

# Paranoid Android:

Why is the security on my *smart* phone so *dumb*?



Herbert Bos

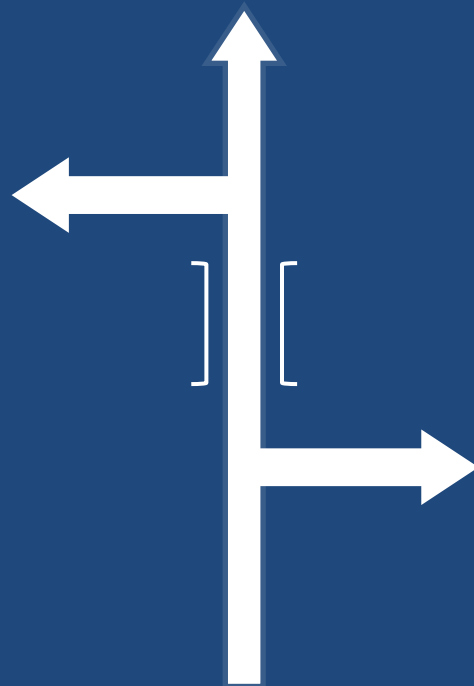
Vrije Universiteit Amsterdam



Herbert Bos  
Vrije Universiteit

research

systems  
networks  
security



courses

networks  
security

Sponsored by these *fine* EU projects:




01 January 2008

**WOMBAT**  
Worldwide Observatory of  
Malicious Behaviours and  
Attack Threats

SEVENTH FRAMEWORK  
PROGRAMME

European Commission  
Information Society and Media



**ICT** Information and Communication Technologies

**SYSSEC : A European Network of Excellence in Managing  
Vulnerabilities in the Future Internet: Europe for the World**



# Smartphones

- Q3 2010: 80 million sold worldwide
- Rich set of features and applications
  - navigation
  - ehealth
  - games
  - email
  - browsing
  - control
  - camera (pics+video)
  - movies / music
  - e-wallet
  - access codes
  - + thousands of others

# Smartphones:

Information security risks, opportunities and recommendations for users



- Risks
- Opportunities
- Recommendations

# Risk 1: Data leakage

- a stolen or lost phone with unprotected memory allows an attacker to access the data on it.



## Risk 2: Improper decommissioning

- the phone is disposed of or transferred to another user without removing sensitive data, allowing an attacker to access the data on it.



# Risk 3: Unintentional data disclosure

- most apps have privacy settings but many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the settings to prevent this.





# Risk 4: Phishing

- an attacker collects user credentials (e.g. passwords, creditcard numbers) using fake apps or (sms,email) messages that seem genuine.



# Risk 5: Spyware

- the smartphone has spyware installed allowing an attacker to access or infer personal data.



# Risk 6: network spoofing

- an attacker deploys a rogue network access point and users connect to it. The attacker subsequently intercepts the user communication to carry out further attacks such as phishing.



# Risk 7: Surveillance

- spying on an individual with a targeted user's smartphone.



# Risk 8: diallerware

- an attacker steals money from the user by means of malware that makes hidden use of premium sms services or numbers.



# Risk 9: Financial Malware

- malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions.



# Risk 10: Network Congestion

- network resource overload due to smartphone usage leading to network unavailability for the end-user.



# Risk 1: Data leakage

<b>Threat description</b>	The smartphone is stolen or lost and its memory or removable media are unprotected, allowing an attacker access to the data stored on it.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	High	Medium	Medium
Employee (E)	Medium	High	High
High official (H)	Medium	Very high	High



## Risk 2: Improper decommissioning

<b>Threat description</b>	The smartphone is decommissioned improperly allowing an attacker access to the data on the device.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	Medium	Medium	Medium
Employee (E)	High	High	High
High official (H)	Medium	Very high	High

# Risk 3: Unintentional data disclosure

Threat description	The smartphone user unintentionally discloses data on the smartphone.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	Very high	High	High
Employee (E)	High	Medium	High
High official (H)	High	Very High	High

