intertrust®

Report

Secure Systems

Security report on global mHealth apps 2020

Contents

Introduction

Mobile technology has revolutionized how patients receive medical care. Patients can now track sleeping patterns, consult with doctors, check records and test results, order prescriptions, and conduct multiple other medical activities—all from their mobile devices. They can even monitor and manage critical health parameters, such as glucose levels or heart rhythms, in real time.

On the clinical side, mobile technology facilitates internal communication and workflow efficiency while vastly improving patient care, outcomes, and reach. Critical patient data sits at physicians' fingertips and they can diagnose and manage care for patients that do not have local access to medical services.

Given the operational benefits and revenue-generating opportunities that mobile apps bring to healthcare, it's no surprise that the global mHealth market is projected to nearly double over the next two years, reaching more than $130 billion by 2022.[1] And those are pre-pandemic projections. The figures will likely end up much higher with the push to reshape care delivery under COVID-19. Some providers are reporting a 50 to 175 times increase in virtual healthcare visits.[2]

In the rush to leverage care-improving technologies, organizations often prioritize speed over security—with potentially devastating consequences.

Compromised mobile apps can be used to access credentials and keys, compromise patient data, steal proprietary algorithms, or even interfere with medical device operation. In the latest Verizon Mobile Security Index, 85% of healthcare organizations acknowledged that a security breach could seriously compromise patient care. Yet 37% of these same organizations admitted sacrificing mobile security to "get the job done."[3]

To uncover the greatest threats to medical application security, Intertrust audited a cross-section of mobile apps on both the iOS and Android platforms, including COVID-tracking apps. This report presents the results of that analysis, together with a deeper look at the most prevalent and serious medical app security risks. It also provides strategies to help mHealth app developers and healthcare organizations mitigate vulnerabilities and risk.

Key findings

Today's mHealth apps are at risk

The assessment revealed major security gaps in mobile medical apps across the board.

71%
of apps have at least one high level vulnerability

91%
of apps fail cryptographic tests

28%
of iOS apps are vulnerable to encryption key extraction

85%
of COVID-tracking apps leak data

34%
of Android apps are vulnerable to encryption key extraction

83%
of high-level threats could have been mitigated using in-app protection

The changing mobile medical app industry

Mobile health and medical apps have had a tremendous impact on the ability to deliver quick, affordable, and reliable health care services.

They also play a critical role in preventative healthcare, with apps for diabetes and asthma care, cardiac rehabilitation, and pulmonary rehabilitation, projected to save the U.S. healthcare system $7 billion per year in fewer hospital admissions and readmissions.[4]

Prior to 2020, the mHealth field was steadily expanding, with a CAGR around 21%,[5] but the COVID-19 pandemic has forced both a rapid acceleration and shift in priorities. In 2019, just 11% of patients used telehealth. By April 2020, it jumped to 46%.[6] Use of mobile apps for prescription refills also skyrocketed, with, for example, U.S. drugstore chain CVS reporting double-digit increases.[7] Most recently, we've seen the advent of COVID-19 contact-tracing apps, opening up an entirely new sector of mHealth apps.

Types of mHealth apps

Excluding general consumer apps such as fitness trackers, diet and nutrition apps, and knowledge repositories, mobile healthcare applications can be roughly segmented into four categories: health-commerce apps, medical devices, telemedicine / patient engagement, and the most recent, COVID-tracking. Some overlap exists, for example telehealth might cover medical device apps for remote patient monitoring.

Health commerce

Health commerce apps largely consist of pharmacies and medical device companies selling products and refilling prescriptions online. In addition to personal information like name, email, physical address, and phone number, these apps may access highly sensitive prescription, medical insurance, and payment information like credit card numbers.

Medical device apps

Medical device apps connect to and work in tandem with a medical device, or transform the mobile device itself into a medical device. These include everything from apps that collect and transmit device data, to those that control the delivery of insulin by sending signals to an insulin pump or CGM, to apps that turn a phone into an electronic stethoscope. In general, mobile medical apps are subject to the same type of regulations as the connected or related medical device.

Telemedicine and patient engagement

Telemedicine apps use video, remote monitoring, and other technologies that allow healthcare institutions to evaluate, diagnose, and treat patients remotely. Patient engagement generally refers to the more administrative aspects such as scheduling appointments, medication adherence, and paying bills. Many customer-facing medical provider apps encompass both. While the use of such apps was already rising, COVID-19 drastically pushed forward patient and provider adoption.

COVID-tracking apps

With governments still trying to get COVID-19 under control, they have partnered with technologists to build apps and systems to identify and notify those who have come into contact with a carrier, as well as trace quarantine compliance. These apps collect personal data including a citizen's identity, live location, address, and, in some cases, payment history.

