Glossary

Mobile App Security

Created By: Joshua Elijah, Teaching Assistant

A

- **Android Debug Bridge:**

The **Android Debug Bridge (adb)** is a versatile command-line tool that lets you communicate with a device. The **adb** command facilitates a variety of device actions, such as installing and debugging apps, and it provides access to a **UNIX shell** that you can use to run a variety of commands on a device.

- **API:**

The **API (Application Programming Interface)**, is a software intermediary that allows two applications to talk to each other. Each time you use an app like **Facebook**, send an instant message, or check the weather on your phone, you're using an API.

- **Attack Surface:**

An **attack surface** is the total sum of vulnerabilities that can be exploited to carry out a security attack. **Attack surfaces** can be physical or digital. The term **attack surface** is often confused with the term **attack vector**, but they are not the same thing.

- **Attack Vector:**

An **attack vector** is a path or means by which a **hacker (or cracker)** can gain access to a computer or network server in order to deliver a **payload** or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

- **Authentication:**

Authentication is the act of proving an assertion, such as the identity of a computer system user. In contrast with **identification**, the act of indicating a person or thing's identity, authentication is the process of **verifying** that identity.

C

- **Certificate Authority (CA):**

In **cryptography**, a **certificate authority** or **certification authority** is an entity that issues digital certificates. A digital certificate certifies the ownership of a **public key** by the named subject of the certificate.

- **Cache:**

In computing, a **cache** is a hardware or software component that stores data so that future requests for that **data** can be served faster.

- **Carrier:**

A **mobile carrier** is a wireless service provider that supplies cellular connectivity services to mobile phone and tablet subscribers. The cellular company you pay for your cell phone usage is either a **mobile carrier** or a **mobile virtual network operator (MVNO).**

- **Certificate Validation:**

The process of verifying and validating the originality of a **digital certificate** is known as certificate validation. There are various complex steps involved in validating a digital certificate.

- **Code Injection:**

Code Injection is the general term for attack types which consist of injecting code that is then interpreted/executed by the application. This type of attack **exploits** poor handling of **untrusted data**.

- **Code Tampering:**

Tampering is the process of changing a mobile app (either the compiled app or the running process) or its **environment** to affect its behavior. For example, an app might refuse to run on your **rooted/jailbroken** test device, making it impossible to run some of your tests.

- **Cross Site Scripting:**

The **Cross-Site Scripting (XSS)** attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. **XSS** attacks occur when an attacker uses a web application to send malicious code, generally in the form of a **browser side script**, to a different end user.

- **Cryptography:**

Cryptography is a method of protecting information and **communications** through the use of codes so that only those for whom the information is intended can read and process it. The prefix "**crypt**" means "hidden" or "vault" and the suffix "**graphy**" stands for "writing."

D

- **Data Breach:**

A **data breach** is an incident that exposes confidential or protected information. A **data breach** might involve the loss or theft of your Social Security number, bank account or **credit card** numbers, personal health information, passwords or email. A **data breach** can be intentional or accidental.

- **Debugging:**

Debugging is the process of finding and resolving defects or problems within a **computer program** that prevent correct operation of computer software or a system.

- **Digital Media:**

The **Digital media** are any media that are encoded in machine-readable formats. Digital media can be created, viewed, distributed, modified and preserved on digital electronics devices. Examples of digital media include software, digital images, digital video, video games, web pages and websites, social media, digital data and databases, digital audio such as MP3, and electronic books.

- **Dynamic Testing:**

Dynamic testing is a term used in software engineering to describe the testing of the **dynamic**

behavior of code. That is, **dynamic analysis** refers to the examination of the physical response from the system to **variables** that are not constant and change with time.

E

- **Emulators:**

In computing, an **emulator** is hardware or software that enables one computer system to behave like another computer system. An emulator typically enables the **host system** to run software or use peripheral devices designed for the **guest system**.

- **Exploitation:**

A **computer exploit**, or **exploit**, is an attack on a **computer** system, especially one that takes advantage of a particular vulnerability the system offers to intruders.

F

- **Forensic Testing:**

Inspection of a **computer** system and its contents for **evidence** or supportive **evidence** of a **crime** or other **computer** use the application of **computer** investigation and analysis techniques in the interests of determining potential legal **evidence**.

G

- **GDPR:**

The **General Data Protection Regulation** 2016/679 is a regulation in EU law on data protection and privacy in the **European Union** and the **European Economic Area**. It also addresses the transfer of personal data outside the EU and EEA areas.

