intertrust®

Report

Secure Systems

The state of mobile app security 2020

Contents

Introduction

The mobile application industry now accounts for more than $150 billion of the global economy, spurred by an increasing number of apps and worldwide mobile adoption. With a market that large comes vulnerabilities, hacks and breaches, which are spawning a mobile application security industry that is projected to reach $8.2 billion by 2025.[1] According to Gartner, market demand for mobile app development services alone is growing five times faster than IT organizations' availability to deliver.

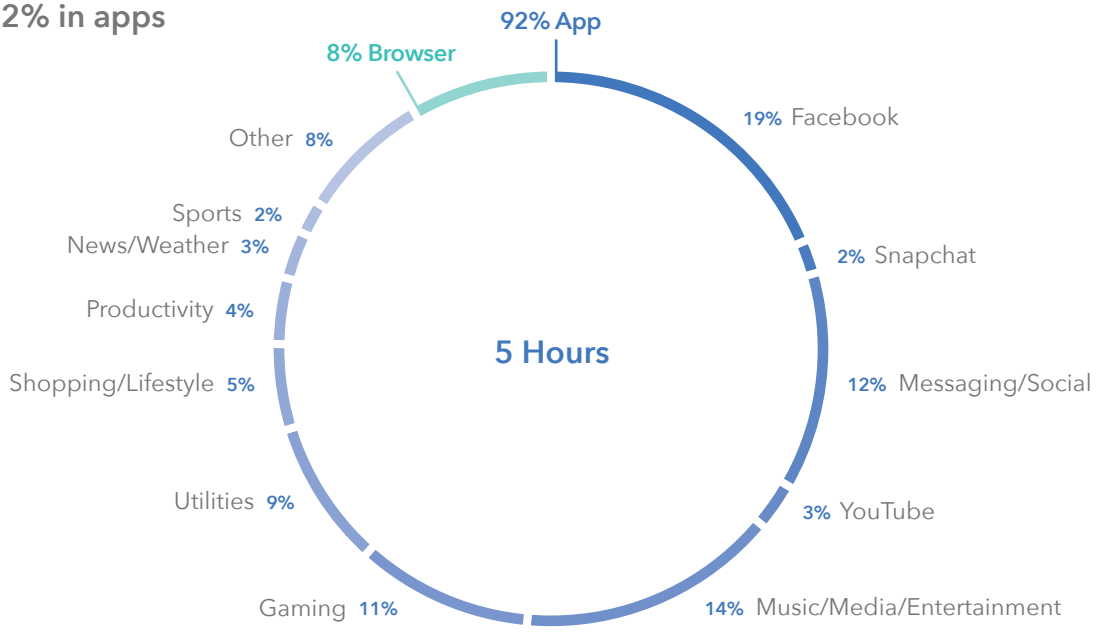
This report covers the role security plays within the mobile application market for 2020. It examines the cost of data breaches, different mobile operating systems and their vulnerabilities, a look at app security for the Internet of Things, and what developers can do to secure their apps.

The mobile application market

- The mobile application industry is expected to grow at a rate of 19.2% CAGR through 2023.
- Mobile phone sales stand at more than 1.7 billion units for 2019 (down slightly from 2018) and will reach nearly 1.8 billion units in 2020.[2]
- Employees today use three different devices in their daily routine, and are expected to increase the number of devices to five or six as the Internet of Things (IoT) becomes more widespread.
- The average mobile app user is spending over 4.6 hours per day[3] in apps with the mobile app market forecast to generate more than $156 billion per year in revenue by 2023.[4]

5 Hours daily spent on mobile devices with 92% in apps

Source: Flurry Analytics



The role mobile security plays

As the number of mobile applications continues to expand at a dizzying rate, the challenge to protect them becomes more difficult. More than one-third of enterprises were compromised last year due to a security incident involving a mobile device.[5]

Mobile security investment remains low across Fortune 500 companies. Many organizations are finding it difficult to be proactive, which results in tactical mobile apps rather than the necessary strategic approach. Often when apps are tactically developed, business needs and time to market are prioritized over security. An average of $34 million per company is spent annually on mobile app development, and only $2 million—or 5.5%—is spent on security.[6]

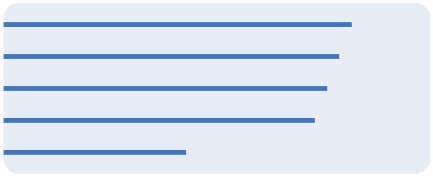
The majority of spending is allocated toward proprietary software and open source software security measures with only 11% spent on penetration testing to lower the risk of insecure applications.

The Open Web Application Security Project (OWASP) has identified the top 10 mobile app security risks. Of those identified, the most challenging to mitigate is broken cryptography, with 70% of respondents in a survey by the Ponemon Institute citing this as 'difficult' or 'very difficult.' Meanwhile, 65% rated unintended data leakage as 'difficult' to mitigate and 62% rated weak server side controls, followed by client side injection and poor authorization and authentication as concerns.[7]

Of the reasons that mobile apps contain vulnerable code, 69% cite pressures on the application development team to release apps quickly. The second most cited reason stems from accidental coding errors, followed by a lack of internal security policies.