The need to rapidly deploy such apps often means there is a lower priority placed on privacy and security. A security flaw in Qatar's contact tracing app potentially exposed the sensitive data of more than one million users,[8] while the Indian government's contact tracing app initially leaked location data,[9] and the UK's NHS had to abandon its contact tracing app due to multiple security issues discovered during its trial run.[10]

Mobile medical app security

Contact tracing apps are not the only type of healthcare app that faces significant security challenges. In fact, healthcare organizations are attacked at more than double the average rate of other industries and stolen healthcare records bring the highest prices on the dark web, with some netting close to $1,000 depending on the completeness of information.[11]

For healthcare organizations, the consequences of a security compromise can be catastrophic, impacting patient health and safety as well as privacy. As a result, medical application vendors are subject to some of the strictest compliance requirements. GDPR, UL 2900-1, HIPAA, EU Medical Devices Regulation, In Vitro Diagnostic Medical Devices Regulation, ISO/IEC 27001, and other regulations, require healthtech vendors to protect data and establish processes to ensure system security. Vendors must be aware and address the risks of storing patient data and facilitating financial transactions through their platforms. Similarly, securing the communications between mobile apps, medical devices, healthcare institutions, and servers, is critical.

Mobile device safeguards and limitations

Mobile device manufacturers and vendors build security mechanisms into their devices, in the form of embedded cryptographic processors and trusted execution environments (TEE), which applications can access via services such as Android Keystore or Apple Secure Enclave. These mechanisms seek to allow applications to safely create cryptographic keys and perform cryptographic functions. Most mobile OSes also support application isolation to prevent apps from viewing or modifying another application's code or data.

Such keystores offer a degree of security. However, they are not available on every device and a lack of standardization across TEEs means that security levels may vary across devices. Moreover, mobile OSes contain numerous security flaws—in 2019 Google patched 461 critical and high-risk vulnerabilities, while Apple fixed 196.[12] Even hardware security can be hacked using side channel attack methods, like differential power analysis (DPA), to extract keys. And in July 2020, hackers found a permanent vulnerability in Apple Secure Enclave, which could put encryption keys at risk.[13]

Jailbroken or rooted devices pose another real threat. Healthcare app providers have no control over the device their application is installed on and once a device is jailbroken or rooted, OS-level security controls are compromised.

Since medical mobile apps store sensitive information, act as an accessory to medical devices, or both, it is important to always practice defense in depth and backstop any device-provided security with embedded software security mechanisms such as application shielding technologies and white-box cryptography.

OWASP Top 10 Mobile risks

M1: Improper Platform Usage
M2: Insecure Data Storage
M3: Insecure Communication
M4: Insecure Authentication
M5: Insufficient Cryptography
M6: Insecure Authorization
M7: Client Code Quality
M8: Code Tampering
M9: Reverse Engineering
M10: Extraneous Functionality

Mobile medical app threats

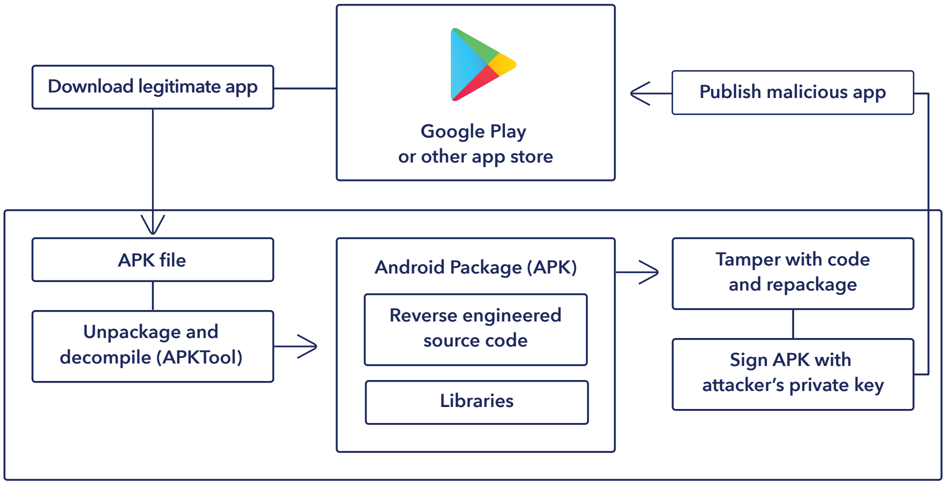
The high value of medical records has made healthcare organizations the most targeted industry for cyberattacks. The 2019 HIMSS Cybersecurity Survey found that 82% of hospitals suffered a "significant security incident" in the past 12 months. An increasing number can be linked to mobile devices–mobile-related healthcare compromises jumped by 52% over the past year, accounting for 38% of incidents.[14]