H

- **Hybrid Development:**

When the core of the application is written using web technologies (HTML, CSS, and JavaScript), which are then encapsulated within a **native application**, it is called a **hybrid mobile app**. Through the use of plugins, these applications can have full access to the mobile device's features.

I

- **Insecure Deserialization:**

Insecure Deserialization is a vulnerability which occurs when untrusted data is used to abuse the logic of an application, inflict a **denial of service (DoS)** attack, or even execute arbitrary code upon it being **deserialized**.

J

- **Jailbreak:**

Jailbreaking is the privilege escalation of an Apple device for the purpose of removing software restrictions imposed by Apple on **iOS**, **iPadOS**, **tvOS**, and **watchOS** operating systems. This is typically done by using a series of **kernel patches**.

- **JWT:**

The **JSON Web Token (JWT)** is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a **JSON** object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret or a public/private key pair.

M

- **MASVS:**

The **OWASP Mobile Application Security Verification Standard (MASVS)** is, as the name implies, a standard for mobile app security. It can be used by mobile software architects and

developers seeking to develop secure **mobile applications**, as well as security testers to ensure completeness and consistency of test results.

- **MiTM Attack:**

In **cryptography** and **computer security**, a **man-in-the-middle (MiTM)** attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

- **MSTG:**

The **Mobile Security Testing Guide** is a comprehensive manual for mobile app security testing and reverse engineering for **iOS** and **Android** mobile security testers.

- **MVNO:**

A **mobile virtual network operator** is a wireless communications services provider that does not own the wireless network infrastructure over which it provides services to its customers.

N

- **Native Development:**

An application that has been written using the native development language and tools specific to that platform is called a **native mobile application**. For example: A native iOS application would be written in either Swift or Objective-C and compiled using **Xcode**, while a native Android application would have been developed using Kotlin or Java and compiled using **Android Studio**.

- **Network Interception:**

An **interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a **network.**

- **Network Testing:**

Network testing is an investigation conducted to provide **stakeholders** with information about the quality of the product or service under test. Network testing can also provide an objective,

independent view of the network to allow the business to appreciate and understand the risks of **network implementation**.

O

- **OEM:**

An **original equipment manufacturer (OEM)** is a company that produces parts and equipment that may be marketed by another manufacturer.

- **Operating System:**

An **operating system (OS)** is system software that manages computer hardware, software resources, and provides common services for computer programs.

- **OWASP:**

The **Open Web Application Security Project (OWASP)** is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

P

- **Payload:**

The **payload** is the part of transmitted data that is the actual intended message. Headers and **metadata** are sent only to enable payload delivery. In the context of a computer virus or worm, the payload is the portion of the **malware** which performs malicious action.

- **Penetration Testing:**

Penetration testing, also called **pen testing** or ethical hacking, is the practice of **testing** a computer system, network or web application to find security vulnerabilities that an attacker could exploit. **Penetration testing** can be automated with software applications or performed manually.

- **Piracy:**

Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software.

- **Public Key Cryptography:**

Public-key cryptography, or **asymmetric cryptography**, is a cryptographic system that uses pairs of keys: **public keys**, which may be disseminated widely, and **private keys**, which are known only to the owner.

- **Proxy:**

In computer **networking**, a proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from **servers** that provide those resources.

R

- **Reverse Engineering:**

Reverse engineering is about looking at a program from the outside in — often by a third party that had no hand in writing the original code.

- **Root:**

Rooting is the process of allowing users of smartphones, tablets and other devices running the **Android** mobile operating system to attain privileged control over various **Android subsystems**.

S

- **Security Vulnerability:**

A **vulnerability** is a weakness which can be exploited by a cyber-attack to gain unauthorized access to or perform unauthorized actions on a computer system. **Vulnerabilities** can allow attackers to run code, access a system's memory, install malware, and steal, destroy or modify sensitive data.

- **Source Code:**

Source code is any collection of code, possibly with comments, written using a **human-readable programming language**, usually as plain text. The source code of a program is specially designed

to facilitate the work of computer programmers, who specify the actions to be performed by a computer mostly by writing source code.

- **SSL:**

SSL, or **Secure Sockets Layer**, is an encryption-based Internet security **protocol**. It was first developed by **Netscape** in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern **TLS** encryption used today.

- **Static Testing:**

Static testing is a **software testing** method that involves examination of the program's code and its associated documentation but does not require the program be executed.

- **System Logs:**

The system log file contains events that are logged by the **operating system** components. These events are often predetermined by the **operating system** itself. System log files may contain information about device changes, **device drivers**, system changes, events, **operations** and more.

