Smartphones, App-stores and HTML 5

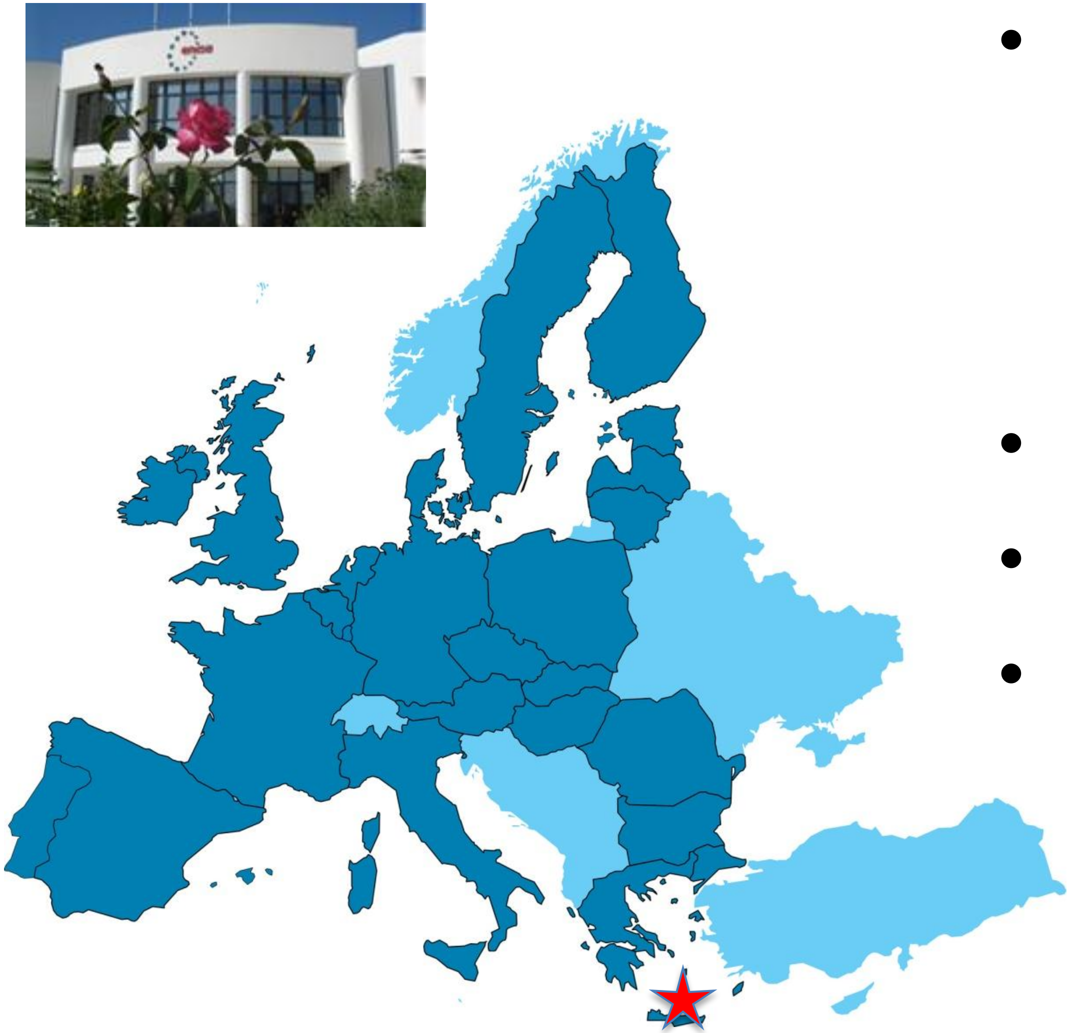
ENISA work on Smartphones and App stores and HTML 5 security

Dr Giles Hogben
Programme Manager, Secure Applications and Services

European Network and Information Security Agency

enisa European Network and Information Security Agency

ENISA

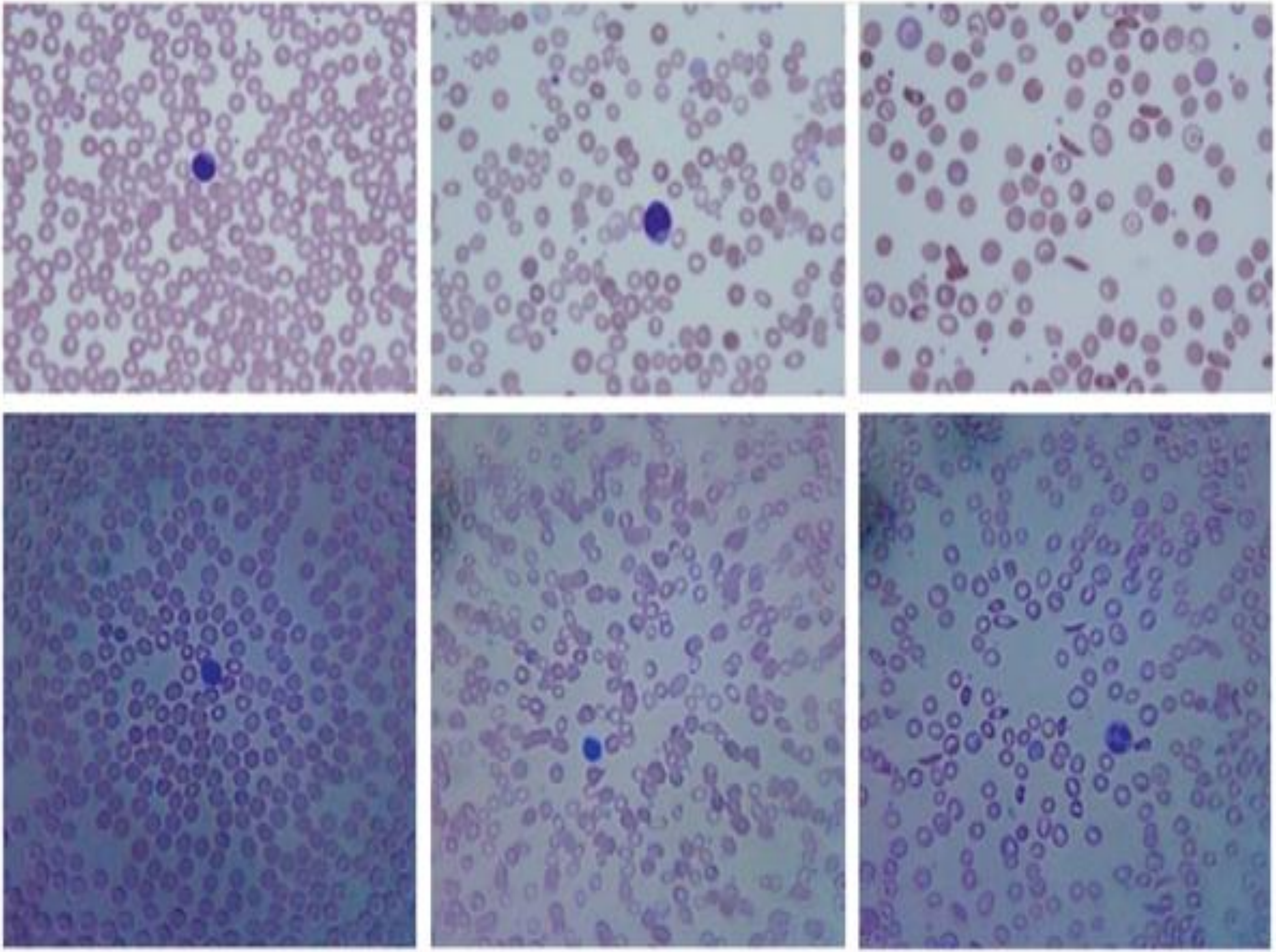


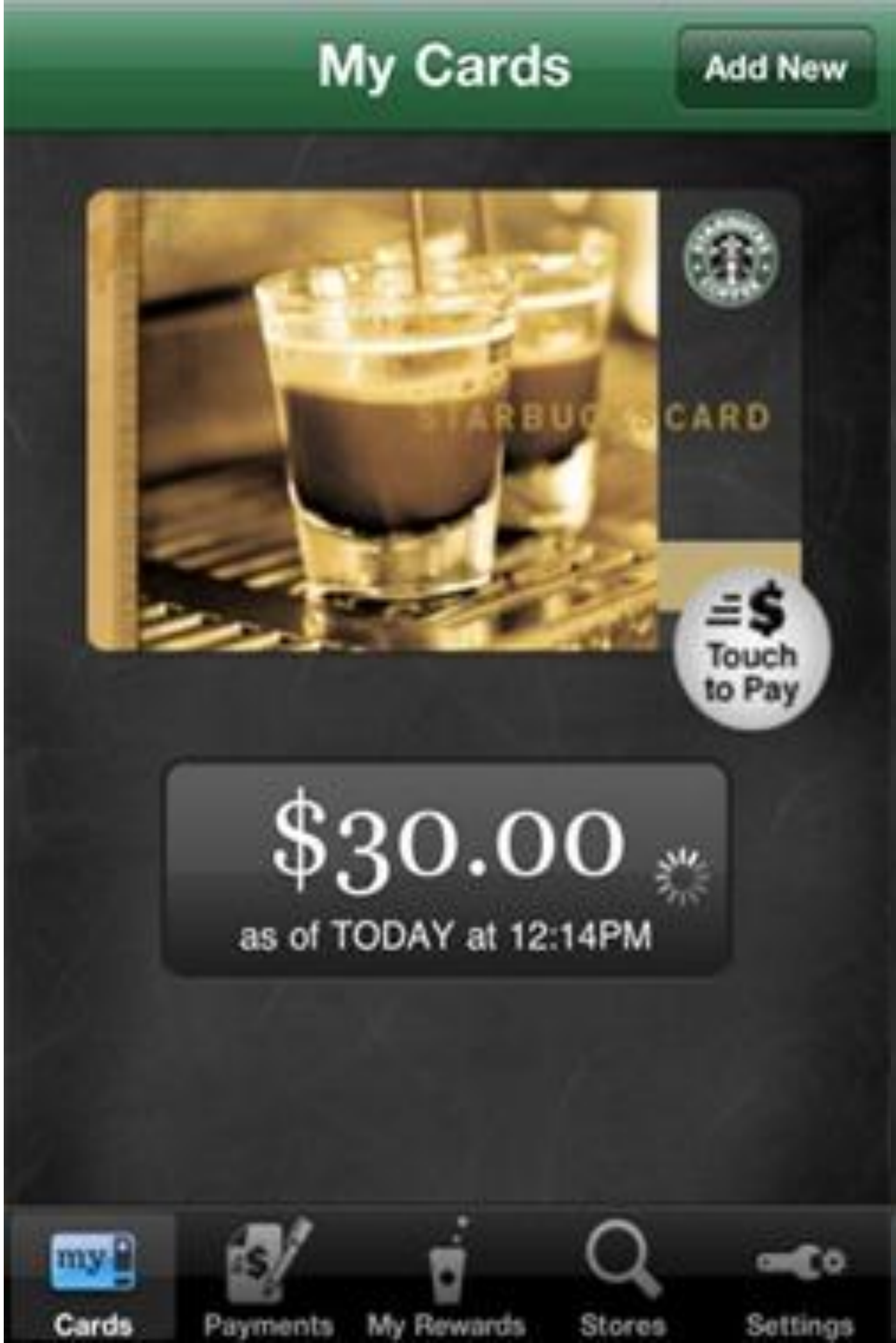
- Supports EU institutions
- Facilitator of information exchange between EU institutions, public sector & private sector.
- Collecting and analysing
- Promoting best practice
- Raising awareness

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”.

