

# Smartphones, App-stores and HTML 5

ENISA work on Smartphones and App stores and HTML 5 security

Dr Giles Hogben

Programme Manager, Secure Applications and Services

**European Network and Information Security Agency**

# Discussion: Smartphones and mobile security

- Smartphones – how to integrate them into your security policy?
- How to avoid the leakage of personal data?
- Can they be used for high-assurance cases:
  - what are the issues that need to be dealt with?
- Smartphones and the ambient intelligence vision (embedded, networked sensors etc...)?
- To what extent is the user ultimately responsible for protecting the confidentiality of their information? How do we address users who don't want to protect themselves or don't understand the risks?

# Discussion: Walled gardens and app-stores

- What recommendations could be given to improve app-store security?
- Pros and cons of app-review vs ex-post censorship models?
- Best way to deal with multiple app-stores?
- Would cross-industry app-store standards be useful?
- Kill-switches – issues, pros and cons.
- What part can users play in app-store security?
- What is "malware"? Should app stores be placed in a position to determine what programs are "malware" and which aren't? For example, are advertising networks "malware" because they upload unique identifiers in order to track served ads?
- Will Walled / Federated Gardens encourage riskier user behavior by forcing them "jailbreak" their phone in order to install apps from outside the "garden"?
- To what extent do Walled Gardens limit user choice and/or application developer innovation?

# Discussion: Consumerisation

- How to manage unknown devices?
- Is it reasonable/feasible for an enterprise to restrict access to/from consumer devices? (Issues/pros/cons)
- Can we secure access to the network from unknown end-points? (NAC as a solution?)
- How to separate functionality on the same device? (Dual-boot/virtualisation as a solution?)



