yakindanegitim.org

MBFuzzer - MITM Fuzzing for Mobile Applications

Fatih Özavcı

Mentor of MBFuzer @ yakindanegitim.org

fatih.ozavci at gamasec.net

gamasec.net/fozavci

Scope

- “Yakindan Egitim” Project
- Security Vulnerabilities of Mobile Applications
- Fuzzing for Mobile Applications
- Man in the Middle Fuzzing
  - Understanding Mobile Services
  - Response Based Fuzzing for Mobile Applications
  - XML/JSON/RAW Response Injections and Corruptions
  - SQL/XSS/Overflow Injections
- MBFuzzer
  - PoC -> 1 June 2013
  - Future Releases and Features

Yakindan Egitim Project

- Web : www.yakindanegitim.org
- Blog : blog.yakindanegitim.org
- Github : github.org/yakindanegitim

- It's a Training Project for Students
- Students Develop, Mentors Manage
- It's Like Google Summer of Code Without Money :(
- Other Security Related Projects
  - Yekk - Necdet Yucel
  - Malwarez - Oguz Yarimtepe
  - VirtLabNet - Emre Yuce
  - NfQuery - Serdar Yigit

Security Vulnerabilities of Mobile Applications

OWASP – TOP 10 Mobile Security Risks

- M1: Insecure Data Storage
- M2: Weak Server Side Controls
- M3: Insufficient Transport Layer Protection
- M4: Client Side Injection
- M5: Poor Authorization and Authentication
- M6: Improper Session Handling
- M7: Security Decisions Via Untrusted Inputs
- M8: Side Channel Data Leakage
- M9: Broken Cryptography
- M10: Sensitive Information Disclosure

Fuzzing

- Automated Data Sending to Test Applications
- Main Target : Crashing Application & Memory Leaks
- Workflow
  - Sending Random Big Data
  - Wait For Crash or Increase Data Size
  - Report the Crash
- Weaknesses
  - Understanding Protocols
  - Random Data is Not Enough!
  - Crash & Vulnerability Detection Problems
  - Smart vs Mutation Based vs Generation Based

Fuzzing for Mobile Applications

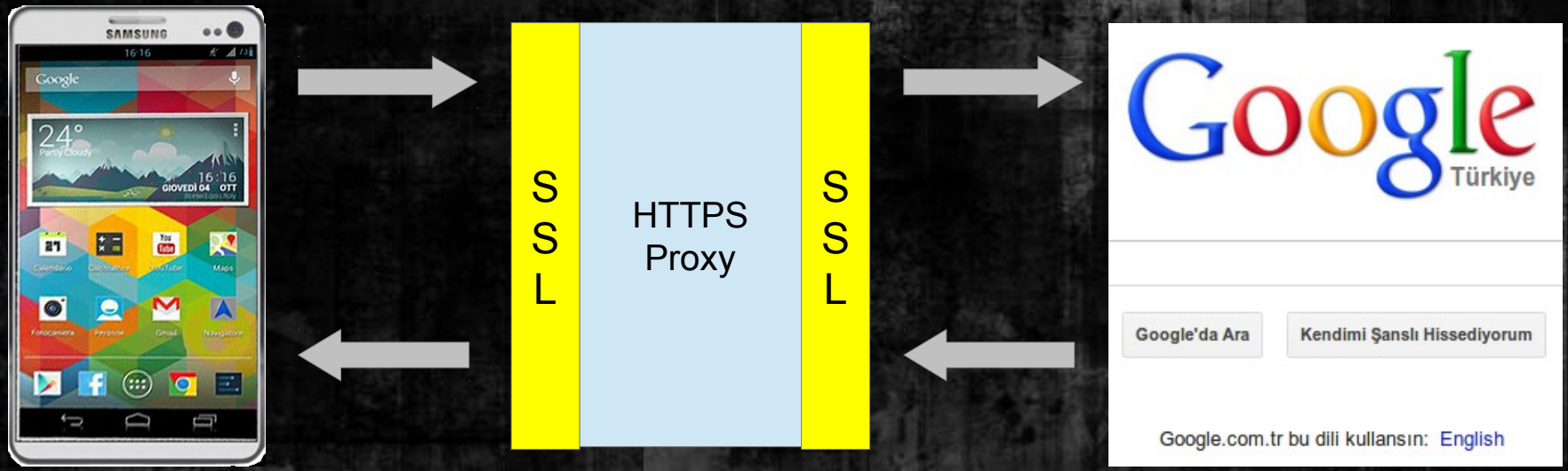
- Out of Scope : Internal Fuzzing of Mobile Applications
- Mobil Applications are Mostly Clients not Servers
  - Fuzzing Should be Implemented as Server Response
  - Man in the Middle Attack Should be Implemented
  - Target is Remote Vulnerabilities
    - Priveledge Escalation & Obtain Information
    - Crashing the Target Application
- Fake Services vs Response Injection
  - Understanding Remote Services
  - Understanding Conditions and Response Types
  - Parsing Request & Response Data
    - XML, JSON, RAW, Binary

Targeted Remote Vulnerabilities

- M3: Insufficient Transport Layer Protection
  - SSL Implementation
  - Flow Manipulation
- M4: Client Side Injection
  - SQL Injection
  - XSS Injection
- M5: Poor Authorization and Authentication
  - Remote Code Execution via Overflows
- M6: Improper Session Handling
  - Flow Manipulation
- M7: Security Decisions Via Untrusted Inputs
  - Memory Corruptions
- M10: Sensitive Information Disclosure
  - Information Leak with Error and Warning Messages

