Consolidated Edition

5th Annual State of Application Security Report

Perception vs. Reality

January 2016

ARXAN

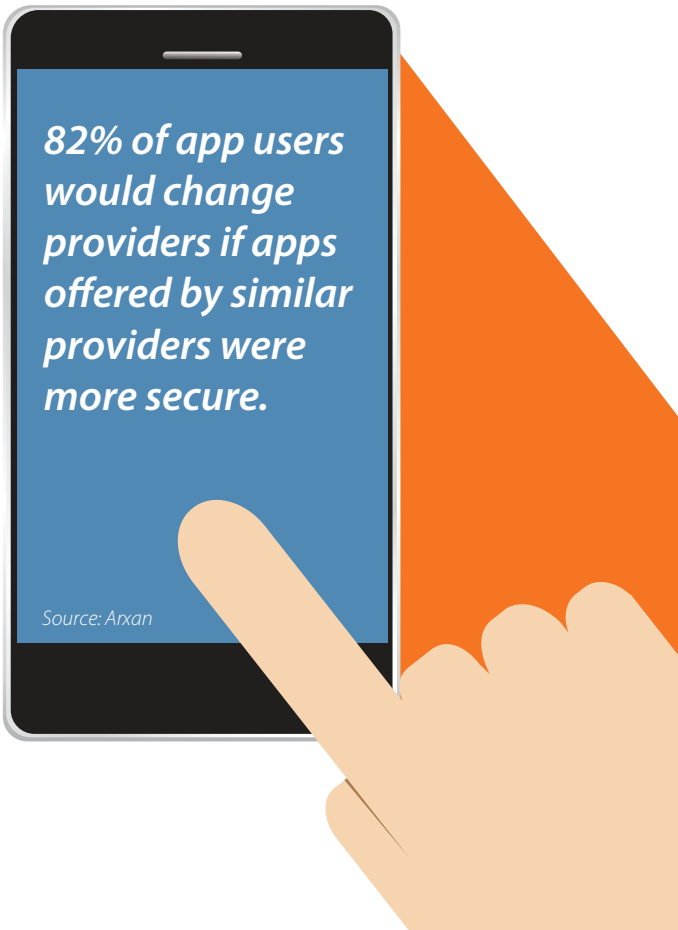
Table of Contents

Executive Summary

Nearly half (48%) of consumers who use mobile health and mobile finance applications expect their apps to be hacked within the next six months. So too do executive IT decision makers (46%) who have oversight or insight into the security of the mobile healthcare and mobile finance apps they produce. This sentiment makes it sound like mobile applications are at a hopeless state of security where, despite Herculean efforts to thwart attackers, adversaries are expected to prevail. But it's not hopeless. It's careless. Especially when you consider that 50% of organizations have zero budget allocated for mobile app security[1].

It is crucial for organizations with mobile apps to double-down on app security. Why? If they don't, they risk losing customers.

80% of consumers indicated they would change providers if they knew the apps they were using were not secure. And 82% of consumers would change providers if they knew alternative apps offered by similar service providers were more secure. While millennials are driving the adoption of mobile apps, their views on the importance of app security were equally as strong as the older non-millennials. In general, survey results showed very little geographical discrepancies across the US, UK, Germany, and Japan, and also very little discrepancy between health apps and finance apps. Interestingly, however, while the iOS operating system is often viewed as more secure than Android, iOS apps were shown to be more vulnerable than Android apps in this study.



Executive Summary (cont'd.)

So should we expect a critical mass of consumers to walk away from organizations because their mobile apps do not have the level of security protection they expect? Based on these research findings, perhaps. When put to the test, the majority of mobile apps failed security tests and could easily be hacked. Among 126 of the most popular mobile health and mobile finance apps tested for security vulnerabilities, 90% were shown to have at least two OWASP Mobile Top 10 Risks[2]. Such vulnerabilities could allow the apps to be tampered and reverse-engineered, put sensitive health or financial information in the wrong hands and, even worse, potentially force critical health apps to malfunction or redirect the flow of money. Surprisingly, US Food and Drug Administration (FDA)-approved apps and formerly UK National Health Service (NHS)-approved apps were among the vulnerable mobile health apps tested, indicating that there is more work to be done by governing bodies to better understand the cybersecurity threats to mobile apps and to improve the minimum acceptable security standards or regulations for mobile app development.

Mobile app security is becoming an increasingly important decision-making factor for consumers seeking to do business with organizations they can trust to protect their privacy and provide robust security. For businesses with mobile apps, this means that security can be used as a competitive differentiator to help attract and retain customers.

While it's clear *why* organizations should mitigate the security, financial, and brand risks associated with vulnerable mobile apps, it's less clear what organizations and consumers should do to improve protection. This report provides recommendations for how organizations and consumers can minimize the risk of their mobile apps being hacked.

