

Security... is there an app for that?

An overview of ENISA's smartphone security report

April 28th, Coudenberg BELvue Museum, Brussels
Special Spring Event by ISACA, ISSA, LSEC

Marnix Dekker, ENISA

Mobility



App stores

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





**BIENVENIDO
AL FUTURO**

Spanish to English

**WELCOME
TO THE FUTURE**





Ophiuchus

Serpens

Libra

Pluteus

Scorpius

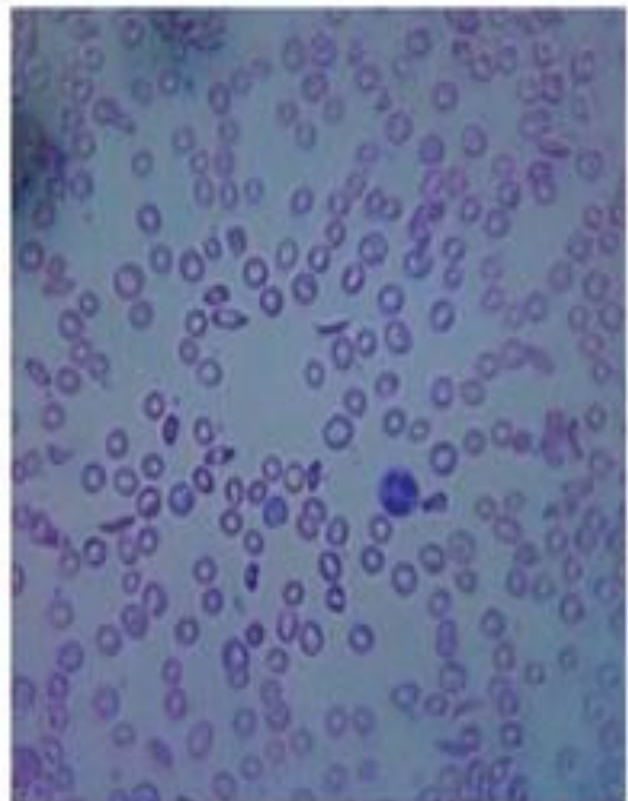
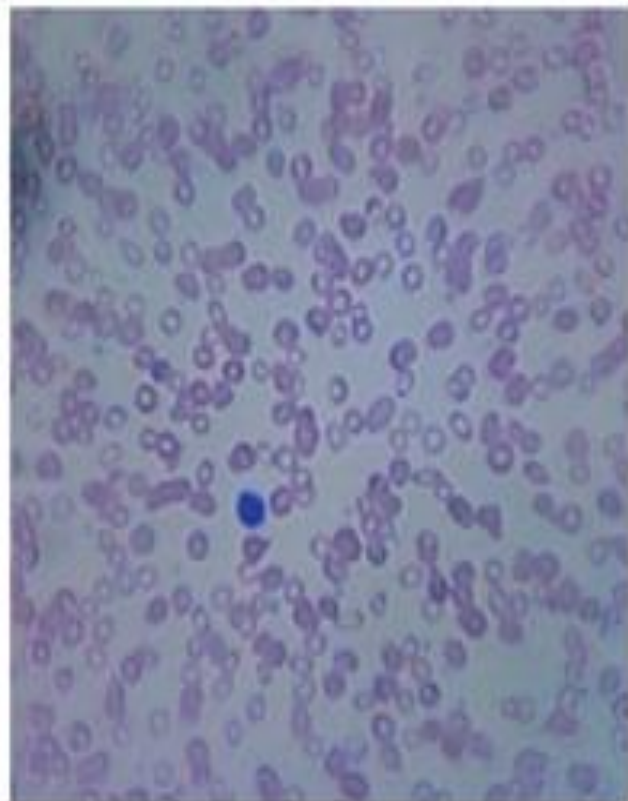
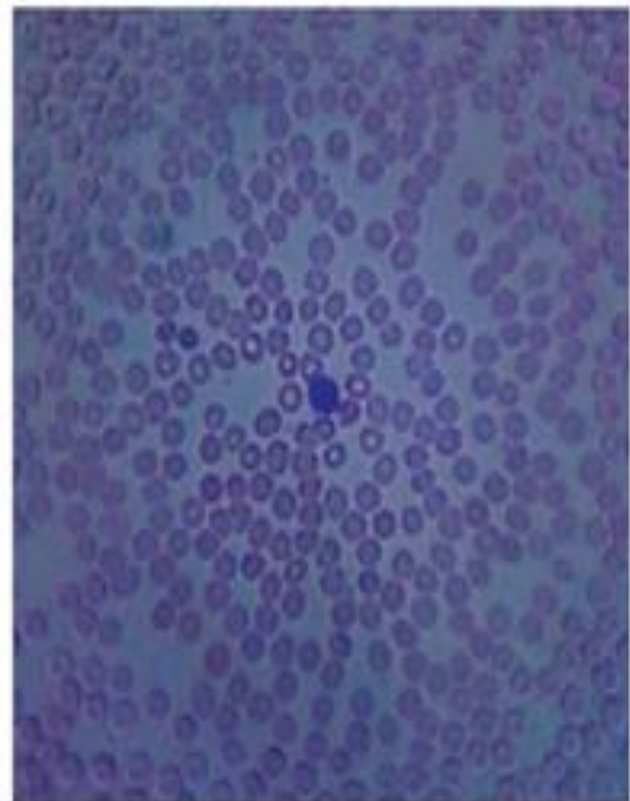
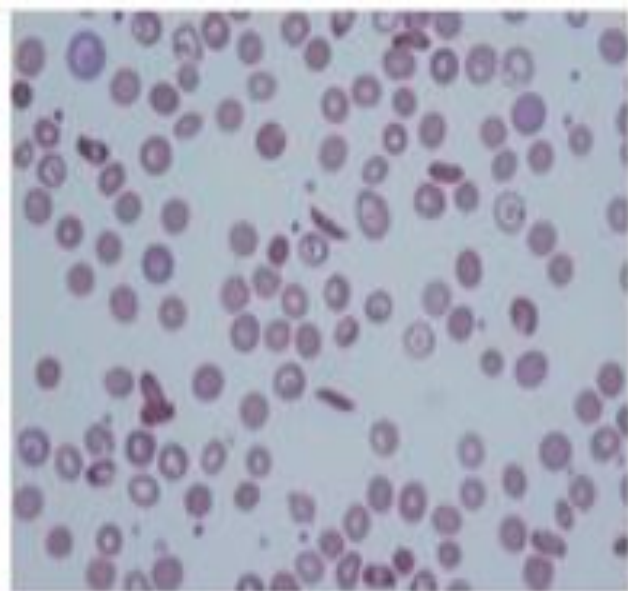
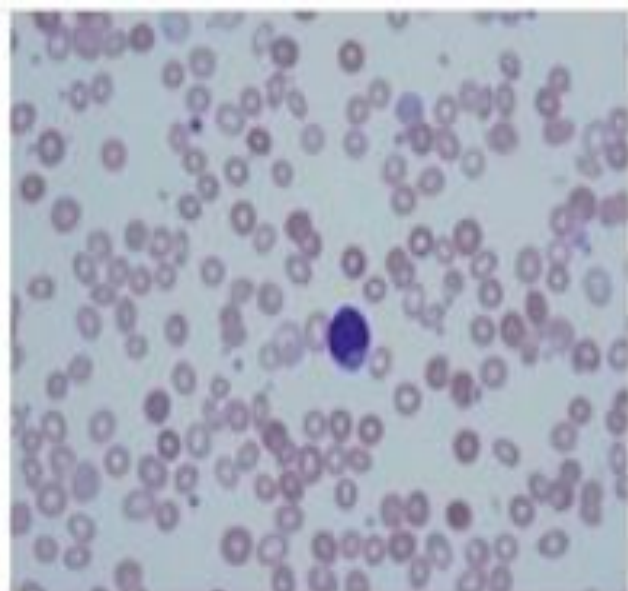
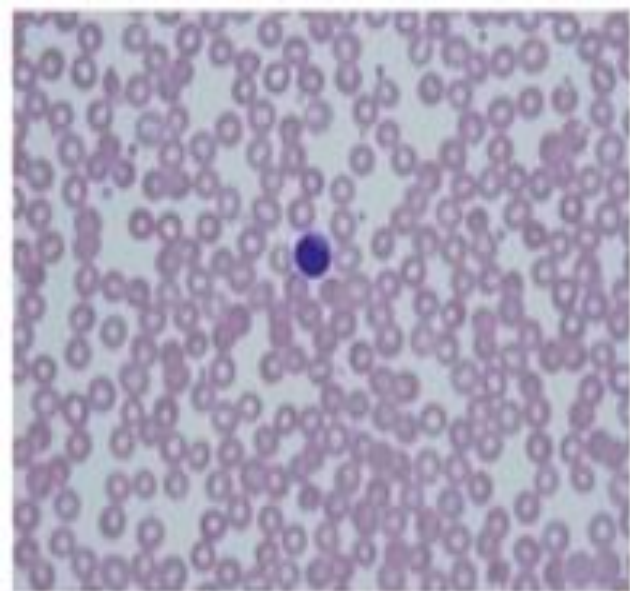
Sagittarius