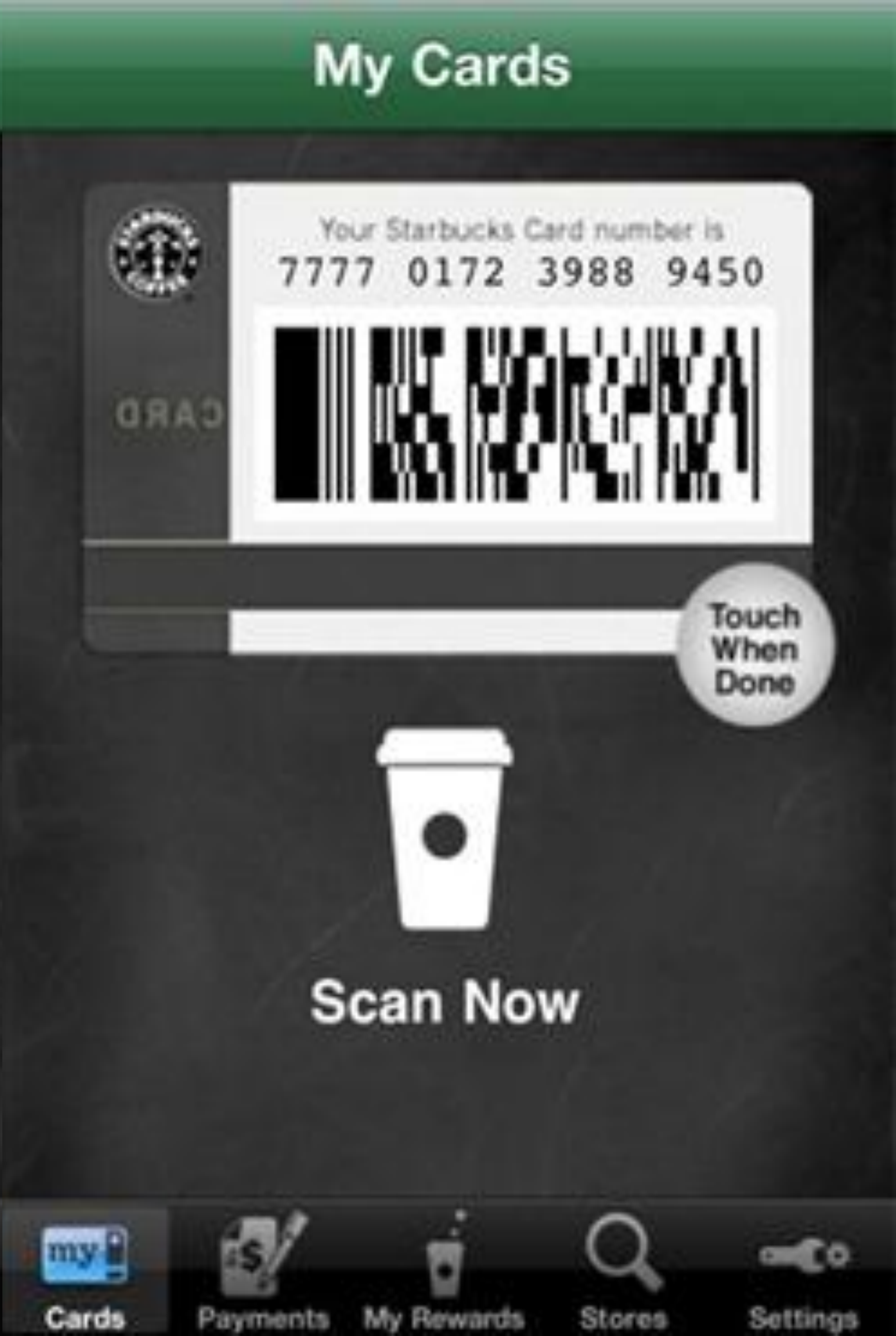
BIENVENIDO
AL FUTURO
Spanish to English
WELCOME
TO THE FUTURE





