



A mobilitás biztonsági kihívásai

Dr. Krasznay Csaba
HP Magyarország

Hírek az elmúlt hetekből

How cybercriminals can target you on public networks

Posted on 29 April 2013.



The widespread use of mobile communication, including cell phones, laptops and tablets, makes consumers particularly vulnerable to fraud and malware risks over public internet connections.



Mobile technology boosts a connected cafe culture – consumers feel safe and comfortable checking Facebook, sending and receiving emails, downloading pictures, shopping online, conducting mobile banking and even accessing sensitive documents over public Internet connections. Often, consumers are unaware of the severe cybercrime risks posed by these seemingly harmless tasks.

Forrás: Help-Net Security, CIO.com

Researcher refuses to help Saudi telco to spy on people

Posted on 14 May 2013.



You would think that a Saudi Arabian telecom firm interested in monitoring its users' mobile communications would not be asking a well-known pro-privacy researcher such as Moxie Marlinspike for help, but you would be wrong.



Marlinspike - the author of the [GoogleSharing](#) proxy service; creator of [Convergence](#), an alternative to the flawed CA trust model; co-founder and CTO of Whisper Systems, which [offered](#) its free voice and text encryption software to Egyptian users during the 2011 revolution; author of the MitM tool [sslstrip](#); and finally a [former Twitter employee](#) that was involved in writing its TLS code - described the "pitch" in a blog post.

Booming Mobile Industry Spawning Global Criminal Marketplace

In an alarming 'post-PC' era alert, working group says criminal infrastructure created much faster than it was for PC fraud.

By John P. Mello, Jr.
Thu, May 16, 2013



[CSO](#) — Mobile devices have become enticing targets for criminals around the world, so much so that an underground industry has begun to grow to support malicious activity aimed at those devices, according to a report released on Wednesday by the Anti-Phishing Working Group (APWG).

"In a 'post-PC era,' mobile devices increasingly present an attractive, practical and economical alternative to traditional desktops," said [the report](#), "Mobile Threats and the Underground Marketplace."

"In the coming years," it continued, "global mobile payments are predicted to exceed \$1.3 trillion, moreover, presenting a mother load of opportunity for cybercrime gangs who appreciate the vulnerabilities of these peripatetic communications and computing platforms."

First California Lawsuit Over Mobile Privacy Issues Crashes

A California state court has dismissed a closely watched lawsuit charging that Delta Air Lines failed to comply with state privacy laws for mobile applications.

By Jakumar Vijayan
Tue, May 14, 2013



[Computerworld](#) —



A California state court has dismissed a closely watched lawsuit charging that Delta Air Lines failed to comply with state privacy laws for mobile applications.

In a brief ruling last week, California Superior Court Judge Maria Miller agreed with Delta's claim that the federal Airline Deregulation Act (ADA) of 1978 supersedes state statutes.

The ADA prevents states from enforcing laws that could impact the prices, routes or services offered by an airline.

Növekvő biztonsági és adatvédelmi fenyegetések

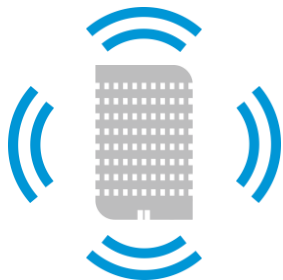
- **Az egymással együttműködő szervezett bűnözői csoportok** olyan képességekkel rendelkeznek, melyek minden korábbinál jelentősebb módon ássák alá a biztonságot és az adatvédelmet.
- **A mobileszközök elterjedése** megnöveli azon hozzáférési pontok számát, ahol az adatlopás megtörténhet.
- **Az IT konzumerizációja**, azaz az IT eszközök személyes és hivatalos felhasználása növeli az adatlopási lehetőségeket – és „ugyanannak” a jelszónak a használatának a valószínűségét
- **Az IT felhasználók relatív tudáshiánya**: az IT egyre egyszerűbb a felszínen, de egyre komplexebb a háttérben – ez megnöveli annak valószínűségét, hogy a felhasználó eszköze egy összetett támadás egyik „közkatonájává” válik.
- **A mindenhol jelenlévő közösségi hálózatok** megnövelik a social engineering támadások sikerességének esélyét



