Technical -Approach

Mobile Application Security Testing

Infopercept

INVINSENSE

The OWASP Top Ten Highlights the following Threats to Mobile Applications

01 Insecure Data Storage

02 Weak Server-Side Controls

03 Insufficient Transport Layer Protection

04 Client Side Injection

05 Poor Authorization and Authentication

06 Improper Session Handling

07 Security Decisions via Untrusted Inputs

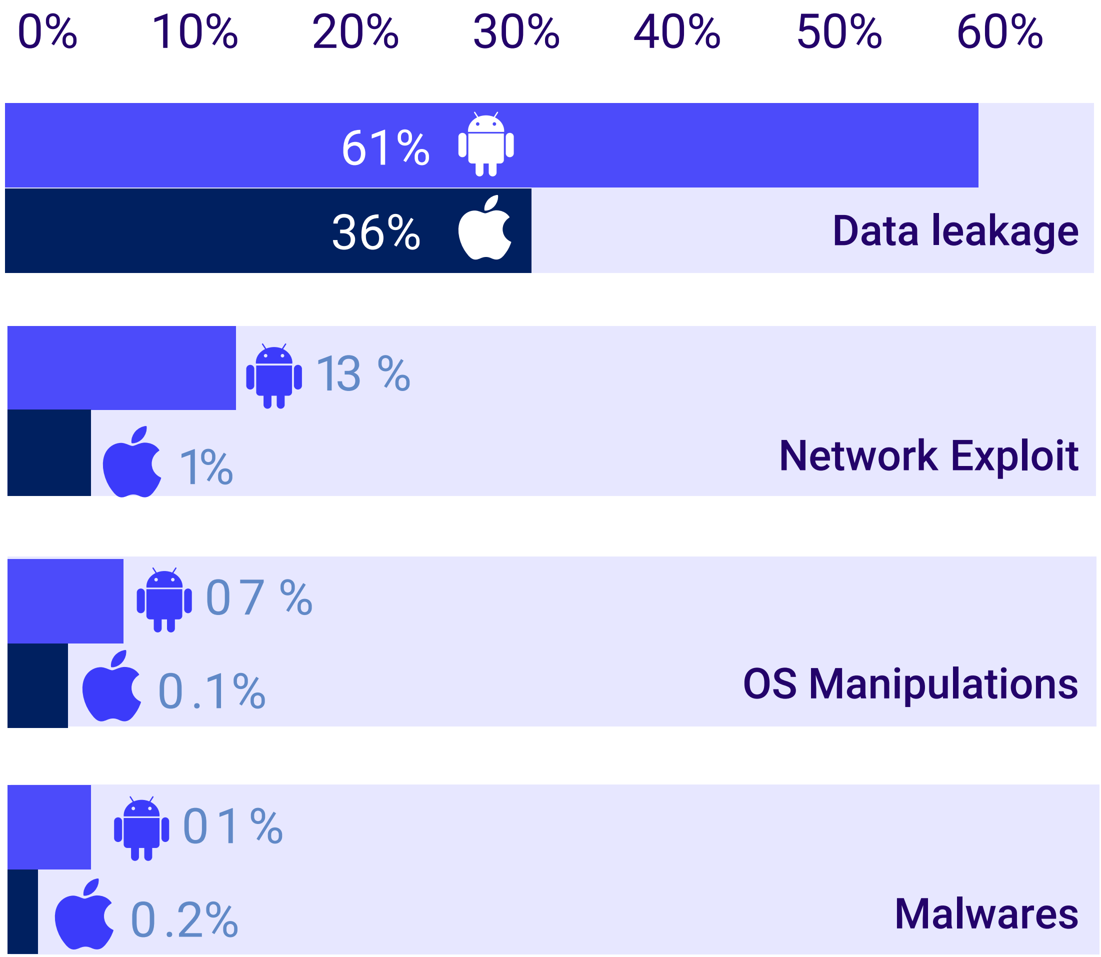
08 Side Channel Data Leakage

09 Broken Cryptography

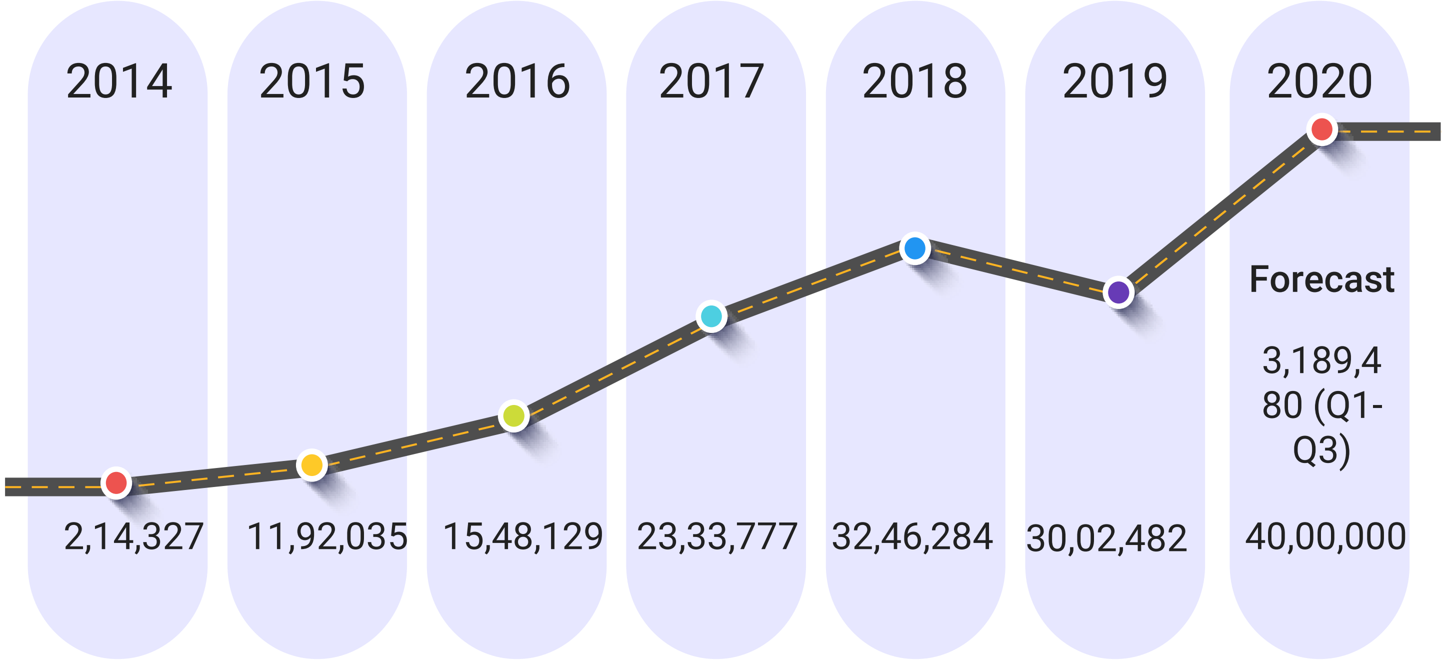
10 Sensitive Information Disclosure

Highest Security Risk

The world is getting to be more intelligent regularly with more brilliant portable innovation. There is an expanded interest for brilliant applications