# Risk 4: Phishing

<b>Threat description</b>	An attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps or (SMS, email) messages that seem genuine.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	Medium	High	Medium
Employee (E)	Medium	High	Medium
High official (H)	Medium	Very high	High

# Risk 5: Spyware

Threat description	The smartphone has spyware installed, allowing an attacker to access or infer personal data. Spyware covers untargeted collection of personal information as opposed to targeted surveillance.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	High	Medium	High
Employee (E)	Medium	High	Medium
High official (H)	Medium	Medium	Medium

# Risk 6: network spoofing

<b>Threat description</b>	An attacker deploys a rogue network access point (WiFi or GSM) and users connect to it. The attacker subsequently intercepts (or tampers with) the user communication to carry out further attacks such as phishing.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	Medium	Medium	Medium
Employee (E)	Medium	High	Medium
High official (H)	Medium	High	High

# Risk 7: Surveillance

<b>Threat description</b>	An attacker keeps a specific user under surveillance through the target user's smartphone.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	Low	High	Medium
Employee (E)	Low	High	Medium
High official (H)	Medium	Very high	High

# Risk 8: diallerware

<b>Threat description</b>	An attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	High	High	High
Employee (E)	Medium	Medium	Medium
High official (H)	Low	Low	Low

# Risk 9: Financial Malware

<b>Threat description</b>	The smartphone is infected with malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	Medium	High	High
Employee (E)	Low	High	Medium
High official (H)	Low	Low	Low



# Risk 10: Network Congestion

<b>Threat description</b>	Network resource overload due to smartphone usage leading to network unavailability for the end-user.		
<b>Rating</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk</b>
Consumer (C)	Low	Low	Low
Employee (E)	Low	Low	Low
High official (H)	Low	Low	Low

# Opportunities

- **Sandboxing and capabilities:** most smartphones use sandboxes for apps and capability-based access control models.
- **Controlled software distribution:** gives providers *the opportunity* to have more control over app security by vetting apps submitted for security flaws and removing insecure apps.
- **Remote application removal:** functionality allowing removal of malware from devices after installation (NB caveats described in this section – e.g. the judgement about whether a particular app is malicious may not be clear-cut).
- **Backup and recovery:** most smartphones ship with convenient backup and recovery functions to address risks to data availability.
- **Extra authentication options:** smartphones can function as a smartcard reader, giving additional options for authentication and non-repudiation.
- **Extra encryption options:** several third-party applications are now offering encryption for smartphone voice calls, on top of the standard encryption provided by mobile network operators.
- **Diversity:** smartphones are diverse in terms of hardware and software, which makes it more difficult to attack a large group of users with one virus.

# Recommendations: Consumers

- **Automatic locking:** configure the smartphone in such a way that it locks automatically after some minutes.
- **Check reputation:** before installing or using new smartphone apps or services, check their reputation. Never install any software onto the device unless it is from a trusted source and you were expecting to receive it.
- **Scrutinize permission requests:** scrutinize permission requests when using or installing smartphone apps or services.
- **Reset and wipe:** before disposing of or recycling their phone, wipe all the data and settings from the smartphone.

# Recommendations: Employees

- **Decommissioning:** before being decommissioned or recycled, apply a thorough decommissioning procedure, including memory wipe processes.
- **App installation:** if any sensitive corporate data is handled or if the corporate network is accessible to the smartphone then define and enforce an app whitelist.
- **Confidentiality:** use memory encryption for the smartphone memory and removable media.

# Recommendations: High Officials

- **No local data:** do not store sensitive data locally and only allow online access to sensitive data from a smartphone using a non-caching app.
- **Encryption software:** for highly confidential usage, use additional call and SMS encryption software for end-to-end confidentiality.
- **Periodic reload:** smartphones may be periodically wiped (using secure deletion) and reloaded with a specially prepared and tested disk image.

