Mobile Device Security

R. R. Mittar
DDG(NGN), TEC
Department of Telecom
Ministry of Communication & IT
INDIA
“For many professionals, the mobile phone has become a mobile office,”
- Mike Jones, Symantec

"There is no question that mobile security will eventually equal – if not surpass – PC security as a threat to IT departments,"
- Denise Culver, Heavy Reading Mobile Networks Insider
Range of Threat

- 914 Million Mobile Subscribers
- 75% overall
- 140% tele-density in urban
- 205 Million Internet users
- 53 Million Broadband subscribers

Attackeders can reach a larger audience and much faster than pre-mobile internet era, causing more damage to the victims.

Digital Illiteracy & Content/dialogue in English only add to level of threat.
## Mobile Device Security - Use of Social Media

<table>
<thead>
<tr>
<th>Social Media</th>
<th>Global Users</th>
<th>India’s share</th>
<th>India’s % share</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whatsapp</td>
<td>600 Million</td>
<td>60 Million</td>
<td>10%</td>
<td>India is one of largest source of growth</td>
</tr>
<tr>
<td>Facebook</td>
<td>1.3 Billion</td>
<td>92 Million</td>
<td>7.7%</td>
<td>2nd after US</td>
</tr>
<tr>
<td>Twitter</td>
<td>271 Million</td>
<td>33 Million</td>
<td>12%</td>
<td>2nd after China</td>
</tr>
</tbody>
</table>
Arsenals for Attackers

• Personal information
  – Photos
  – Videos
  – Chat/ Messages

• No awareness about Security Attacks

• Jailbreaking/ rooting more vulnerable to attacks

Multi-media digital information on mobile internet such as on facebook, instant messaging, e-mail, digital photos etc. add to the arsenal of attackers and advanced social engineering attacks.
Impact of Security Attack

• Mobile Banking, Internet Banking, Mobile Wallet
  – Multi-factor Authentication
• Personal Health Records Access
• Enterprise/ Corporate confidential Information Access

Amount of personal information available online is increasing, including financial information. Attackers may be able to arbitrarily choose their victims.
Mobile Devices-M2M

- Mobile Devices in Critical Infrastructure
  - Smart Grid
  - Intelligent Transport Systems
  - Water Management

In utility Sector telecom networks will provide critical control & management of Smart grids, smart water management, Intelligent Transport Systems etc. security concerns in telecom networks will have much wider ramifications than ever before.
Mobile Devices-National Security Issues

- BlackBerry
- Skype
- TrueCaller
- Whatsapp

Encryption by applications on Mobile Devices, authentication based on mobile device identities are matter of concern from lawful interception perspective.
Mobile Devices Management

- Device Management
  - Secure, Monitor & Manage Govt. owned Devices or Employee owned Devices (BYOD)

- Application Management
  - API standardization, testing & certification

- Content management
  - Content Filtering, Encryption

Mobile Device Management for government related services are being discussed for better security & safety of data. Best practices in MDM implementation may be shared for this type of implementation.
Security issues-Cloning of Mobile Device Identity

• Cloning of IMEI

• Filtering Genuine/ Fake

• Device registration
Identity Management Framework

Mobile/SIM based Authentication

• ME based Authentication for Application
• UICC based Authentication for Applications
• PKI based authentication for Applications
Crowd sourcing of information from Mobile/ SIM-Privacy issues

- Mobile as key meta-information provider
  - Location
  - Citizen Reporting
  - Feedback

Mobile Pseudonym, data hiding
Security assessment in TEC

• Exploring vulnerability assessment of mobile apps like .apk through cloud based security testing tools

• Open source tools are also being used in TEC lab for the penetration testing of the vulnerabilities present in applications.
Way Ahead

• Collaboration
  – Prototype

• Co-operation

• Information Exchange
  – Best Practices

• Trainings