particularly in the region of Banking and Retail area. The expanding dependence on these applications has offered ascend to real security issues. While most endeavors center around discharging versatile applications in a limited capacity to focus time to stay aware of the rivalry, security contemplations are regularly neglected. Contrasted with work area or Mobile applications, versatile applications are hard to test for security since they keep running on gadgets that are not overseen by the venture which stores colossal measure of individual, business and monetary information that draws in both focused on and mass-scale assaults.



Threats Continue to Rise



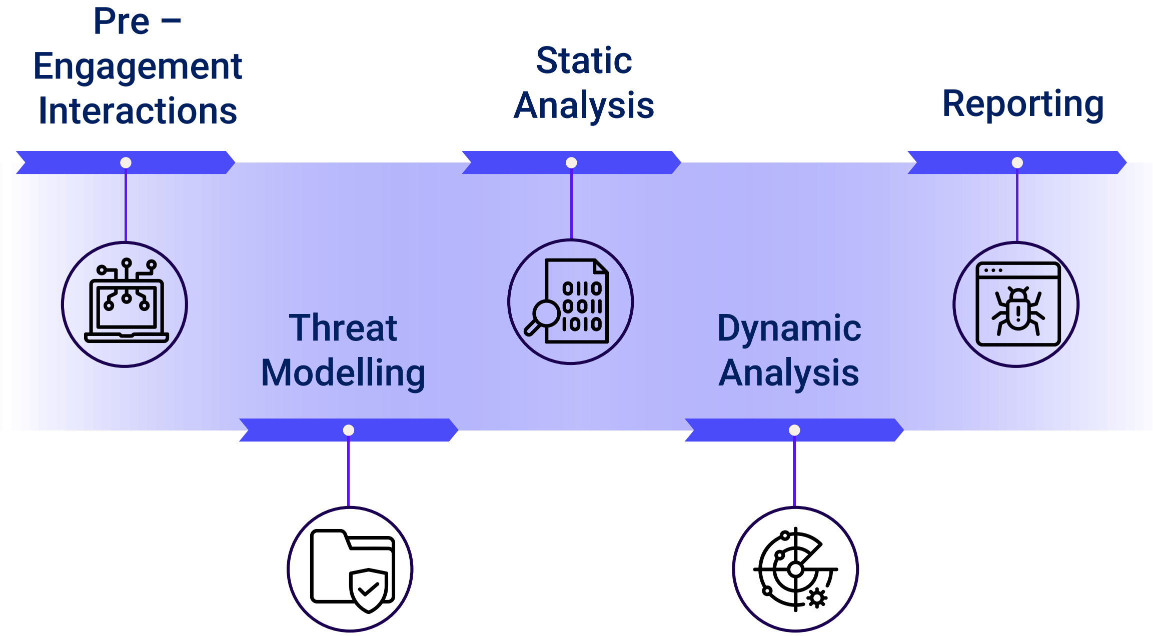
New Android malware samples (per year)

