Privacy Issues with the Google Android Market

Thorben Krüger benthor@os3.nl
Bastiaan Wissingh bastiaan@os3.nl

February 2, 2011

Outline

Definition of Terms

Definition of Terms

- Android

Definition of Terms

- Android
- Google Android Market

Definition of Terms

- Android
- Google Android Market
- XMPP

Definition of Terms

- Android
- Google Android Market
- XMPP
- *App*

Original Question

Google Android Market - Remotely Controllable?

Original Question

Google Android Market - Remotely Controllable?

- To what exact extent?

Original Question

Google Android Market - Remotely Controllable?

- To what exact extent?
  - Suspicion: Highly Privileged Remove Administration Functionality

Original Question

Google Android Market - Remotely Controllable?

- To what exact extent?
  - Suspicion: Highly Privileged Remove Administration Functionality
- What Privacy Issues?

Original Question

Google Android Market - Remotely Controllable?

- To what exact extent?
  - Suspicion: Highly Privileged Remove Administration Functionality
- What Privacy Issues?
- Proposed Mitigations?

Current Research: Status

Current Research: Status

- Market uses XMPP over SSL

Current Research: Status

- Market uses XMPP over SSL
- Google Android: A State-of-the-Art Review of Security Mechanisms

Current Research: Status

- Market uses XMPP over SSL
- Google Android: A State-of-the-Art Review of Security Mechanisms
- AppBrain

Approach: SSL Man-In-The-Middle

Approach: SSL Man-In-The-Middle

- Idea: Traffic Introspection

Approach: SSL Man-In-The-Middle

- Idea: Traffic Introspection
- Methods: Lots Of Dirty Hacks

Traffic Analysis: Results

Traffic Analysis: Results

- Confirmed: XMPP-Triggered Installation

Traffic Analysis: Results

- Confirmed: XMPP-Triggered Installation
- Unconfirmed: Additional Functionality

Approach: Reverse Engineering

Approach: Reverse Engineering

- Analyze Market Package

Approach: Reverse Engineering

- Analyze Market Package
- Core System Application

Binary Analysis: Findings

Binary Analysis: Findings

- Binary Decodable To "Assembly"

Binary Analysis: Findings

- Binary Decodable To “Assembly”
- Results Hardly Readable

Binary Analysis: Findings

- Binary Decodable To "Assembly"
- Results Hardly Readable
- Evidence: Remotely Triggerable Functionality

Binary Analysis: Findings

- Binary Decodable To "Assembly"
- Results Hardly Readable
- Evidence: Remotely Triggerable Functionality
  - `INSTALL_ASSET`
  - `REMOVE_ASSET`

Binary Analysis: Findings

- Binary Decodable To "Assembly"
- Results Hardly Readable
- Evidence: Remotely Triggerable Functionality
  - `INSTALL_ASSET`
  - `REMOVE_ASSET`
- Evidence: Persistent Connection

Privacy Implications

Privacy Implications

- No Evidence For: Advanced Remote Control Functionality

Privacy Implications

- No Evidence For: Advanced Remote Control Functionality
- Possible Issue For Some: Remotely Triggered Application Removal

Mitigation Idea: Patch Script

Mitigation Idea: Patch Script

- "Assembly" Rebuildable To Binary

Mitigation Idea: Patch Script

- "Assembly" Rebuildable To Binary
- Result Still Executable

Mitigation Idea: Patch Script

- "Assembly" Rebuildable To Binary
- Result Still Executable
- Assembly-Level Patch: Remove Unwanted Functionality

Accidental Finding: Market App Honors Permission System

Accidental Finding: Market App Honors Permission System

- Error For Patched Market: No Permission To Install Apps

Accidental Finding: Market App Honors Permission System

- Error For Patched Market: No Permission To Install Apps
- Very Unexpected

Digression: Android Permission System

Digression: Android Permission System

- Central Part Of Android Architecture

Digression: Android Permission System

- Central Part Of Android Architecture
- Open Source!

Digression: Android Permission System

- Central Part Of Android Architecture
- Open Source!
- Uses: Plain XML Files

Digression: Android Permission System

- Central Part Of Android Architecture
- Open Source!
- Uses: Plain XML Files
- Problem: Very Coarse Grained UI

Android Permission System: Current Research

Android Permission System: Current Research

- `permissionBlocker.apk`

Android Permission System: Current Research

- `permissionBlocker.apk`
- Apex

Proposal: Extension of Apex

Proposal: Extension of Apex

- Requires: Changes To Software Stack

Proposal: Extension of Apex

- Requires: Changes To Software Stack
- Hurdle: System App Permissions Handled Differently

Proposal: Extension of Apex

- Requires: Changes To Software Stack
- Hurdle: System App Permissions Handled Differently
- Red Tape: Nothing Has Been Released

Conclusion

Conclusion

- Current Market App Less Evil Than Expected

Conclusion

- Current Market App Less Evil Than Expected
- Binary/Assembly Patches Possible

Conclusion

- Current Market App Less Evil Than Expected
- Binary/Assembly Patches Possible
- Alternative Approach: Permission Management

Outlook

Outlook

- Reimplement Apex: NLnet funding?

Questions?