# Another perspective



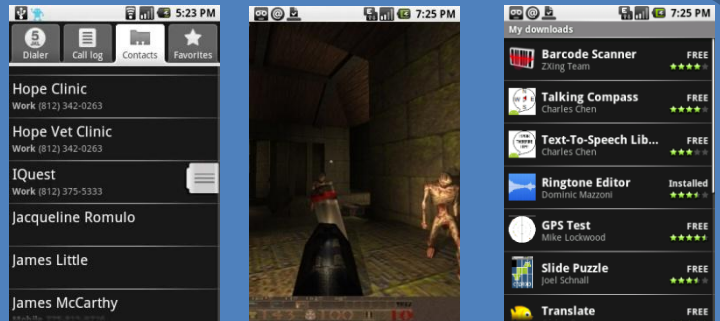
# Why Protect Smartphones?

- They are used to:
  - Store sensitive data
  - Used like PCs++
  - Perform calls
  - E-wallets
- Packed with sensors
  - GPS, Mic, camera, accelerometer, etc.
- Large codebases, and many users

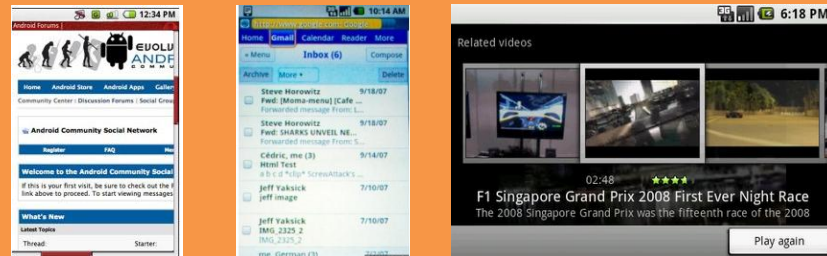


# Smartphones Like PCs

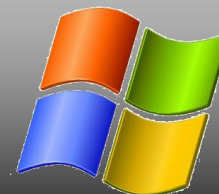
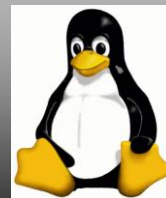
## Applications