Corona Australis

Lupus

Norma

Ara



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



HIGHSCORE: 19960

SCORE: 0



Angry Birds Bonus Levels



Install Angry Birds Bonus Levels

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

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=53.2178555556,6.9900805556>
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=48.8548333333,2.3158333333>
23 minutes ago · [Map Location](#) · [View Tweet](#) · [View Picture](#) · [Reply to andreajanke](#)



ICanStalkU was able to stalk [Djuku](#) at
<http://maps.google.com/?q=51.5482277778,4.8011194444>
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](#)

what is foursquare





Android trojan in China (Geinimi, botnet-like)



[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	welcome to Orange Partner Connect



amazon.com[®]

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

Bm

A

G

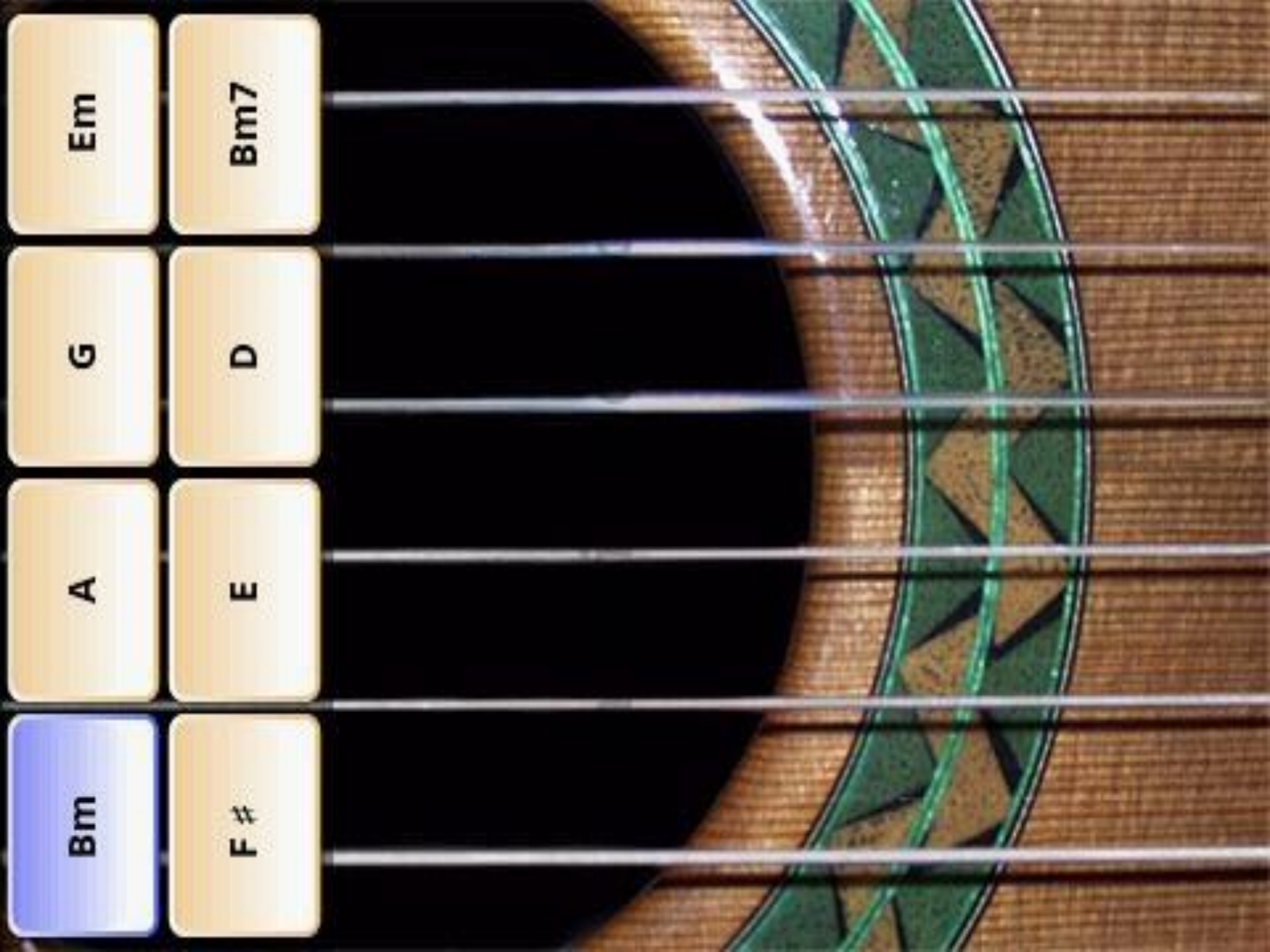
Em

F #

E

D

Bm7



Talk outline

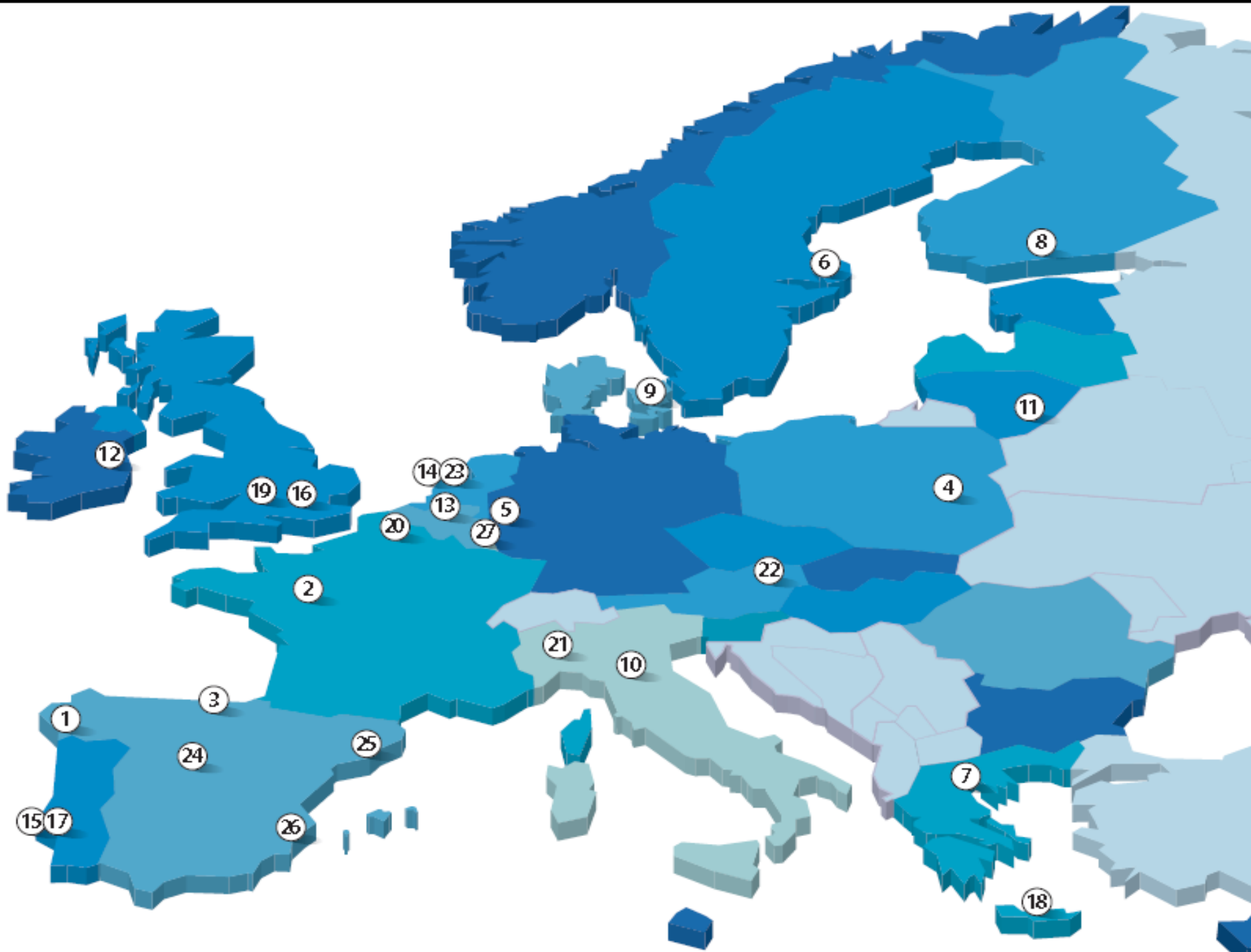
- About ENISA
- ENISA's Smartphone report
 - Risks
 - Opportunities
 - Recommendations
- Future work