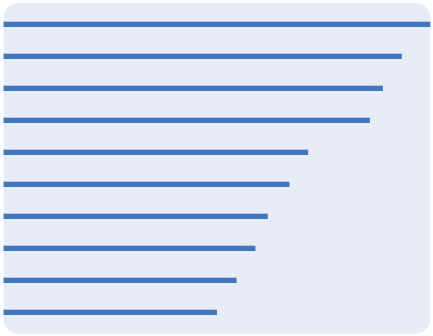
Top five means of securing mobile apps

Source: Ponemon Institute



How difficult is it to minimize the OWASP top 10 mobile app security risks?

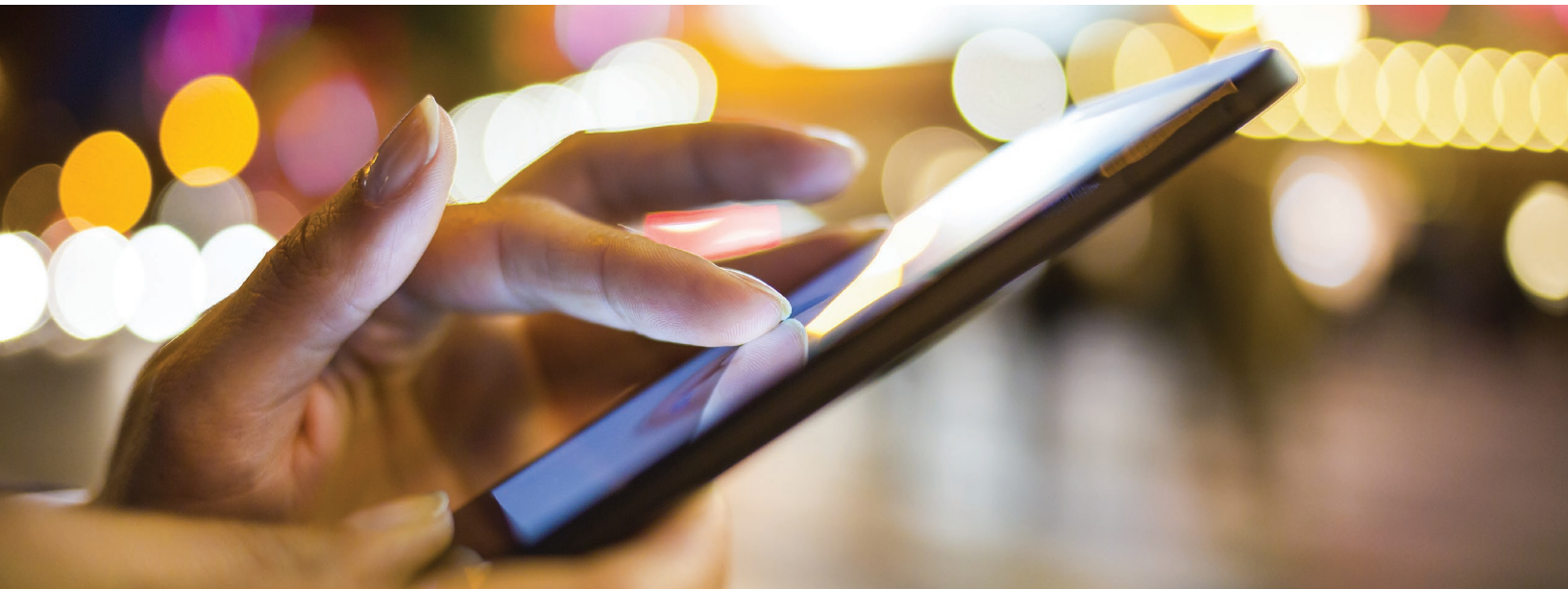
Source: Ponemon Institute



The four horsemen of mobile security

Mobile security usually falls into four categories: physical threats, network threats, malware and vulnerabilities.

1. **Physical threats:** Mobile device management is one way to manage devices that require the configuration of security policies such as password policies, device encryption, Wi-Fi settings and detection of jailbroken devices. Without such controls, mobile devices are vulnerable to unauthorized access and compromise of sensitive information.
2. **Network threats:** Mobile devices today connect 10 to 100 times more to networks than PCs. Wi-Fi networks are used to lift sensitive information such as keys and data, or intellectual property, and to reverse engineer apps. Traffic redirection, decryption and Man-in-the-Middle (MitM) attacks are also performed over Wi-Fi—even once the Wi-Fi is turned off.
3. **Malware:** Malicious downloads are some of the most prevalent methods for corrupting a device. Active threat detection can be added as well as risk-based mobile management for more advanced threats. It is also important to prevent jailbreaking, which breaks the security model, potentially allowing malicious apps to access data owned by other applications.
4. **Vulnerabilities:** Login-related weaknesses, such as bypassing login prompts, or allowing users to create weak passwords, are easy-to-crack vulnerabilities. Other common vulnerabilities include storing sensitive data on the device and transmitting it unencrypted, and cryptographic keys hard-coded into the app that can be easily accessed with hacking tools.



The cost of data breaches

The global average cost of a data breach has hovered around the $4 million mark for the past several years, with the average cost for each lost or stolen record currently at $150.[8] But while the average data breach cost has leveled out in recent years, the chance that an organization will be compromised is steadily increasing. According to the Ponemon Institute's 2019 Cost of Data Breach Study, the chance of experiencing a data breach within two years is nearly 30%, up from about 28% the year previously. Moreover, breaches are getting bigger—the average number of records breached is now more than 25,500.