## Internet



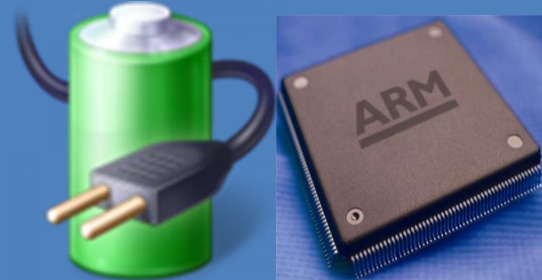
## Operating Systems





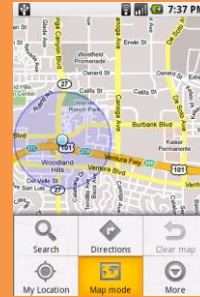
# Smartphones Unlike PCs

## Hardware



## Sensitive Information

Password,  
PIN,  
Credit Card  
No



## E-Payments



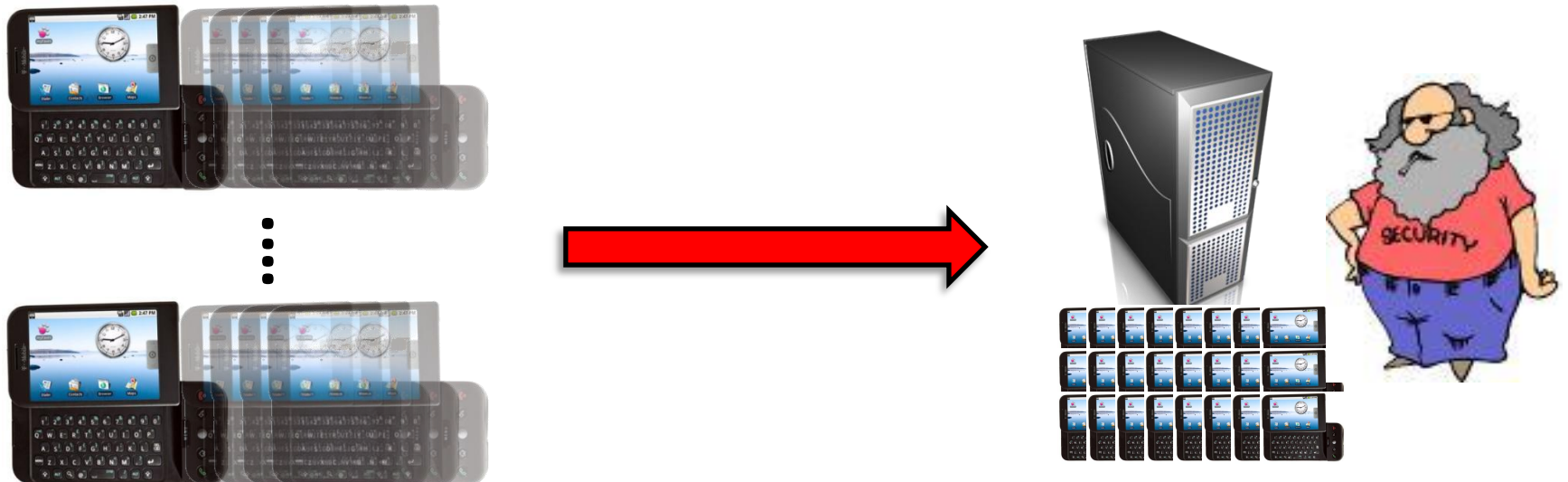
# Our Targets



- Create a solution that enables multifaceted security with fixed overhead
  - Including support for heavyweight mechanisms like Dynamic Information Flow Tracking
- Enable backup and recovery of device data
- Attackers cannot disable the check