A mobilitás csak az egyik kihívás

Nyílt & kiterjedt

Az információs vagyon védelme



Együttműködés

Security 2.0

Proaktív kockázatmenedzsment

Konzumerizáció

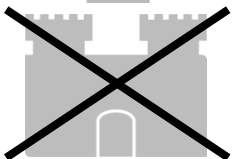
Mobilitás, eszköz & közösségi média



Cloud
Public, private



Eszköz/adat komplexitás

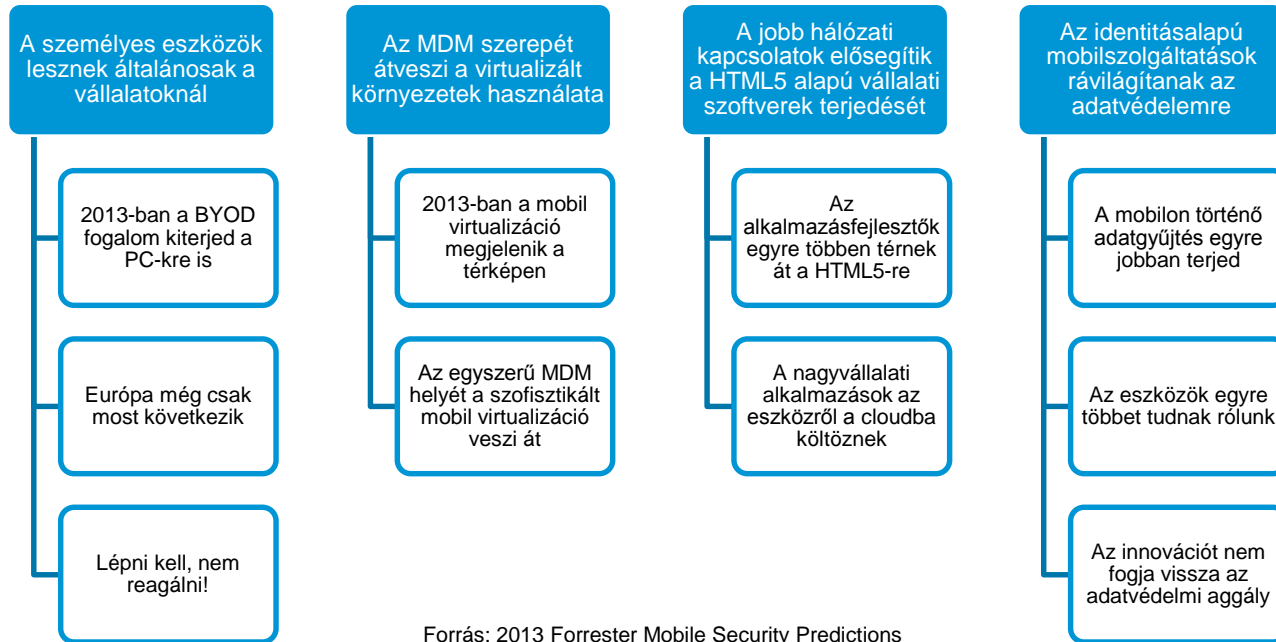


Erőd
Reaktív határvédelem

Big data
Tartalom, kontextus,
struktúrátlan

```
1100010100100010000  
0100100010000  
10001011  
1100010100100010000
```

