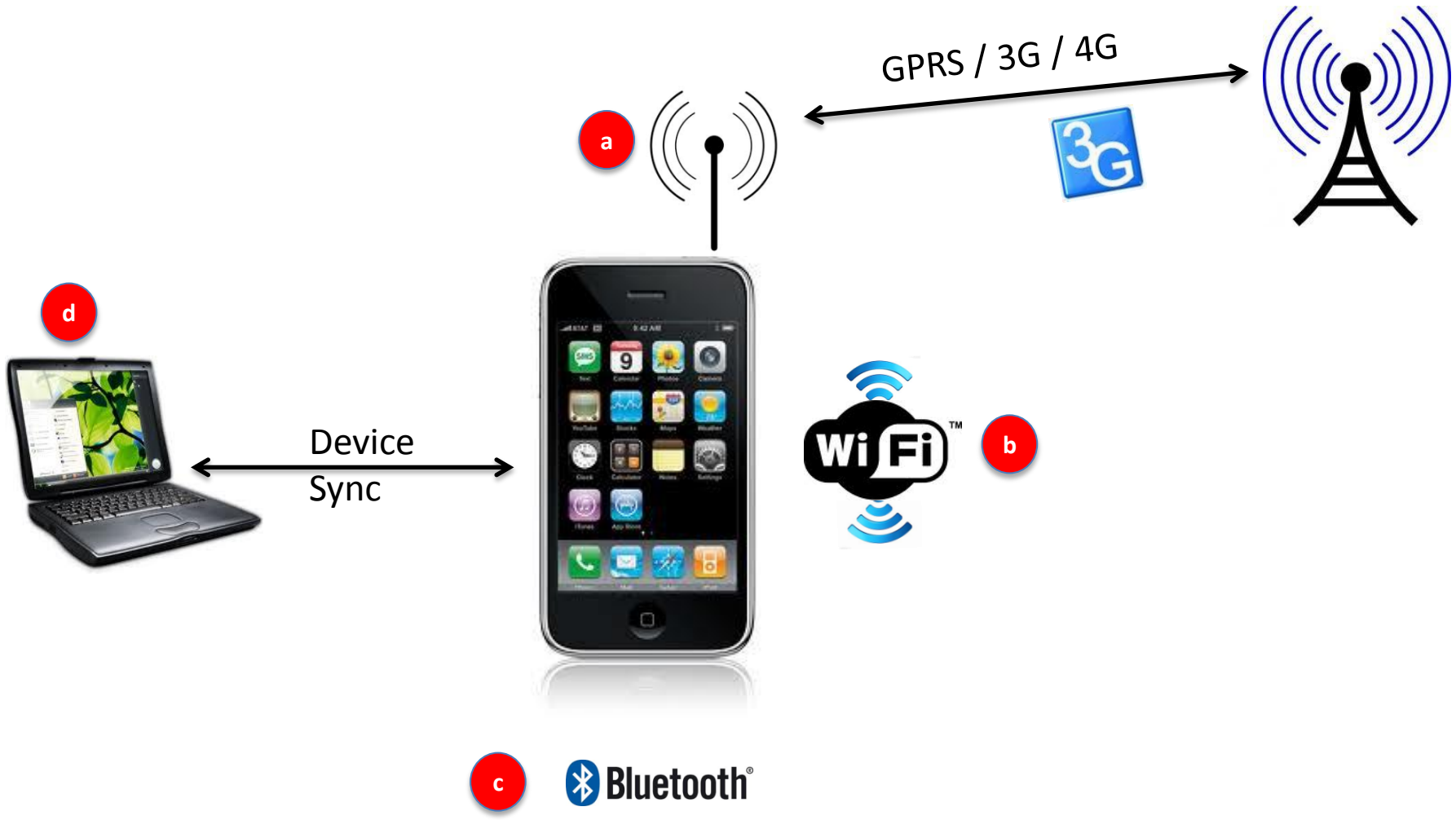
3

Networks

Threats

- Heterogeneous Network Risks
  - GPRS/3G/$G
  - Wi-Fi
  - Bluetooth
  - PC Synchronization
- "ON" by default open up to network based attacks
- Every access mechanism has security implications
- Difficult to control and prevent unauthorized access
- Requires custom solution to address each
  - Difficult to apply uniformly across all devices on the network

Understanding **M**obile **C**onnectivity



Full **D**isclosure: **H**acking **M**obile **P**hones using **B**luetooth!