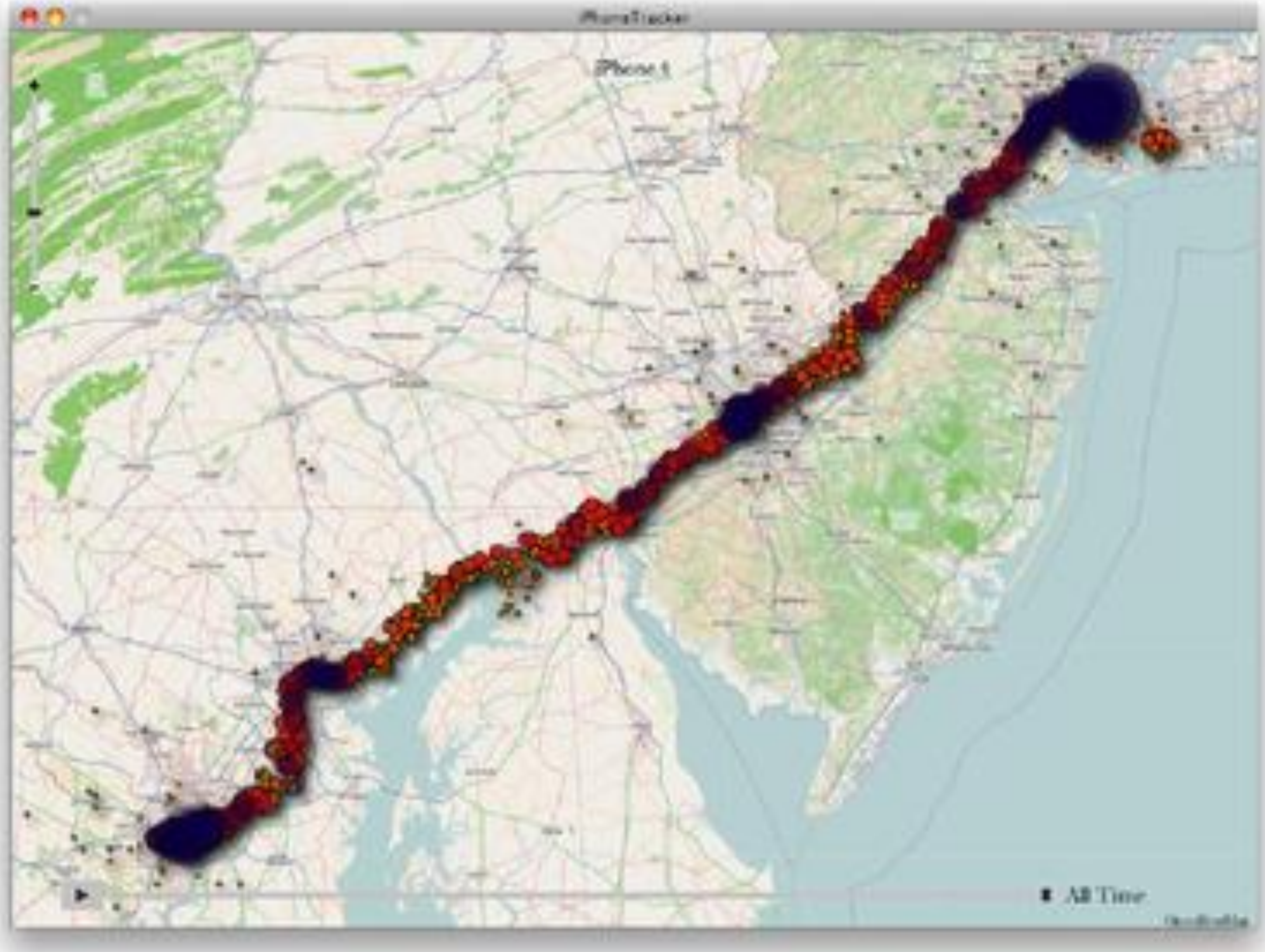
$30.00

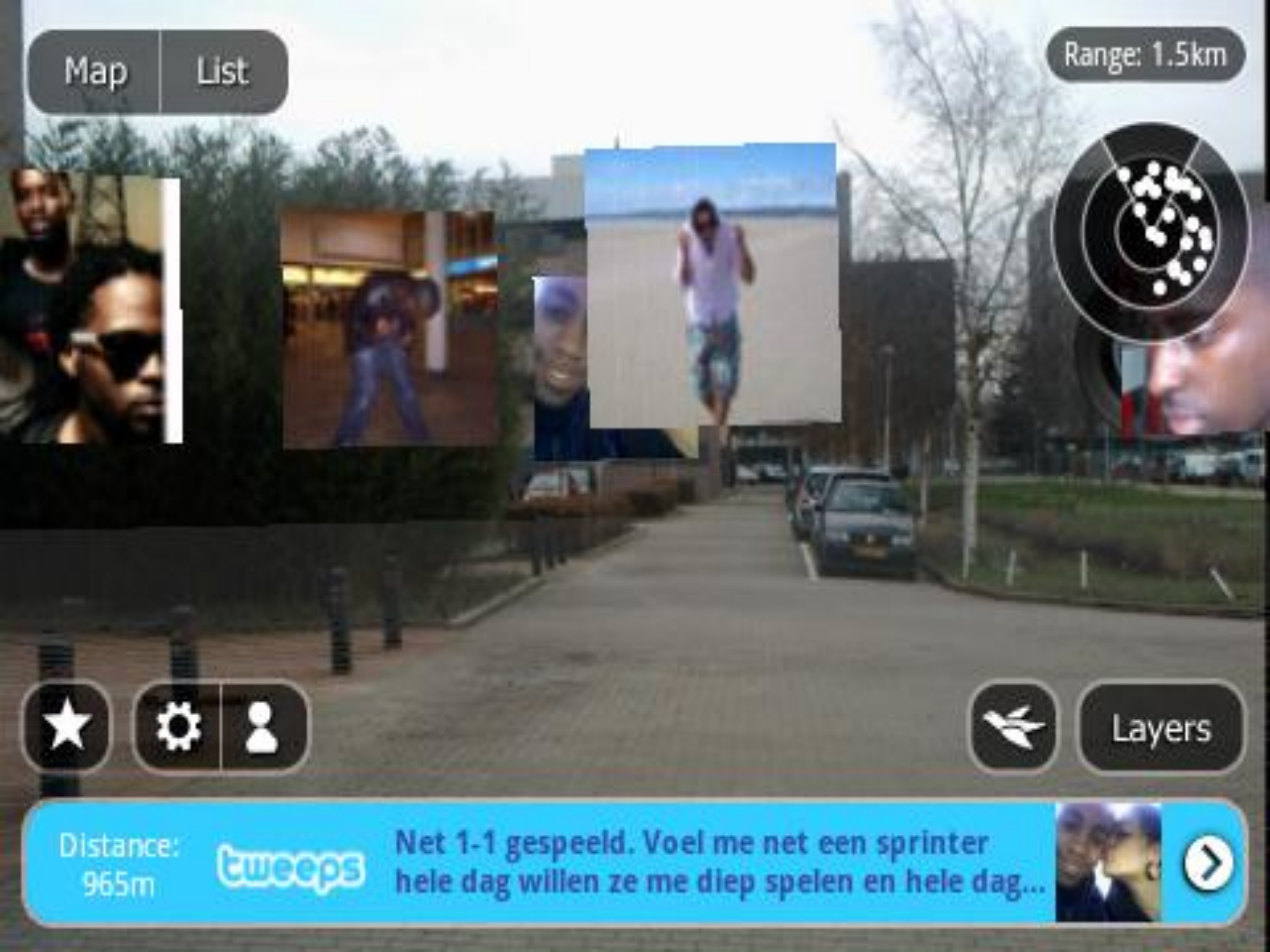
as of TODAY at 12:14PM



Your Starbucks Card number is

7777 0172 3988 9450

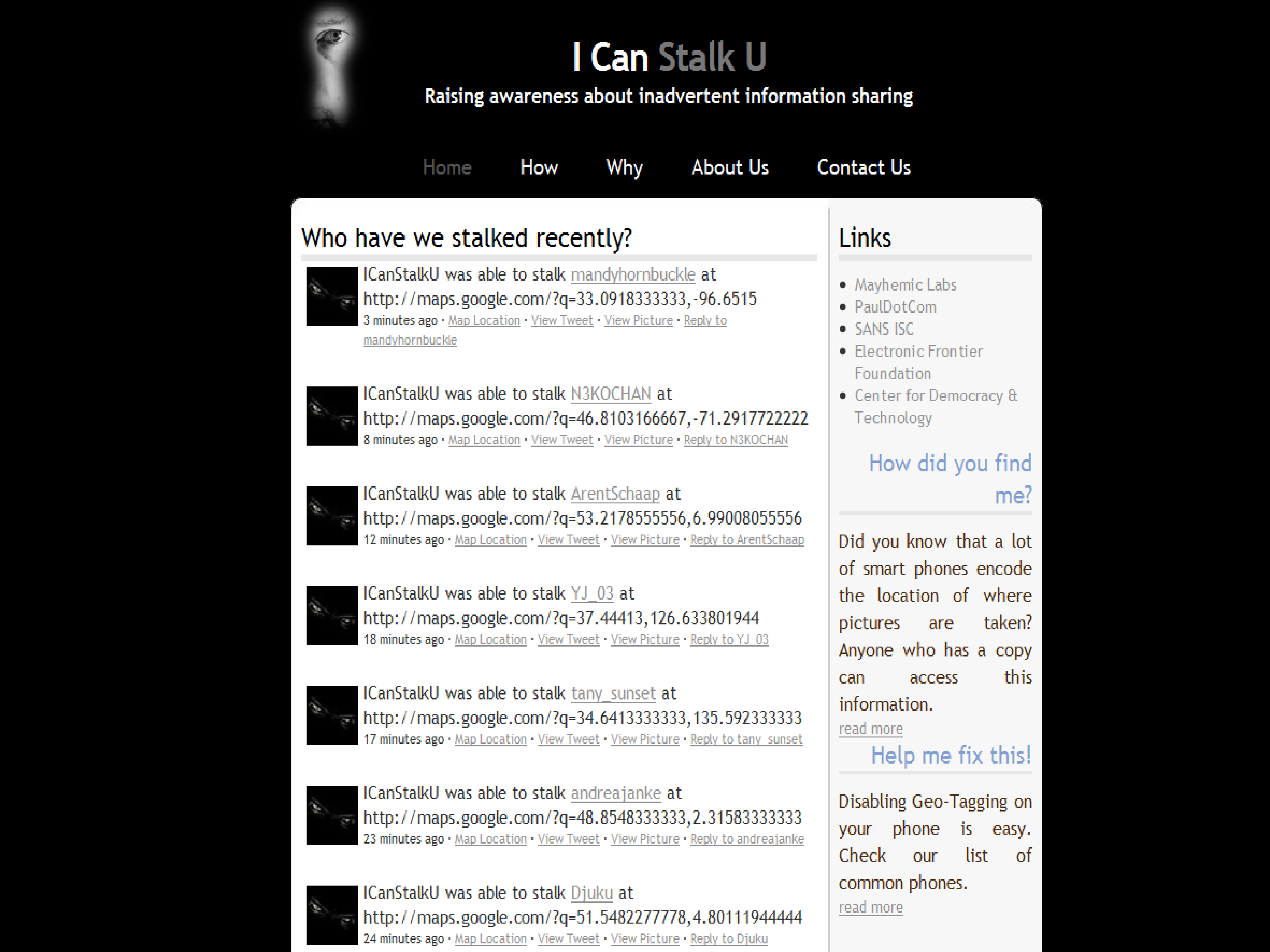

iPhoneTracker
iPhone 4
All Time
OpenStreetMap



Range: 1.5km

Distance: 965m

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

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=34.6413333333,135.592333333
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=48.8548333333,2.31583333333
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
- Secure Smartphone Dev Guidelines Project
- App-store security
- HTML 5 + security analysis preliminary results

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)

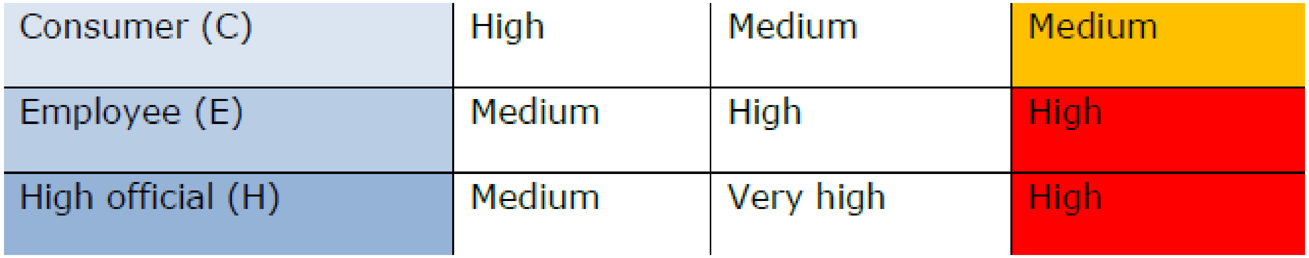
Risks in different usage scenarios

- 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

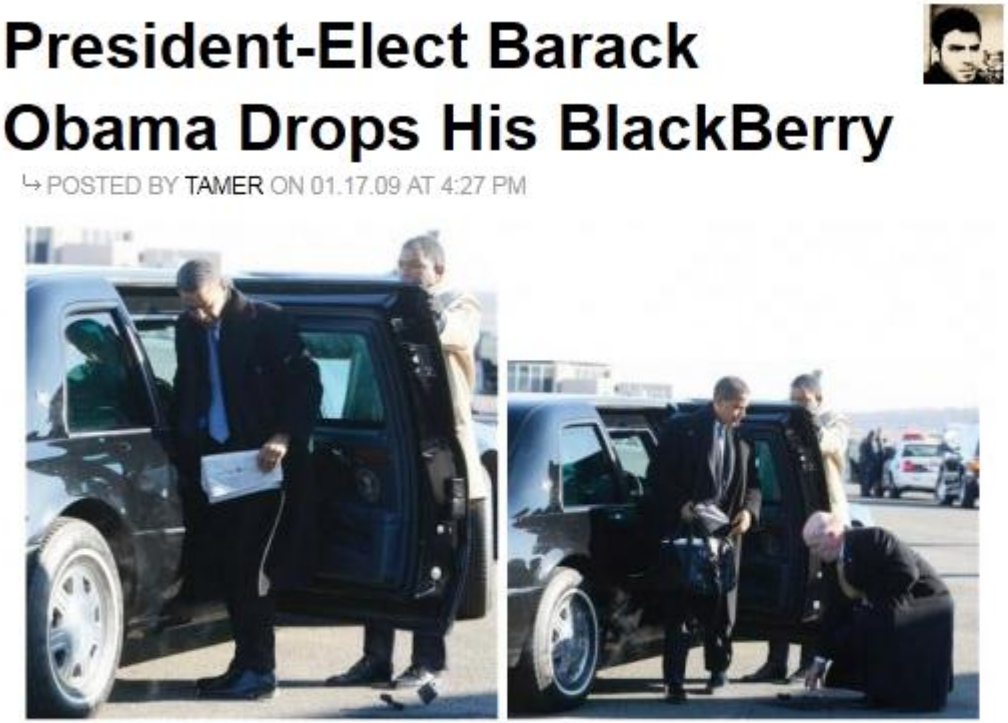
1. Device loss leading to data leakage
2. Improper decommissioning
3. Unintentional data disclosure
4. Phishing attacks
5. Spyware
6. Network spoofing attacks
7. Surveillance attacks
8. Diallerware
9. Financial malware
10. Network congestion