T

- **Third-party Components:**

A third-party software component is a **reusable software** component developed to be either freely distributed or sold by an entity other than the original vendor of the **development platform**.

- **TSL:**

The **Transport Layer Security**, and its now-deprecated predecessor, **Secure Sockets Layer (SSL)**, are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and **Voice over IP (VoIP)**.

U

- **UNIX Shell:**

A **UNIX shell** is a command-line interpreter or shell that provides a command line user interface for Unix-like operating systems. The shell is both an interactive command language and a scripting language, and is used by the **operating system** to control the execution of the system using shell scripts.

- **UX/UI:**

UX design refers to the term “user experience design”, while **UI** stands for “user interface design”. Both elements are crucial to a product and work closely together.

V

- **VPN:**

A **virtual private network**, or **VPN**, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from **eavesdropping** on the traffic and allows the user to conduct work remotely.

X

- **Xcode:**

Xcode is an integrated development environment for **MacOS** containing a suite of software development tools developed by Apple for developing software for MacOS, iOS, iPadOS, watchOS, and tvOS.

References

1. https://developer.android.com/studio/command-line/adb
2. https://www.mulesoft.com/resources/api/what-is-an-api
3. https://whatis.techtarget.com/definition/attack-surface
4. https://searchsecurity.techtarget.com/definition/attack-vector
5. https://en.wikipedia.org/wiki/Authentication
6. https://en.wikipedia.org/wiki/Certificate_authority
7. https://en.wikipedia.org/wiki/Cache_(computing)
8. https://www.lifewire.com/what-is-a-mobile-carrier-2373339
9. https://www.geocerts.com/blog/understanding-ssl-certificate-authentication-validation
10. https://owasp.org/www-community/attacks/Code_Injection
11. https://mobile-security.gitbook.io/mobile-security-testing-guide/general-mobile-app-testing-guide/0x04c-tampering-and-reverse-engineering
12. https://owasp.org/www-community/attacks/xss/
13. https://searchsecurity.techtarget.com/definition/cryptography
14. https://www.lifelock.com/learn-data-breaches-data-breaches-need-to-know.html
15. https://en.wikipedia.org/wiki/Debugging
16. https://en.wikipedia.org/wiki/Digital_media
17. https://en.wikipedia.org/wiki/Dynamic_testing
18. https://en.wikipedia.org/wiki/Emulator
19. https://searchsecurity.techtarget.com/definition/exploit
20. https://searchsecurity.techtarget.com/definition/computer-forensics
21. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
22. https://ionicframework.com/resources/articles/what-is-hybrid-app-development
23. https://www.acunetix.com/blog/articles/what-is-insecure-deserialization/
24. https://en.wikipedia.org/wiki/IOS_jailbreaking
25. https://jwt.io/introduction/
26. https://owasp.org/www-project-mobile-security-testing-guide/
27. https://en.wikipedia.org/wiki/Man-in-the-middle_attack
28. https://en.wikipedia.org/wiki/Mobile_virtual_network_operator
29. https://www.informit.com/articles/article.aspx?p=680830&seqNum=2
30. https://netbeez.net/blog/why-network-testing-is-important/
31. https://en.wikipedia.org/wiki/Original_equipment_manufacturer

32. https://en.wikipedia.org/wiki/Operating_system
33. https://en.wikipedia.org/wiki/OWASP
34. https://en.wikipedia.org/wiki/Payload_(computing)
35. https://searchsecurity.techtarget.com/definition/penetration-testing
36. https://www.pandasecurity.com/mediacenter/panda-security/software-piracy/
37. https://en.wikipedia.org/wiki/Public-key_cryptography
38. https://en.wikipedia.org/wiki/Proxy_server
39. https://securitytoday.com/articles/2019/02/26/reverse-engineering-is-one-of-your-best-weapons-in-the-fight-against-cyberattacks.aspx
40. https://en.wikipedia.org/wiki/Rooting_(Android)
41. https://www.upguard.com/blog/vulnerability
42. https://en.wikipedia.org/wiki/Source_code
43. https://www.cloudflare.com/learning/ssl/what-is-ssl/
44. https://whatis.techtarget.com/definition/static-testing
45. https://www.webopedia.com/TERM/S/system_log.html
46. https://en.wikipedia.org/wiki/Third-party_software_component
47. https://en.wikipedia.org/wiki/Transport_Layer_Security
48. https://en.wikipedia.org/wiki/Unix_shell
49. https://careerfoundry.com/en/blog/ux-design/the-difference-between-ux-and-ui-design-a-laymans-guide/
50. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html