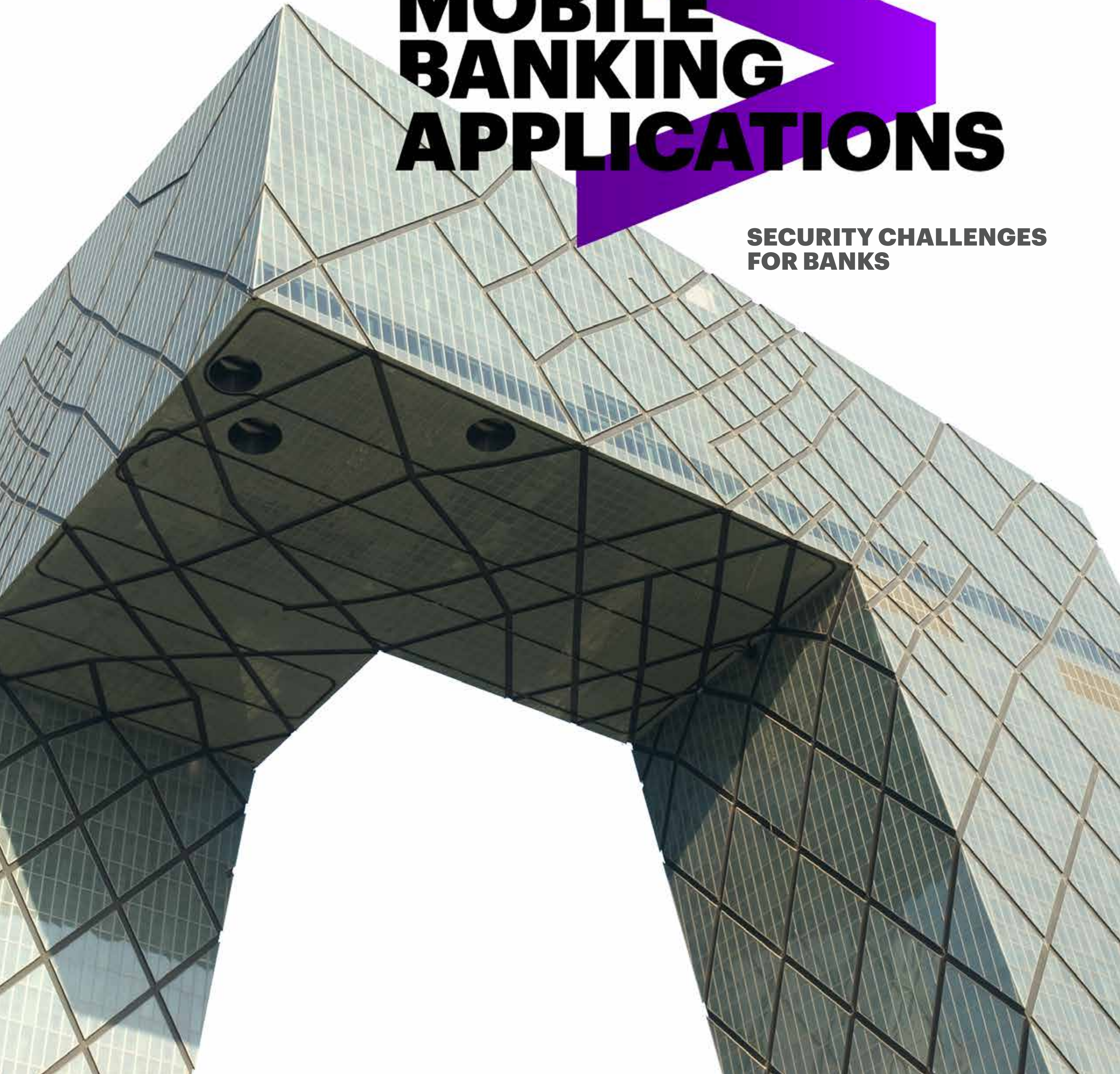
accenture consulting

NowSecure™

MOBILE BANKING APPLICATIONS

SECURITY CHALLENGES FOR BANKS



THE PROLIFERATION OF MOBILE DEVICES, APPS (APPLICATIONS) AND OPERATING SYSTEMS HAS CREATED INCREASED OPPORTUNITIES FOR INNOVATION IN THE MOBILE ECOSYSTEM, WITH USER CONVENIENCE TOP-OF-MIND. NEW OPPORTUNITIES, HOWEVER, HAVE CREATED NEW RISKS, THAT IF NOT MITIGATED, CAN INCREASE THE MOBILE ATTACK SURFACE, AS WELL AS LEAD TO THE COMPROMISE OF PERSONAL, SENSITIVE, PROPRIETARY AND CLASSIFIED INFORMATION ON MOBILE DEVICES.