Hacking Bluetooth enabled mobile phones and beyond – **Full Disclosure**

Adam Laurie Marcel Holtmann Martin Herfurt

21C3: The Usual Suspects

21st Chaos Communication Congress
December 27th to 29th, 2004
Berliner Congress Center, Berlin, Germany

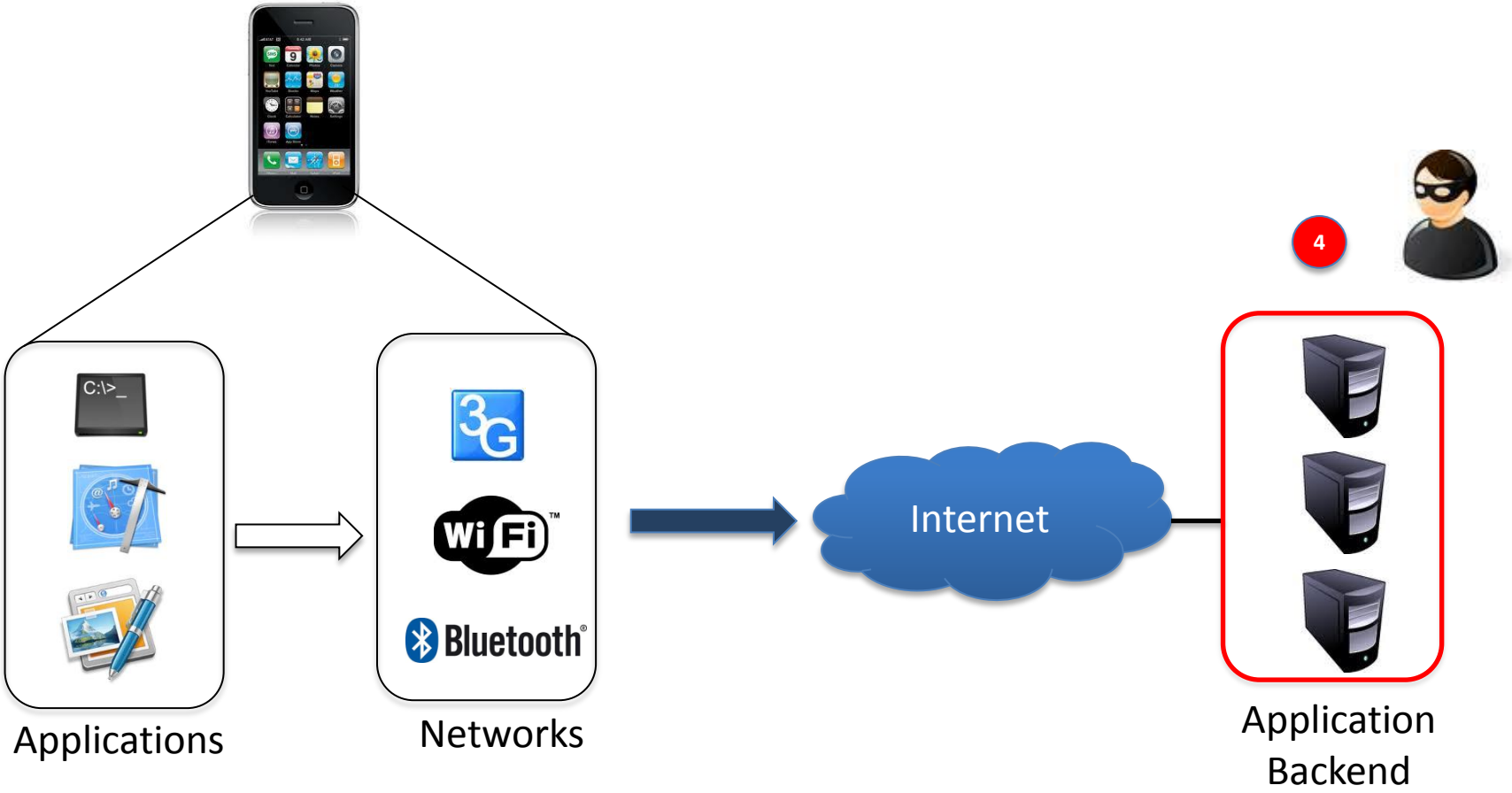
Secure Practices Recommendations

Use device inventory and track all mobile devices before and after allowing network access-You can't protect or manage what you can't see

Non compliant mobile phones should be denied network access until they have been scanned, patched or remediated.

Do not access corporate secured sites over public Wi-Fi

Mobile Threatscape



Application **B**ackend **S**ecurity

Application Backend

Threats

- Application farm security vulnerabilities
  - Web server security bugs
  - Database server security bugs
  - Storage server security bugs
  - Load balancer security bugs
- Web application security vulnerabilities
  - OWASP Top 10 security problems
  - Advanced Web Application attacks
- Web service security vulnerabilities
- Client application security vulnerabilities

Security **B**reach **T**argets **i**Pad **S**ervers

EXCLUSIVE

Like 15K

Apple's Worst Security Breach: 114,000 iPad Owners Exposed

Ryan Tate — Apple has suffered another embarrassment. A security breach has exposed iPad owners including dozens of CEOs, military officials, and top politicians. They—and every other buyer of the cellular-enabled tablet—could be vulnerable to spam marketing and malicious hacking.

Confidential **I**nformation **E**xposed!!