About ENISA



- The European Network and Information Security Agency
 - gives expert advice on NIS issues to national authorities and EU institutions
 - acts as a forum for sharing good NIS practices
 - facilitates information exchange and collaboration between EU institutions, national authorities and businesses on NIS issues.
 - Set up in 2004 – EC proposed a new mandate for 2012.
 - Around 30 security experts and 20 staff.
- ENISA has an advisory role (not operational) and the focus is on prevention and preparedness.



Report background

- Smartphone market is booming
 - Q2 2010 numbers
 - 65 million smartphones sold worldwide
 - 20% of the total of mobile phones sold are smartphones
 - 61 million smartphone users in the EU5 alone (UK, Germany, France, Spain, and Italy).
- Across all sectors of society
- Gartner predicted at the end of 2010:
In 2013 more smartphones than PC's.
- "I had not used a computer in the 8 years I spent in the White House... and now, like everyone in the U.S., I have [a smartphone] in my hand every moment. I'm addicted to it."



Report background

- Smartphones are 24/7 within 1 meter of their owner.
 - *Practical difference with a surgically implanted device is not great.*
- The *ambient intelligence* vision is already being implemented with smartphones.
 - *"live surrounded by networked computing devices, conspicuously embedded in the surroundings"*



Report setup

- Group of 30 security/smartphone experts
 - All big smartphone vendors (except one)
 - Standards bodies
 - Governmental IT departments (ministeries)
 - Corporate IT departments (banks, telco's)
- Surveys, reviews, discussions.
- Generalize across different smartphones
- Focus on the differences with
 - Traditional handsets
 - Traditional (desktop and laptop) PC's
- Target audience
 - IT officers of governmental and business organisations
 - Consumers and consumer organizations.



Talk outline

- About ENISA
- ENISA's Smartphone report
 - **Risks**
 - Opportunities
- Future work



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).

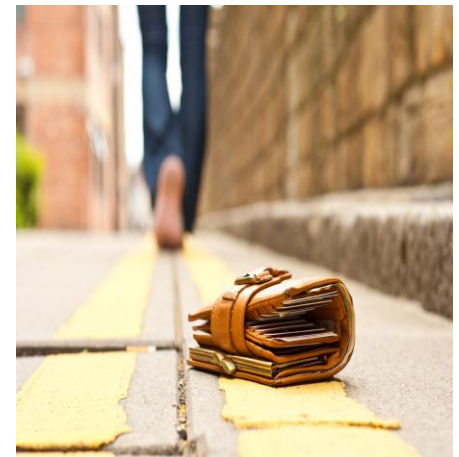
10 information security risks

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 leading to 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



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”)
 - Google buzz example
- 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
- Phishing is (quite) platform independent
- 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 about the Android market: “70% of 50.000 apps are 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 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

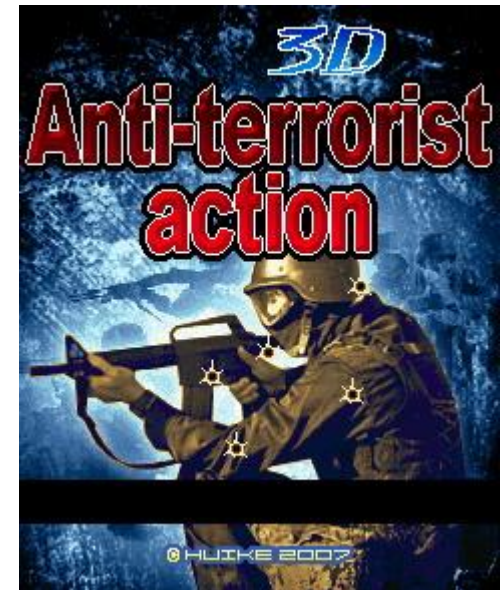
Consumer (C)	High	High	High
Employee (E)	Medium	Medium	Medium
High official (H)	Low	Low	Low