The wealth of information stored on and transmitted via mobile devices creates unique security risks and provides a valuable target for attackers, regardless of motive.

Mobile apps store and transmit, not just general user information, but also confidential and sensitive information—such as financial and transactional data on a customer-facing mobile banking app—that can be used in identity theft and fraud scenarios.

In addition, mobile devices used to access corporate content are often personally owned, such as those covered by Bring Your Own Device (BYOD) programs, leading to difficulties in the regulation of end-user access by corporate security teams or third parties. These complexities increase the attack surface with mobile devices constantly challenging the boundaries of an organization's security perimeter. If compromised, this can result in both financial and non-financial impacts such as legal risks, regulatory and compliance issues, loss of proprietary data or intellectual property, reputational damage, and recovery costs. Lost or stolen devices can also create an additional avenue for attackers to perform malicious activities, such as using a device as a launching point for an attack or fraud scenario.

The mobile universe continues to expand, driving an increase in mobile app development. Many developers have not previously had to think about some of the dynamic complexities involved in the mobile environment. Mobile apps collect, store and transmit data that web apps, for instance, never did—such as a photo of a check which includes a bank account number. Developers should become more security aware and use secure designs tailored for each unique app throughout the development lifecycle.

Accenture and NowSecure, Inc. (NowSecure) analyzed the mobile banking app threat landscape based on industry research, customer-facing mobile banking app vulnerability assessments performed by NowSecure, and Accenture's industry knowledge and experience working with banking institutions. We collaborated to perform vulnerability assessments for 30 customer-facing mobile banking apps in the North American market. The assessment methodology and approach used the NowSecure Lab Automated tool, which is a fully automated, cloud-based platform providing dynamic and static analysis.

The sample-based approach was designed to provide an understanding of the current-state security environment for customer-facing mobile banking apps, as well as answer some key questions about the state of mobile banking app security, including:

1. Do financial institutions continue to encounter challenges with timely identification and remediation of high-risk mobile app vulnerabilities?
2. Do mobile banking app security issues continue to be exposed as new apps and device features are frequently released?
3. How have banking institutions adopted additional control layers, such as multi-factor authentication, to help offset unsecure user behavior for customer-facing mobile banking apps?

THE MOBILE LANDSCAPE

Mobile devices continue to replace legacy hardware. This shift in user behavior has contributed to the ongoing expansion of the mobile universe, as well as an increase in mobile app development.

Given the increase in mobile development, it is critical that security remains top-of-mind and is embedded within the app development lifecycle, using an approach that has appropriate controls in place from the onset.

End-user behavior and secure development practices are essential to the security of sensitive data, such as the information stored (device) and transmitted (server-side) using mobile banking apps. According to NowSecure analysis, 35 percent of communications sent by mobile devices are unencrypted and the average device connects to over 160 unique IP addresses daily. NowSecure also estimates that 43 percent of mobile device users do not use a passcode, PIN or pattern lock on their devices, and that one in four mobile apps include at least one high-risk security flaw.[1]

Application, infrastructure, and access vulnerabilities, along with sensitive data protection and increasing network connection points create additional challenges that are unique to the mobile environment. Solving these challenges through improved mobile security can allow for increases in flexibility and productivity as end-users are able to connect from anywhere without compromising the security of sensitive data.

According to NowSecure analysis, 35 percent of communications sent by mobile devices are unencrypted

CUSTOMER-FACING MOBILE APP PLATFORMS

The leading mobile platforms are Apple's iOS®[2] and Google's Android™ operating system.

These two platforms make up the majority of the mobile ecosystem in North America. The mobile development field is a complex environment that is constantly evolving, which creates a hyper-dynamic environment for developers. New development tools and capabilities emerge rapidly, and development teams typically hasten to adapt the latest tools. Developers should also stay abreast of the latest security practices in a constantly evolving environment, as they might impact the design of an app across various platforms.

