RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -11

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- The primary Google security services are
- Platform security architecture
- Security program overview
- MCQ
- References

THE PRIMARY GOOGLE SECURITY SERVICES ARE:

The primary Google security services are

Google Play:

Google Play is a collection of services that allow users to discover, install, and purchase apps from their Android device or the web. Google Play makes it easy for developers to reach Android users and potential customers. Google Play also provides community review, app license verification, app security scanning, and other security services.

Android updates:

The Android update service delivers new capabilities and security updates to selected Android devices, including updates through the web or over the air (OTA).

App services:

Frameworks that allow Android apps to use cloud capabilities such as (backing up) app data and settings and cloud-to-device messaging (C2DM) for push messaging.

THE PRIMARY GOOGLE SECURITY SERVICES ARE:

The primary Google security services are

Verify Apps:

Warn or automatically block the installation of harmful apps, and continually scan apps on the device, warning about or removing harmful apps.

Safety Net: A privacy preserving intrusion detection system to assist Google tracking, mitigate known security threats, and identify new security threats.

Safety Net Attestation:

Third-party API to determine whether the device is CTS compatible. Attestation can also identify the Android app communicating with the app server.

Android Device Manager: A web app and Android app to locate lost or stolen device.

PLATFORM SECURITY ARCHITECTURE

Platform security architecture

Android seeks to be the most secure and usable operating system for mobile platforms by repurposing traditional operating system security controls to:

1. **Protect app and user data**
2. **Protect system resources (including the network)**
3. **Provide app isolation from the system, other apps, and from the user**

To achieve these objectives, Android provides these key security features:

1. **Robust security at the OS level through the Linux kernel**
2. **Mandatory app sandbox for all apps**
3. **Secure interprocess communication**
4. **App signing**
5. **App-defined and user-granted permissions**

SECURITY PROGRAM OVERVIEW

Security program overview

The key components of the Android Security Program include:

Design review:

The Android security process begins early in the development lifecycle with the creation of a rich and configurable security model and design. Each major feature of the platform is reviewed by engineering and security resources, with appropriate security controls integrated into the architecture of the system.

Penetration testing and code review:

During the development of the platform, Android-created and open source components are subject to vigorous security reviews. These reviews are performed by the Android Security Team, Google's Information Security Engineering team, and independent security consultants. The goal of these reviews is to identify weaknesses and possible vulnerabilities well before major releases, and to simulate the types of analysis that are performed by external security experts upon release.

SECURITY PROGRAM OVERVIEW

Security program overview

Open source and community review:

AOSP enables broad security review by any interested party. Android also uses open source technologies that have undergone significant external security review, such as the Linux kernel. Google Play provides a forum for users and companies to provide information about specific apps directly to users.

Incident response:

Even with these precautions, security issues may occur after shipping, which is why the Android project has created a comprehensive security response process. Full-time Android security team members monitor the Android-specific and the general security community for discussion of potential vulnerabilities and review security bugs filed on the Android bug database. Upon the discovery of legitimate issues, the Android team has a response process that enables the rapid mitigation of vulnerabilities to ensure that potential risk to all Android users is minimized. These cloud-supported responses can include updating the Android platform (AOSP updates), removing apps from Google Play, and removing apps from devices in the field.

Monthly security updates:

The Android security team provides monthly updates to Google Android devices and all our device manufacturing partners.

MCQ

1. 11. Which of the following comes after scanning phase in ethical hacking?

   a) Scanning

   b) Maintaining access

   c) Reconnaissance

   d) Gaining access

12. In __________ phase the hacker exploits the network or system vulnerabilities.

   a) Scanning

   b) Maintaining access

   c) Reconnaissance

   d) Gaining access

13. Which of the following is not done in gaining access phase?

   a) Tunnelling

   b) Buffer overflow

   c) Session hijacking

   d) Password cracking

14. Which of the below-mentioned penetration testing tool is popularly used in gaining access phase?

   a) Maltego

   b) NMAP

   c) Metasploit

   d) Nessus

REFERENCES

- ❑https://source.android.com/security