Seven mega trends in data breaches

1. Data breaches are a consistent cost of doing business today. Organizations should build this permanent cost into their data protection strategies.
2. The largest consequence of a data breach is lost business. Following a data breach, organizations face a significant challenge in winning back customers' trust to sustain financial stability.
3. Malicious attacks have the highest cost per record and take the longest amount of time to repair. Most data breaches continue to be a result of malicious activity as opposed to human error or system glitches.
4. Detection and escalation costs have increased, suggesting investments are being made to detect and contain breaches.
5. Industries with the strictest regulations and fines, healthcare and financial services, have the highest cost per data breach.
6. Improvements to reduce the cost of data breaches include incident response plans, hiring a CISO, business continuity management strategy and employee training and awareness programs.
7. Investing in data loss prevention controls such as encryption and endpoint security is essential to prevent data breaches, as described in the next section.

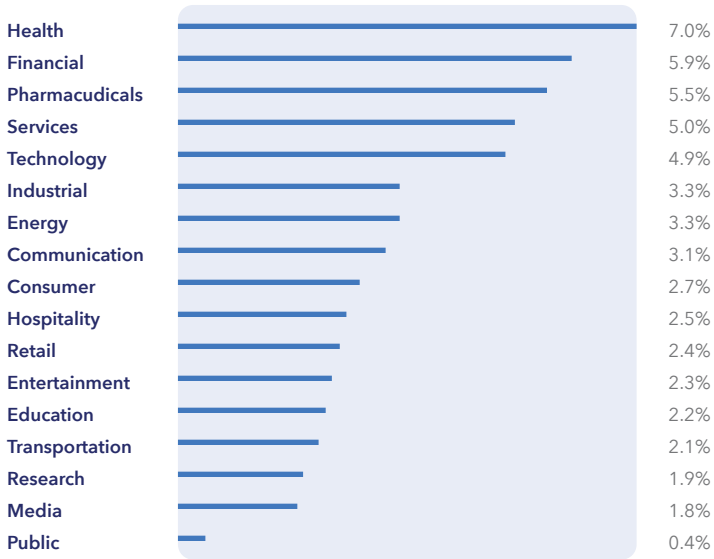
Recent data breach statistics

- Data breaches cost the most per record in the U.S. and Germany. With an average cost of $242 in the U.S. and $193 in Germany per record. However, the Middle East had the highest average number of records breached, putting it in second place for average organizational cost. Average organizational cost in 2019 was $8.19 million in the U.S., $5.97 in the Middle East and $4.78 million in Germany.
- The cost of lost business, including abnormal customer turnover, increased customer acquisition costs, business disruption, and system downtime, accounts for 36% of the total cost of a data breach at an average of $1.42 million.
- Healthcare had the highest cost per record by far at $429 compared to the average of $150 per stolen record. In financial, the average cost was $210 followed by technology at $183, and pharmaceutical at $178.
- Hackers and criminals caused the most data breaches with 51% of all breached records caused by malicious attacks.
- The cost for a data breach ranges from $2.2 million for a loss of less than 10,000 records to $6.4 million for a loss of 50,000 records or more.
- Health, financial, and pharmaceutical organizations experienced the highest abnormal churn following a data breach, evidencing the loss of customer trust.

