CERIAS

The Center for Education and Research in Information Assurance and Security

Verifying End-Users' Security & Privacy: Mobile Application Developer Software Trends

Oyindamola Oluwatimi

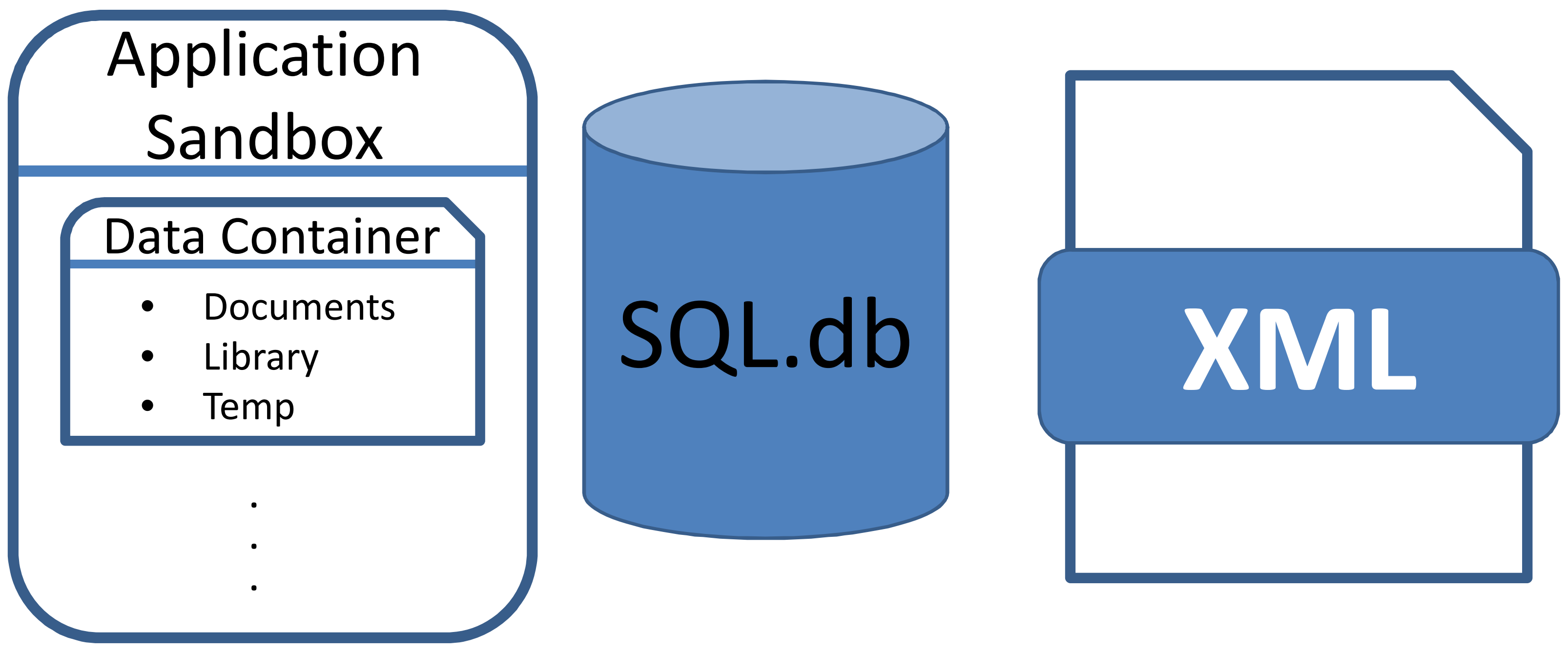
(Work in Progress)

Background: Companies that build software-based products strive to produce new and exciting solutions that incorporate the latest and greatest technology trends, and most often, security is an afterthought in the software development life-cycle. That is, mobile app developers are so focused on the implementation of new features in their mobile apps that they do not consider, or simply ignore, that each new added feature expands the attack surface of the application. Such lack of concern for security can also be attributed to (and highly evident in) software developers publishing brand new applications.

Measure of Success: In order to determine if applications store sensitive information, we must understand what sensitive is or could be. We define ''sensitive information'' as any set of information a user deems confidential, private, or as something that must be kept secret. A very common violation of users' security and privacy is the storing of usernames and passwords in plaintext form. Plaintext is simply text in a clear and human-intelligible format rather than ciphertext which is the opposite. An attacker could use this information to impersonate the original user. Other information that could be leveraged maliciously could be credit card information, purchase history, location-based information, etc.

Entities on the iOS Platform to Investigate

- Application Sandbox
- SQLite Databases
- Property Lists (XML)



Problem: End-users are potentially open for attack by cyber criminals that exploit security vulnerabilities in mobile apps. Cyber criminal organizations may realize that attacking the platform can yield significant results by stealing sensitive information that is stored by mobile applications such as banking data or medical data[1].

Much research has been conducted that investigate the necessary and basic set of security and privacy practices to adhere to when developing mobile apps in order to protect end-users. The objective for this work can be summarized with the following question: *do recently published applications adhere to any of the established security and privacy practices developed to protect users from malicious exploit by cyber criminals*? The author also analyzes popular and well-established mobile apps for the purpose of a comparative analysis with recently published apps.

System Setup:

Application	Release Date
Facebook	2008-07
Snapchat	2011-09
Trump Wall	2016-03-04
Space Adventure Frozen Time	2016-03-04
Damn Daniel	2016-03-07

The applications investigated in this work and their release date.

iPhone 4 OS:	Version 7.1.2 (11D257)
Operating System:	Windows 10 Enterprise version 1511
Host Platform:	iMac Desktop
Processor:	Intel Core i3 CPU
Ram:	8.00 GB
MPE+:	Version 5.6.0.8

Information regarding various components of investigative system. MPE+ : Mobile Phone Examiner Plus

1. Morrissey, S. (2010). iOS Forensic Analysis for iPhone, iPad, and iPod Touch. In (pp. 25–66)

PURDUE
UNIVERSITY