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

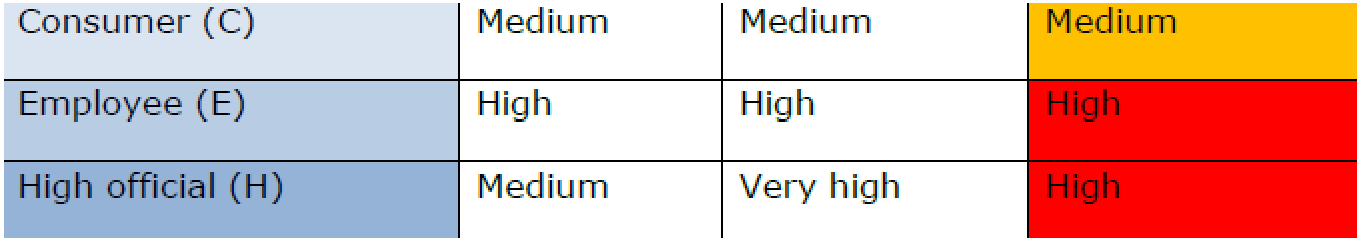
↳ POSTED BY TAMER ON 01.17.09 AT 4:27 PM

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

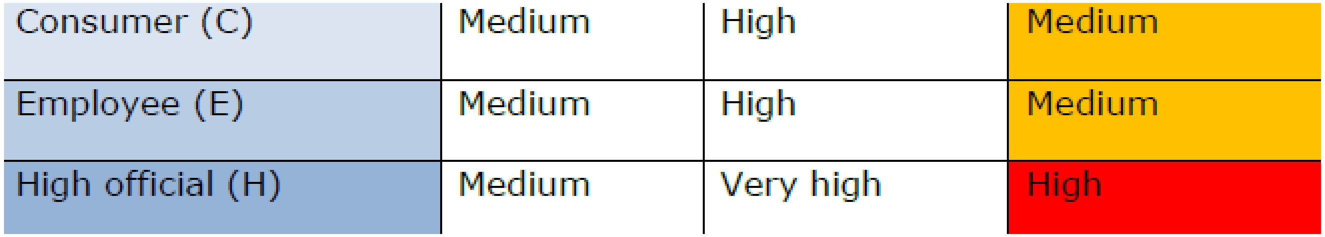
3.Attacks on decommissioned phones



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

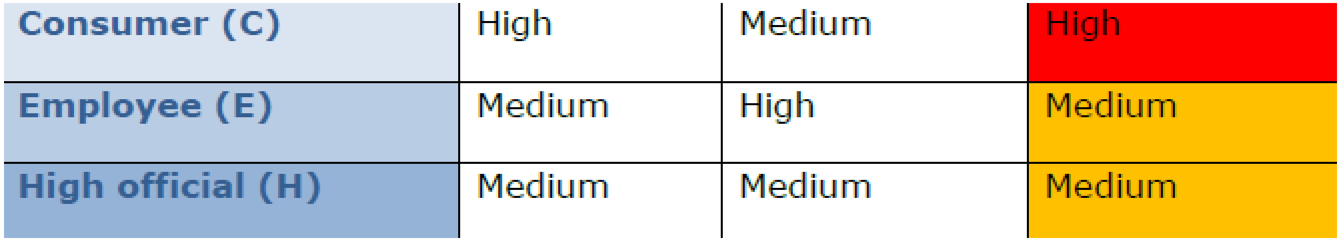
4.Phishing



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.

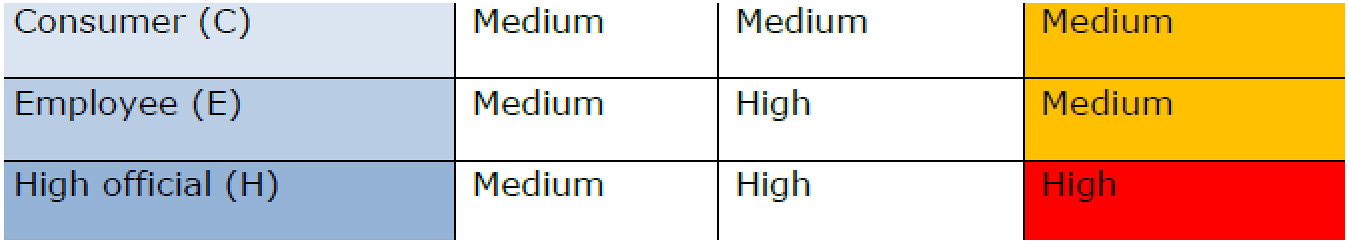
5.Spyware



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.

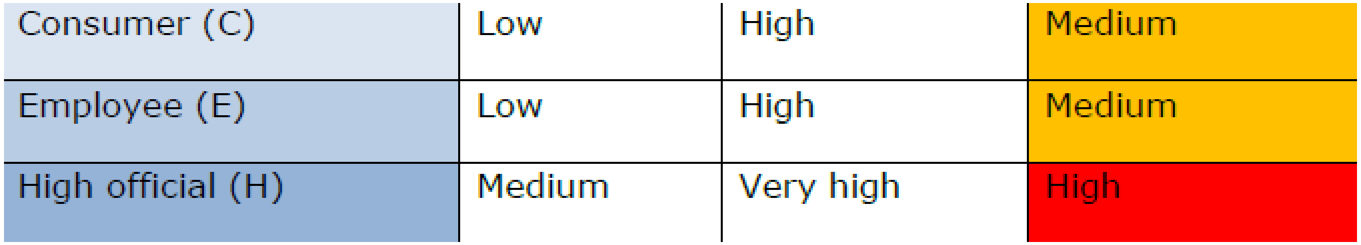
6.Network spoofing



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



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

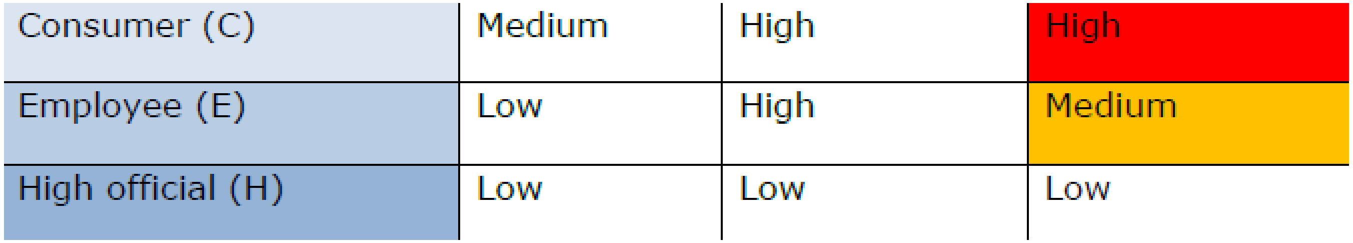
- Smartphones for keeping someone under surveillance.
- Android app Tap snake is a frontend for GPS spy.
- Any method: Unintentionally disclosed data, steal phone, network spoofing, phishing...

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

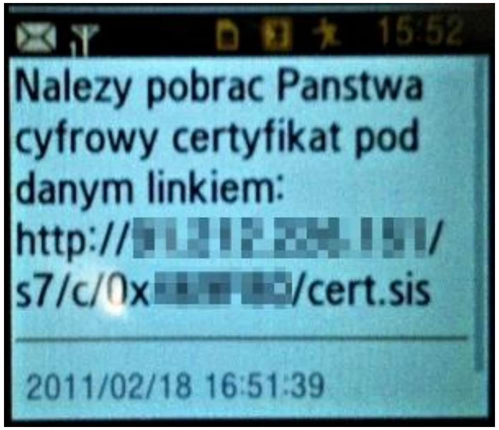


Consumer (C)	Medium	High	High
Employee (E)	Low	High	Medium
High official (H)	Low	Low	Low

- 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.



Nalezy pobrac Panstwa cyfrowy certyfikat pod danym linkiem:
http://[redacted]/
s7/c/0x[redacted]/cert.sis

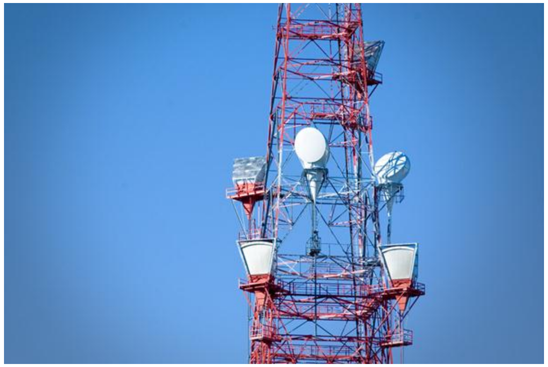
2011/02/18 16:51:39

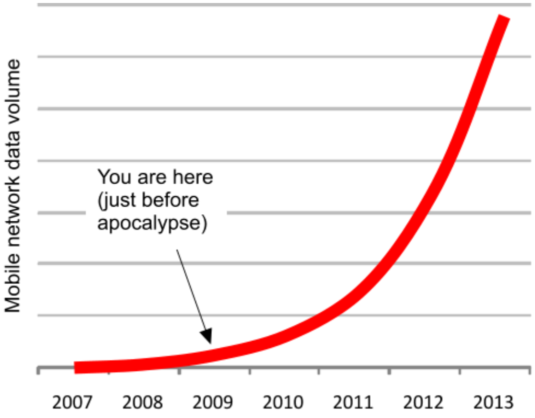
http://www.isarg.in/blog/2011/02/23/zitmo-the-new-mobile-threat/

10. Network and signalling overload

Rating	Likelihood	Impact	Risk
Consumer (C)	Low	Low	Low
Employee (E)	Low	Low	Low
High official (H)	Low	Low	Low