Abnormal customer turnover by industry

3.9% global average

Source: Ponemon Institute



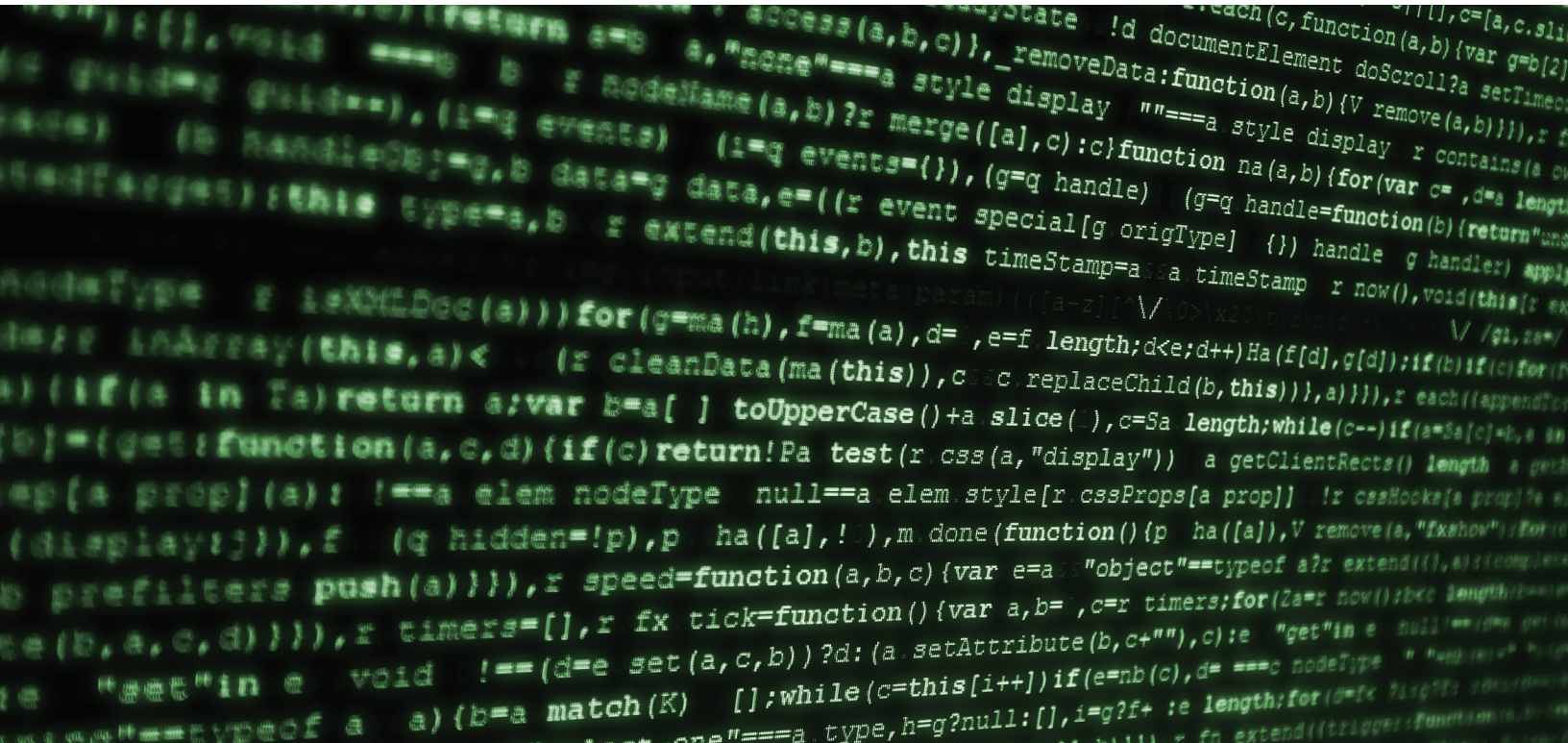
Broken cryptography in mobile apps

Mobile apps have become a primary target for malicious behavior. Meanwhile, the operating systems can't keep up. In the first half of 2019 alone, iOS and Android patches were released for 440 different security vulnerabilities.[9] In addition, according to Gartner, 75% of mobile apps would fail basic security tests.

Digging deeper, Veracode found that 83% of applications have at least one security flaw in their initial scan and 68% fail the OWASP Top 10, implying that many mobile and web-based applications contain critical security vulnerabilities. Cryptographic issues and information leakage are the top two flaws, with 62% of apps containing cryptographic issues.

The consequences of broken cryptography are especially problematic in healthcare applications as HIPAA requires personal health data meet higher standards for security and privacy. Doctors and medical centers increasingly employ mobile apps to address patient care issues and the majority of patients themselves use mobile health apps.

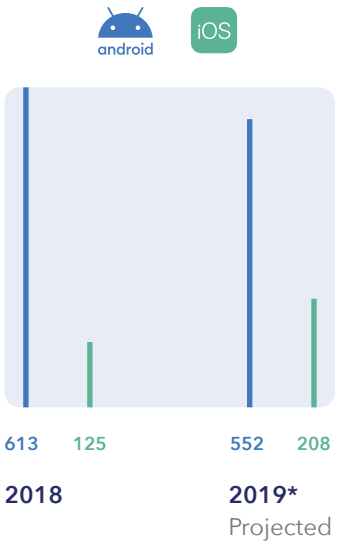
The Pew Research Center found that more than half of all smartphone users gather health data on their devices. The high prevalence of broken cryptography means there will be unintended data leakage and other issues as the demand for mobile healthcare applications continues to rise.



A closer look at iOS and Android

Mobile vulnerabilities by operating system published by CVE Details

Source: CVE Details



Many organizations assume iOS is a far more secure platform than Android. This common misconception started because iOS has more restrictive controls over developers and a strict vetting process to prevent malware. However, because application security must take place in the application or in the code, all OSes can be exploited unless additional security measures are in place. Both iOS and Android rank among the top five most vulnerable operating systems when looking at the total number of distinct vulnerabilities.[10] The Veracode report found that 91% of iOS applications and 95% of Android apps contain flaws. While these figures do not discriminate between high and low severity vulnerabilities, the information suggests there is an overwhelming need for hardened applications.

Android attacks become stealthier and more damaging

Android malware has steadily become more devious—and continues to cause more damage. Modern malware strains incorporate stealth techniques such as obfuscation that allow them to bypass signature-based security software. Despite Google's response to critical vulnerabilities and patches of critical issues in the Android OS, end users are still dependent on device manufacturers for these updates.

This was evident when seven vulnerabilities dubbed 'Stagefright,' in reference to libStagefright, the underlying code in the OS library shared by applications, could compromise devices by sending a malicious multimedia message. Stagefright was especially alarming as it did not require the user to download an infected app to receive the MMS message. The cybercriminal simply needed to know the intended target's phone number to launch the attack.

This attack brought to surface the delays involved when issuing updates as users remained at risk until carriers and manufacturers rolled out updates. In the interim, two more Android vulnerabilities were discovered, allowing an attacker to gain control over a compromised device through an .mp3 or .mp4 file. The previous patch had fixed the libStagefright library to where it no longer automatically processed messages; however, it was still possible for attackers to exploit libStagefright through the mobile browser. Dubbed Stagefright 2.0, these new vulnerabilities could be exploited through a man-in-the-middle (MitM) attack and through third-party applications.

Recently, Android has seen additional sophisticated attacks through a phishing Trojan that tricks users into entering their banking credentials. In this case, fake login pages pop up on top of legitimate banking apps.

iOS infiltrated on non-jailbroken devices

Apple's tight control over the app store and mobile operating system once kept threats to iPads and iPhones at a minimum. This no longer holds. A case in point is the August 2019 revelation of a two-year long iPhone hacking campaign that exploited fourteen different iOS vulnerabilities spread across five active attack chains.[11] The vulnerabilities affected almost every iOS version since iOS 10 and, once they gained access, attackers could monitor live location data and grab photos, contacts, and even passwords and other sensitive information from the iOS Keychain.

