Privacy Concerns in Public Web APIs

SCG Seminar - Marc-Andrea Tarnutzer
Agenda

- Introduction
- Implementation & Analysis
- Results
- Demo
- Lessons Learned
- Future Work
Web APIs are Everywhere
Project Overview

API URL Extraction  API Security Testing  Vulnerability Assessment
# Approach

**API URL extraction**
Extract URLs from APK corpus (100k apps, size: 750 GB)

**Purification of found URLs**
Parsing and purification of URLs found in 100k log files

**App decompilation**
E.g. for further analysis of parameters, JSON structure, ...

**API is-alive tests**

**Hand crafted exploits**
APK
- Android Package (APK)
- Package file format
- Used for app distribution and installation on the Android OS
- APK contains compiled source code, assets, resources, certificates, … of a program

JSON
- JavaScript Object Notation (JSON)
- Open-standard file format
- Used to transmit data objects
- Key-value pairs
- Often used in APIs to send and receive data
API URL Parser

Parsing
Concurrent parsing of URLs found in 100k log files (4 GB)

Filtering & Sorting
Filter URLs for certain criteria (App occurrence, URL occurrence, API keyword, HTTP, HTTPS, contains credentials, contains query string, ...)

Concurrent parsing of URLs found in 100k log files (4 GB)
API Fetcher

API is-alive tests
Concurrently send HTTP HEAD requests (don’t request response body to save time)
Results I

- Unique URLs: 981458
- URLs occur in one app: 736827
- URLs occur only once: 440992
- Contains "api": 92156
- HTTPS: 84355
- HTTP: 399059
- HTTPS (cred): 4608
- HTTP (cred): 7982
Results II

![Bar chart showing results for different categories: Containing "apf", HTTPS, HTTP, HTTPS (cred), HTTP (cred). The chart displays the counts for offline and online results.](chart.png)
Manual API Analysis

- API analysis with Postman / CocoaRestClient & JADX

- Findings
  - Hardcoded credentials / API keys / authentication tokens / ...
  - Insecure query strings / account management
  - HTTP for sensitive data
  - Missing authentication
Findings - Examples I

http://api.t.sina.com.cn/oauth/access_token

http://www.tumblr.com/oauth/access_token
Findings - Examples II

http://bubleid.in/api/Api_recharge.aspx?mid=<mid>&username=<unm>&password=<pwd>&amount=<amt>&oid=<oid>&mobileno=<mob>&mo_op=<opt>

https://api.soundcloud.com/tracks/139387810/download?client_id=b45b1aa1f1ac2941910a7f0d10f8e28&oauth_token=1-16343-79761863-1de35dec80806be

http://184.164.151.199:8080/gpstrackernew/mobile/VehicleService?userName=admin&password=spectrum123&action=LIVE_TRACK&imeiNo=
Demo
Lessons Learned

- Communication security is a problem
  - HTTP vs. HTTPS
  - Query strings instead of HTTP headers and HTTP message body for sensitive information

- Omnipresent issues
  - Hardcoding
  - Vulnerable Chinese apps
  - Offline API URLs
  - Ad services

- Also popular services have security problems
Future Work

- SSL certificate checking
- Automated search of API parameters
- SQL injection
- DoS attacks and boundary checks
Summary

- Introduction

- Implementation & Analysis
  - API URL Parser & API Fetcher

- Results & Examples

- Demo

- Lessons Learned

- Future Work