- 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
- Secure Smartphone Dev Guidelines
- App-store security
- HTML 5 + security analysis preliminary results

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	**C**	**Reset and wipe:** 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.
	E	IT officers should have policy rules on: **Decommissioning:** 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).
	H	Idem

Talk outline

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

Secure Smartphone App Dev Guidelines

- ENISA/OWASP project follow up on top 10 risks
  - Risk based
    - Secure design principles
    - Controls
    - Platform specific how-tos how-not-tos, common errors and vulnerabilities.
    - Code (on how to implement common controls), how not-to app (mobile version of WebGoat).
    - Open source libraries - mobile version of ESAPI

How to get involved

- Wiki is here:
  - Project outline: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Secure_Development_Guidelines
  - Controls and principles: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Controls
- We need
  - Reviewers for design principles and controls (still time to contribute too)
  - Drafters and contributors for platform-specific how-tos and how-not-tos (from July)
  - Open source libraries

Talk outline

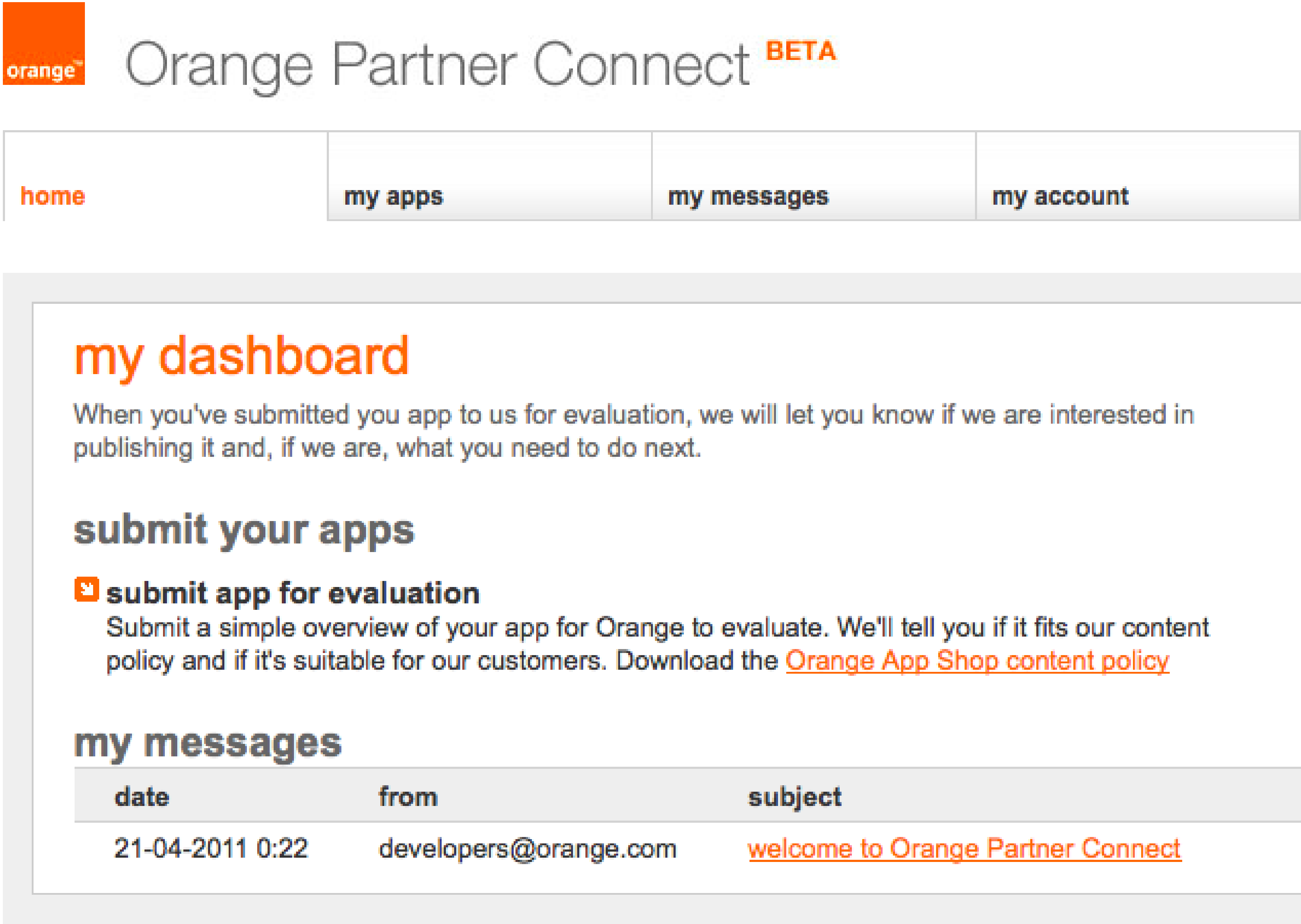
- ENISA's Smartphone report
  - Top 10 Risks
  - Opportunities
  - Recommendations
- Secure Smartphone Dev Guidelines
- **App-store security**
- HTML 5 + security analysis preliminary results

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
- …..



my dashboard

When you've submitted you 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

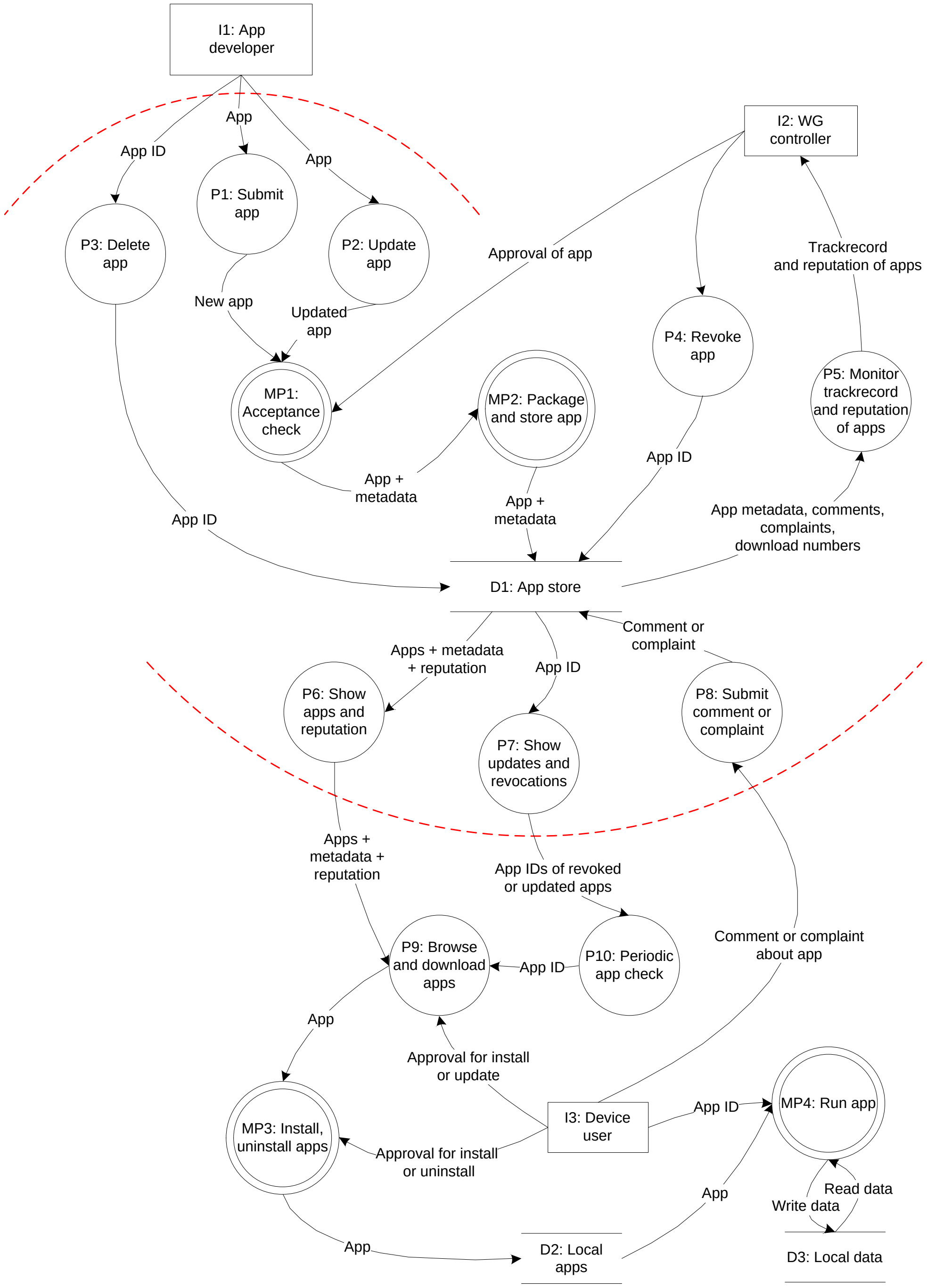
submit app for evaluation

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	welcome to Orange Partner Connect

amazon.com®


I1: App developer
App ID
App
App
P3: Delete app
P1: Submit app
P2: Update app
New app
Updated app
MP1: Acceptance check
MP2: Package and store app
App + metadata
App + metadata
I2: WG controller
Approval of app
P4: Revoke app
App ID
Trackrecord and reputation of apps
P5: Monitor trackrecord and reputation of apps
App metadata, comments, complaints, download numbers
App ID
D1: App store
Apps + metadata + reputation
App ID
Comment or complaint
P6: Show apps and reputation
P7: Show updates and revocations
P8: Submit comment or complaint
Apps + metadata + reputation
App IDs of revoked or updated apps
Comment or complaint about app
P9: Browse and download apps
App ID
P10: Periodic app check
App
Approval for install or update
MP3: Install, uninstall apps
Approval for install or uninstall
I3: Device user
App ID
MP4: Run app
App
Read data
Write data
App
D2: Local apps
D3: Local data