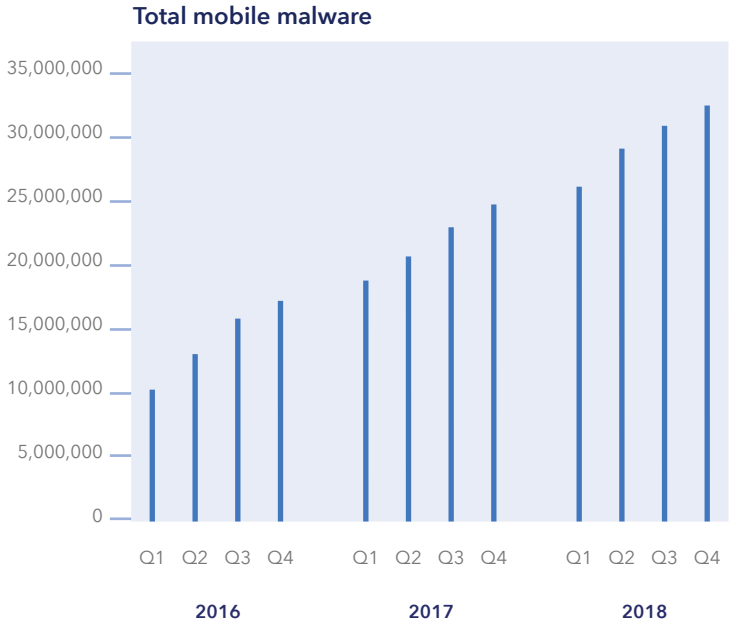
Another iOS threat, XcodeGhost, infected an estimated 4,000 apps before it was discovered in unofficial versions of Apple's integrated development environment (Xcode).

Developers using the infected environment were unknowingly allowing malicious code to be inserted into their official iOS applications. Once the infected app had been downloaded, XcodeGhost could perform actions such as creating fake phishing alerts to steal usernames and passwords, uncovering passwords copied from a password management tool or hijacking the browser to open specific URLs.

Neither of these threats required a jailbroken device, increasing their threat level. Even more alarming, an un-fixable exploit was recently discovered through reverse-engineering that could allow the jailbreaking of nearly every pre-2018 iOS device.[12]

Mobile malware threat statistics

Source: McAfee Labs



App security for the internet of things: from proof-of-concept to real-world attacks

The issues that stem from vendors implementing mechanisms are often used for proof-of-concept security flaws; however, it's inevitable that these will be followed by real-life attacks. Connected devices often lack security measures with many attacks able to exploit vulnerabilities in the underlying Linux-based operating systems used by IoT devices and routers. In the U.S., there are about eight online devices per person. With the Internet of Things, the astronomical number of sensors will generate a vast amount of data. IDC Research estimates 79.4 zettabytes by 2025 with 90% of the data processed locally. This amount of data, along with the poor state of security on connected devices, creates an easy target for cybercriminals.

Connected car

Today's car has the computing power of 20 personal computers and features more than 100 million lines of programming code. The connected car, controlled by software and high-tech features, may be one of the more significant advancements from the past few years. Features such as connected infotainment systems, web browsing, Wi-Fi access points, and remote-start mobile phone apps, help to enhance the enjoyment of the vehicle while adding more opportunities for advanced attacks.

According to a report by Upstream Security, 2019 saw 176 digital, electronic, and cyberattacks aimed at vehicles, more than doubling from the previous year.[13] One hacker reverse-engineered two GPS tracker apps and discovered that all customers are given a default password. He used this information to break into tens of thousand of accounts, allowing him to monitor vehicle locations and potentially turn off their engines while in motion.

"It seems that every time we introduce a new space in IT, we lose 10 years from our collective security knowledge. The Internet of Things is worse than just a new insecure space: it's a Frankenbeast of technology that links network, application, mobile and cloud technologies together into a single ecosystem, and it unfortunately seems to be taking on the worst security characteristics of each."

Daniel Miessler,
OWASP IoT Top 10 Project

We've also seen thieves hack keyless entry systems in the UK to steal cars as well as commercial vehicles like vans, taxis, and minibuses, demanding thousands in ransom for their safe return. Meanwhile, software recalls have doubled within the past year and soon they will match mechanical recalls.

Risks for connected cars

Stealing personally identifiable information (PII)
Connected cars collect a significant amount of data and interface with multiple after-market devices. For example, financial information, personal trip information, and diagnostics can all be accessed through a vehicle's system.

Manipulating a vehicle's operation
Catastrophic incidents resulting in personal injury, property destruction, and legal and brand consequences are closer than you'd think. Security researchers Charlie Miller and Chris Valasek demonstrated they could remotely hijack a Jeep's vehicle's systems while in operation.[14]

Unauthorized vehicle entry
Car thieves have new methods to break into locked vehicles including intercepting the wireless communication between the vehicle, or intercepting the fob for the driver. Many vehicle technologies have opted to replace physical ignition systems with keyless systems using mobile applications or wireless key fobs. In addition to gaining access to the vehicle, flaws in mobile apps have led to controlling features independently, as discovered when Nissan had to pull its NissanConnect EV app for the Nissan Leaf. The poor security of the app allowed security researchers to connect to the Leaf via the internet and remotely turn on the car's heated seating, heated steering wheel, fans, and air conditioning.