# Smartphones



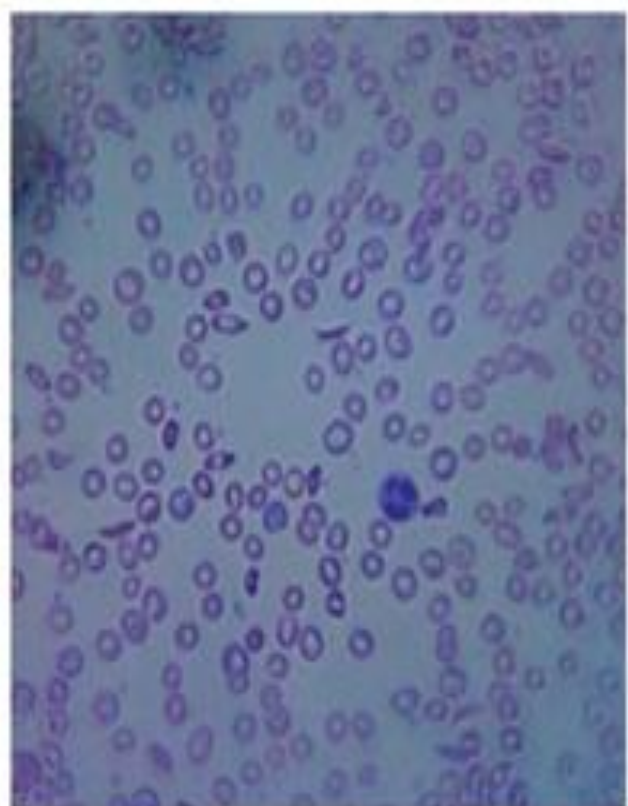
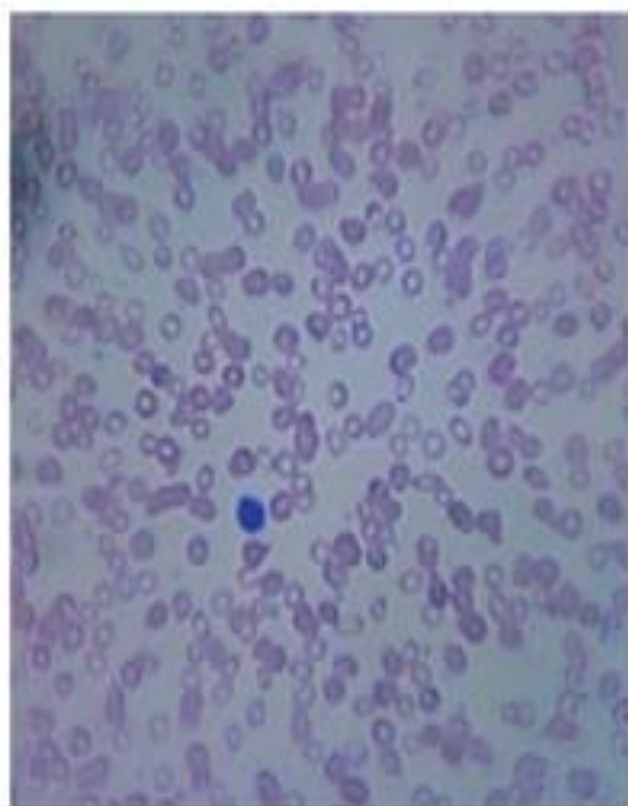
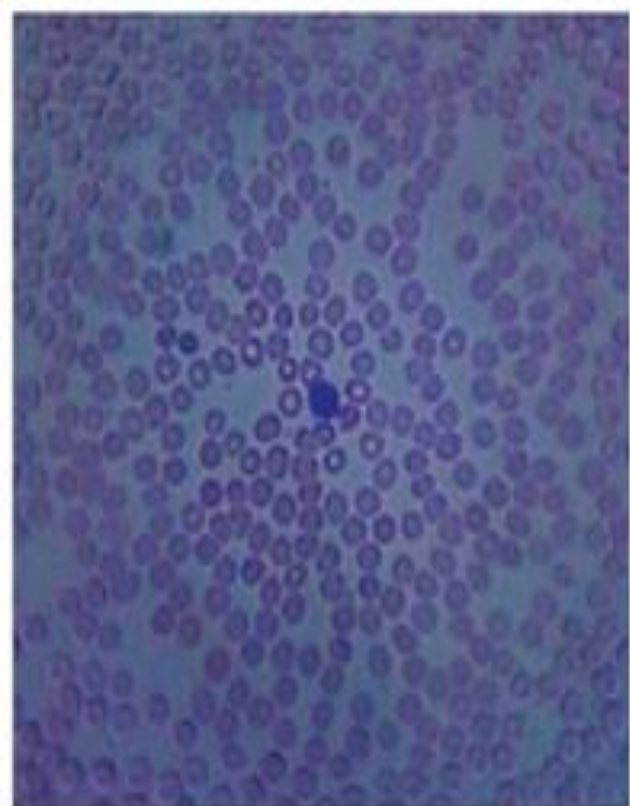
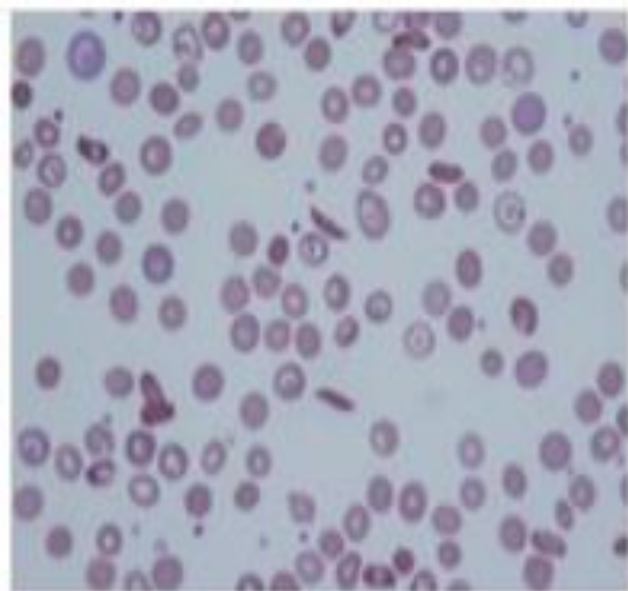
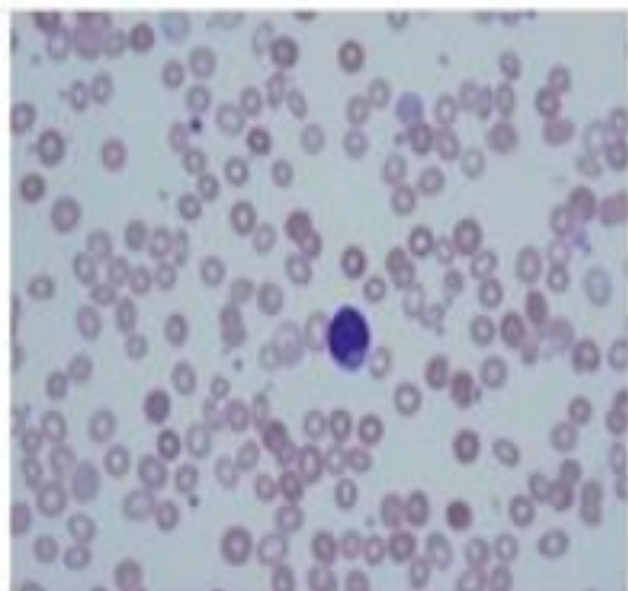
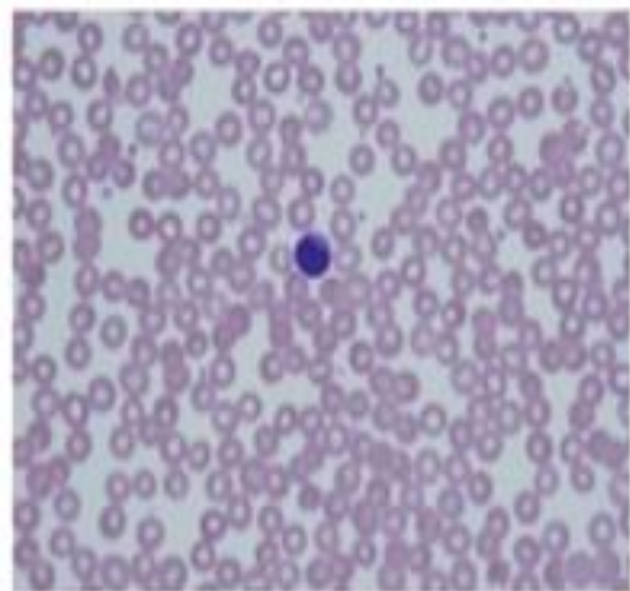
- Sensors: Precise position, Camera, Mic, Acceleration, Orientation, Magnetic field, Temperature, ....
- Full internet access through a standard browser
- Computer in your pocket – high-powered processor.
- Download third party applications from “marketplaces”.