Mobile **S**ecurity **A**ssessment

4 Application Backend Security Audit

3 Mobile Network Security Audit

2 Mobile Application Security Audit

1 Mobile Platform Security Audit

MOBILE SECURITY CHALLENGES IN AN ENTERPRISE ENVIRONMENT

Enterprise Mobile **Security Challenges**

- **LACK OF KNOWLEDGE ABOUT RISK**

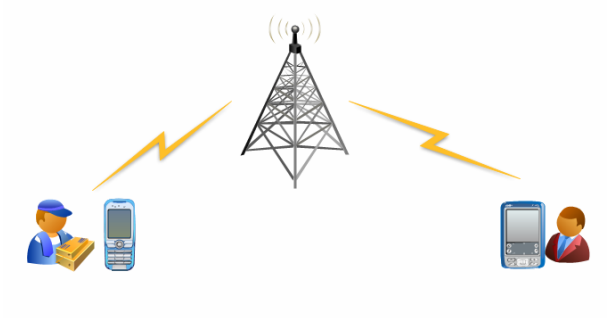
- **INFORMATION DISCLOSURE POLICIES**

- **DIFFICULTY AND COMPLEXITY IN IMPLEMENTATION**

Enterprise Mobile **Security Challenges**

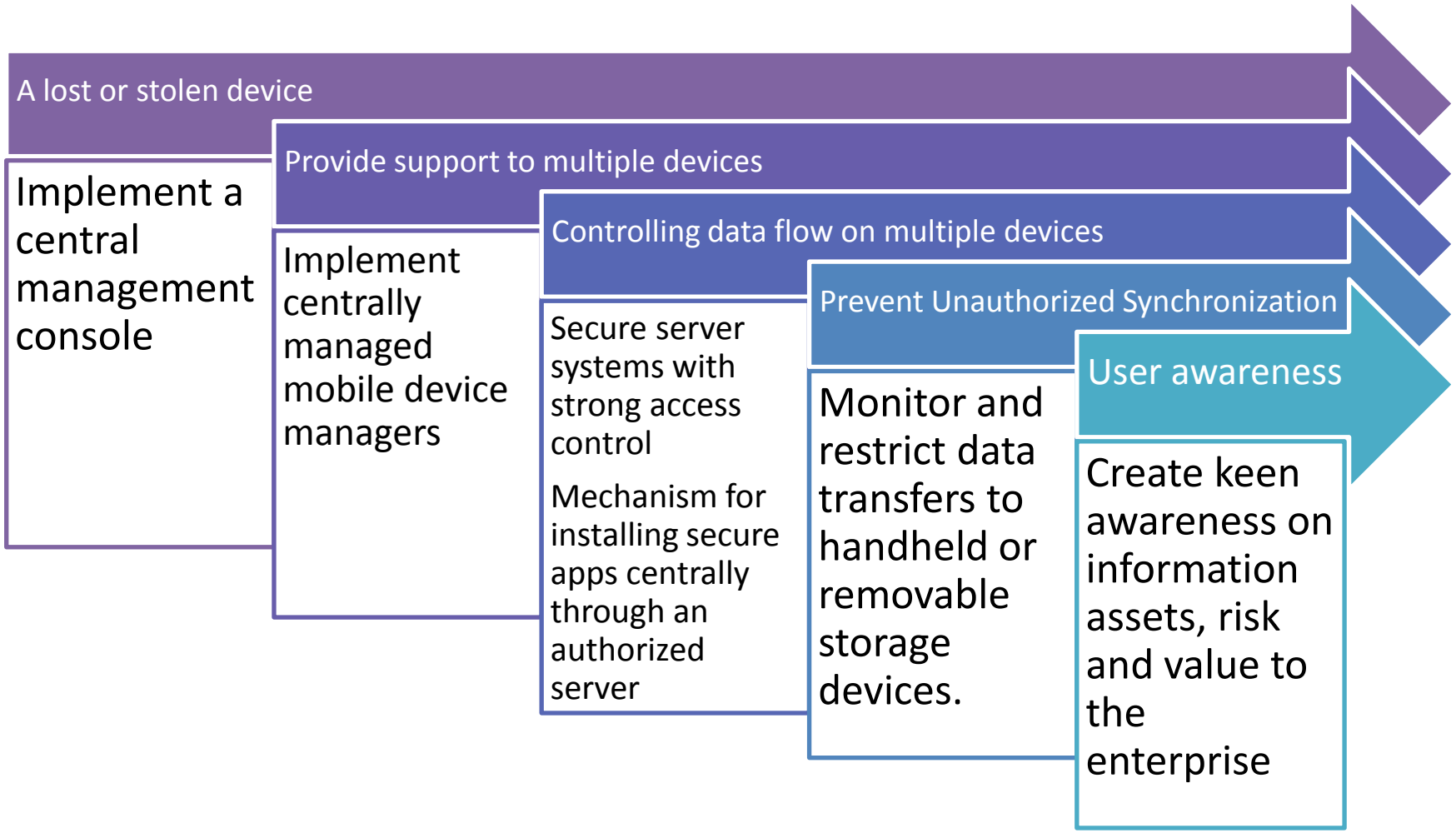
- **RESTRICTING MOBILE INTERNET ACCESS**

- **REMOTE CONTROL, TRACKING AND DATA WIPING**



- **ENTERPRISE WIDE MOBILE SECURITY POLICIES**

Enterprise Security **R**ecommendations



The Future

- Mobile and Cloud will turn traditional IT and computing on it's head.
- It's about user experience (U-Ex)
- Virtual smart phones (Mobile Hypervisor)
- Dynamic context- and content-aware Data Protection
- NFC enabled smart phones to take center stage and may replace cards

Thank you!

Santosh Satam


ssatam@mielesecurity.com


www.securitycrunch.in


@satamsantosh


http://in.linkedin.com/in/santoshsatam


https://www.facebook.com/satamsantosh

Any people that would give up liberty for a little temporary safety deserves neither liberty nor safety.

Benjamin Franklin

References

- **SECURING MOBILE DEVICES ISACA EMERGING TECHNOLOGY WHITEPAPER**
- **DEVELOPING SECURE MOBILE APPLICATIONS FOR ANDROID** *An introduction to making secure Android applications* Jesse Burns
- **Mobile banking: Safe, at least for now,** Elinor Mills