



# Data Security Solutions

Riga, Latvia

**Izplatītākie mobilo iekārtu  
lietošanas riski, kas apdraud  
organizācijas datu un  
informācijas sistēmu drošību**

**Raivis Kalniņš**  
2015, Riga



Informācijas tehnoloģiju  
drošības incidentu  
novēršanas institūcija





# What We Do?



Endpoints



Networks



Applications



Data



Mobility



Identity



Management



Cloud



Data Security Solutions





# DSS Global Partnerships

Lumension  
IT Secured. Success Optimized.  
 SpectorSoft  
 symantec.  
 McAfee  
Proven Security™  
 VASCO  
THE AUTHENTICATION COMPANY  
 IBM  
 Accellion  
 beyondtrust  
Beyond Traditional Security  
 LogRhythm™  
 MobileIron  
 observe it  
people audit  
 IPOGLE  
 SECPOINT  
www.secpoint.com  
 WhatsUpGold  
 DeviceLock  
Proactive Endpoint Security  
 radware  
 Centrify  
 varonis  
all about the data  
 Cellcrypt  
 BalaBit  
IT Security





# BYOD Changes the Security Landscape for Enterprises

- Mobile technology has grown more than any other in the last few years
- Lack of awareness of users on the risks related to an improper use of mobile devices
- Initiatives sometimes approved without a business case
- Governance not well understood by many organisations





# Mobile Security Risk Types

- **Physical Security**
  - Lost, Stolen, Compromised
- **Network Security**
  - WiFi & Cellular, hacking tools, 24/7 exposure
- **Malware Security**
- **Vulnerabilities**
  - OS & app-level, Patching challenges



# Myths about mobile security

- Mobile devices don't store sensitive corporate data.
- Strong authentication schemes, password management controls, and device PINs are sufficient to prevent unauthorized access.
- Users are running the latest versions of iOS and Android, so they're up to date with bug fixes and other security patches.
- Public app stores like Apple's App Store and Google's Play are safe sources, because they verify apps and block malware.



# Security Mistakes People Make With Their Mobile Device

- Failing to lock down your device
- Not having the most up to date versions of your apps
- Storing sensitive, work-related data on an unauthorized device
- Opening questionable content
- Not adhering to your company's social media policies
- Using public or unsecure Wi-Fi





# Mobile App Risks

- Activity monitoring and data retrieval
- Unauthorized dialing, SMS, and payments
- Unauthorized network connectivity (exfiltration or command & control)
- UI Impersonation
- System modification (rootkit, APN proxy config)
- Unsafe sensitive data transmission
- Unsafe sensitive data storage







# Activity monitoring and data retrieval

- Risks:
  - Sending each email sent on the device to a hidden 3rd party address – Listening in on phone calls or simply open microphone recording.
  - Stored data, contact list or saved email messages retrieved.
- Examples of mobile data that attackers can monitor and intercept:
  - Messaging (SMS and Email)
  - Audio (calls and open microphone recording) – Video (still and full-motion)
  - Location
  - Contact list, Call history
  - Input, Browsing history
  - Data files





# Unauthorized dialing, SMS, and payments

- Directly monetize a compromised device
- Premium rate phone calls, premium rate SMS texts, mobile payments
- SMS text message as a spreading vector for worms.





# Unauthorized network connectivity (exfiltration or command & control)

- Spyware or other malicious functionality typically requires exfiltration to be of benefit to the attacker.
- Mobile devices are designed for communication. Many potential vectors that a malicious app can use to send data to the attacker.
- The following are examples of communication channels attackers can use for exfiltration and command and control:
  - Email, SMS, HTTP get/post, TCP socket, UDP socket, Bluetooth





# Unsafe sensitive data storage

- Mobile apps often store sensitive data:
  - banking and payment system PIN numbers, credit card numbers, or online service passwords.
- Sensitive data should always be stored encrypted.
  - Make use of strong cryptography to prevent data being stored in a manner that allows retrieval.
  - Storing sensitive data without encryption on removable media such as a micro SD card is especially risky.





# Unsafe sensitive data transmission

- It is important that sensitive data is encrypted in transmission lest it be eavesdropped by attackers.
- Mobile devices are especially susceptible because they use wireless communications exclusively and often public WiFi, which is known to be insecure.
- SSL is one of the best ways to secure sensitive data in transit.
  - Beware of downgrade attack if it allows degrading HTTPS to HTTP.
  - Beware of not failing on invalid certificates. This would enable that a man-in-the-middle attack.







# Summary and Key Points

- Mobile devices present enormous opportunities to businesses, but can also bring risk that is significantly different from the risks that a business is used to managing
- Effective mitigation of these risks requires policies that work with the user; and also require user education and effective technical controls
- There are a great many mobile platforms and devices, and they present widely differing risks; security policies need to account for these many differences





Data Security Solutions

Raivis Kalniņš

[raivis@dss.lv](mailto:raivis@dss.lv)

+371 2 611 35 45

Riga, Latvia

[www.dss.lv](http://www.dss.lv)

LinkedIn: <http://ow.ly/FAfIz>

Twitter: <http://ow.ly/FAfv0>

Facebook: <http://ow.ly/FAfzZ>

Youtube: <http://ow.ly/FAfEN>

SlideShare: <http://ow.ly/FAfHd>





Data Security Solutions

Think Security First

Thank you