**BIENVENIDO  
AL FUTURO**

Spanish to English

**WELCOME  
TO THE FUTURE**





# My Cards

Add New



   
Touch to Pay

\$30.00 

as of TODAY at 12:14PM

# My Cards



Your Starbucks Card number is  
7777 0172 3988 9450



STARBUCKS CARD

Touch  
When  
Done



Scan Now



Cards



Payments



My Rewards



Stores



Settings



Cards



Payments



My Rewards



Stores



Settings



Map

List

Range: 1.5km



Layers

Distance:  
965m

tweeps

Net 1-1 gespeeld. Voel me net een sprinter  
hele dag willen ze me diep spelen en hele dag...





# I Can Stalk U

Raising awareness about inadvertent information sharing

[Home](#)

[How](#)

[Why](#)

[About Us](#)

[Contact Us](#)

## Who have we stalked recently?



ICanStalkU was able to stalk [mandyhornbuckle](#) at  
<http://maps.google.com/?q=33.0918333333,-96.6515>  
3 minutes ago · [Map Location](#) · [View Tweet](#) · [View Picture](#) · [Reply to mandyhornbuckle](#)



ICanStalkU was able to stalk [N3KOCHAN](#) at  
<http://maps.google.com/?q=46.8103166667,-71.2917722222>  
8 minutes ago · [Map Location](#) · [View Tweet](#) · [View Picture](#) · [Reply to N3KOCHAN](#)



ICanStalkU was able to stalk [ArentSchaap](#) at  
<http://maps.google.com/?q=53.2178555556,6.99008055556>  
12 minutes ago · [Map Location](#) · [View Tweet](#) · [View Picture](#) · [Reply to ArentSchaap](#)



ICanStalkU was able to stalk [YJ\\_03](#) at  
<http://maps.google.com/?q=37.44413,126.633801944>  
18 minutes ago · [Map Location](#) · [View Tweet](#) · [View Picture](#) · [Reply to YJ\\_03](#)



ICanStalkU was able to stalk [tany\\_sunset](#) at  
<http://maps.google.com/?q=34.6413333333,135.5923333333>  
17 minutes ago · [Map Location](#) · [View Tweet](#) · [View Picture](#) · [Reply to tany\\_sunset](#)



ICanStalkU was able to stalk [andreajanke](#) at  
<http://maps.google.com/?q=48.8548333333,2.315833333333>  
23 minutes ago · [Map Location](#) · [View Tweet](#) · [View Picture](#) · [Reply to andreajanke](#)



ICanStalkU was able to stalk [Djuku](#) at  
<http://maps.google.com/?q=51.5482277778,4.80111944444>  
24 minutes ago · [Map Location](#) · [View Tweet](#) · [View Picture](#) · [Reply to Djuku](#)

## Links

- [Mayhemic Labs](#)
- [PaulDotCom](#)
- [SANS ISC](#)
- [Electronic Frontier Foundation](#)
- [Center for Democracy & Technology](#)

[How did you find me?](#)

Did you know that a lot of smart phones encode the location of where pictures are taken? Anyone who has a copy can access this information.

[read more](#)

[Help me fix this!](#)

Disabling Geo-Tagging on your phone is easy. Check our list of common phones.

[read more](#)

# Talk outline

- **ENISA's Smartphone report**
  - Top 10 Risks
  - Opportunities
  - Recommendations
- App-store security



# Report Contributions

- Group of 30 security/smartphone experts
  - All big smartphone platform vendors (except one)
  - Standards bodies (e.g. GSMA)
  - Governmental IT departments (ministries)
  - Corporate IT departments (banks, telcos)



# Risks in different usage scenarios

- Risks are rated in three usage scenarios
  - **Consumer** usage
    - Daily life, social networks, emails, games.
  - **Employee** usage
    - Business phone, corporate email, some workflow apps.
  - **High official or aide**
    - Business phone, corporate email, sensitive data.
- Important: **Cross-over** from one scenario to another is common (daily, weekly or ad-hoc).



