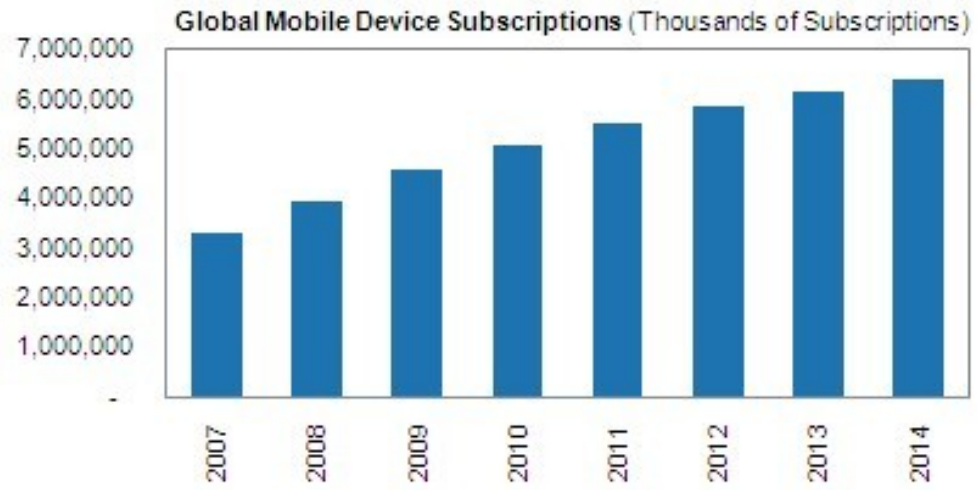
Mobile Application Security

Antonis Lilis

niobiumlabs.com

Numbers

- 5 Billion Wireless Subscriptions in Sept 2010



Source: iSuppli Corp

- Smartphone-Feature Phone Convergence
- More devices are connected to the Internet
- Mobile Devices are becoming interesting

What do you put on your phone?

- Phone numbers /Call history
- Media (Audio/Video/Photos)
- Location Information (Privacy/Security)
- Email/SMS
- Keys/Passwords

...

➢ **Data more valuable than devices**

Security Issues

- Physical Security (Lost/Stolen Phones)
- Secure Data Storage
- Hardware Limitations
- Operating System Limitations
- Browsing Environment
- Virus, Worms, Trojans, Spyware and Malware

Many Platforms

- Symbian
- Apple iOS
- Android
- Windows Mobile /Windows Phone 7
- BlackBerry

  …
- Java Mobile Edition
- Mobile Web Applications

Security Features

- Application Sandboxing
- Application Signing
- Permission Model
- Buffer Overflow Protection Mechanisms
- File Encyption
- Secure Update Mechanisms

Tips for Secure Development

- Follow Secure Programming Practices
- Use TSL/SSL
- Validate Input
  - listening services, rpc interfaces, android intents,…
  - specify how input should be formatted
- Discard data after use if not needed and keep data anonymous (eg Location data)
- Understand the Mobile Browser’s Security Strengths and Limitations

Tips for Secure Development (2)

- Use the Least Privilege Model for System Access (Web, Filesystem, Location etc)
- Leverage the provided Permission Mechanisms
  - Define Permissions (Android Manifest, JAD file)
  - Custom Permissions
  - Protection Level (Android: normal, dangerous etc)
- Ask the user for confirmation before

Tips for Secure Development (3)

- Use High-level APIs to reduce the threat of classic C exploits
- Buffer Overflows
  - avoid manual memory management when possible (eg use Cocoa objects)
- Try to detect problems (eg check for Integer Overflows)
- Leverage Error Handling Mechanism

Tips for Secure Development (4)

- Avoid external storage for sensitive data
- Encrypt data
- SQL Injection
  - Separate data from query logic and use parameterized queries
- Turn on compiler warnings
- Use static analysis tools (eg. Clang Static Analyzer)

Conclusions

- Mobile devices will be (are?) the default computing method
- New hardware/software/applications
- New security threats
- Leverage experience
- Interesting new industry

Thank you!

niobiumlabs.com