FIELD NOTE / ANDROID

SSLPinDetect: Advanced SSL Pinning Detection for Android Security Analysis

Petruknisme · 1 Aug, 2025 · 3 min to read

In the ever-evolving landscape of mobile application security, SSL pinning has become a crucial defense mechanism against man-in-the-middle attacks. However, for security researchers and penetration testers, identifying these implementations can be a time-consuming and complex task.

Why I Created SSLPinDetect

The purpose I created this tool is to create some pattern detection when scanning SSL pinning implemented in the app. It will be easier to do static analysis first before running the app. Traditional approaches to SSL pinning detection often require manual code review or dynamic analysis, which can be inefficient and resource-intensive. SSLPinDetect bridges this gap by providing automated pattern recognition that allows security professionals to quickly identify potential SSL pinning implementations before diving into deeper analysis or runtime testing.

What Makes SSLPinDetect Special?

Performance-Driven:

- Uses multi-threading to scan multiple files at once
- Employs memory-mapped reading for faster access to large codebases
- Shows real-time progress with interactive bars

Precision Detection:

- Uses pre-compiled regex for accurate SSL pinning detection
- Ensures high accuracy, low false positives, and includes line numbers/code previews
- Supports various frameworks and custom implementations

Flexible & User-Friendly:

- Offers verbose mode for detailed logs or minimal output for quick use
- Allows **custom patterns** for specialized needs

How It Works

SSLPinDetect follows a straightforward yet powerful workflow:

1. **APK Decompilation**: Uses `apktool` to extract and decompile the target APK
2. **Smali Code Analysis**: Scans through decompiled smali files using optimized pattern matching
3. **Pattern Recognition**: Identifies SSL pinning implementations based on known signatures
4. **Detailed Reporting**: Provides comprehensive results with file locations and code snippets

Pattern Detection Capabilities

SSLPinDetect comes with built-in patterns for detecting common SSL pinning implementations, including:

- **OkHttp Certificate Pinning**: Detects OkHttp3 and legacy OkHttp implementations
- **TrustManager Overrides**: Identifies custom X509TrustManager implementations
- **Network Security Config**: Recognizes Android's declarative security configurations
- **Custom SSL Context Configurations**: Catches manual SSL/TLS implementations

Extensible Pattern System

The tool supports custom pattern files in JSON format, allowing you to:

- Add patterns for proprietary SSL pinning libraries
- Customize detection rules for specific use cases
- Share pattern definitions across your security team

Example pattern file structure:

```
{
    "OkHttp Certificate Pinning": [
        "Lcom/squareup/okhttp/CertificatePinner;",
        "Lokhttp3/CertificatePinner;",
        "setCertificatePinner"
    ],
    "TrustManager Override": [
        "Ljavax/net/ssl/X509TrustManager;",
```

```
            "checkServerTrusted"
        ]
    }
```

SSLPinDetect has demonstrated significant value in the following areas:

- Security Assessments: Facilitates the rapid identification of SSL pinning mechanisms prior to penetration testing.
- Code Reviews: Enables automated detection of SSL pinning during secure code review processes.
- Compliance Audits: Assists in verifying adherence to SSL pinning implementation requirements.
- Research: Supports both academic and professional research focused on mobile security practices.

Getting Started

Setting up SSLPinDetect is simple and straightforward:

Prerequisites

- Python 3.8 or higher
- Java (accessible via system PATH)
- Apktool

Installation

```
git clone https://github.com/aancw/SSLPinDetect
cd SSLPinDetect
pip install -r requirements.txt
```

Basic Usage

```
python sslpindetect.py -f app.apk -a apktool.jar
```

Advanced Usage with Verbose Output

```
python sslpindetect.py -a apktool_2.11.0.jar -f sample/app-release.apk -v
```

This will provide detailed output including:

- Processing status updates
- Scan progress with timing information
- Pattern match details with file locations and line numbers

Demo



SSLPinDetect demo

The Future of SSL Pinning Detection

As mobile security continues to evolve, SSLPinDetect is designed to grow with the landscape. The modular pattern system ensures that new SSL pinning techniques can be quickly incorporated, keeping your security assessments current and comprehensive.

Get Involved

SSLPinDetect is open source and welcomes contributions from the security community. Whether you want to:

- Add new detection patterns
- Improve performance optimizations
- Enhance reporting capabilities
- Fix bugs or suggest improvements

Your contributions help make mobile security analysis more accessible and effective for everyone.

*SSLPinDetect is available under the MIT License. For the latest updates and pattern definitions, visit the **project repository** (https://github.com/aancw/SSLPinDetect) and the **smali-sslpin-patterns** (https://github.dev/aancw/smali-sslpin-patterns) collection.*

- GitHub - aancw/SSLPinDetect: SSLPinDetect is a tool for analyzing Android APKs to detect SSL... (https://github.com/aancw/SSLPinDetect)
- GitHub - aancw/smali-sslpin-patterns: A collection of Smali patterns to detect SSL pinning... (https://github.com/aancw/smali-sslpin-patterns)

Originally published on Medium (https://petruknisme.medium.com/sslpindetect-advanced-ssl-pinning-detection-for-android-security-analysis-1390e9eca097).

Android # Security # Tools