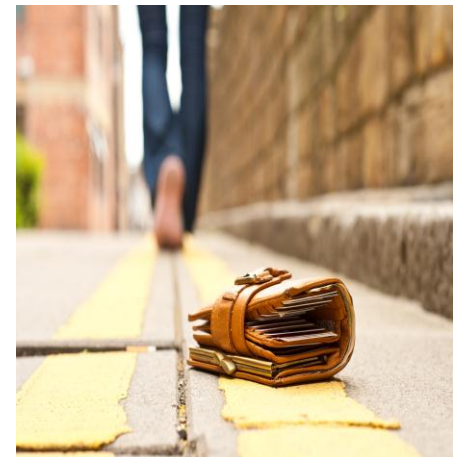
# 10 information security risks

1. Device loss leading to data leakage
2. Improper decommissioning
3. Unintentional data disclosure
4. Phishing attacks
5. Spyware
6. Network spoofing attacks
7. Surveillance attacks
8. Diallerware
9. Financial malware
10. Network congestion

# 1. Device loss -> data leakage

Consumer (C)	High	Medium	Medium
Employee (E)	Medium	High	High
High official (H)	Medium	Very high	High

- Smartphones are full of sensitive (corporate) data and carried around.
- Not always auto-locked and password-protected.
- Encryption schemes are sometimes insecure.
  - E.g. iOS3 disk encryption has flaws.
- UK government survey:
  - 2% reported their mobile phone was stolen last year



# President-Elect Barack Obama Drops His BlackBerry



↳ POSTED BY TAMER ON 01.17.09 AT 4:27 PM



# 2. Unintended disclosure of data

- Smartphone is loaded with personal data, with sensors and network interfaces.
- Collecting meaningful consent is difficult
- Covert channels
  - Photos may contain location data
  - Address book may contain private data
  - “I can stalk u” (smartphone version of “Please rob me”)
- Interface to privacy and security settings is not easy



Consumer (C)	Very high	High	High
Employee (E)	High	Medium	High
High official (H)	High	Very High	High

# 3. Attacks on decommissioned phones

Consumer (C)	Medium	Medium	Medium
Employee (E)	High	High	High
High official (H)	Medium	Very high	High

- Decommissioning PC's is common, not yet for smartphones.
- By 2012 100 million phones will be recycled per year.
- In a recent study, 26 mobile phones were bought second-hand on eBay
  - 1 from a senior sales director
  - 2 with “embarrassing details of personal nature”
  - 4 allowed to identify the owner
  - 7 allowed to identify the owner's employer



# 4. Phishing

Consumer (C)	Medium	High	Medium
Employee (E)	Medium	High	Medium
High official (H)	Medium	Very high	High



- Phishing is a big problem
- On smartphones
  - Trust cues are harder to find or absent
  - Phishing apps can be used
  - Attackers can phish using SMS, or bluetooth
    - SMiShing: SMS from your bank asking to confirm or cancel a purchase, by visiting a site or calling a number.

# 5.Spyware

Consumer (C)	High	Medium	High
Employee (E)	Medium	High	Medium
High official (H)	Medium	Medium	Medium

- Taintdroid: “Half of apps studied share location information and unique identifiers with advertisers.”
  - Phone number, device ID’s, IMSI, ICC-ID, Location data
- S-Mobile study: “70% of 50.000 apps suspicious. “
- iPhone keyboard cache and addressbook are by default accessible to apps. And other files with private data.

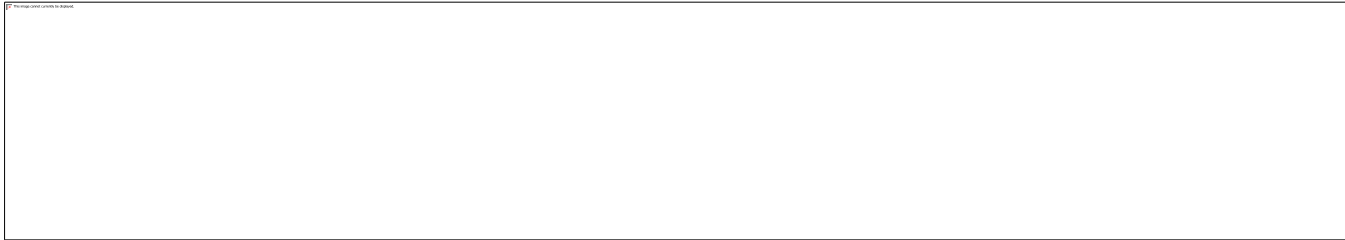
# 6. Network spoofing

Consumer (C)	Medium	Medium	Medium
Employee (E)	Medium	High	Medium
High official (H)	Medium	High	High

- Mobility in the network sense
- Network spoofing at airports e.g.
- Should be prevented by SSL but... most users skip warnings.
- Worked at Blackhat
  - Blackhat 2009 SSL downgrade
- But people can't do without hotspots.
  - Hackers too: Blackhat 2010 Fake GSM basestation



# 7. Surveillance attacks



- Smartphones for keeping someone under surveillance.
- Android app Tap snake is a frontend for GPS spy.
- Any method: Unintentionally disclosed data, steal phone, network spoofing, phishing...