App-store dangers

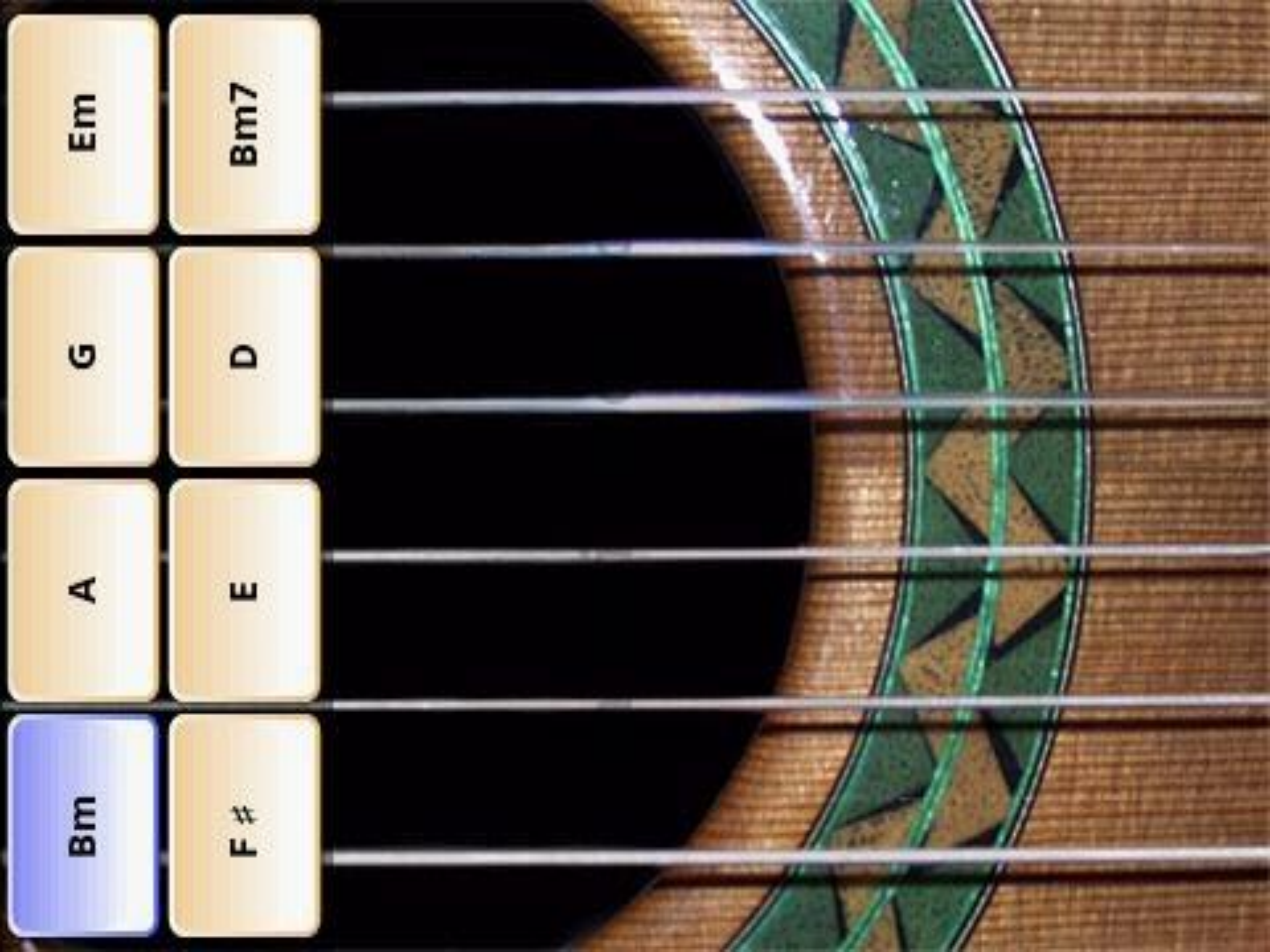
- **Update processes** – slow and cumbersome, vulnerable to attack.
- **Spoofed apps** (e.g. banking, recent Android attacks) can piggy-back reputation.
- **Malicious apps** can circumvent walled garden defences through:
  - Runtime interpreters
  - Elevation of privilege (through permissions fatigue)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

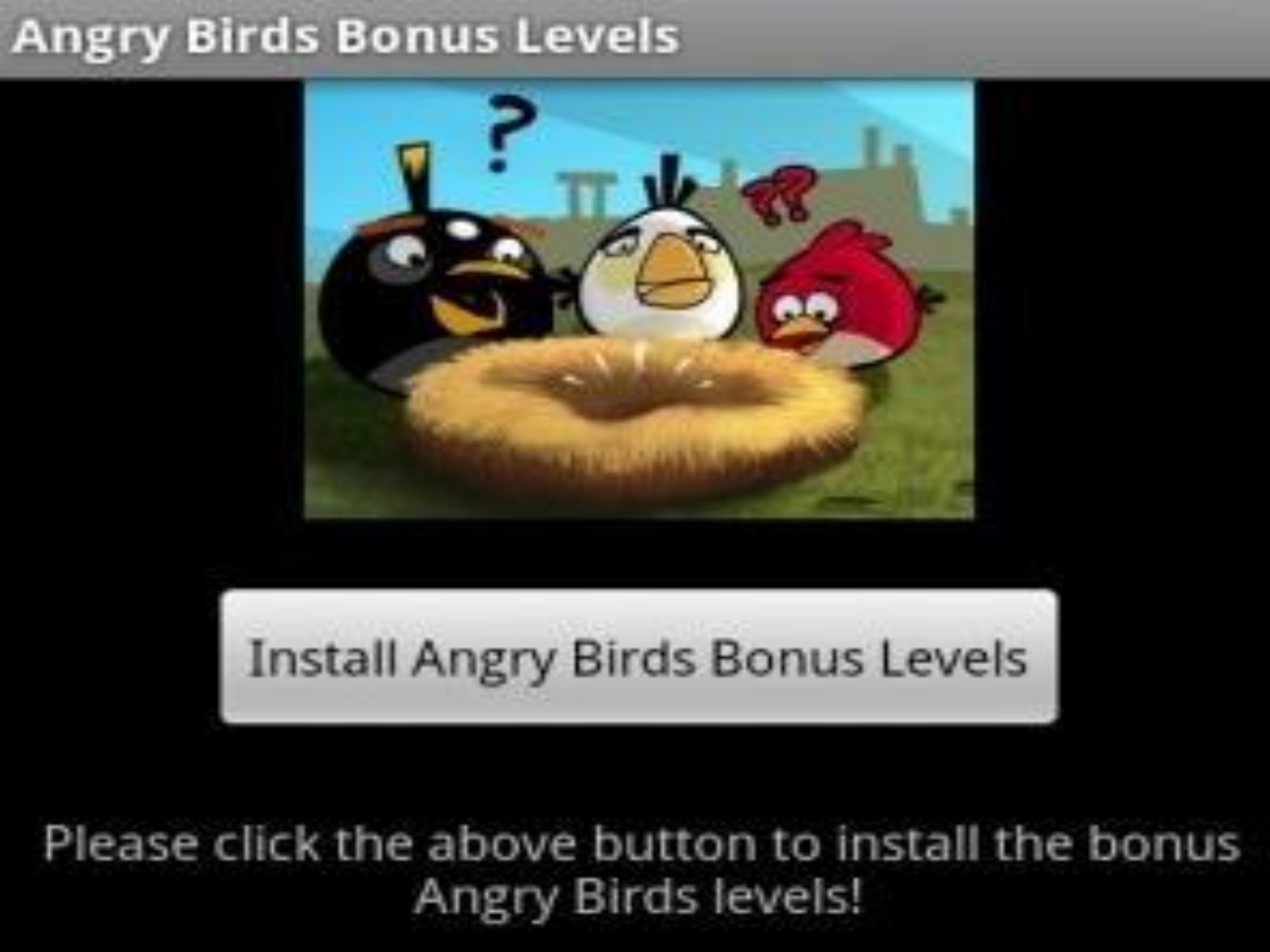
App-store dangers

- **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.