Ransomware poses another serious threat, as the need for healthcare organizations to maintain continuous access to medical records means that most will pay up immediately. When a ransomware attack on the NHS shut down hospitals across the UK, thousands of patient appointments and surgeries had to be canceled or transferred to other clinics. Recently the ante has been upped with double-extortion ransomware, where attackers penetrate and hide on networks, steal valuable data, and later deploy the ransomware payload. The stolen data is used to pressure the victim organization into paying the ransom. In an April 2020 report, researchers warned that the combination attack is now moving to mobile devices.[15]

Medical app security risks

Vulnerabilities and security flaws within medical mobile applications are also putting patient information and healthcare organizations at risk. The Open Web Application Security Project (OWASP) identifies and publishes a list of the top security risks to mobile apps.[16] Data leakage, insecure communications, authentication and authorization issues, weak cryptography, and susceptibility to code tampering and reverse engineering pose the greatest threats. Attackers can leverage these to steal information and secret keys, develop competing applications using your code and IP, and hijack applications for malicious purposes. For example, malware on the device can intercept and modify application API calls to manipulate data in transit.

A sample healthcare app attack flow


Download legitimate app
Google Play
or other app store
Publish malicious app
APK file
Unpackage and decompile (APKTool)
Android Package (APK)
Reverse engineered source code
Libraries
Tamper with code and repackage
Sign APK with attacker's private key

How secure are today's mHealth apps?

Given the unprecedented growth in mHealth applications, the rise in threats to these apps, and the consequences of a security compromise, Intertrust decided to test the security level for 100 popular healthcare apps.

What we measured and why

Security assessments were conducted on 100 publicly available mHealth apps from four major categories: health-commerce, medical devices, telemedicine / patient engagement, and COVID-tracking. All apps were downloaded directly from their respective stores (Apple Inc.'s App Store® and Google Play™). Apps were selected based on the critical and sensitive data they possess, the number of downloads, and the size of the organization. All apps were analyzed using both static application security testing (SAST) and dynamic application security testing (DAST), based on OWASP guidelines. Assessments were performed by a third-party security provider, Appknox, using their Vulnerability Assessment solution.

Threats were classified as None, Low, Medium, and High according to the Common Vulnerability Scoring System (CVSS). See the Appendix for classification details and a complete list of tested vulnerabilities.

Top threats detected

While most of the tested vulnerabilities were detected in multiple apps, some threats stood out in terms of severity, prevalence, or both.

Storing information in SharedPreferences

SharedPreferences are a set of APIs in Android that allow apps to store and retrieve data from the device. Unencrypted sensitive information should never be stored in SharedPreferences as the data is readily readable and editable by attackers and malicious apps. This medium severity issue falls within the OWASP Mobile Top 10 category M2, Insecure Data Storage, and violates HIPAA 164.312(a)(1) regarding safe access control. Of the Android apps tested, 60% were found vulnerable to this issue.

Weak derived crypto keys

The predominant Android Java Security API defaults to using ECB block cipher mode for AES encryption, which is less secure than other methods as it results in the same ciphertext for identical blocks of plain text. Developers that rely on the default OS-provided encryption process run the risk of information and code theft. This high severity issue falls within the OWASP Mobile Top 10 category M5, Insufficient Cryptography, and violates HIPAA 164.312(a)(1) regarding safe access control. Of the Android apps tested, 34% were found vulnerable to this issue.

Misconfigured App Transport Security (ATS)