Common issues with app security and the connected home

Home automation

The convenience of controlling electronic locks, thermostats, ovens, sprinklers, and motion sensors by remote control has created new vulnerabilities in IoT cloud platforms. Cybersecurity researchers at the University of Michigan were able to hack into the leading 'smart home' automation system and obtain the PIN code to the home's front door. The 'lock-pick malware app' was one of four attacks aimed at a large consumer electronics manufacturer app store in what was believed to be the first platform-wide study of a real-world connected home system.

The targeted app store has more than 500 apps from third-party developers. When a security analysis was performed on the framework, they came up with four proof-of-concept attacks. In the first two, a door lock was exploited through the use of an app and PIN. In one scenario, the hackers could eavesdrop on the PIN code being set. The third was the ability to turn off vacation mode of the home through the app, and the fourth allowed a fire alarm to be set off.

Three common issues with app security and the connected home

1. Applications often request excess permissions beyond what is required to perform their function. Such 'over-privilege' puts sensitive data at risk.
2. Weaknesses in the TLS/SSL implementation can be exploited to eavesdrop on or compromise the integrity of communications between app and device. If an attacker gains access to the cryptographic keys, they can impersonate an authenticated device and decrypt sensitive data or even inject malicious code.
3. Weak cryptographic implementations can expose sensitive information or allow attackers to extract private APIs and secret keys that give them access to a device or cloud endpoint.

Mobile banking

Mobile banking is becoming the most important deciding factor when customers switch banks, with 60% of survey respondents citing this over fees (28%), branch location (21%) and services (21%).[15] The Federal Reserve notes that mobile banking use closely correlates with age, with 67% of individuals ages 18-29 using mobile banking, and 58% ages 30-44. Therefore, banking institutions that want to grow their customer base must offer mobile banking to cater to new customers. In addition to the demand for these services, there is an overwhelming awareness and concern around security and fraud. Among non-mobile banking users, more than 57% say mobile banking is unsafe, and an additional 18% state they don't know if mobile banking is safe or not.

In another study by Deloitte, of the respondents who do not use a mobile device for financial services, 61% cited security issues as the prime reason.

Since the first banking malware targeting mobile devices, dubbed Svpeng, was identified in 2014, mobile banking malware has grown exponentially. Today, there are more than 150,000 unique known mobile banking trojans, with many incorporating sophisticated evasive techniques that allow them to go undetected by security mechanisms. These include delaying execution to avoid sandbox detection, layered code obfuscation, and turning off anti-malware protections. Once in, they can steal payment data, credentials and funds from the victims' banks. Fraudulent banking apps are another rapidly growing attack vector.

Using your mobile phone, have you done these in the past 12 months?

Source: Federal Reserve

"Locking the door doesn't do any good if the key is under the doormat where anyone can find it."

Tony DeLaGrange,
Security Analyst

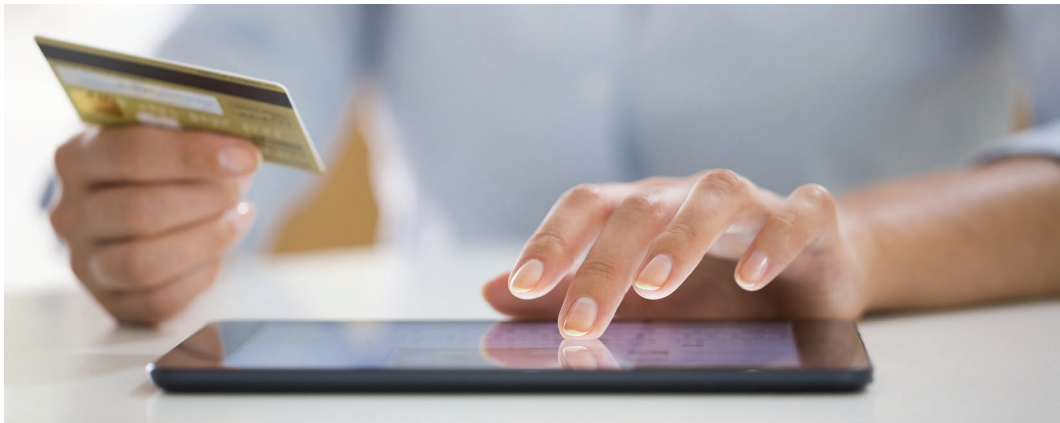
Cybercriminals can easily access an app, alter the code to perform malicious actions, re-package it, and upload to an app store for unsuspecting customers to download and install. A report from the Fraud and Risk Intelligence unit at RSA found attacks originating from fake apps that appear to belong to legitimate banks tripled in the first half of 2019 alone.

The main defense against mobile banking malware starts with mobile app developers who need to adequately understand the risks that proliferate in the mobile data, connections, and transactions ecosystem.

- Fake apps or hacked apps are an escalating security threat. Consumers who download fraudulent apps may expose sensitive financial information. Therefore, app developers must prevent reverse engineering through code level obfuscation and tamper resistant software protection.
- Many mobile banking apps lack adequate implementation of SSL (Secure Sockets Layer)/TLS (Transport Layer Security) or certificate validation. Use the two digital security protocols along with a mechanism to keep the keys secure to ensure server authenticity and to establish encrypted links including SSL/TLS.
- When an app is distributed to millions of devices and mobile banking users, it's not guaranteed that those devices are safe environments even when running security software. This is especially true with the trend toward jailbroken devices. By hardening the app with security services during the application development process, the app is able to bring security with it no matter where it goes.