# 8. Mobile diallerware

Consumer (C)	High	High	High
Employee (E)	Medium	Medium	Medium
High official (H)	Low	Low	Low

- Unauthorized access to premium number or sms
  - Premium SMS services
  - Pay through SMS schemes
  - In app purchases
- Quick money (ask telco's)



# 9. Banking malware

Consumer (C)	Medium	High	High
Employee (E)	Low	High	Medium
High official (H)	Low	Low	Low

- Every bank is going “app” now
- Phishing banking apps on Android market
- Example: Zeus in the Mobile (SymbOS/Zitmo)
- Undetected by anti-virus software



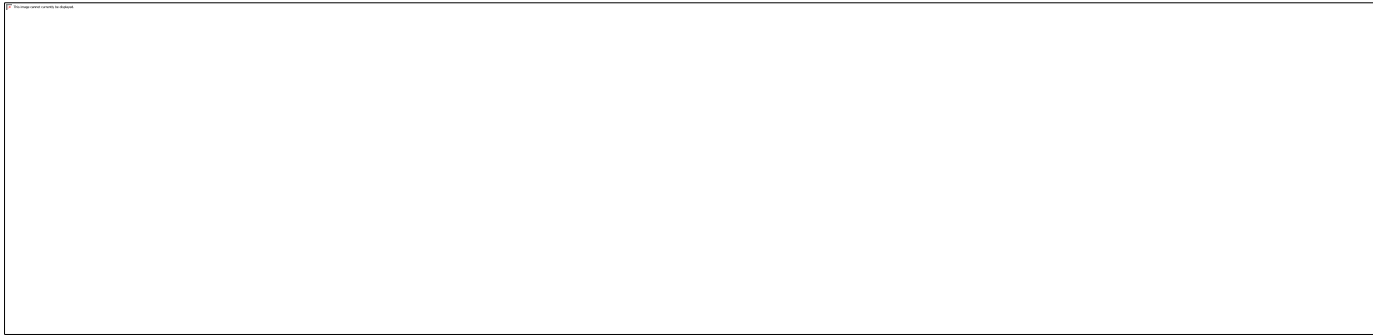
# Using Zitmo

- Attacker steals online username and password using a malware (Zeus 2.x) and **get's the user's mobile number** by phishing.
- Attacker infects the smartphone by sending an SMS with a link to Zitmo. The user must accept ('Nokia update').
- Attacker logs in with the stolen username and password, using the user's PC as a proxy and performs a banking transaction.
- An SMS is sent to the smartphone with the authentication code. Zitmo intercepts the SMS and sends it to malware authors.
- The SMS is never displayed on the victim's phone.
- Attacker fills in the SMS code and completes transaction.

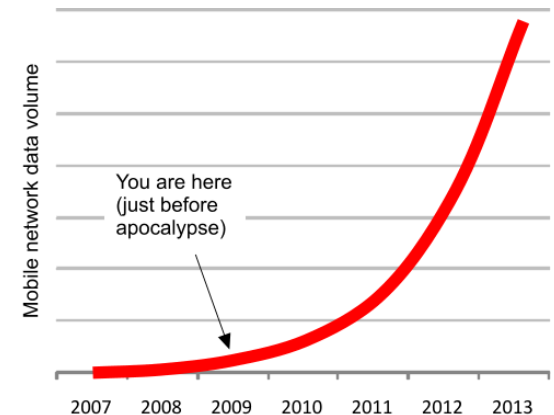


<http://www.isarg.in/blog/2011/02/23/zitmo-the-new-mobile-threat/>

# 10. Network and signalling overload



- Signalling overload: Typical smartphone 8 X more signalling traffic than a laptop with a USB dongle .
- Data capacity overload: 39 fold increase between 2009 and 2014 (Cisco).
- **BUT** - In Europe, Analogue TV spectrum and spectral efficiency gains will help a lot!
- Developers should design software accordingly – esp for flash events.



# Talk outline

- ENISA's Smartphone report
  - Top 10 Risks
  - **Opportunities**
  - Recommendations for IT officers
- App-store security



# Information security Opportunities

1. Sandboxing and capabilities
2. Controlled software distribution
3. Remote application removal
4. Backup and recovery
5. Extra authentication options  
E.g. smartphone as OTP generator.
6. Extra encryption options  
E.g. end-to-end voice encryption.

# Talk outline

- ENISA's Smartphone report
  - Risks
  - Opportunities
  - **Recommendations**
- Secure Smartphone Dev Guidelines
- App-store security
- HTML 5 + security analysis preliminary results



# Recommendations

- Recommendations are risk-based, addressing the highest risks first.
- Incremental (mostly) from E to H.
- We urge IT administrators to issue advice regarding consumer usage.
- Recommendations for IT administrators are in the form of policy rules.
- Top three recommendations:
  - Turn on auto-lock
  - Encrypt data on your phone
  - Install only apps you trust
- Follow-up – secure smartphone development guidelines.