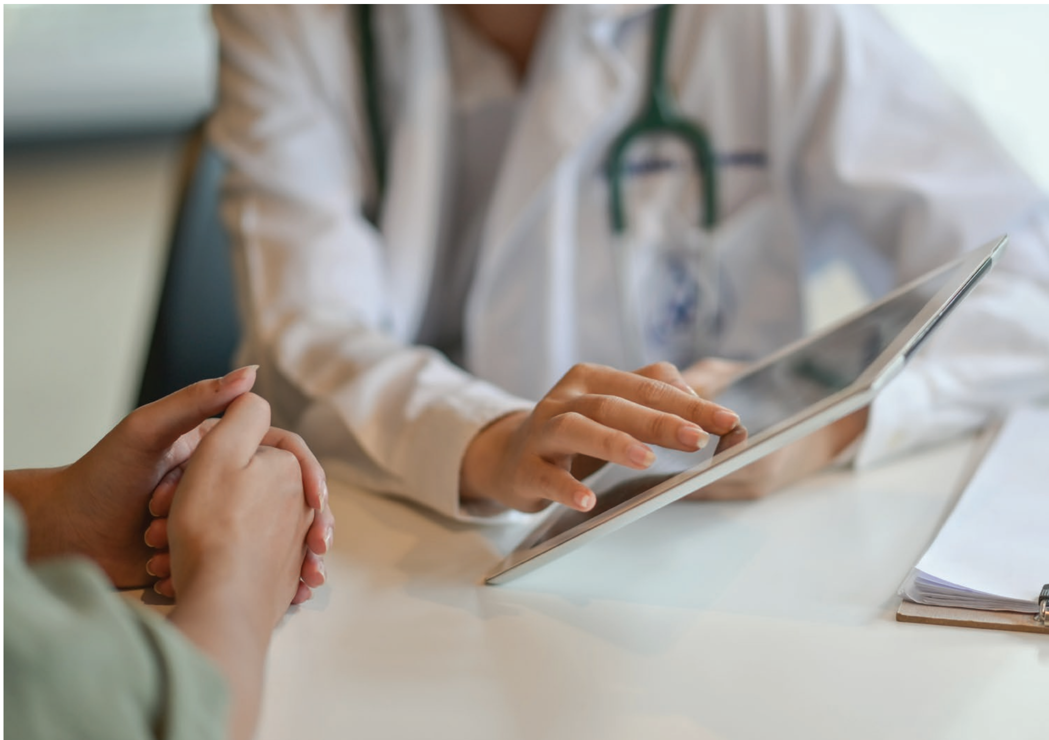
Approximately 70% of all tested iOS apps were found to have misconfigured ATS, an iOS networking security feature that ensures network connections employ the most secure protocols and ciphers. When used incorrectly, data can be intercepted and exploited. This high severity issue falls within the OWASP Mobile Top 10 category M3, Insecure Communication, and violates HIPAA 164.312(e)(1), regarding transmission integrity and encrypted transmission of ePHI.

Disabled SSL CA validation and certificate pinning

Pinning associates a host with their expected X509 certificate or public key. The most secure certificate pinning method adds the certificate or public key to the application at development time. If certificate pinning is poorly implemented, attackers can use false credentials to access traffic between the application and the web server and steal confidential data. This medium to high severity issue falls within the OWASP Mobile Top 10 category M3, Insecure Communication, and violates HIPAA 164.312(e)(1), regarding transmission integrity and encrypted transmission of ePHI. Approximately 80% of tested Android apps either did not implement certificate pinning at all or implemented it insecurely.

Sensitive information in SQLite3 databases

Approximately 40% of tested Android apps and 58% of iOS apps stored unencrypted sensitive information in an SQLite3 database. SQLite3 databases are used by applications to store persistent or temporary data for later use. SQLite3 does not have built-in support for encryption, which means sensitive information is stored in plain-text unless custom encryption mechanisms, such as white-box cryptography, are being used. If the local device is compromised then the stored data is easily compromised. This is considered a medium severity issue within the OWASP Mobile Top 10 category M2, Insecure Data Storage, and violates HIPAA 164.312(a)(1) regarding safe access control.



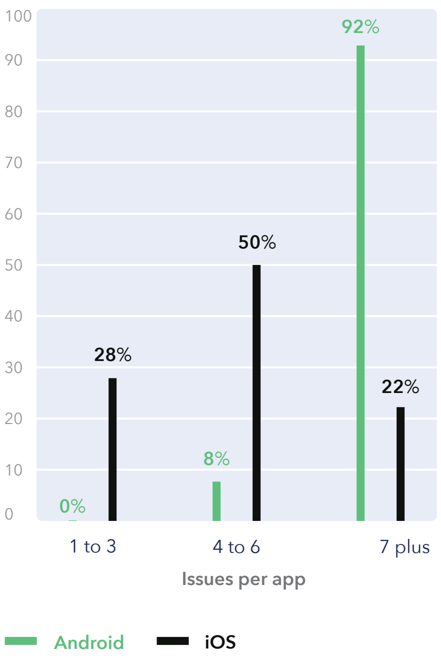
Detailed findings

Every app had at least one basic security issue, more than 90% had cryptographic issues, and 71% contained flaws that present high-level risks to healthcare organizations and their patients.
This indicates that despite increased awareness of healthcare cyberthreats and tightened regulations, mHealth security is not keeping up with the pace of development. Across all four application categories, we found widespread insecure coding practices and a general lack of application security controls and in-app technology protections such as application shielding, runtime application self-protection (RASP), and white-box cryptographic key protection.

