

Mobile (in)Security

Giuseppe Augiero



18 WEB
MID
WORLD



**E' interessante parlare
di sicurezza degli
smartphone?**



Utilizzo



Sensori

- Gps.
- Microfono.
- Camera.
- Touch Screen.
- Accelerometro /Giroscopio.
- Bussola digitale.
- Batteria.
- Sensore di prossimità.



Smartphone vs Gsm (2G)



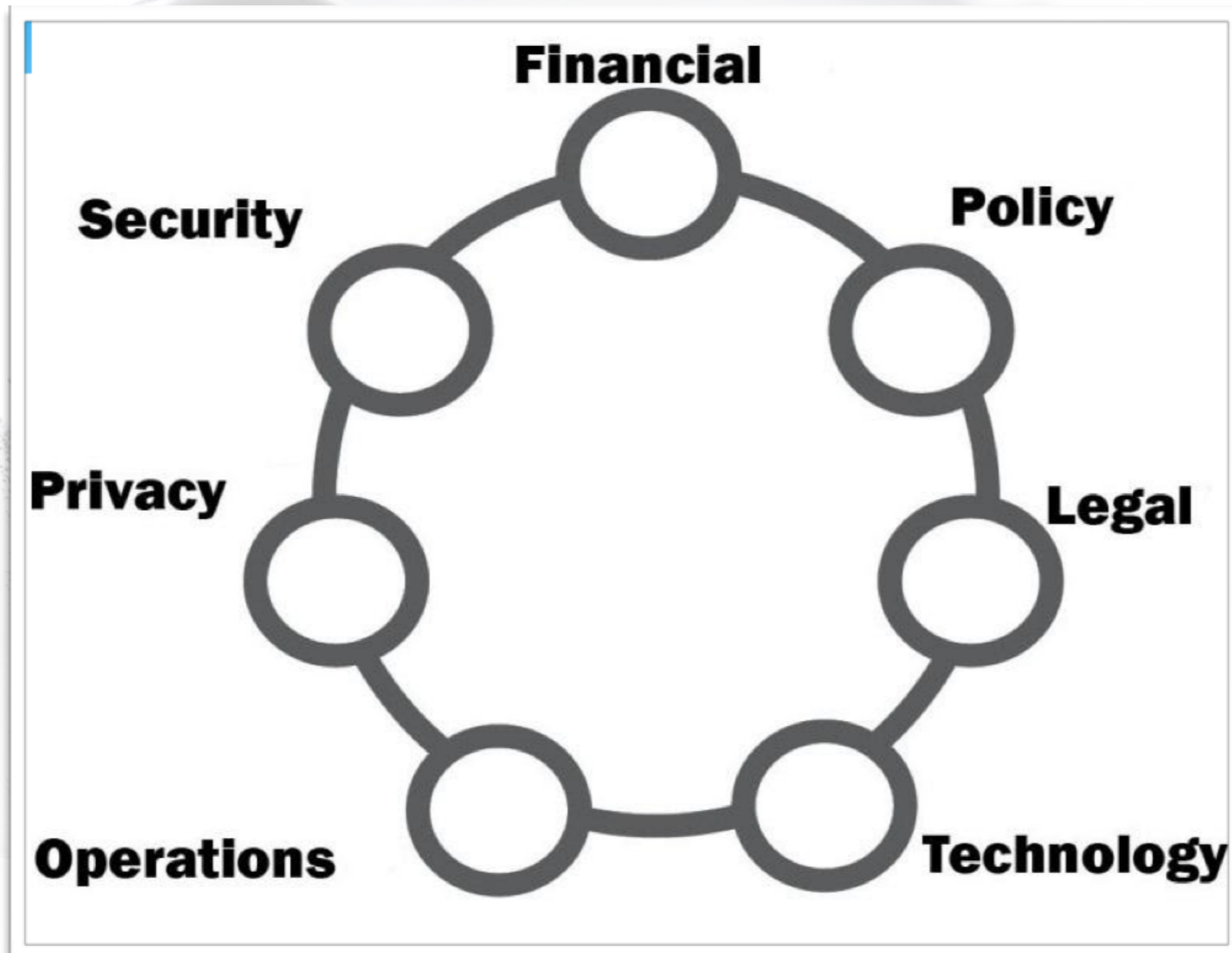
GSM - Network



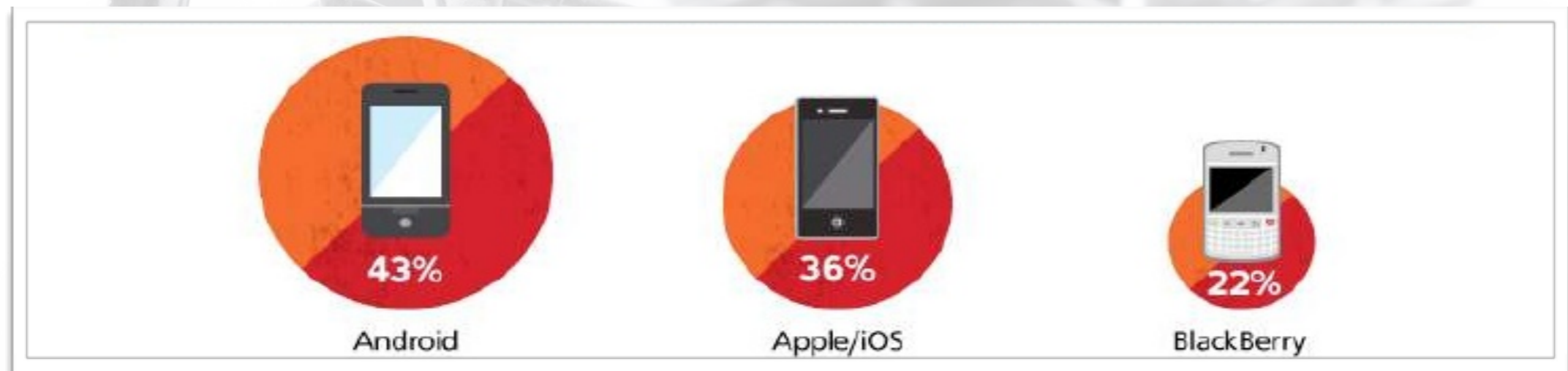
Computer Forensic



Categorie di rischi



Chi presenta maggiori rischi?



Attacchi



Attacco fisico



Vendita



Network

- Wifi sniffing.
- Bluetooth sniffing.
- Network exploit.



Web based

- Phishing scam (email).
- Drive by download.
- Browser exploit.
- Malicious site.



Application based

- **Malware.**
- **Premium SMS Billing (Privacy Threats).**
- **Email-SMS Phishing (Privacy Threats).**
- **Spyware.**
- **Vulnerabilità applicative.**



Malware

- Android presenta notevoli rischi per la sicurezza.
- Il kernel presenta un numero non banale di vulnerabilità.
- Applicazioni sconosciute.
- Malicious code.
- Parco eterogeneo (versionamento).



Spyware

- **Facilmente installabili sul vostro telefono.**
- **Permettono di tenere traccia delle vostre chiamate, posizione, messaggi ecc.**
- **Possono nascondersi e non essere visibili nella lista delle applicazioni installate.**



Cimice ambientale

- **Ralf-Phillip Weinmann attack**



Gemini

- Malware agganciato alla applicazione reale
- App Store cinesi.
- App ufficiale non infetta.



Zitno

- Zeus in Mobile
- Trojan usato per rubare dati bancari.
- Cattura messaggi SMS.





















DroidDream

- Android Market.
- Aggiungere il malware ai download.
- 200.000 download in pochi giorni.
- **Falso tool di rimozione.**



ios vs Android

Types of Attack	Apple iOS	Google Android
 Web-based attacks		
 Malware attacks		
 Social engineering attacks		
 Resource abuse/ Service attacks		
 Data loss (malicious and unintentional)		
 Data integrity attacks		


Little or No
Protection


Moderate
Protection


Full
Protection



Perché le app sono insicure?