The way apps are designed to leverage mobile device capabilities adds another layer of complexity to the security picture. The capabilities of any given device (such as web browsing, GPS (global positioning system), motion detection, or camera) can vary but the ability to innovate—leveraging a combination of mobile device capabilities and app functionality—can create security challenges unique to the mobile environment. For example, a widely adopted feature of mobile banking apps is mobile deposit capabilities, whereby users can take photos of a check and deposit into a bank account via the app.

OPEN WEB APP SECURITY PROJECT (OWASP)

Both Accenture and NowSecure are contributors to the Open Web Application Security Project (OWASP), a worldwide not-for-profit charitable organization focused on improving the security of software.[3] Content and thought leadership provided is incorporated into the development of the OWASP Top 10 Mobile Risks.

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

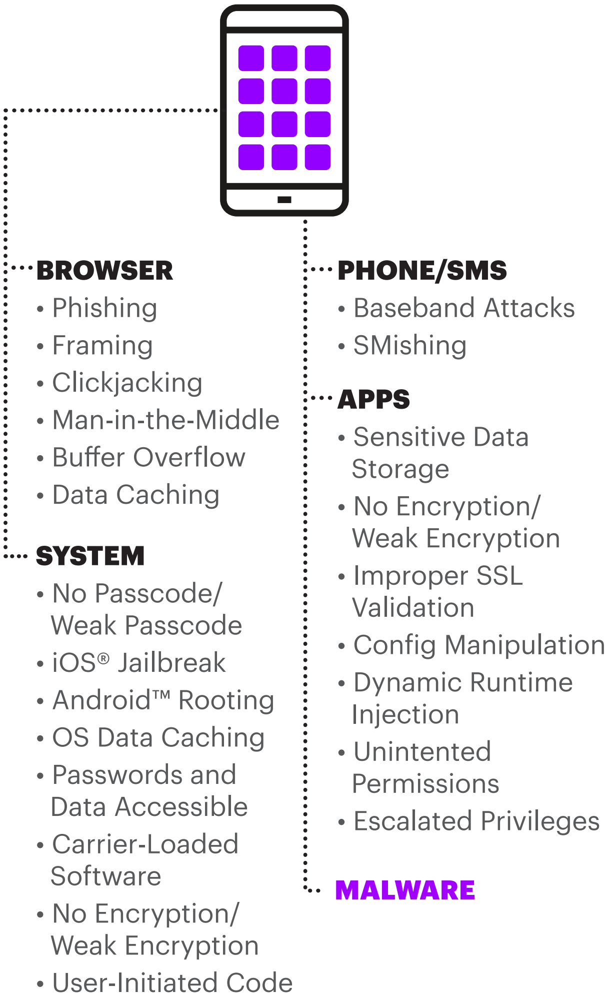
Source: This OWASP Top 10 Mobile Risks list is the published version available at the time this report was published. All information in this section is published by OWASP and publicly available. Access at: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Ideally, customer-facing mobile apps should be designed with an understanding that they are going to be used by diverse sets of users and in varying environments. If this is baked into the development environment through a "security first" mindset, and coupled with periodic execution of vulnerability and/or configuration assessments, source code review, app fuzzing, and pen-testing of apps to confirm whether security vulnerabilities exist prior to production, developers can avoid introducing serious security design flaws and high-risk vulnerabilities into production.

As illustrated in Figure 1 below, there are three points in the mobile technology chain where parties may exploit vulnerabilities to launch malicious attacks—the device, network and data center.

Figure 1. The Mobile Attack Surface

ATTACK SURFACE: THE DEVICE



BROWSER
- Phishing
- Framing
- Clickjacking
- Man-in-the-Middle
- Buffer Overflow
- Data Caching

SYSTEM
- No Passcode/ Weak Passcode
- iOS® Jailbreak
- Android™ Rooting
- OS Data Caching
- Passwords and Data Accessible
- Carrier-Loaded Software
- No Encryption/ Weak Encryption
- User-Initiated Code

PHONE/SMS
- Baseband Attacks
- SMishing

APPS
- Sensitive Data Storage
- No Encryption/ Weak Encryption
- Improper SSL Validation
- Config Manipulation
- Dynamic Runtime Injection
- Unintented Permissions
- Escalated Privileges

MALWARE

ATTACK SURFACE: THE NETWORK
- Wi-Fi (No Encryption/Weak Encryption)
- Rogue Access Point
- Packet Sniffing
- Man-in-the-Middle (MITM)
- Session Hacking
- DNS (Domain Name System) Poisoning
- SSL (Secure Sockets Layer) Strip
- Fake SSL Certificate