## 4.3 Addressing the risk of attacks on decommissioned phones

Risk addressed		Recommendations
R3. Attacks on decommissioned smartphones	<b>C</b>	<b>Reset and wipe:</b> before disposing of or recycling the phone, wipe all the data and settings from the smartphone. This goes beyond a factory reset of the smartphone's settings.
	<b>E</b>	IT officers should have policy rules on:  <b>Decommissioning:</b> before being decommissioned or recycled, pass used phones a thorough decommissioning procedure, including memory wipe processes. Include removable media and memory. For wiping memory, use a standard procedure, such as the NIST standard (60) (61).
	<b>H</b>	Idem

# Talk outline

- ENISA's Smartphone report
  - Top 10 Risks
  - Opportunities
  - Recommendations
- **App-store security**



# App stores

(10 Billion apps downloaded from Apple's app store, e.g.)



# Walled gardens: A new (old) way of distributing software

- Apple app-store
- Android market
- Google chrome store
- Mozilla store
- Windows phone seven
- Linux repositories
- Amazon app-store
- .....



[home](#)[my apps](#)[my messages](#)[my account](#)

## my dashboard

When you've submitted your app to us for evaluation, we will let you know if we are interested in publishing it and, if we are, what you need to do next.

## submit your apps

### submit app for evaluation

Submit a simple overview of your app for Orange to evaluate. We'll tell you if it fits our content policy and if it's suitable for our customers. Download the [Orange App Shop content policy](#)

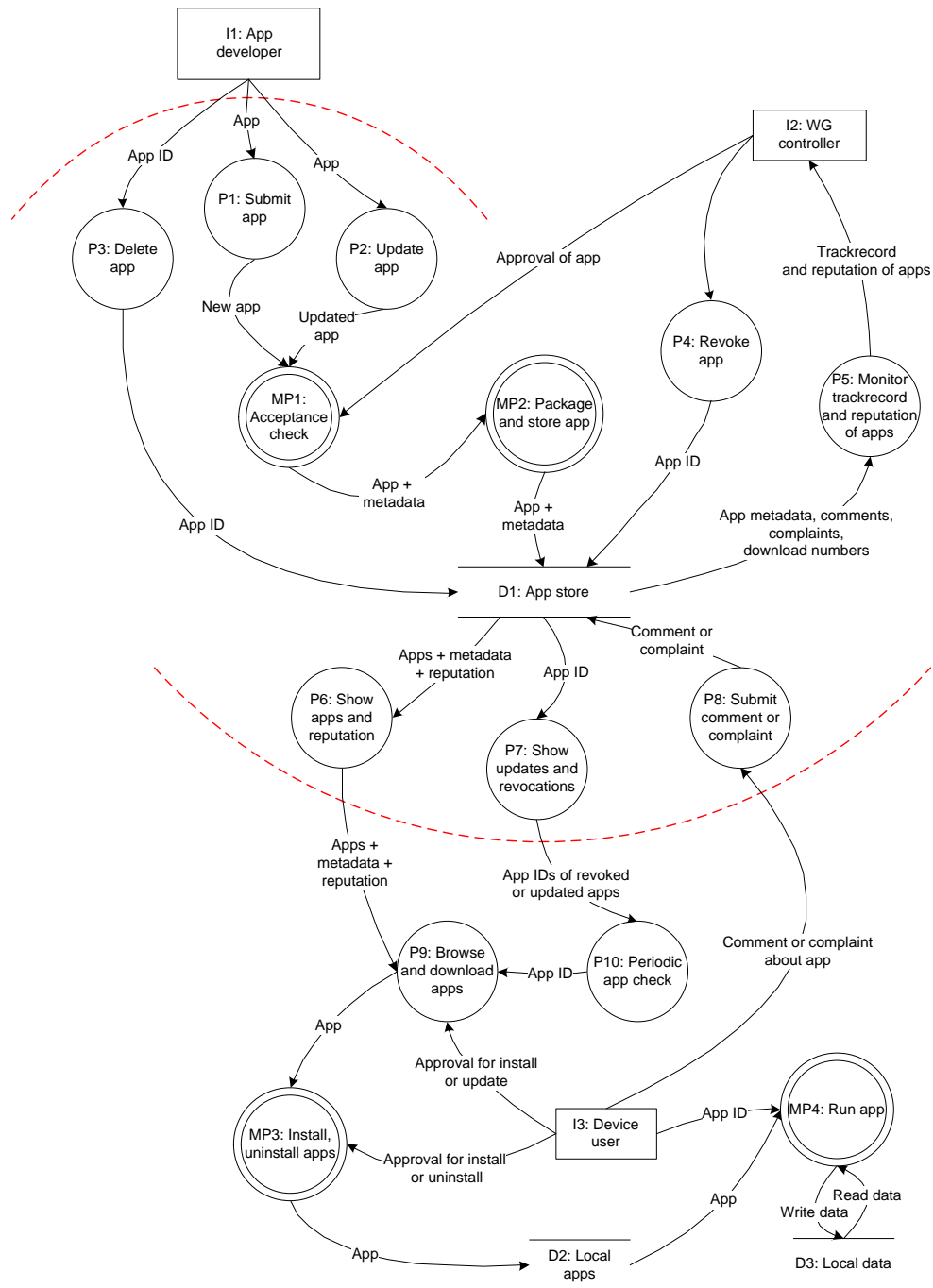
## my messages

date	from	subject
21-04-2011 0:22	developers@orange.com	<a href="#">welcome to Orange Partner Connect</a>



**amazon.com<sup>®</sup>**

The Amazon logo, consisting of a curved orange arrow pointing from the letter 'a' to the letter 'z'.