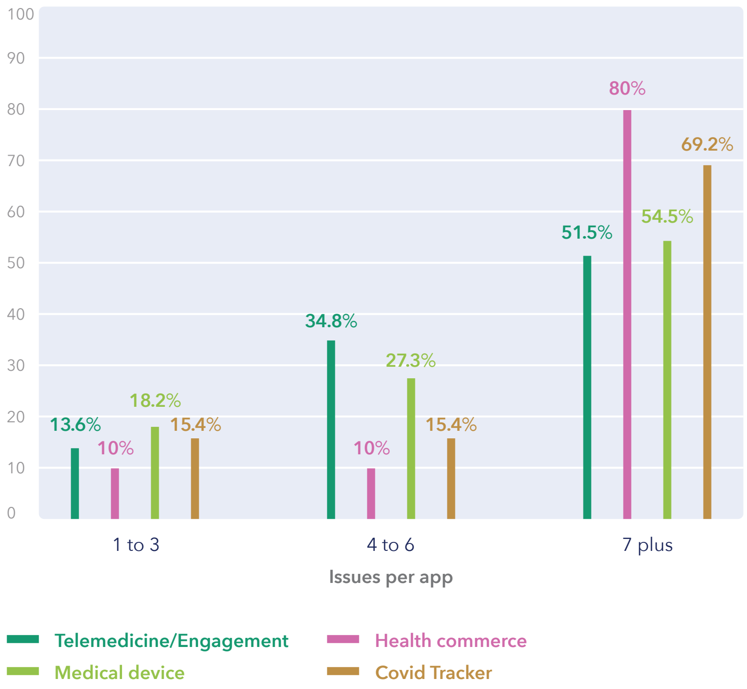
Number of vulnerabilities

A total of 741 vulnerabilities were discovered across the 100 apps. When looking at vulnerabilities on a per app basis, every Android app and 72% of iOS apps had four or more security flaws. Android apps had far more issues than iOS apps. Across the different mHealth app categories, health commerce apps had the most security issues (90% with four or more issues per app), followed by telemedicine/patient engagement apps (86.4%), COVID trackers (84.6%), and medical device apps (81.2%).

Number of issues per app by OS



Number of issues per app by app type

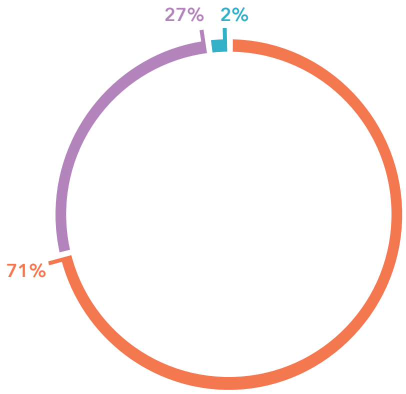


Breakdown by severity level

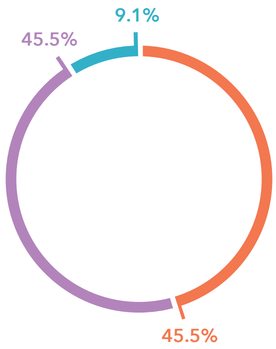
71% of all apps had at least one threat of high severity. When looking at the different mHealth app categories, telemedicine/patient engagement apps had the greatest percentage of apps with at least one high severity vulnerability (80.3%), followed closely by health commerce apps (80%), then medical device apps (45.5%). Surprisingly, COVID-tracking apps had the smallest percentage of apps with a high severity vulnerability (38.5%).

Severity level

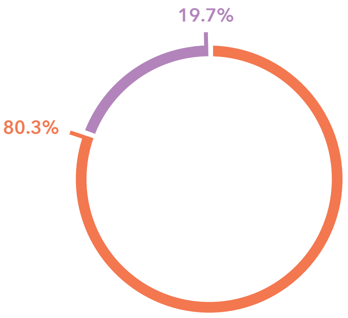
▬ High ▬ Medium ▬ Low or none



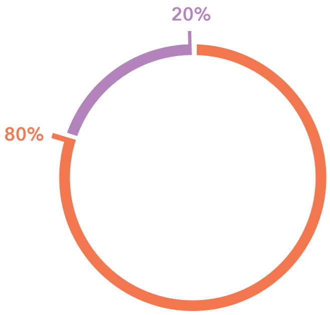
Apps with at least one high severity vulnerability



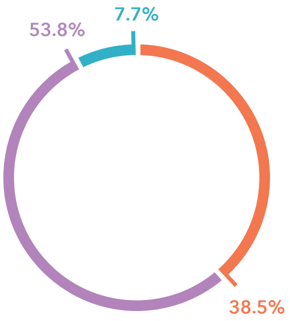
Medical device apps with at least one high severity vulnerability



Telemedicine/patient engagement apps with at least one high severity vulnerability