Forrester jóslatok a mobilbiztonság területén



Forrás: 2013 Forrester Mobile Security Predictions



Forrester jóslatok a mobilbiztonság területén

Lehetőségek és fenyegetések a mobilpiac játékosainak

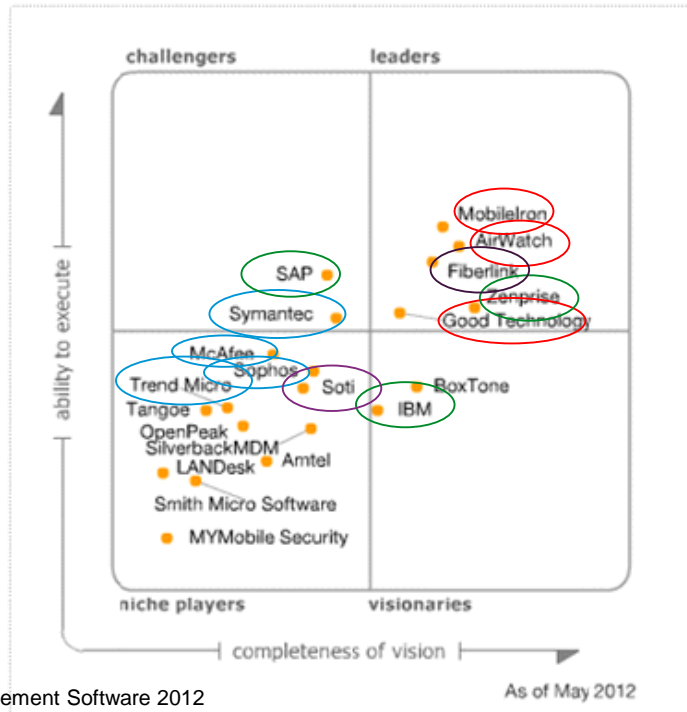
	Lehetőségek	Fenyegetések
MDM gyártók	Enterprise mobility platformok, technológiai innováció	Elavult MDM platformok
Mobil operátorok	Növekvő cloud-mobil forgalom, mobile management a vállalatoknak	Csökkenő bevétel a hang és üzenet forgalomban
Cloud szolgáltatók	Növekvő felhasználás az okos eszközökön, vállalati szolgáltatások speciális biztonsági és adatvédelmi területeken	Hatalmas verseny, szigorú adatvédelmi előírások
Eszközgyártók	Nagyvállalati biztonsági igények megjelenítése az eszközökben	Az eszközök tömegcikké válnak, a hardveren kevesebb a haszon
IT biztonság gyártók	Megoldások kiterjesztése a mobil fenyegetésekre, SecaaS megoldások, mint új csatorna	Ragaszkodás a hagyományos nagyvállalati szoftver mentalitáshoz

Forrás: 2013 Forrester Mobile Security Predictions



A mobilpiac jelenleg

A Gartner 2012-es Magic Quadrantja szerint...



- MDM gyártók, mobilközpontú megoldásokkal, telco partnerek
- IT biztonsági gyártók
- Széles spektrumú IT gyártók
- Gyártói partner
- SecaaS szolgáltató

Forrás: Gartner Magic Quadrant for Mobile Device Management Software 2012

Technológiai trendek



A mobilbiztonság kiterjesztetten értendő!

Biztonság a mobilitást támogató infrastruktúrában

Dinamikus hálózatok

- Kisebb hálózati cellák
- Integrált WiFi hotspotok
- Intelligens offload (user-device autentikáció)
- Önoptimalizáló hálózati szoftverek