What is Mobile Application Security?

Mobile use is developing constantly. Not at all like the circumstance 10 years prior, today. There have been extraordinary propels in portable registering. Individuals can download applications that assistance them mingle, stay in shape, get headings, execute, shop, and considerably more. There are a large number of portable applications accessible in application stores that make our basic life easier.

A form of stress testing, which exposes weaknesses or flaws in a Application, Art of finding an ways to exploit Application.

Mobile application security testing can help ensure there aren't any loopholes in the software that may cause data loss. The sets of tests are meant to attack the app to identify possible threats and vulnerabilities that would allow external persons or systems to access private information stored on the mobile device.



Methodology for Mobile Application Security

Application Discovery

- Open source intelligence
- Understanding the platform
- Client side vs server side scenarios

Assessment / Analysis

- Static analysis
- Achieve analysis
- Local file analysis
- Network and web traffic
- Reverse engineering
- Inter process
- communication

Exploitation

- Attempt to exploit the vulnerability
- Privilege escalation

Report

- Risk assessment
- for final findings
- Final report

Methodology for Mobile Application Security

Application Discovery

Knowledge gathering is the most vital stage in an application Penetration test. The capacity to find shrouded prompts that may reveal insight into the presence of a weakness may be the distinction between an effective and unsuccessful pen testing.

Assessment/Analysis

The way toward evaluating Mobile applications is special since it requires the Penetration Tester to check the applications when establishment. The distinctive evaluation methods that are experienced inside the MAPTM

Exploitation

The pen tester follows up on the data found from the data gathering procedure to assault the mobile application. Completely performed insight gathering ensures a high shot of successful exploitation thus a fruitful task.

Reporting

A decent report conveys to the management in basic dialect, unmistakably demonstrating the found vulnerabilities, outcomes to the business and conceivable remediation or recommendation.