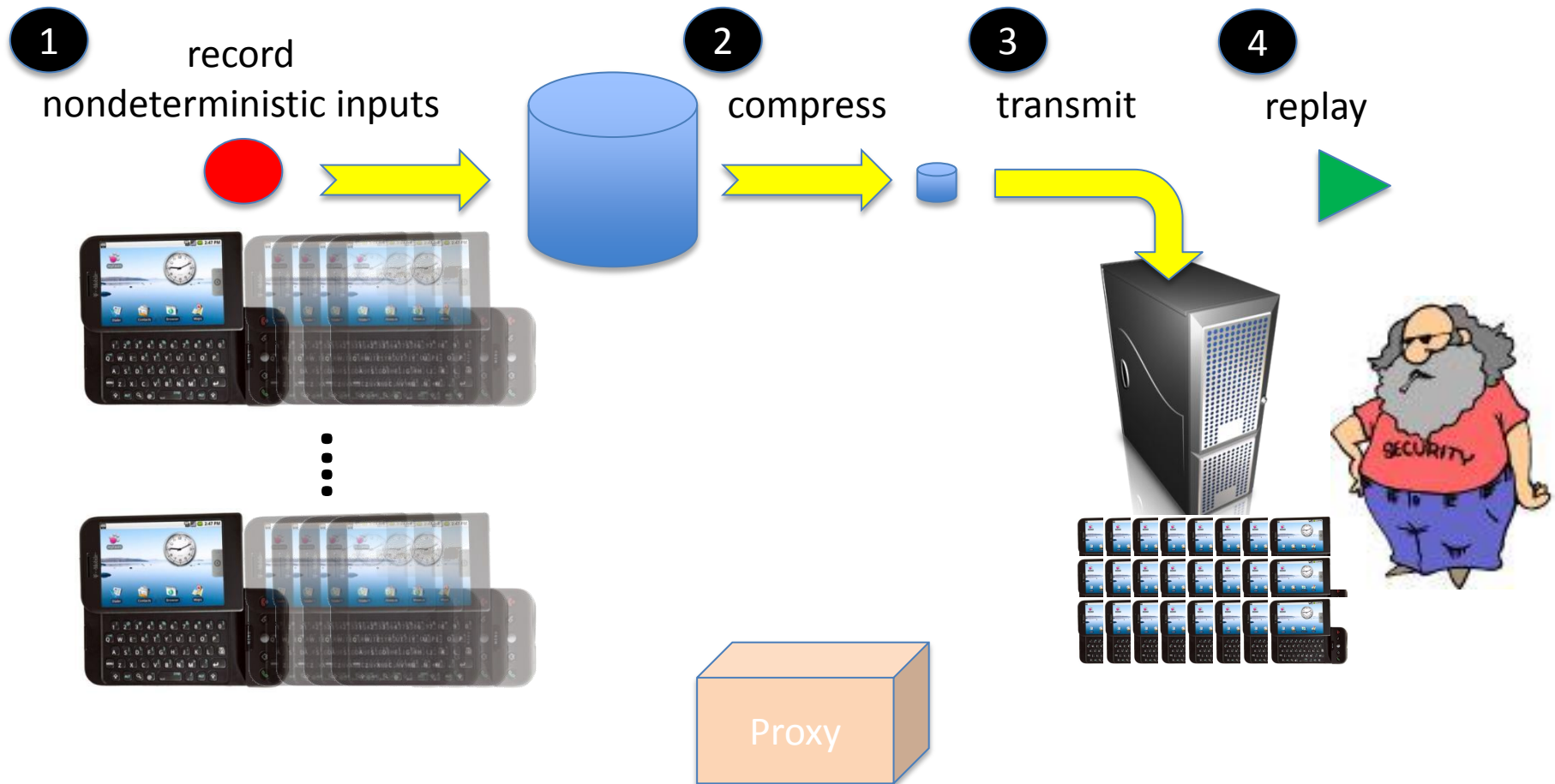
# Our Approach

- Faithfully replicate smartphone execution in remote servers
- Apply security checks on replicas



# new security model

# Recording and Replaying in a Nutshell



# Disconnected Operation

- Connectivity not always available
  - Events stored in local storage
  - Transmit on reconnection
  - Risky?
- ➔ Data are stored on the device
  - We use **tamper-evident storage**



# Security Server



- Any detection technique
- The same as applying the check on the device
- Checks can be added transparently
- A server can host many replicas

