iOS Application Hardening via Obfuscation

Master thesis

Supervisors: Prof. Dr. Alexander Pretschner, Sebastian Banescu
Email: {alexander.pretschner, sebastian.banescu} @ in.tum.de
Phone: +49 89 289 – 17, 314
Starting date: immediately

Context
The proprietary logic and data inside iOS applications are often left unprotected with software hardening techniques in the hope that legislation and the security measures existent on iOS devices will be enough to deter attackers. However, history has proven that attackers always find ways of jail-breaking iOS devices at which point they can access the code of all applications on the device and steal proprietary logic and data from them.

Software obfuscation is a code transformation technique which aims to make software applications harder to reverse engineer, than the original (un-obfuscated) software. Therefore, some vendors such as Google recommend using software obfuscation tools for hardening mobile applications.

Goal
The goal of this thesis is to evaluate the security-cost trade-off for a set of obfuscation techniques and tools for iOS applications. The student may also need to implement one or more obfuscation techniques, which are not offered by existing tools. This implementation would be based on the LLVM framework and would be integrated in the ISA2R tool1.

A concrete case-study will be performed using the Dox2 iOS application offered by a company called Brainloop, which has agreed to be the industry partner for this thesis topic. Brainloop Dox is a secure file sync & share solution offered to enterprise customers.

Work-plan
1. Develop knowledge of state-of-the-art obfuscation techniques and tools for iOS:
   a. Read references [1], [2], [3], [4] and find related work on this topic.
   b. Identify obfuscation tools suitable for iOS applications.
   c. Write state-of-the-art survey, which presents and compares the investigated techniques and tools.
2. Perform a security analysis of the Brainloop Dox iOS application:
   a. Identify the application assets that need to be protected.
   b. Identify and perform attacks to extract the assets from the application.
   c. Identify countermeasures based on obfuscation.
3. If countermeasures identified in step 2 require obfuscation transformations which are not available in free tools, then implement those obfuscation techniques:
   a. Choose technique(s) described in literature and/or propose a new technique; argument your choice (e.g. security versus cost tradeoff) in written form.
   b. Implement the chosen technique(s) based on the LLVM framework2 and document design decisions.

---

1 https://www22.in.tum.de/isa2r/
3 http://llvm.org/
4. Evaluation of the existing tools and possibly own implementation (case-study):
   a. Measure effectiveness of obfuscation against the same attacks identified in step 2. If no new obfuscation techniques are implemented in step 3, then the student must implement an automated de-obfuscation attack in this step.
   b. Measure performance and size impact of the obfuscation on the Dox application.
   c. Measure the performance of the obfuscation transformation/tool itself.
   d. Analyze and discuss security versus performance trade-offs.

5. The final thesis document must contain:
   a. Description of the problem and motivation for the chosen approach
   b. State of the art survey, including analysis of security and performance
   c. Security analysis of the Branloop Dox application
   d. Rationale for choosing certain technique(s) for implementation
   e. Implementation description
   f. Performance evaluation of implementation
   g. Discussion on potential security and performance trade-offs
   h. Conclusions and future work.

Deliverables
- Virtual machine able to run a demo of the implementation, including instructions on how to run the demo.
- The VM should also include the source code of the implementation.
- Technical report with comprehensive documentation of the implementation, i.e. design decision, architecture description, API description and usage instructions.
- Final thesis report written in conformance with TUM guidelines.

References