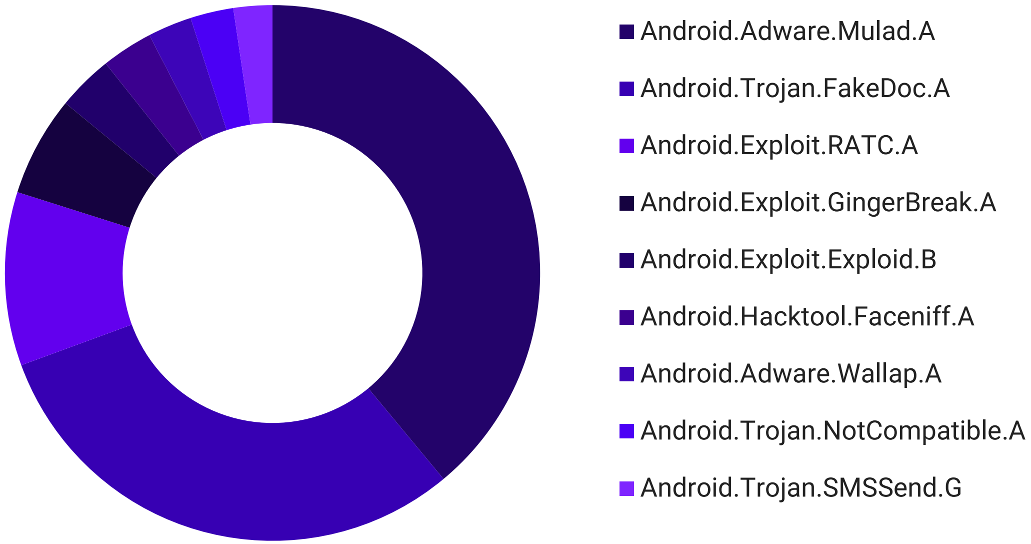
iOS Application Penetration Testing

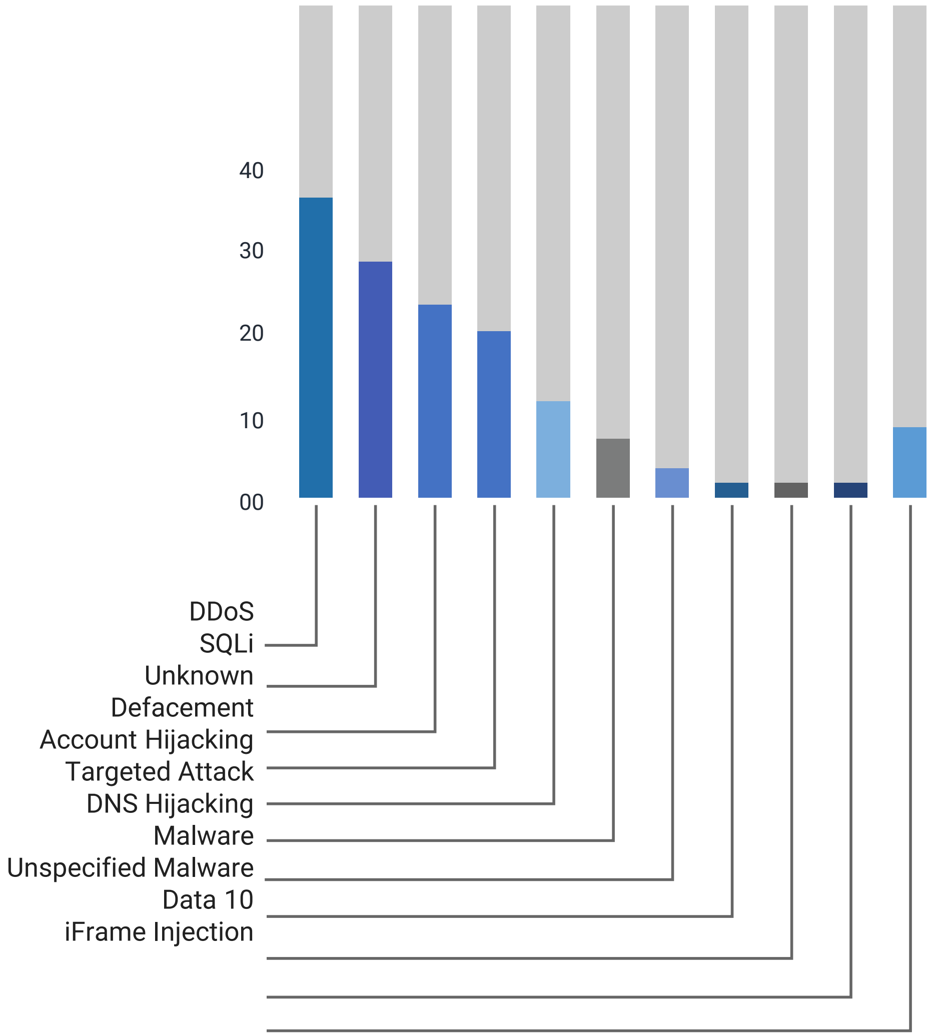
- Access Filesystem on iDevice
- Reverse Engineering and Static Analysis
- Dynamic and Runtime Analysis
- Network Analysis and Server Side Testing
- Bypassing Root Detection and SSL Pinning
- Security Libraries

6. Network Device Configuration Audit

- Reverse Engineering and Static Analysis
- Dynamic and Runtime Analysis
- Network Analysis and Server Side Testing
- Bypassing Root Detection and SSL Pinning
- Security Libraries

Deliverables


■ Android.Adware.Mulad.A
■ Android.Trojan.FakeDoc.A
■ Android.Exploit.RATC.A
■ Android.Exploit.GingerBreak.A
■ Android.Exploit.Exploid.B
■ Android.Hacktool.Faceniff.A
■ Android.Adware.Wallap.A
■ Android.Trojan.NotCompatible.A
■ Android.Trojan.SMSSend.G



Organize Data/related results for Management Reporting

- Consolidation of Information gathered.
- Analysis and Extraction of General conclusions.
- Recommendations.

”Infopercept Proprietary Material - Please do not copy or distribute”/ © Infopercept Consulting

About Infopercept

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

Imprint

© Infopercept Consulting Pvt. Ltd.

Address

3rd floor, Optionz Complex
Opp. Hotel Regenta,
CG Road, Navrangpura,
Ahmedabad - 380 009,
Gujarat, India.

Contact Info

M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

Global Office

United State of America
+1 516 713 5040

United Kingdom
+44 2035002056

Sri Lanka
+94 702 958 909

Kuwait

India
+91 9898857117

Infopercept