# Marvin: A Paranoid Android Prototype





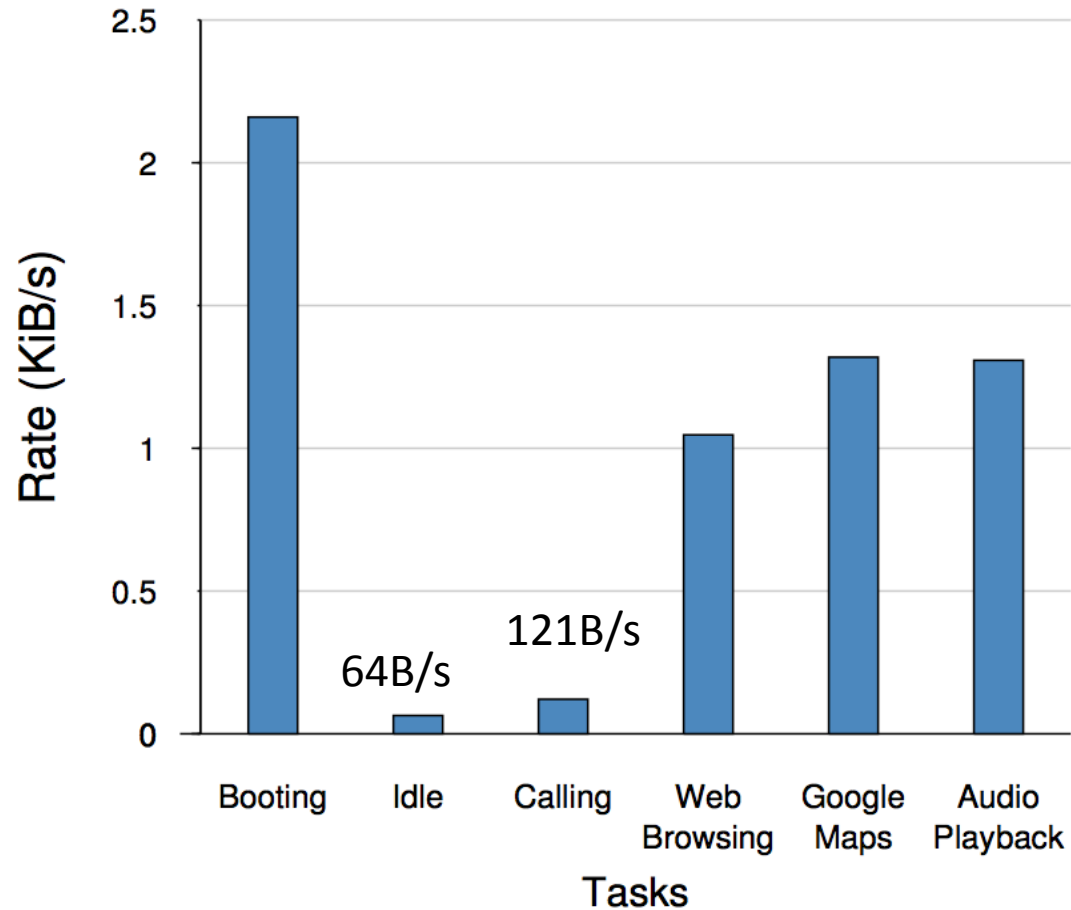
# Security Server

- Replica hosted on Android QEMU emulator
  - Virus scanner
    - Detects viruses stored in the file system
  - Information flow tracking
    - Detects memory corruption attacks