- **Corsa al rilascio.**
- **Test minimi e limitati (e spesso troppo tardi).**
- **L'ambiente mobile è molto appetibile per un attaccante.**
- **Sicurezza delle App inesistente.**
- **Mancanza di professionisti di cybersecurity.**



Business



Byod



Architetture



Funzionalità di sicurezza

- **Controllo degli accessi**
 - Cerca di proteggere il dispositivo utilizzando tecniche di autenticazione come password e blocco dello schermo inattivo.
- **Crittografia**
 - Cifra i dati presenti sul dispositivo per proteggerlo da perdita o da furto.



Funzionalità di sicurezza (II)

- **Provenienza dell'applicazione**
 - Ogni applicazione è firmata con identità del suo autore allo scopo di renderla resistente alla manomissione. Un utente può decidere di utilizzare o meno l'applicazione in base all'identità dell'autore.
- **Sicurezza dell'applicazione**
 - Limita la capacità delle applicazioni di accedere a dati o sistemi sensibili su un dispositivo.
 - Controllo degli accessi basato su permessi: concede set di permessi a ciascuna applicazione.



Funzionalità di sicurezza (III)

- **Isolamento dei processi**
 - Utilizzo di sandbox.
 - Ogni applicazione può parlare con un'altra attraverso gli intent (messaggi), l'inter-process communication o il Content-Provider (data storage).

-



Come difendersi



Regole generali

- Non perdere il proprio telefono.
- Attivare il finding del cellulare.
- Proteggi una password il telefono.
- Verifica i permessi che dai alle applicazioni.



Regole specifiche

- Blocca gli sms a valore aggiunto.
- Safe Browsing.
- VPNS.



Antivirus

• **E' consigliabile usare un antivirus aggiornato sul proprio smartphone.**



Regola d'oro

Non “rootare” i telefoni



I sette errori da non commettere

1. Non “bloccare” il proprio cellulare.
2. Aprire siti di dubbia sicurezza.
3. Salvare dati sensibili “ovunque”.
4. Non aggiornare app e sistema operativo.



I sette errori da non commettere (II)

5. Non “bloccare” il proprio cellulare.
6. Non usare la cifratura.
7. Utilizzare wifi pubblici.



Sfatiamo alcuni miti

- Pensare che gli smartphone non immagazzinino dati sensibili.
- L'utilizzo di strong authentication, pin, puk, ecc.. possa evitare l'accesso indesiderato da parte un utente malevolo.



Sfatiamo alcuni miti (II)

- Sentirsi al sicuro tenendo sempre aggiornato il sistema operativo dello smartphone (Ios,Android).
- Scaricare app dei market ufficiali permetta di sentirti al sicuro.



Sfatiamo alcuni miti (III)

- **Non sentirsi al sicuro se si utilizza un accesso pubblico.**



Abbiamo finito?



Api

- <https://goo.gl/MmiSba>

Response

Raw Headers Hex XML

```
HTTP/1.1 200 OK
Server: nginx/1.10.1
Date: Sun, 15 Jul 2018 22:21:06 GMT
Content-Type: application/xml; charset=UTF-8
Connection: close
activityID:
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Allow-Headers:
authorization, Access-Control-Allow-Origin, Content-Type, SOAPAction
Content-Length: 13525

<attributeList>
  <codiceEsito>00</codiceEsito>
  <descrizioneEsito>Successo: Chiave trovata</descrizioneEsito>
  <attribute>
    <name>msisdn</name>
    <value>340</value>
  </attribute>
  <attribute>
    <name>anagrafica.data_attivazione</name>
    <value>20/08/2016 00:00:00</value>
  </attribute>
  <attribute>
    <name>anagrafica.tipo_cliente</name>
    <value>C</value>
  </attribute>
  <attribute>
    <name>anagrafica.prepagato_abbonato</name>
    <value>P</value>
  </attribute>
  <attribute>
    <name>anagrafica.sesso</name>
    <value>M</value>
  </attribute>
  <attribute>
    <name>anagrafica.anno_nascita</name>
    <value>1997</value>
  </attribute>
</attributeList>
```