# App-store dangers

- **Update processes** – slow and cumbersome, vulnerable to attack.
- **Spoofed apps** (e.g. banking, recent Android attacks) can piggy-back reputation.
- **Malicious apps** can circumvent walled garden defences through:
  - Runtime interpreters
  - Elevation of privilege (through permissions fatigue)
  - Errors in vetting.



# App-store dangers

- **Federation** (Amazon, Google, etc...) -> jailbreaking or voluntary opening of the garden.
- **Misplaced sense of trust** – in review process/reputation system
  - maybe the app-store does not promise any security checks at all.



# Example incident 1



- [DroidDream](#) was hidden in look-alike versions of popular apps on the marketplace (piggybacking on their reputation).
- In a matter of days, there were around 200.000 downloads.
- Following the attack, [Google released](#) an "Android Market security update"
- Immediately after this, researchers found [malware versions of the Android security update](#) (with a virus called Android.Bgserv) in third-party Android markets.

**Bm**

**A**

**G**

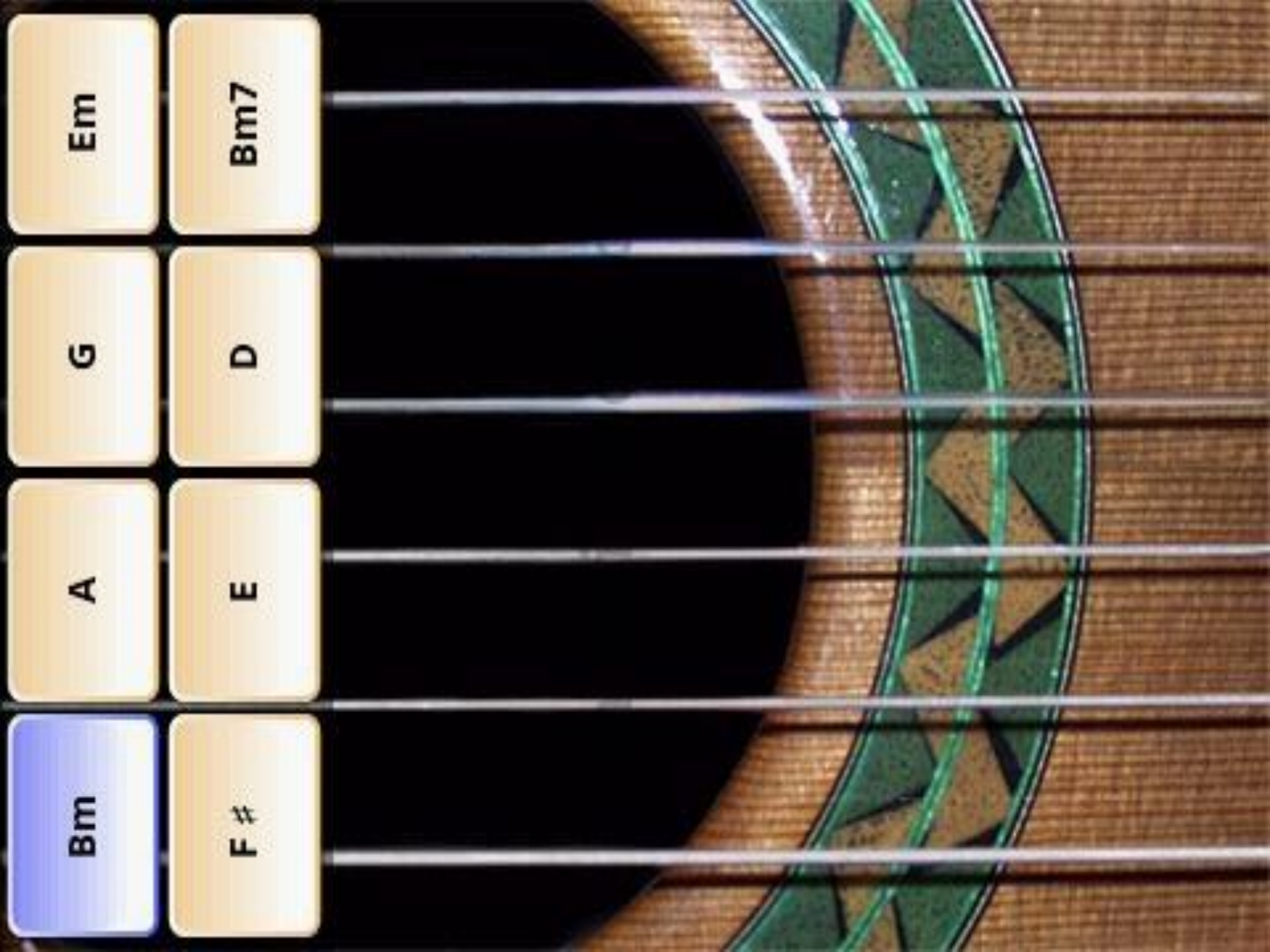
**Em**

**F #**

**E**

**D**

**Bm7**



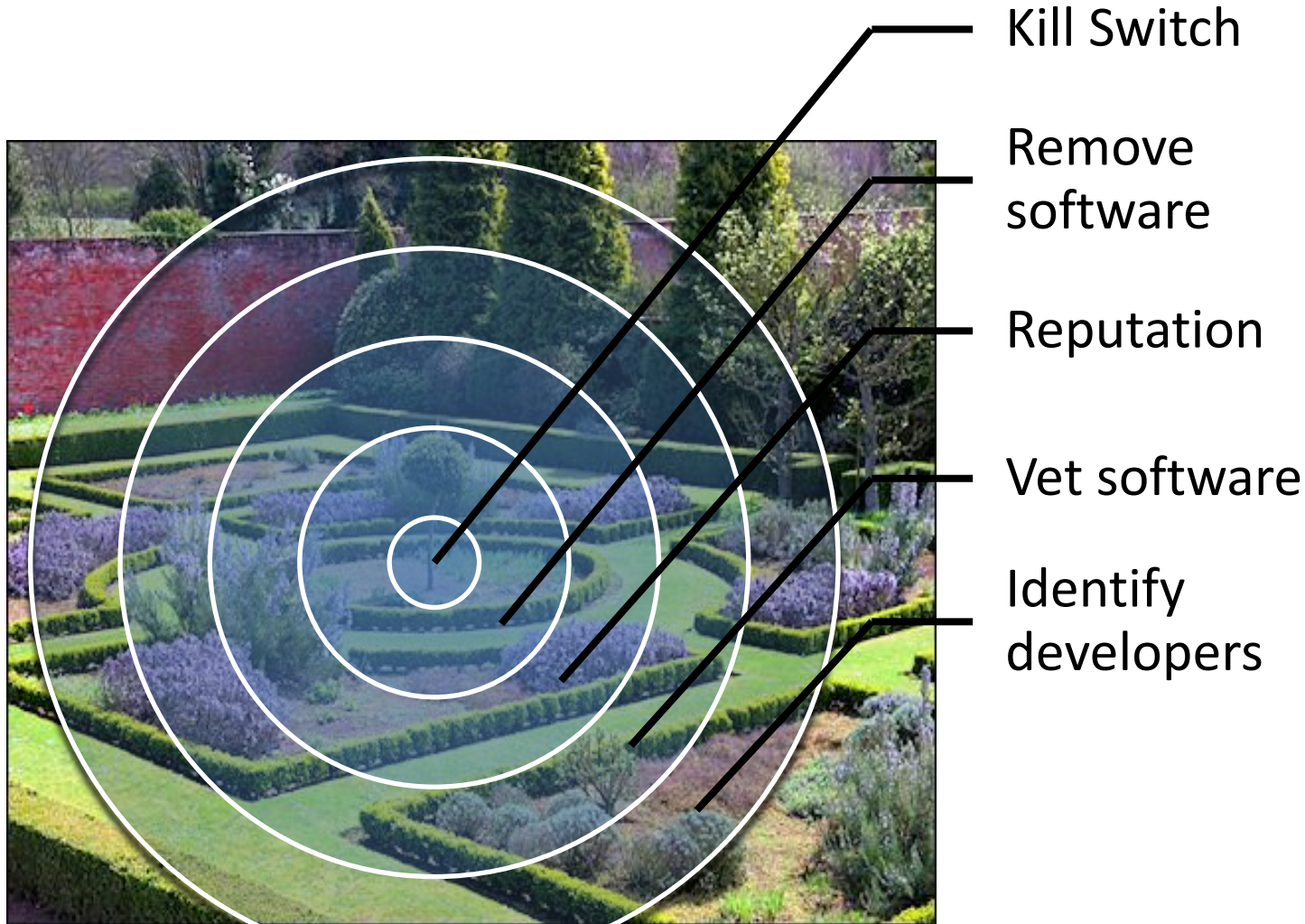
## Angry Birds Bonus Levels



Install Angry Birds Bonus Levels

Please click the above button to install the bonus Angry Birds levels!

# Walled gardens: The 5 layers of defence



# Thoughts on Kill switches

- Benefits
  - Fix the problem when the malware is already in the wild.
  - In many ways this is what we need for malware – bot-hunters love it.
- Risks
  - False positives and market-driven kills
  - Access to the user's device may be against legislation on access to computer systems.
  - May violate security policy in high-assurance cases
  - Only covers malicious apps – what about other software flaws – e.g. pdf reader.



# Consumerisation

- 95% of the workers who responded have used technology they purchased themselves for work
- Nato provides anti-virus support for home PC's