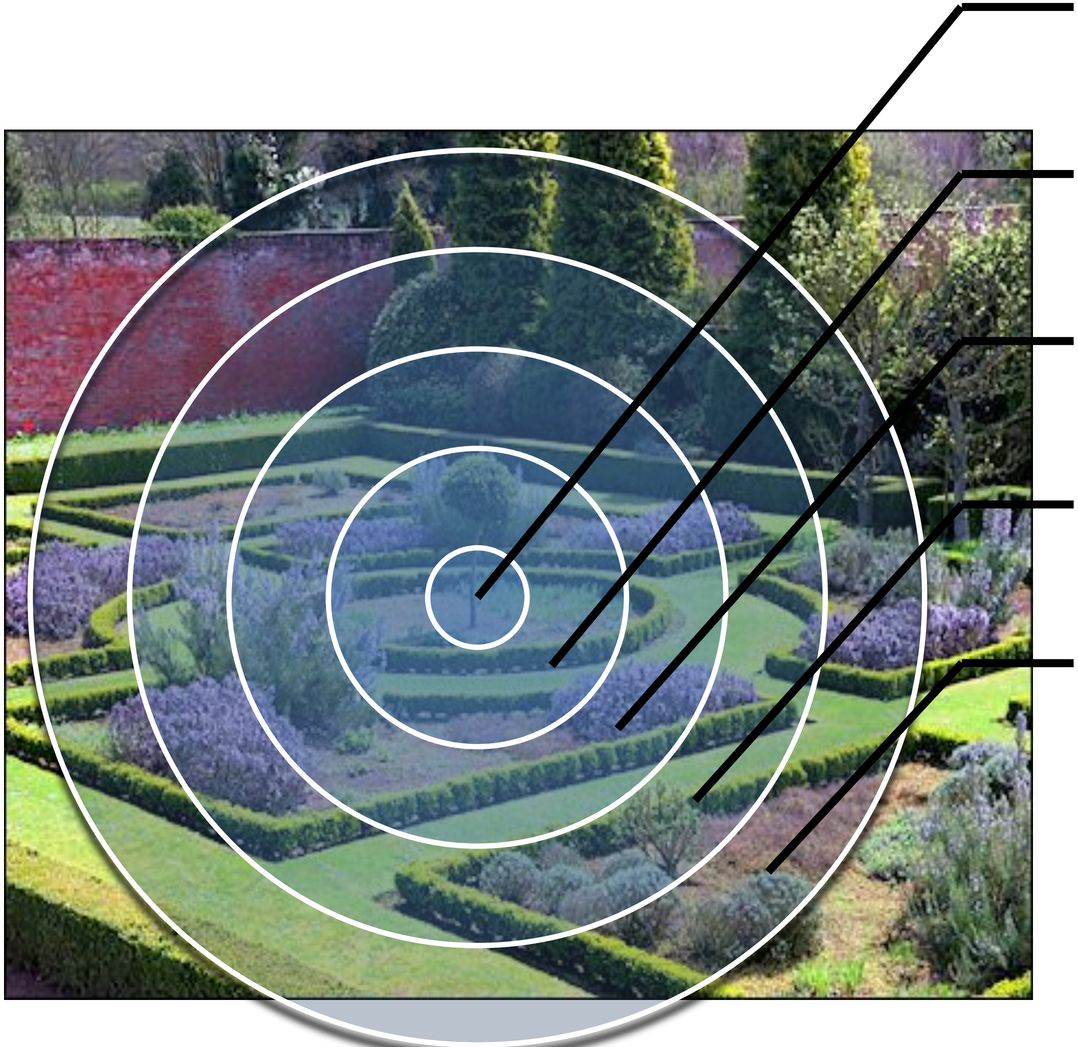

Bm7
D
E
F#
Em
G
A
Bm



Angry Birds Bonus Levels

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

Walled gardens: The 5 layers of defence



Kill Switch

Remove software

Reputation

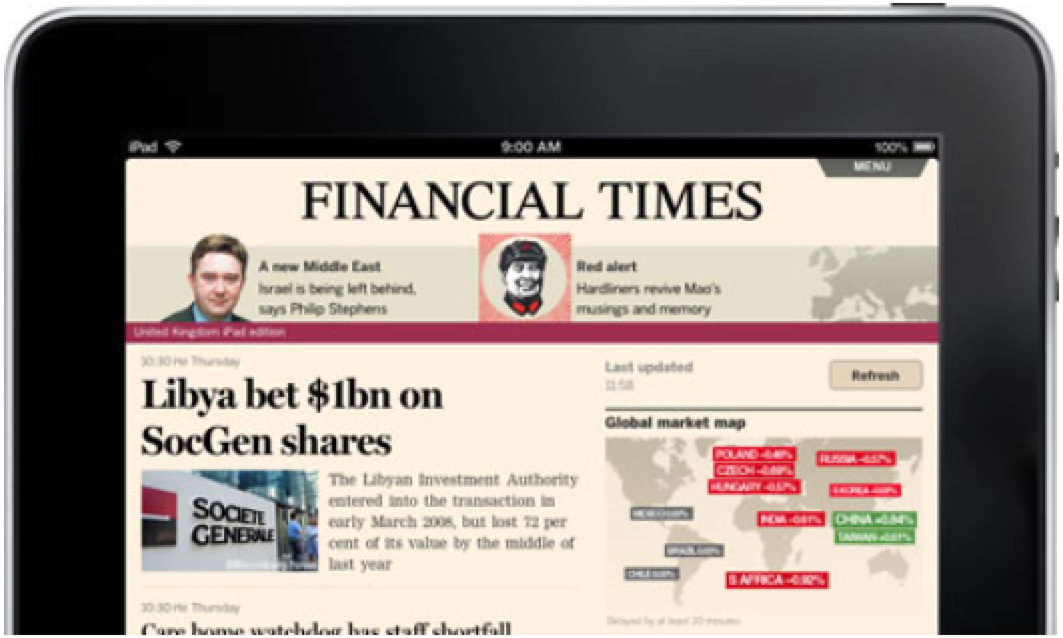
Vet software

Identify developers

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.

New FT app bypasses iTunes to deal directly with readers


iPad
9:00 AM
100%
MENU
FINANCIAL TIMES
A new Middle East
Israel is being left behind, says Philip Stephens
Red alert
Hardliners revive Mao's musings and memory
United Kingdom iPad edition
Libya bet $1bn on SocGen shares
SOCIETE GENERALE
The Libyan Investment Authority entered into the transaction in early March 2008, but lost 72 per cent of its value by the middle of last year
Last updated
Refresh
Global market map
POLAND
CZECH
HUNGARY
RUSSIA
S.KOREA
INDIA
CHINA
TAIWAN
S AFRICA
Care home watchdog has staff shortfall

The FT's new iPad app is available via browsers rather than iTunes

The **Financial Times** has introduced a new browser-based app for tablets, claiming it as "a major first by a news publisher."

The automatically updating app will enable readers to access its editorial content across a broad range of tablet and smartphone devices.

According to an article in today's FT, the app will bypass Apple's iTunes store and Google's android market.

It will therefore overcome the problem posed by Apple's reluctance to share detailed data on the identities and behaviour of users. Publishers have railed against that barrier.

Talk outline

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

W3C specifications in scope

- HTML 5 specification
- Cross-origin messaging specification
  - XML Http Request levels 1 and 2
  - Uniform Messaging Policy
  - Cross-Origin Resource Sharing
  - HTML5 Web Messaging
- Device API specifications
  - Media Capture API
  - System Information API
  - Permissions for Device API Access
  - Device API Privacy Requirements
  - Web Storage
  - Geolocation API Specification
- Widget specifications
  - Widget Access Request Policy
  - Digital Signatures for Widgets

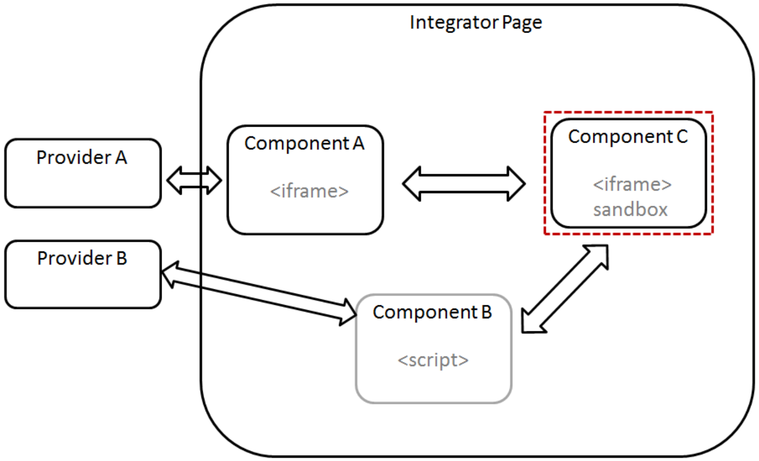
In collaboration with

KATHOLIEKE UNIVERSITEIT LEUVEN

DistriNet RESEARCH GROUP

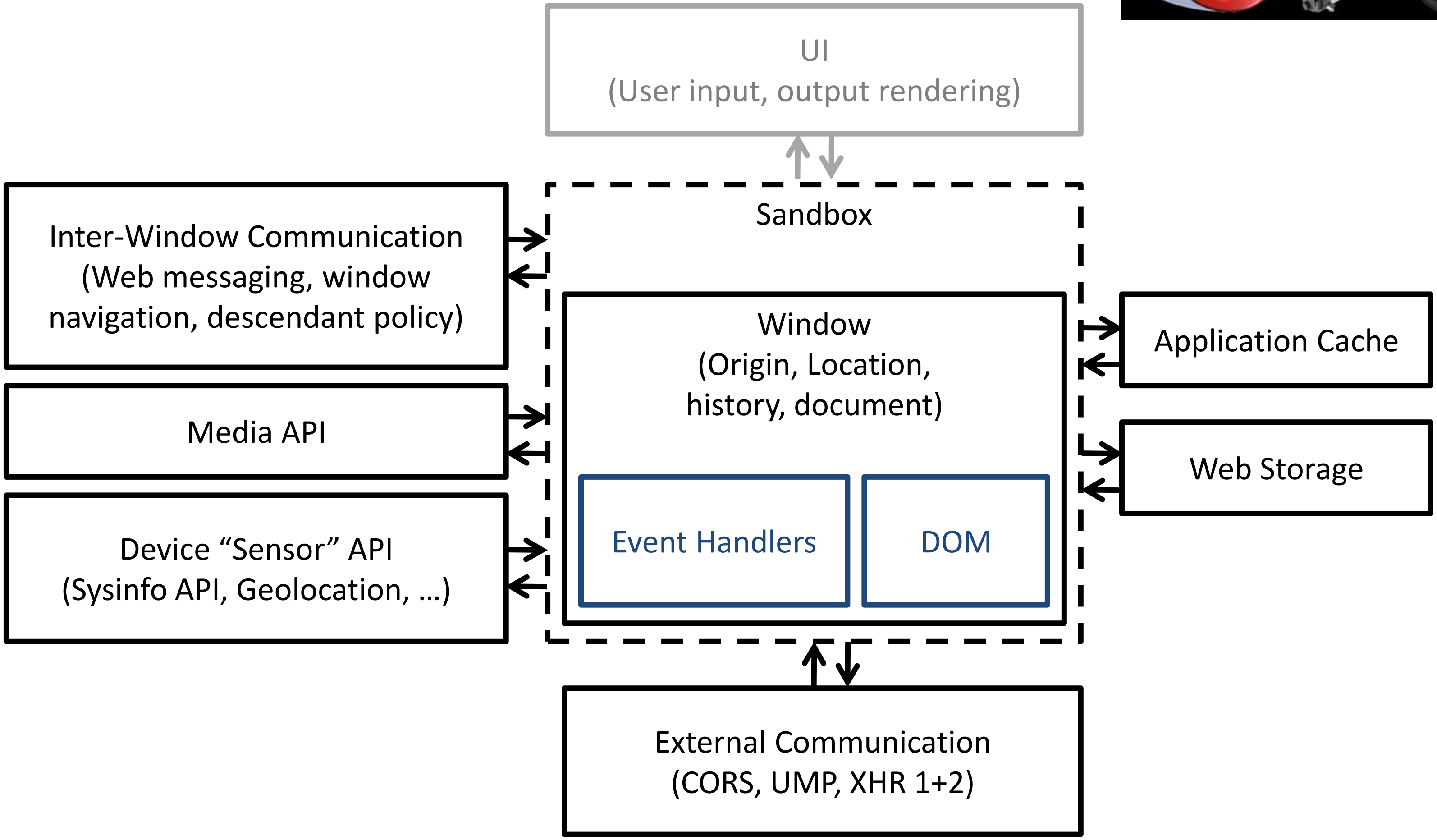
Scope of the analysis

- Attacker model
  - Web attacker - controls malicious website(s)
  - Gadget attacker - controls malicious gadget, embedded in an integrator page.
- Focus on:
  - Cross-origin, multi-provider applications
  - Persistent client-side storage
  - Integration of device APIs
  - What can be fixed within the spec
  - Risks to end-users (whether the spec is fixed or not)
- Out of Scope:
  - HTML x<5 web security problems (such as XSS, SQL/code injection, session management) are out of scope