Methodology

Arxan commissioned a third-party, independent research organization in November 2015 to undertake an electronic survey of 1,083 individuals in the US, UK, Germany, and Japan:

- 815 consumers who use mobile health and mobile finance apps
- 268 IT decision makers within organizations that produce mobile health and mobile finance apps and who also have oversight or insights into the security of those mobile apps

Also in October and November 2015, a third-party independent analysis of a total of 126 popular mobile health and mobile finance apps from each of the four countries was undertaken leveraging Mi3 Security solutions. Arxan selected the apps from among the most popular mobile health and finance apps for the Android and iOS platforms for each region. Included among the apps tested were 19 mobile health apps approved by the US Food and Drug Administration (FDA) and 15 mobile health apps that were previously approved[3] by the UK National Health Service (NHS).

The Findings

- *84% feel their mobile apps are adequately secure (83% consumers / 87% app execs)*
- *63% feel everything is being done to protect the mobile apps (57% consumers / 82% app execs)*

Source: Arxan

Folks *think* their apps are adequately secure.

Thumbs up — both consumers and IT decision makers with security insights into the mobile apps they develop strongly believe that their mobile apps are secure. In fact, the majority feel that app providers are doing everything they can to protect their apps.

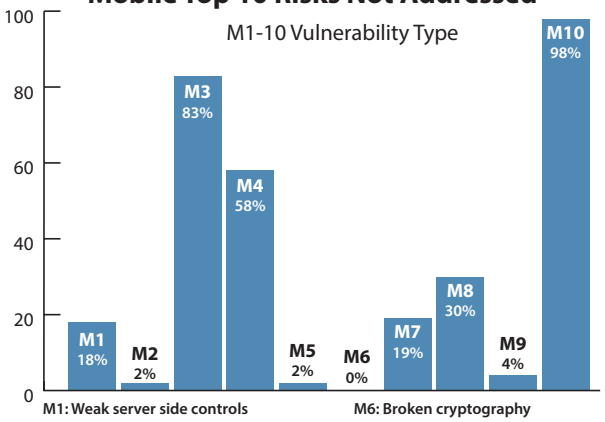
90% of 126 apps tested had at least two critical security vulnerabilities

Source: Arxan

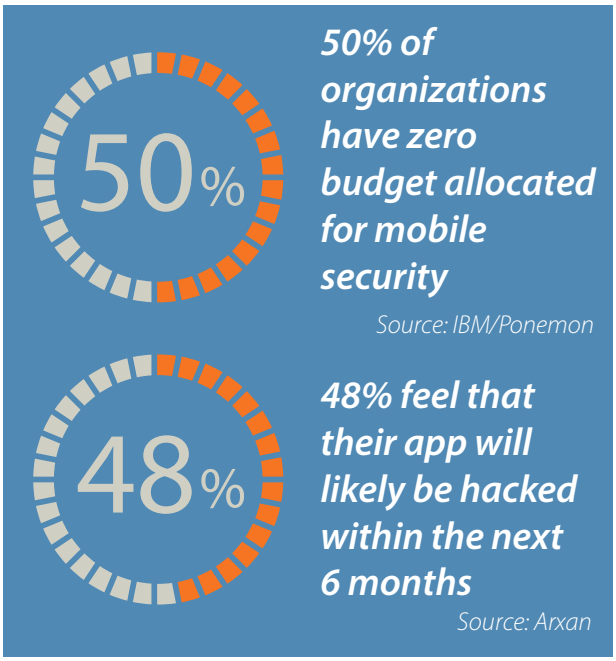
However, perception is not reality.

Thumbs down — most apps have significant vulnerabilities. Vulnerability assessments of 126 mobile health and finance apps in the US, UK, Germany, and Japan revealed that 90% were not adequately addressing two or more of the Open Web Application Security Project (OWASP) Top 10 Mobile Risks.