Health commerce apps with at least one high severity vulnerability

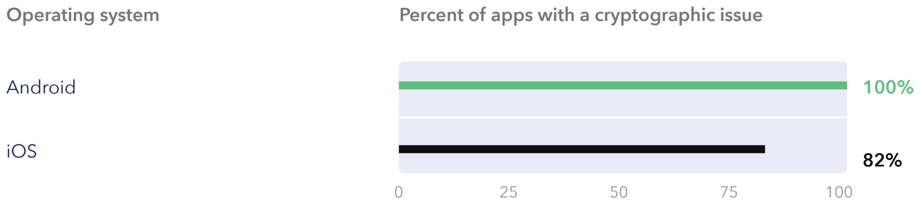


Covid tracking apps with at least one high severity vulnerability

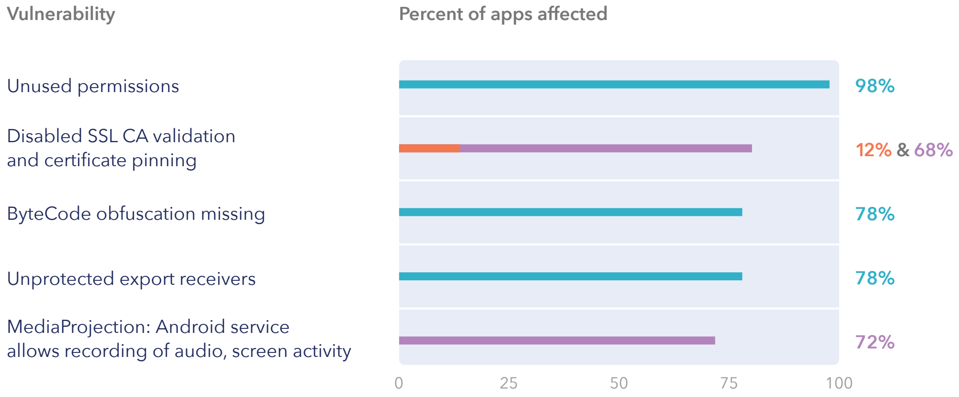
Cryptographic issues

91% of tested apps had at least one cryptographic issue including exposed encryption keys, poor implementation of cryptographic algorithms, insufficient key size, and failure to securely encrypt the communication of sensitive data. Susceptibility to cryptographic key extraction falls within this class of vulnerabilities.

The analysis found that 34% of Android apps and 28% of iOS apps are vulnerable to cryptographic key extraction. Across the app types, a full 40% of health commerce apps, 30.3% of telemedicine/patient engagement apps, 27.3% of medical device apps, and 30.8% of COVID-tracking apps are vulnerable to cryptographic key extraction.



Top 5 threats Android

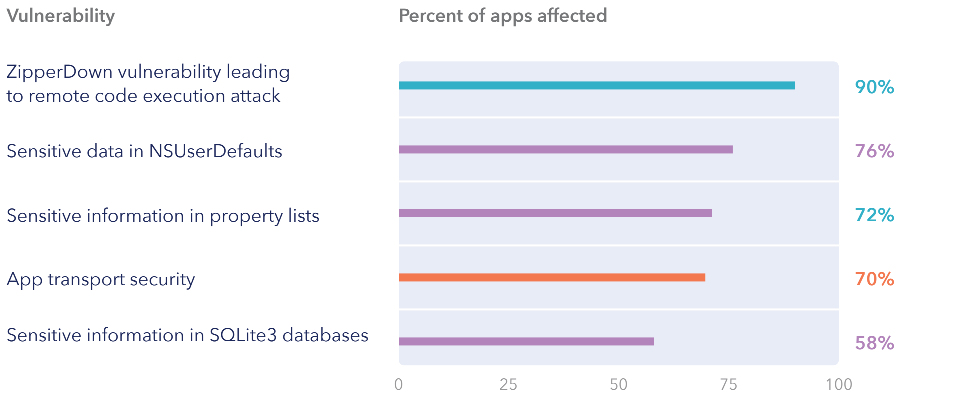


Severity level

🟧 High 🟪 Medium 🟦 Low

Note: Our analysis revealed an usually high number of mHealth apps with the issue "MediaProjection: Android Service Allows Recording of Audio, Screen Activity" (72%). By comparison, our report on financial services apps found that only 32% had this issue.[17] The most likely reason for this discrepancy is that media projection is a necessary functionality for telehealth apps. However, this data shows it is being insecurely implemented on the majority of mHealth apps, which could allow sensitive information and sessions to be captured if installed on devices running Android OS versions 5 through 7.

Top 5 threats iOS



Building a more secure mHealth app

As revealed by this assessment, despite some of the strictest industry regulations, healthcare and medical apps have serious security gaps that can put patient data, privacy, and health outcomes at risk.

There is a disconnect between the level of mobile threat concern expressed by healthcare organizations–73% rated the risk to their organization as moderate to significant[18]–and the level of security of the apps they and their patients use.

The growing demand and complexity of medical mobile services, combined with the evolving threat landscape and the high sensitivity of data collected, make it imperative to eliminate or mitigate any application vulnerability. Best practices dictate a multi-pronged approach to strengthen security while continuing to efficiently service patients in a changing healthcare landscape.