*Based on attacker types used by Barth et al. in 'Securing frame communication in browsers' (USENIX Security Symposium 2008)

Model



UI
(User input, output rendering)

Sandbox

Inter-Window Communication
(Web messaging, window navigation, descendant policy)

Media API

Device “Sensor” API
(Sysinfo API, Geolocation, …)

Window
(Origin, Location, history, document)

Event Handlers

DOM

Application Cache

Web Storage

External Communication
(CORS, UMP, XHR 1+2)

Methodology

- Iterative and repeatable process
  - Applied to the 13 specifications in scope
  - 1000+ pages of specification!
- 3 step analysis
  - Summary of security-relevant features in spec
  - Threat analysis of specification in isolation
  - Cross-specification analysis results
- 4 security questions drive analysis

Four security questions

1. Are core security-relevant aspects of new capabilities secure, well-defined?

   -privacy problems, unprotected features, …

2. Do the new specifications violate isolation properties between origins or restricted contexts?

   -sandboxes or private browsing mode

3. Is the new specification consistent with other specifications?

   -Permission management, access control, …

4. How do security-relevant aspects of the specification rely on correct user security decisions?

3-step analysis

- Step 1: Security-focused study of the specification in isolation:
  - Capabilities: functional capabilities offered by the spec
    - e.g. establish a message channel with another browsing context
  - User Involvement: how and when is the user involved in granting access
    - e.g. give consent for an origin to access location information
  - Security/privacy considerations: both explicit and implicit considerations
    - Explicit: e.g. image capture is only possible with explicit permissions
    - Implicit: e.g. an established message port cannot be passed to other origins

Step 2: Identification of specification-specific threats and underspecified behavior

- Example threat: retrieving the timing of location events from location cache via binary search.
- Example under-specification: requirements for browser behavior when asking permissions

Step 3: identification of cross-specification issues:

- Inconsistencies between the specifications
- Interaction of features across specifications
  - E.g. Operation in restricted contexts (sandbox or private browsing mode)

Analysis results

	Well-defined / Secure	Isolation Properties	Consistency	User Involvement
HTML5	6	3	2	2
Web Messaging	1	2		
XMLHttpRequest 1 + 2	1			
CORS	2	1		
UMP				
Web Storage	3	1	1	
Geolocation API	4	1	3	1
Media Capture API				
System Information API	2	1	1	2
Widgets - Digital Signatures				2
Widgets - ARP	2			1
Total	**21**	**9**	**7**	**8**

Analysis sample: Geo-location API

- Capabilities:
  - Access to the current location
  - Both one-shot and monitoring
- Security and Privacy Assumptions
  - Consent is required!
  - Spec already explicitly mentions several privacy considerations
    - Recipients must not retransmit the location information

Analysis sample: Geolocation API (1)

- Threat: Cache Polling
  - Location retrieval from cache can be forced
  - ➢ ***Using a maxAge attribute, the age of the location can be determined***
- Underspecification: Monitoring Lifetime
  - The location can be monitored with a “watch process”
  - This process can be canceled
  - ➢ ***Does it disappear if the document no longer exists?***

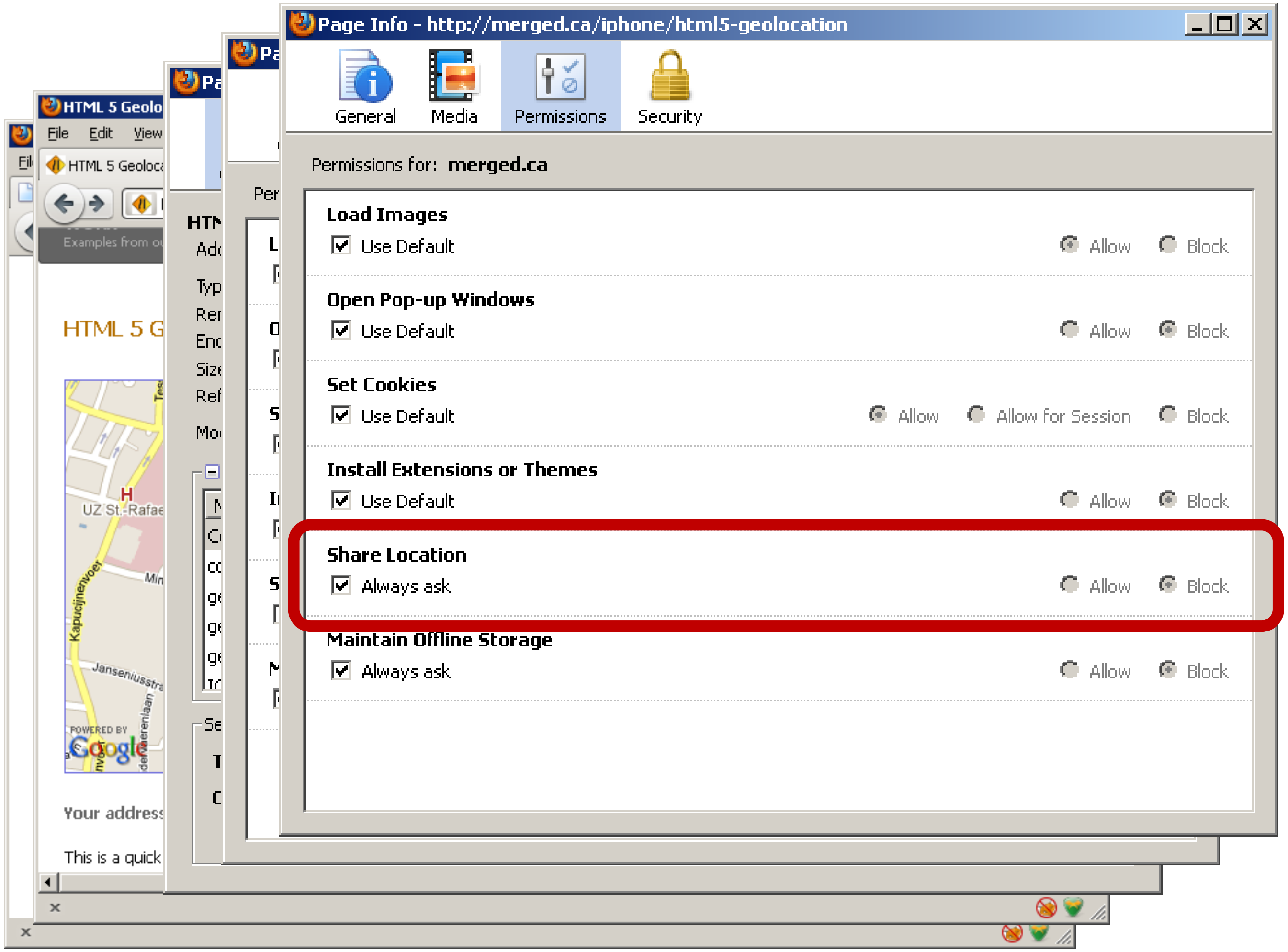
Analysis sample: Geolocation API (2)

- Underspecification: Behavior in restricted contexts
  - Can sandboxed document request location?
    - Which origin is used in the consent UI?
    - Can the permission be stored?
  - Private browsing mode?
    - Are stored permissions valid?
    - If a permission is obtained in private browsing mode, can it be stored?

Analysis sample: Geolocation API (3)

- User Involvement: Permission management
  - UI elements
    - The UI has to mention the origin
    - ➢ ***The UI does not have to indicate the nature of the permission (one-shot or monitoring)***
  - Long-term permission management
    - Vaguely specified: “should be easily revocable”
    - In practice: non-intuitive implementation

Non-Intuitive Implementation (Firefox)



Page Info - http://merged.ca/iphone/html5-geolocation

Permissions for: **merged.ca**

Load Images
☑ Use Default ● Allow ○ Block

Open Pop-up Windows
☑ Use Default ○ Allow ● Block

Set Cookies
☑ Use Default ● Allow ○ Allow for Session ○ Block

Install Extensions or Themes
☑ Use Default ○ Allow ● Block

Share Location
☑ Always ask ○ Allow ● Block

Maintain Offline Storage
☑ Always ask ○ Allow ● Block

Conclusions 1. Controlling functionality

- Huge set of new capabilities
  - Only coarse-grained access policies for capabilities available
    - E.g. on/off switch for scripts in sandbox environments
- Newly introduced elements and attributes increase the XSS attack surface
  - E.g. The HTML5 Security Cheatsheet identifies 10+ additional HTML5 vectors

Preliminary conclusions 2.

Under-specification and inconsistency across specifications

- Many issues involve under-specification and inconsistencies
- Use in restricted context (sandbox or private browsing mode)
  - User-consent
  - Consistent permission management

Preliminary conclusions 3.
Dependency on end-user and need for thorough analysis

- Strong dependency on end-user policing
  - Both for granting access as well as long-term permission management and cleanup

- Formal analysis helps:
  - Subsets that were formally analyzed (e.g. CORS) have substantially less defects
  - Formal analysis of the full set of specifications is however a huge effort...
  - Also quite some discrepancies between specification and browser implementations

Timelines

- HTML 5 – Late July
- App-stores –Early July
- Secure dev guidelines
  - principles – 1st draft End-June
  - Code- level controls, Sept.

You might also be interested in…

- Botnets: Detection, measurement, disinfection and defence – best practice and analysis. http://www.enisa.europa.eu/botnets
- Botnets: 10 hard questions – Analysis by ENISA and expert group. http://www.enisa.europa.eu/botnets-10Q
- Cloud computing: https://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Contact me

Giles Hogben (giles.hogben**Q**enisa.europa.eu)

Secure applications and services, ENISA

https://www.enisa.europa.eu/act/application-security