Percentage of OWASP Mobile Top 10 Risks Not Addressed

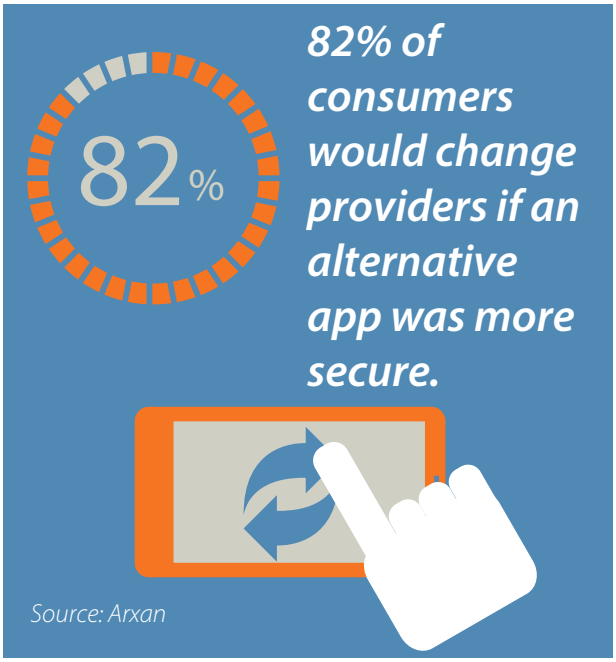


M1: Weak server side controls
M2: Insecure data storage
M3: Insufficient transport layer protection
M4: Unintended data leakage
M5: Poor authorization and authentication
M6: Broken cryptography
M7: Client-side injection (malware)
M8: Security decisions via untrusted inputs
M9: Improper session handling
M10: Lack of binary protection



Shocking? Not really.

Many companies are not investing in mobile app security. According to IBM Security/Ponemon[4], 50% of organizations allocate no budget for mobile app security. Perhaps this is why nearly half of all respondents feel that their apps are likely to be hacked within the next six months.



Who cares? You do.

Even without experiencing an attack on their mobile apps, 80% of consumers would change providers if their app is known to be vulnerable or if an alternative app is more secure. Interestingly, more than 90% of app executives also believed that consumers would change providers if they knew their apps were insecure or if a similar provider offered a more secure mobile app.

Ignorance *must* be bliss.

If folks actually knew how vulnerable their apps really were, according to this study, we should expect a mass exodus of customers fleeing to providers of more secure, trusted mobile apps. Among the most prevalent OWASP Mobile Top 10 Risks identified among the mobile health and finance apps tested are: 1) lack of binary protection (98%) – this was the most prevalent vulnerability; and 2) insufficient transport layer protection (83%). These vulnerabilities make applications susceptible to reverse-engineering and tampering, in addition to privacy violations and theft.

According to Arxan CTO Sam Rehman, "The impact for businesses and users can be devastating. Imagine having your mobile health app reprogrammed to instruct you to deliver a lethal dose of medication. Or imagine your mobile finance app draining your bank account by redirecting funds."

Recommendations

What can be done? A lot.

While it's clear *why* organizations should mitigate the security, financial, and brand risks associated with vulnerable mobile apps, it's less clear *what* organizations and consumers should do. Among the recommendations:

Source: IBM Security / Ponemon research[1]

For businesses:

- ***"Set your security bar above the regulators"*** – Regulatory bodies (and likely will always) lag behind cyber criminals. Apps "approved" by trusted sources such as regulatory / governing bodies like the US FDA or the UK NHS are no more secure than unapproved apps.

- ***Strengthen the weakest links.*** Address elements of the OWASP Mobile Top 10 Risks that are being neglected. 83% of the apps tested had a transport layer vulnerability. 98% of the apps tested lacked binary code protection.

- ***Make security a source of competitive advantage.*** Market the strength of security you offer to attract and retain customers.

- ***Align spending with risks:*** IBM Security and Ponemon research[5] reveals that the majority of risks are happening at the application layer, but the spending is largely focused on networks and data.

For consumers:

- ***Get apps only from authorized app stores.*** Most authorized app stores have some security protocols in place to help ensure apps can be trusted.

- ***Don't jailbreak or root mobile devices.*** Jailbreaking/rooting devices negates security measures that are designed to help protect you and your data.

- ***Demand more transparency about the security of the apps you are using.***
  As cliché as it is, knowledge is power – many foods you eat are usually required to be labeled with nutrition information to help you make better-informed decisions. Before you download a mobile app, wouldn't you want to know what risks you may be opening yourself up to? Become an advocate for app security certification and risk transparency.

For policymakers and regulators:

- ***Establish a "Good Housekeeping" seal of approval for app security.*** Require apps to make available an OWASP Mobile Top 10 risk rating for critical apps. Consumers need to know what risks they are accepting before downloading or "consuming" an app. And the healthcare community and financial services industry need to incorporate risk as a fundamental consideration before making app recommendations to consumers, patients and app users.

Learn More

- View and share the infographic: https://www.arxan.com/resources/state-of-application-security/
- Download a Mobile App Security Handbook: https://www.arxan.com/resources/mobile-application-protection-handbook/

Contact Us

Stephen McCarney
Arxan Technologies
Tel: +1 301-968-4295
Email: smccarney@arxan.com

Footnotes

[1] IBM Security / Ponemon study: *The State of Mobile Application Insecurity* (February 2015)
[2] The Open Web Application Security Project identifies the most critical application security risks facing organizations
[3] The UK NHS Health Apps Library included 79 apps, which were approved by the NHS. The NHS library of approved apps closed in October 2015 after Arxan had tested a sample of 15 NHS-approved apps
[4] *Ibid.* [1]
[5] *Ibid.* [1]