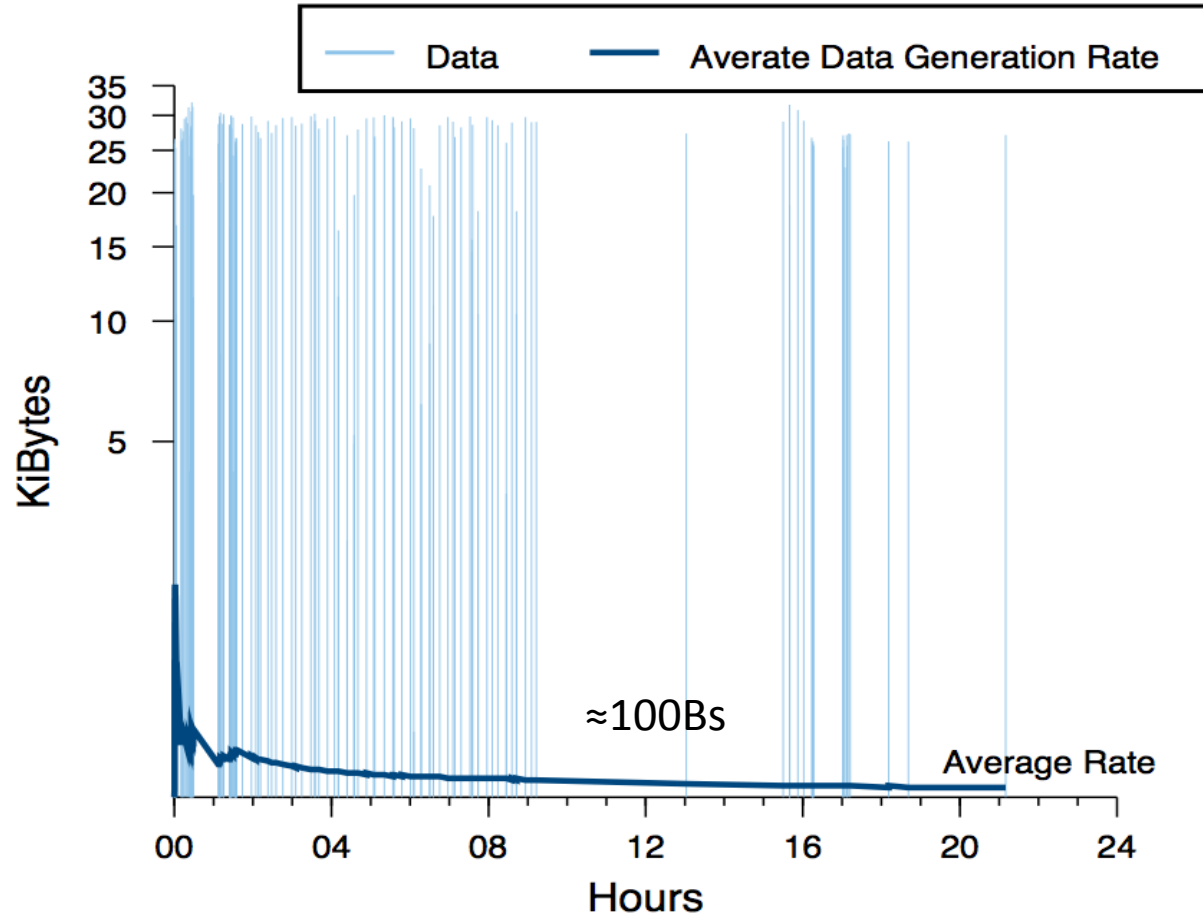
# Results

# Data Generation Rate for Various Tasks



**Data generated by various tasks**

# Marvin Data Generation Rate



User operated device for 1 day

# Performance

- Idle operation and performing calls
  - CPU load and battery life are not affected
- During high usage like browsing
  - CPU load average increased by  $\approx 15\%$
  - Battery consumption increased by  $\approx 30\%$
- Other activities
  - minimal overhead

# Conclusions

- Smartphones are valuable targets, and they will be under attack
- Current security solutions are not sufficient for security sensitive organizations
- Outsourcing security is feasible, and can provide multifaceted security

# Android Vulnerability So Dangerous, Owners Warned Not to Use Phone's Web Browser: Updated

By Sarah Perez / February 12, 2009 8:40 AM / 92 Comments

Tweet 2

Like

101

Hacker News

Share 11



Over the weekend at the **Schmoocon** hacker conference in Washington D.C., security researcher **Charlie Miller** presented a new vulnerability in Google's mobile OS **Android** which allows hackers to remotely take control of the phone's web browser and related processes. If a phone became compromised, the hackers could gain access to the saved credentials stored in the browser and browser history. They could also snoop on your web transactions, even if encrypted.

## Another iPhone Attack

Posted: 11 Nov 2009



Symantec Security Response

View user profile.

Symantec Official Blog

The first iPhone worm, known as **iPhoneOS.Ikee**, to show that jailbroken iPhones had a flaw that could be exploited. It was a minor issue since the author decided to simply **Rickroll** many warnings that the publicly released code could be used to exploit other vulnerabilities.

## iPhone Attack Reveals Passwords in Six Minutes

PCWorld

Buzz up! 0 votes

Share 16

retweet 4

Email

Print

kaspersky predicts more iPhone, Android attacks in 2010

## iPhone 2010: iPhone hacker SMS database hijacked

By Ryan Naraine | March 24, 2010, 3:50pm PDT

### Summary

Using an exploit against a previously unknown vulnerability, the duo — Vincenzo Iozzo and Ralf Philipp Weinmann — lured the target iPhone to a rigged Web site and exfiltrated the SMS database in about 20 seconds.



## Ikee Worm Rickrolls Jailbroken iPhones

Posted: 09 Nov 2009



Symantec Security Response

SYMANTEC EMPLOYEE

Symantec Official Blog

On the heels of a similar iPhone attack by a Dutch teenager, an Apple employee has warned that the first iPhone worm for jailbroken iPhones. The worm has been spreading to iPhones to log in and spread. Please note that the worm has been spreading to iPhones to log in and spread.