The Man in The Middle

- Proxy Behaviors
- Implementing Fake Services
- SSL and Certificate Problems
- Real-Time Response Fuzzing



Proxy Implementation

- Multi-Threaded Proxy Support
- Invisible and Reverse Proxy Support
  - Mobile Proxy Settings Could be Bypassed
- SSL Support
  - SSL and TLS Support
  - HTTPS Connect Conversion Support
  - On-The-Fly x.509 Certificate Generation
    - Using Information of Target Server's Certificate
    - Bypassing Weak Server Certificate Pinning
- Parsing Data
  - XML, JSON, RAW, Binary

Fake Server Implementation

- Multi-Thread Support
- SSL Support
  - SSL and TLS Support
  - HTTPS Connect Conversion Support
  - On-The-Fly x.509 Certificate Generation
    - Using Information of Target Server's Certificate
    - Bypassing Weak Server Certificate Pinning
- Parsing Data
  - XML, JSON, RAW, Binary
- Learning Flow from Configuration File
  - Request & Response Types
  - Fuzzing Targets

Parsing and Manipulating Server Responses

- XML & JSON Data
  - Corrupting XML/JSON Type, Language, Structure
  - Manipulating Labels and Seperators
  - Injection Data to Variables and Values
- RAW Data and Binary Data
  - Random Injections
  - HTML, JS and File-Type Fuzzing (Images, PDF etc)
- Flow Manipulation
  - Timing Attacks, Logical Attacks
  - Replay Attacks
  - Parsing UDP/TCP Data and Creating Flow

Fuzzing Server Responses For...

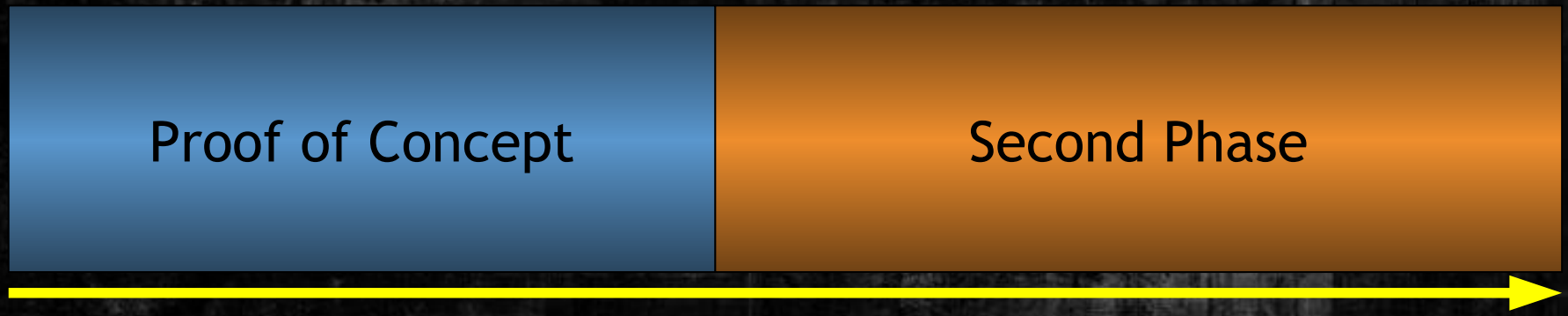
- Memory Corruptions and Overflows
  - Big Data, A*20000
  - Format String Data (%n %x)
  - Big Numbers for Arithmetic Overflows
  - Null Data, Fake Variables, Missing Variables
- SQL Injections → Mobile Applications Sqlite Databases
- Cross-Site Scripting → Manipulating Interface
- Path Injections (NSFileManager etc.)
- Protocol and Library Based Fuzzing
  - SSL, Raw Proto and HTTP Libraries
  - XML and JSON Libraries
  - Image, PDF and Office Files Libraries

MBFuzzer Project

- MBFuzzer → Mobile Application Fuzzer
- Real-Time Fuzzing for Mobile Applications
  - Proxy Support (Invisible & Reverse Support)
  - Fake Service Support (Flow Based)
  - SSL Support
    - HTTPS Connect Conversion
    - On-The-Fly Certificate Generation
  - Response Based Fuzzing
    - XML/JSON/Raw/Binary Data Fuzzing
- Fuzzing Support For
  - Memory Corruptions and Overflows
  - SQL Injections, Cross-Site Scripting, Path Injections
  - Protocol and Library Based Fuzzing

MBFuzzer Project Timeline

- Mentor : Fatih Ozavci
- Developer Candidate : Loading....



- Basic Proxy Support
- SSL Implementation
  - Cert Generation
  - HTTPS Connect
- MITM Fuzzing
  - Big Data, Format String

1 June 2013

- Fake Service Support
- Flow Manipulations
- Client Side Monitoring & Scripting
- Additional Fuzzing Supports
  - SQL Injection, XSS
  - File Type Manipulations

Unknown 2013

References

- Yakindan Egitim Project
  http://www.yakindanegitim.org
  http://blog.yakindanegitim.org

- MBFuzzer Project Page
  http://github.org/yakindanegitim/mbfuzzer

- Fatih Ozavci Personal Page & Blog for Mobile Security
  http://gamasec.net/fozavci
  http://fozavci.blogspot.com