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



Using diallerware

- Example: Diallerware for Windows mobile
 - Game demo on shareware site was infected
 - (search for “3D anti terrorist dialler trojan”)
 - Trojan sleeps 31 days then calls 5 numbers
 - Satelite line, antarctica, africa, south america
 - International premium numbers (short-stopped)
 - Attacker spends 1 ct, and receives 12 euro



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
- iPhone prototype worm targeted unlikely target
- Phishing banking apps on Android market
- Currently big problem for PC’s (Zeus)
- Example: Zeus in the Mobile (SymbOS/Zitmo)
- Undetected by anti-virus software



Using Zitmo (thx to S21sec)

- Attacker steals online username and password using a malware (ZeuS 2.x)
- 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 socks/proxy and performs a banking transaction.
- An SMS is sent to the smartphone with the authentication code. Zitmo forwards the SMS to the attacker.
- Attacker fills in the SMS code and completes transaction.

Talk outline

- About ENISA
- ENISA's Smartphone report
 - Risks
 - **Opportunities**
- Future work

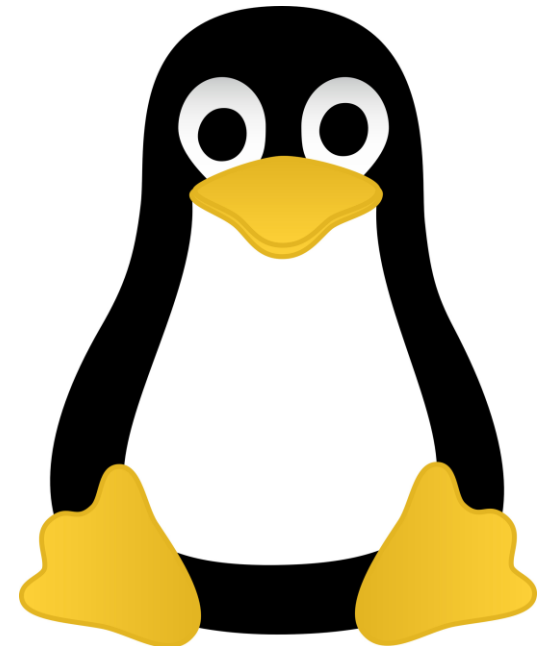


Information security Opportunities

1. Sandboxing and capabilities
2. Controlled software distribution
3. Remote application removal
4. Backup and recovery
5. Extra authentication options
6. Extra encryption options
7. Diversity

1. Sandboxing and capabilities

- Most smartphones use sandboxes for apps and capability-based access control models
- For example, Symbian, Android, iOS



2. App stores and 3. app removal

- Controlled software distribution
 - Not all appstores check software but most do
 - More info on appreview.tumblr.com
 - Similar to Linux distro's
 - Doable, scalable?
 - Example: easter eggs
- Remote app removal
 - Will it deal with rootkits
- Controversial topic
- Different models confuse consumers



4. Backup and recovery

- Backup and recovery is easy
 - Backups are small
 - Backups are automatic
- Additional “measures”
 - Remote location
 - Remote wipe



5. Better authentication options

- Smartphone is more personal than a PC
- Smartphone can be used for OTP authentication
 - Classic: OTPs printed on pdf or paper
 - Classic: OTPs via SMS
 - Classic: Hardware token (RSA, Verisign, for example)
 - New: Google authenticator “turns your smartphone in a second factor”
 - Several open source implementations of HOTP
- Also in m-commerce
 - NFC communication for credit card payments
 - Google Gingerbread

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

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

- About ENISA
- ENISA's Smartphone report
 - Risks
 - Opportunities
- **Future work**



Follow up in 2011

- Next generation Apps
 - Walled gardens
 - A new (old) and better software distribution model?
 - Seen in social networks (Facebook appstore)
 - Seen on real computers (OSX Lion, Vista widgets)
 - How do app stores relate to HTML5?
- Secure app development
 - Collaboration with OWASP
 - Secure architecture and design principles.
 - Secure coding techniques
- Authentication with smartphones (Google Authenticator e.g.)
 - Collaboration with OpenID, Kantara, Google, Microsoft, eBay, Intel...

Contact us

Marnix Dekker (marnix.dekker@enisa.europa.eu)

or

Giles Hogben (giles.hogben@enisa.europa.eu)

Secure applications and services, ENISA

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