How safe do people believe their personal information is when using mobile banking?

Source: Federal Reserve



Healthcare

Mobile device use in the healthcare industry has rapidly expanded over the past several years. In 2013, only eight percent of doctors used mobile devices to manage in-patient data. By 2016, the number had grown to 70%, and now an estimated 90% of healthcare providers are using mobile devices in their medical practice. Patients are also using their devices to make and confirm appointments and to access medical records through mobile apps. At the same time, the number of healthcare organization data breaches has jumped, with 89% of healthcare providers experiencing a data breach in the past two years. Of these, mobile-related breaches are growing the fastest—more than 25% of healthcare organizations suffered a mobile-related breach last year according to Verizon's Mobile Security Index 2019.

Healthcare providers must consider if the information and data they share, and how they share it, fall within HIPAA guidelines. There are significant fines and guidelines for failing to follow the rules. Yet, for many providers, their mobile device is a wild card, lacking the security measures and considerations given to other healthcare records, emails and sensitive conversations. Healthcare apps and insurance app developers should also consider if they are putting patients at risk.

In addition to mobile application data breaches, hospitals face catastrophic consequences through device tampering as their equipment continues to upgrade its mobile communications.

More than three-quarters of hospitals have invested in some form of mobile app to support communications between care team members.[16] Meanwhile, 82% of hospitals expressed 'grave concern' about the ability to support and protect mobile devices, patient data and hospital IT infrastructure as a result of the growing threat of cybersecurity attacks.

Whether it's device tampering, patient safety, or securing HIPAA patient data, mobile devices are the most vulnerable gateway since they are not the traditional endpoints in the cybersecurity chain, such as servers and internet within the IT perimeter.

- Mobile introduces bring-your-own device (BYOD), which opens up malicious Wi-Fi and cellular network-based attacks. Containerization and continuous VPN tunneling are more of an interruption to productivity and often cited as an infringement on privacy. Therefore, BYOD concerns are likely to persist.
- Hackers can trick healthcare providers into exposing passwords, insurance information and other data by introducing fake profiles run by the hacker.
- When an app is reverse engineered, the branding and IP are lifted from the app, causing the patient to potentially reveal their name, password, social security number and medical ID to a counterfeit app.

How to protect your patients, patient records, and health care organization

- The majority of FDA-approved apps lack application shielding and have insufficient transport layer protection. Applications should have in-app security measures to protect against threats in the highly distributed mobile environment.
- To protect patient data, it is essential to secure APIs that the mobile app uses to communicate with the server. Make sure to hide cryptographic keys within the application, and don't store the keys in memory, as this is a common path to back-end servers.
- Develop an app that stores the most sensitive information server-side rather than in the mobile app to reduce liabilities.

Drones

Drones, like other connected devices, can be hacked and turned to malicious purposes. Security researcher Nils Rodday demonstrated how easily this can be accomplished when he hijacked a drone by exploiting two security vulnerabilities, stating the drone was 'crackable in seconds.' The exact model of the drone is protected under NDA; however, the $20,000 model is commonly used for power-line inspections, professional photography and agriculture applications.

According to Rodday, the weak point in many drones is the failure to properly implement strong encryption between the drone and its controller module, leaving the drone open to an MitM attack. In another hack, the popular domestic Parrot Drone was the subject of security research when an expert from the firm Planet Zuda demonstrated a takedown of a Parrot A.R. exploiting the built-in Wi-Fi. It was discovered that anyone with a free Parrot app on a mobile device could control the Parrot drone while the Unmanned Aerial Vehicle is flying. The principle of the attack is to first disconnect the legitimate control app from the drone, then take control with an app from another device. With drones weighing up to 45 pounds and flying up to 55 mph, hacking these machines becomes a legitimate concern.

Entertainment

Global entertainment and media companies have increased their value through innovative global streaming services, programs, live concerts, daily behind-the-scenes interviews, live sports broadcasts, and a variety of music and news events that can be viewed on mobile devices. More importantly, consumers can now view specific entertainment content on their own devices just about anywhere, including planes, taxis, and other forms of public transportation.

To protect the content from being stolen, digital rights management (DRM) systems must be in place, and to protect the players' apps themselves, mobile security app solutions are a necessity. Developers should add a layer of protection to prevent hackers from reverse engineering and tampering with the service.

What developers can do

The mobile application industry is pushing forward a new level of interoperability that will require heightened security and privacy measures. App developers especially are in a position where they can reduce the number of vulnerabilities before the app ships.

App design

Make sure to design the app for secure data storage. For example, Starbucks was storing usernames, email addresses and passwords in clear text on the device, where a hacker could access the information by simply connecting the device to a PC. With many people using the same passwords for other accounts, this faulty storage approach had many far-reaching implications. To avoid this, design apps so that critical information is not stored on the device. iOS passwords should be stored in the encrypted data section in the iOS keychain.

'Less is more' with app design. To lower the risk of exposing sensitive data, minimize the amount of data exposed.

1. Enterprise mobile app data often stays server side and is only viewable within range.
2. Have IT teams mobilize only a handful of 'must haves' when it comes to Customer Relationship Management. Often, the stripped down app version works better than the full-blown version because it functions faster.
3. Consider using icons instead of text. For instance, instead of having a birthday in text, use a 'gift' icon.