Approach security holistically

While embedded device protection systems provide security advantages, they are not enough. Combine hardware security with proven software security, like application hardening and key protection solutions, to build a more robust and reliable security infrastructure. Routinely educate staff, patients, and partners on good security practices and implement policies that bring stronger security without significantly impeding productivity or efficiency.

Implement secure application design

Healthcare app developers need to be aware of and follow secure app design practices. For example, do not store critical information on the device unless necessary; make sure all data the app receives is subject to input validation; use strong encryption methods implemented correctly; store passwords only when protected by strong encryption. Following a DevSecOps framework will build security into the development lifecycle.

Comply with regulations

Governmental bodies such as the FDA, and regulations such as GDPR, UL 2900-1, HIPAA, EU Medical Devices Regulation, US Postmarket Management of Cybersecurity in Medical Devices, In Vitro Diagnostic Medical Devices Regulation, ISO/IEC 27001, and others, require medical application vendors to protect data and establish processes to ensure system security, including testing for and addressing vulnerabilities. Non-compliance puts both healthcare organizations and their patients at risk.

Strengthen apps with application shielding

Even following secure design practices, it's impossible to eliminate every application vulnerability. Application shielding, also called in-app protection, protects vulnerabilities from attack by hardening the application code so that it's much more difficult to penetrate, modify, or reverse engineer. It involves a number of protective techniques including code obfuscation, anti-debugging, iOS jailbreak and Android rooting detection, integrity protection, and tampering detection and response. The most robust tools shield applications from both static and dynamic threats as well as sophisticated side-channel attacks like DFA and DPA, making it a reliable first line of defense.

Protect secrets and keys

Encryption protections are useless if the encryption keys are compromised. Too often, they are hard-coded into applications where hackers can easily extract them, or are exposed in memory as they are being used in cryptographic operations. OS provided Keystores provide some protection, but their security is negated on jailbroken or rooted devices. Organizations can build powerful software-based key protection into their apps using white-box cryptography.

Embed trusted identities into medical devices using PKI

Many of the technological innovations in healthcare are powered through the internet of things (IoT), which requires interconnectivity and communication between devices, applications, and other systems. It is essential that medical devices carry cryptographically secure device identities to authenticate, control access, and securely interact within the medical ecosystem. Public key infrastructure (PKI) technology can be used to provision trusted identities into IoT medical devices.

Conclusion

The rapid expansion of mHealth and the high value of healthcare data means that threats are becoming more frequent, more complex, and more difficult to prevent using standard security measures.

Data breaches cost healthcare providers an average of $7.13 million per breach, the greatest of any industry and an increase of 10.5% over last year.[19] Yet, as our assessment indicates, the healthcare industry has failed to scale up its application security practices. Recommended improvements and mitigations include:

- Stop storing sensitive data in multiple insecure locations. This makes the data easy to extract and exploit. This information should be protected by obfuscation and secure encryption using technologies like white-box cryptography.
- The vast majority of mHealth apps (91%) have poorly implemented and/or weak encryption that puts them at risk for data theft and code manipulation. Key protection technologies such as white-box cryptography should be used to secure the encryption process.
- Nearly every healthcare application tested lacked safeguards to detect and stop analysis and reverse-engineering by hackers. Anti-tampering and run-time protections are critical here.

Intertrust can help

Intertrust's whiteCryption subsidiary provides advanced in-app protection and white-box cryptography solutions that protect patient data and proprietary algorithms, thwart attacks, and help you comply with healthcare regulations.

whiteCryption Code Protection embeds advanced security defenses into applications, enabling them to run securely in zero-trust environments. It uses multiple methods including advanced code obfuscation and real-time intrusion detection to prevent tampering, reverse engineering, and other techniques used by cybercriminals to discover vulnerabilities and gain access to sensitive information and IP contained in mobile health apps.

whiteCryption Secure Key Box is a state-of-the-art white-box cryptography library that keeps secret cryptographic keys protected within the app code, even during runtime. Extremely easy to integrate and use, it provides an extensive set of high-level classes and methods for operating with the most popular cryptographic algorithms across multiple platforms.

Intertrust Seacert provides cryptographically secure device identities so that healthcare and medical devices can safely interact within secure ecosystems. Seacert PKI service is both WebTrust compliant and ISO 9001:2015 certified.

intertrust.com/products/application-shielding

Appendix

Vulnerability scoring

Vulnerabilities were rated according to the CVSS which is based on exploitability, scope, impact, and other qualitative metrics.