ndpi

- <https://goo.gl/WmvXJa>

ntop



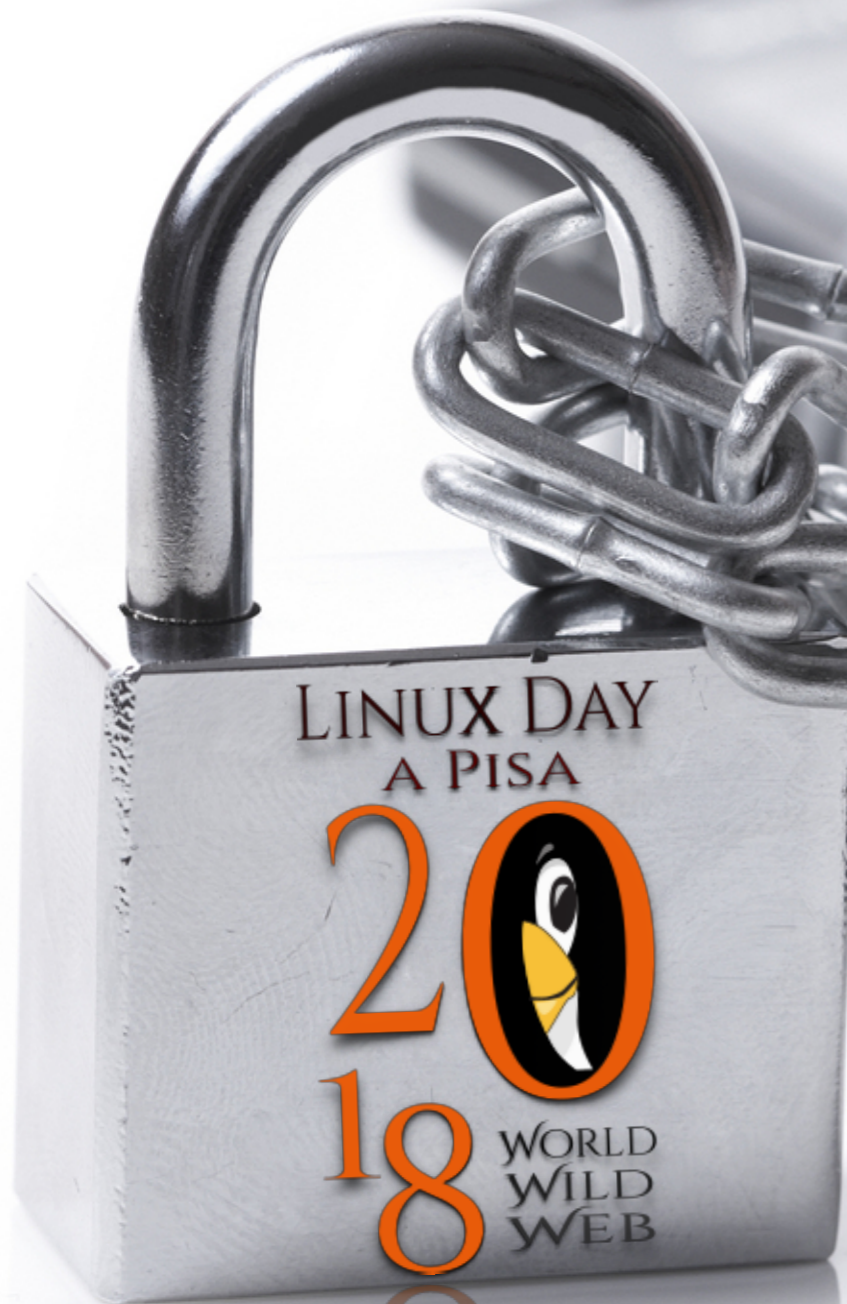
Conclusioni

- **La tecnologia non può essere fermata?**
- **Consapevolezza.**
- **I dati personali hanno un grande valore.**



Mobile (in)Security

Giuseppe Augiero



Web: www.augiero.it

Email: talk@augiero.it

Twitter: [@GiuseppeAugiero](https://twitter.com/GiuseppeAugiero)