Client side vulnerabilities

Source: Positive Technologies

60% of vulnerabilities are on the client side

89 %of vulnerabilities can be exploited without any physical access

56% of vulnerabilities can be exploited without administrator rights (jailbreak or root)

Server side controls

Depending on the view, server side may or may not fall under mobile security; however, it's important to make sure back-end services are hardened against malicious attackers. APIs should be checked and verified for proper security methods to ensure only authorized personnel have access. A number of back-end APIs wrongly assume that an app will be the only item that will access it; however, the servers the app is accessing should have security measures in place.

Untrusted inputs

A mobile app can accept data from all kinds of sources. Without sufficient encryption, attackers can modify inputs and environment variables. Ensure that all of the data the application receives from an untrusted third-party application can be subject to input validation.

Reverse engineering

Before a vulnerability is exposed, attackers can obtain a public copy of an application and reverse engineer it. Popular applications are often repackaged into 'rogue apps' containing malicious code and are posted on third-party app stores to lure unsuspecting users. The main reasons an app is reverse engineered is to expose sensitive information, such as the keys or data. The other is to lift or expose the intellectual property from the application binary to develop counterfeit apps. The best prevention from reverse engineering includes techniques such as code obfuscation, where the code is purposely obscured, and code flattening, which restructures the code to make it hard to decipher, despite operating the same way.

Broken cryptography

Broken cryptography usually occurs for one of two reasons. Either the app is using a weak algorithm for encryption and decryption, or the app is using a strong encryption algorithm but implementing it in an insecure way.

- Common mistakes for weak algorithms include usage of an algorithm not accepted by the security community such as MD5 for hashing. Always use state-of-the-art encryption APIs within mobile platforms and invest in manual analysis, such as penetration testing and threat modeling.
- Typical mistakes for key management include app key storage in the byte code. Many organizations use strong encryption algorithms, but implement their keys and certificates in areas that are vulnerable to attackers. When an app ships with the keys stored in the byte code, the keys are common across all app installs and can be easily decrypted.
- Many developers make the mistake of relying on OS encryption services. However, OS-level protections are highly vulnerable on a jailbroken or rooted device.

Unintended data leakage

Statistically speaking, one of the largest risks with mobile app security comes from data leakage and privacy invasive behaviors from legitimate applications. In an examination of 315,000 iOS and Android apps, 48% of iOS and 87% of Android apps leaked data. The percentages were much higher when looking at privacy invasive behaviors with 62% of iOS apps engaging and 86% of Android apps. Many advertisers, government agencies and hackers covet the personal information stored in apps. For example, one of the most popular gaming apps of all time was used for surveillance through third-party ad networks.

How Intertrust whiteCryption can help

All mobile app developers know that hackers will attack their apps' software instructions. whiteCryption by Intertrust provides the most advanced code obfuscation and white-box cryptography technologies that protect apps with sensitive information and thwart attacks on apps. Today, whiteCryption protects mobile payment apps, healthcare apps, smart car apps, connected home apps, and major media players. The applications are limitless, and as devices proliferate, whiteCryption is rapidly becoming the standard of care against app hacking.

whiteCryption protects mobile apps, desktop applications, firmware and embedded applications, and offers two security components—Secure Key Box and Code Protection.

Secure Key Box

whiteCryption Secure Key Box is a state-of-the-art white-box cryptography tool that keeps secret cryptographic keys well hidden 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, including ciphers, signing, verification, key generation, wrapping, unwrapping, digests and key agreements.

Code Protection

whiteCryption Code Protection injects self-defending capabilities into applications, enabling them to run securely in zero-trust environments. It prevents tampering, reverse engineering and other techniques used by cyber-criminals to gain access to sensitive information and resources contained in applications. whiteCryption Code Protection uses multiple techniques including code obfuscation, code flattening, and real-time intrusion detection to strengthen and deepen your app's security self-reliance.

Sources

1 Global Mobile Application Security Market Size and Forecast to 2025, Verified Market Research, 2018

2 Gartner Says Global Device Shipments Will Decline 3.7% in 2019, Gartner, 2019

3 U.S. Consumers Time-Spent on Mobile Crosses 5 Hours a Day, Flurry Analytics, 2017

4 The State of Mobile in 2019 – The Most Important Trends to Know, App Annie, 2019

5 Mobile Security Index 2019, Verizon, 2019

6 The State of Mobile Application Insecurity, Ponemon Institute, 2015

7 Study on Mobile and IoT Application Security, Ponemon Institute, 2017

8 Cost of a Data Breach Report 2019, Ponemon Institute and IBM Security, 2019

9 State of Enterprise Mobile Security, Zimperium, 2019

10 https://www.cvedetails.com/top-50-products.php?year=0, retrieved November 1, 2019

11 A very deep dive into iOS Exploit chains found in the wild, Google Project Zero, August, 2019

12 Unfixable iOS Device Exploit Is the Latest Apple Security Upheaval, WIRED, September, 2019

13 Global Automotive Cybersecurity Report, Upstream Security Ltd., 2020

14 Hackers Remotely Kill a Jeep on the Highway—With Me In It, Wired, July 21, 2015

15 Consumers and Mobile Financial Services 2016, Board of Governors of the Federal Reserve System, 2016

16 Clinicians Weigh-In on Clinical Communications and Workflow, HIMSS Analytics, 2017

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

intertrust®

Building trust for the connected world

Learn more at: intertrust.com
Contact us at: +1 408 616 1600

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085