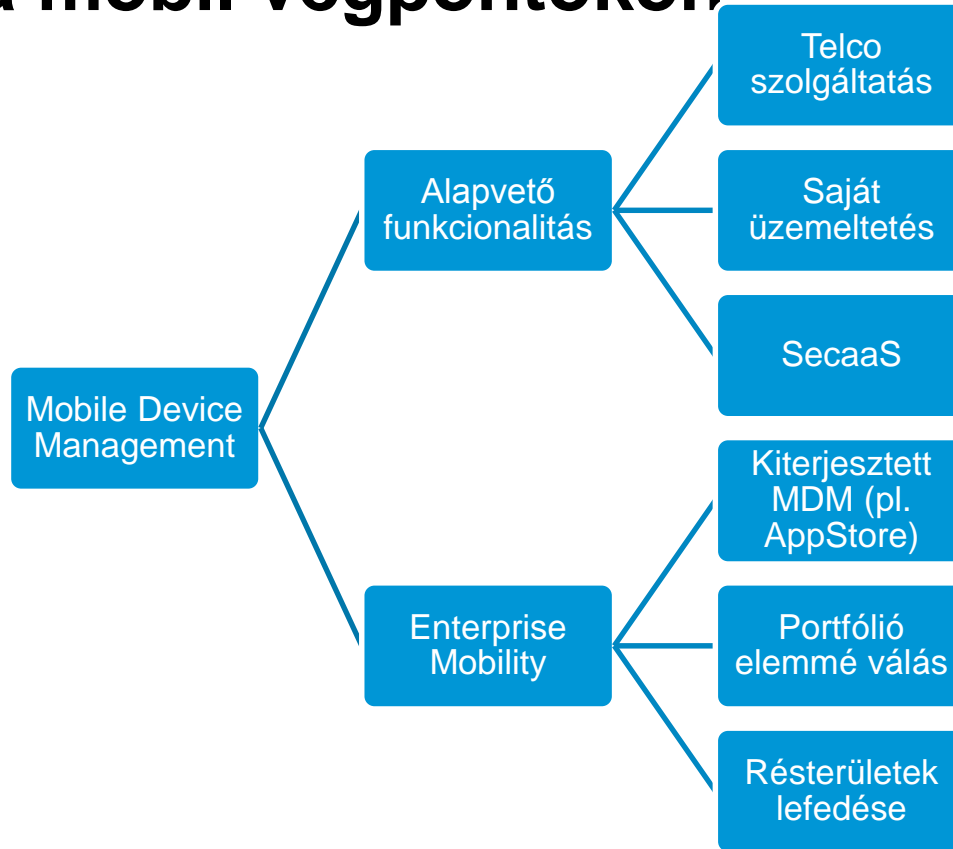
Virtuális környezet

- Privát cloudok elterjedése
- Publikus IaaS megoldások bevonása
- Biztonságos adatelérés VDI környezetben

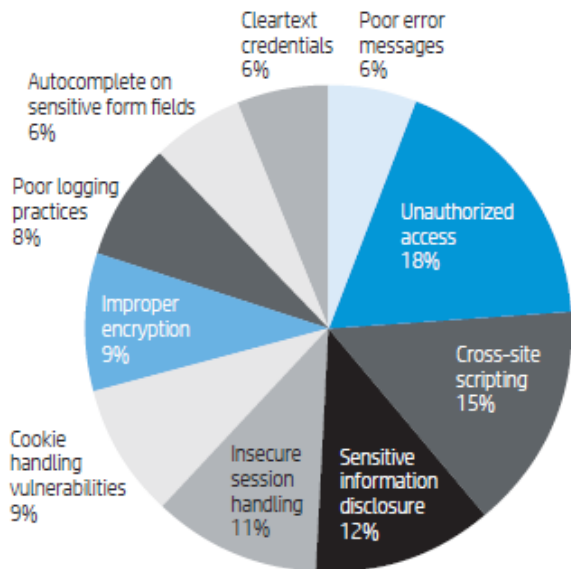
Okos végfelhasználói eszközök

- Biztonságos nagyvállalati smartphone-ok és tabletek
- Mobilizált laptopok
- Alkalmazkodó irodai infrastruktúra (pl. nyomtatás)

Biztonság a mobil végpontokon



Biztonság a mobilalkalmazásokban



Top 10 mobilalkalmazás sebezhetőség

Forrás: HP 2012 Cyber Risk Report

☐ CLOUD

Cloud alapú szolgáltatások elérése a preferált mobil eszközökről

☐ INTEGRÁCIÓ

Integráció több technológiai szinten, az eszköztől az adatig

☐ ELEMZÉS

Környezetfüggő mobilalkalmazások, melyek feldolgozzák a profilt, a preferenciákat, a környezetet, a helyszínt és a korábbi történéseket

☐ BIZTONSÁG

Beépített biztonság a mobilalkalmazásokba és az eszközökbe a jogosulatlan hozzáférések megakadályozására

Összefoglalás

- **Amikor mobilbiztonságról beszélünk, nem csak a mobileszköz biztonságáról kell beszélnünk!**
- **Minden mobillá válik, az alapinfrastruktúrától kezdve, az eszközökön át, az alkalmazásig bezárólag. Éppen ezért NEM technológiát, hanem INFORMÁCIÓT kell védeni.**
- **A mobilplatformokon történő információvédelem technológiája még nem kiforrott – érdemes a területre odafigyelni!**
- **A mobilitást meggátolni nem lehet, ezért kontrollálni kell! Ha tudjuk...**



Köszönöm a figyelmet!

E-mail: csaba.krasznay@hp.com

Twitter: twitter.com/csabika25

