Christopher Foley

Z15092976

Assignment 3

Q1. In databases accessed in our company we can control authorization in the user interfaces connected to the DBMS through a local area network. Can we do the same in the web browser, i.e., when the user fills a form to define an SQL query we could check if he is or not authorized to access what he has requested? This would eliminate SQL injection attacks. Evaluate this idea.

We could create a web interface that securely connects to the data base and parses the input parameters. It could be created to validate the user and their access rights. This would ensure that form created input is valid. However this would not eliminate SQL injection attacks from sources not under the control of the web server.

A key element in security is to check at all points of access, the proposed method will prevent users who use the provided web interface from accessing improper data, but it does not eliminate threats from outside web interface.

The Equifax fiasco is a perfect example of this. The Web based interface gave users access to the data, and validated that they had rights to access the data they requested. Due to misconfiguration and poor planning, hackers who sent queries outside the web browser bypassed any forms based protection and were able to access data without respect to security.

Q2. Compare the security of iPhone X to Google Nexus 6P.

Consider their features and decide if one of these phones is more secure than the other. Consider their complete architectures and use security patterns to evaluate their security (using patterns is easier to find missing defenses than looking at implementation details), Completeness and references matter in your answer.

Initially announced in 2015 the Google Nexus 6P is a pure Android device from Huwaei. Originally released with Android Marshmallow it may be updated through regular patches to Android Oreo.[1] The iPhone X was released in 2017 by Apple. Both have similar features, yet there are differences:[2]

Feature	Android	IOS	Notes
Screen Lock	Passcode, biometric id	Passcode, biometric id	Frequently disabled by users, causing data security breach
Data partitioned	Limits access between users/apps	Limits access between users/apps	
Limited Hardware Access	No direct access, only through OS	No direct access, only through OS	
Application Distribution	Multiple Sources	Only Apple Store	Multiple sources provide multiple ways to inject malicious application
Encryption	Various Levels	Various Levels	Data synced to PC is frequently transmitted as plain text
Security Testing	Must be provided by vendor	Done by Apple. Apple has approved then disapproved apps.	Multiple sources provide security breach. Both stores have had security breaches.
UI	Customizable by Seller	Apple provided	
OS	Open Source available for inspection	Core modules are open source Linux, however most is proprietary	
Updates[3]	Google updates monthly, only Nexus and Pixel users get update automatically	Frequently done.	
	Controlled by users and	Triggered by Apple	See [4] for chart showing

[1] "Everything You Need To Know About the Nexus 6P", https://www.androidcentral.com/nexus-6p accessed 13 Nov 2017.

[2] "Comparing Android and iOS Security", CA Technologies, https://www.veracode.com/resources/android-ios-security

[3] "Android vs. iOS Security: Compare the Two Mobile Oses", searchmobilecomputing.techtarget.com

Feature	Android	IOS	Notes
	service providers.		OS fragmentation in 2016.
Permissions	Set by user at Install	Checks permissions at run time. Dialog requests access.	
Application Install	Permits remote installation, but prompts phone to accept, remote install/run not possible	Install by apple.	
Geolocation	Separate application	Allows phone to be located if lost.	
Erasure of user data	May be triggered by user	Triggered by user or 10 incorrect entries on Keypad	
Hardware	Various	Tightly controlled by apple	

Analysis, the industry seems to believe that iOS is more secure as evidenced by bounty programs.[5] However, it should be noted that more devices run Android than iOS. Of particular interest is the Apple Vs. Android study (2017) published by Moon Technolabs Pvt Ltd & Android Pub, which indicates that while Android is used in more phones than iOS, Android use is highly fragmented and may represent a security problem.[6]

As a Blackberry 10 user, I regret that I must conclude that iOS is more secure than Android due to the following reasons:

- Closed source OS
- Tight control over hardware/software
- Single source software
- device encryption
- erasure after 10 failed pass code attempts.

[4] “The State of Mobile Device Security: Android vs. IOs“, http://www.zdnet.com/article/the-state-of-mobile-device-security-android-vs-ios/

[5] “Android vs. iOS: are iPhones Really Safer?”, https://www.barrons.com/articles/android-vs-ios-are-iphones-really-safer-1496254475

[6] “”, https://android.jlelse.eu/apple-vs-android-a-comparative-study-2017-c5799a0a1683

One constant theme in Mobile Device security was that the weakest point in the security is always the USER due to:

- poor passwords (weak or non existent) [7]
- insufficient screening of apps loaded by users.[8] It is estimated that 30% of phishing emails are opened.

Additional References:

Schmerl B. et al. (2016) Architecture Modeling and Analysis of Security in Android Systems. In: Tekinerdogan B., Zdun U., Babar A. (eds) Software Architecture. ECSA 2016. Lecture Notes in Computer Science, vol 9839. Springer, Cham

“The State Of Mobile Device Security”, http://www.zdnet.com/article/the-state-of-mobile-device-security-android-vs-ios/

[7] “Spaceballs Luggage Password”, https://youtu.be/_JNGI1dI-e8

[8] Futurama clip, “Perform Virus Scan – I’m waiting for porn here”, https://youtu.be/UO7W_dmndiY