CVSS Qualitative rating scale

Rating	CVSS score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

The collateral damage implication for each threat category can be broken down as follows:

Threat classification	Impact
None (N)	No potential for loss of assets, revenue or productivity
Low - Medium (L)	Slight damage to assets, or minor loss of revenue productivity
Medium - High (M)	Significant damage or loss
High (H)	Catastrophic damage or loss

Vulnerabilities tested and occurrence

Vulnerability	Severity level	Total
Weak derived Crypto Keys: Android	High	17
Javascript CORS enabled in Webview: Android	High	14
Insufficient transport layer protection: Android	High	12
Content provider file traversal vulnerability: Android	High	1
Disabled SSL CA validation and certificate pinning: Android	Medium to high	40
MediaProjection: Android service allows recording of audio, screen activity: Android	Medium	36
Application logs: Android	Medium	35
Storing information in SharedPreferences: Android	Medium	30
Insecure broadcast receivers registered dynamically: Android	Medium	23
Sensitive information in SQLite database: Android	Medium	20
Broken SSL trust manager: Android	Medium	16
Broken HostnameVerifier for SSL: Android	Medium	14
External data in raw SQL queries: Android	Medium	12
App extending WebViewClient: Android	Medium	12
Android component hijacking via intent: Android	Medium	11
WebView exploits: Android	Medium	3
HostnameVerifier allowing all hostnames: Android	Medium	3
Java object deserialization vulnerability: Android	Medium	1
Unused permissions: Android	Low	49
Unprotected exported receivers: Android	Low	39
Bytecode obfuscation missing: Android	Low	39
Enabled Android application backup: Android	Low	23
Unprotected exported service: Android	Low	23
Unprotected exported activities: Android	Low	17
Deprecated setPluginState in WebView: Android	Low	15
PhoneGap JavaScript injection: Android	Low	4
Unprotected exported provider: Android	Low	1
App transport security: iOS	High	35
Short HMAC Keys: iOS	High	4
Insufficient transport layer protection: iOS	High	2
UIWebView exploits: iOS	High	1
PhoneGap whitelist open access: iOS	High	0
Sensitive data in NSUserDefaults: iOS	Medium	38
Sensitive information in property lists: iOS	Medium	36
Sensitive information in SQLite3 databases: iOS	Medium	29
Insecure cryptographic keys: iOS	Medium	14
Debug logging with NSLog: iOS	Medium	7
Unsecured data in CoreData: iOS	Medium	6
Unsecured data in RealmDB: iOS	Medium	1
ZipperDown vulnerability leading to remote code execution attack: iOS	Low	45
Deprecated NSURLConnection: iOS	Low	13

Sources

1 https://www.statista.com/statistics/938544/mhealth-market-size-forecast-globally/

2 https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality

3 Mobile Security Index 2020: Healthcare spotlight, Verizon, 2020

4 The Growing Value of Digital Health, IQVIA Institute, November, 2017

5 mHealth Apps Market Size, Share & Industry Analysis, Fortune Business Insights, January 2020

6 McKinsey COVID-19 Consumer Survey, April 27, 2020

7 CVS Q1 2020 Earnings Presentation

8 Contact Tracing App Security Flaw Exposed Sensitive Personal Details of More Than One Million, Amnesty International on amnestyusa.org, May 26, 2020

9 https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html

10 Security analysis of the NHS COVID-19 App, Dr Chris Culnane and Vanessa Teague, May 19, 2020

11 https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

12 State of Enterprise Mobile Security, 2019 Report, Zimperium, February, 2020

13 https://9to5mac.com/2020/08/01/new-unpatchable-exploit-allegedly-found-on-apples-secure-enclave-chip-heres-what-it-could-mean/

14 Mobile Security Index 2020: Healthcare spotlight, Verizon, 2020

15 Ransomware Evolved: Double Extortion, Check Point Research, April 16, 2020

16 https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

17 Intertrust Security report on U.S. financial mobile apps 2020, Intertrust Technologies, 2020

18 Mobile Security Index 2020: Healthcare spotlight, Verizon, 2020

19 Cost of a Data Breach Report 2020, IBM Security, July, 2020

About Intertrust

Intertrust provides trusted computing products for leading corporations—from mobile, CE and IoT manufacturers, to service providers, and enterprise software companies. These products include the world's leading digital rights management (DRM), software tamper resistance, and technologies to enable secure data exchanges for various verticals including energy, entertainment, retail, automotive, and fintech.

Intertrust is headquartered in Silicon Valley with regional offices globally. The company has a legacy of invention, with fundamental contributions in computer security and digital trust. Intertrust holds hundreds of patents that are key to internet security, trust, privacy management, mobile code, networked operating environments, web services, and cloud computing.

Start protecting your applications today.
For a free trial of whiteCryption Code Protection, visit:
intertrust.com/code-protection-free-trial

intertrust®

Building trust for
the connected world.

Learn more at: intertrust.com/products/application-shielding
Contact us at: +1 408 616 1600 | info@intertrust.com

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085