ATTACK SURFACE: THE DATA CENTER

WEB SERVER
- Platform Vulnerabilities
- Server Misconfiguration
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (XSRF)
- Weak Input Validation
- Brute Force Attacks

DATABASE
- SQL Injection
- Privilege Escalation
- Data Dumping
- OS Command Execution

Source: "Secure Mobile Development Best Practices," NowSecure, 2016. Access at: https://www.nowsecure.com/ebooks/secure-mobile-development-best-practices/

ASSESSMENT SCOPE AND METHODOLOGY

To assess the security of mobile banking apps against fraud and penetration attempts, static and dynamic analysis was performed using the NowSecure Lab Automated tool.

The vulnerability assessment was performed in late-2016 and included customer-facing mobile banking apps from 15 unique North American financial institutions on both iOS® and Android™ operating systems (OSs) (30 total apps). All apps included in scope were publicly available and downloaded directly from the respective online app stores (Apple Inc.'s App Store® and Google Play™). A total of 780 tests were performed across the apps in scope.

Overall, every app tested had at least one security issue identified. Of the 465 tests completed for banking apps running on Android™ OS, 44 or nine percent had low security issues; 48 or 10 percent had medium security issues; and 10 or two percent had high level security issues. For banking apps running on iOS® OS, a total of 315 tests indicated 24 or eight percent low level security issues; 13 or four percent with medium level issues; and none with high level issues.

Table 1 contains a sample of security risks identified through the vulnerability assessment performed for the thirty (30) customer-facing apps in scope. These risks were identified by vulnerability assessments conducted, leveraging the methodology and approach outlined in this section.

1. **World-Writable Files**—Creating world-writable files is a security risk as it could allow other apps to have write access to files, leading to potential security gaps. Approximately 33% of tested banking apps running on Android™ OS created or modified a file such that the file has permissions that allow other apps to write to it.

2. **Broken SSL Check / Sensitive Data in Transit**—Approximately 13% of tested banking apps running on Android™ OS were not performing proper certificate validation or hostname verification. Lack of proper certificate validation could result in sensitive data being intercepted via a man-in-the-middle attack. Conversely, all tested apps running on iOS® OS performed proper certificate validation or hostname verification.

3. **Writable Executables**—A writable executable file is not a vulnerability all by itself, but in combination with another issue could lead to additional app vulnerabilities and make the app susceptible to remote code execution. Approximately 7% of tested banking apps running on Android™ OS had writable executable files.

4. **Obfuscation**—The source code was not obfuscated for approximately 60% of tested banking apps running on Android™ OS. Intellectual property could be at risk because these apps can easily be reverse-engineered.

5. **SecureRandom**—Apps which use the Oracle® Java Cryptography Architecture (JCA) for key generation, signing, or random number generation may not receive cryptographically strong values on Android™ devices due to improper initialization of the pseudo-random number generator (PRNG). Apps that directly invoke the system-provided OpenSSL PRNG without explicit initialization on Android™ are also affected. Approximately 73% of tested banking apps running on Android™ OS were found to be vulnerable because of issues related to the SecureRandom implementation.

6. **Dynamic Code Loading**—Approximately 33% of tested banking apps running on Android™ OS use dynamic code loading within the APK (Android™ Application Package). This mechanism allows a developer to specify which components of the app should not be loaded by default when the app is started. Typically, core components and additional dependencies are loaded natively at runtime, however, dynamically loaded components are only loaded as requested.

7. **Cookie "HttpOnly"**—Approximately 40% of tested banking apps running on iOS® OS were found to not have the "HttpOnly" flag appropriately set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies, and can help prevent attacks like XSS (cross-site scripting), as the cookie cannot be accessed via client side (for example, using a JavaScript™ snippet code).

8. **Cookie "Secure" Tag**—Approximately 54% of tested banking apps running on iOS® OS were found to not have the "secure" flag appropriately set. When set to true, the "secure" flag tells the browser to only send the cookie if the request is sent using a secure channel. This prevents the cookie from being transmitted over unencrypted requests.

9. **Transport Layer Security Traffic with Sensitive Data**—80% of tested banking apps running on iOS® OS had sensitive values intercepted while proxying SSL and Transport Layer Security (TLS) app communications, such as Username, Password, GPS coordinates, Wi-Fi Mac (Media Access Control) Address, IMEI (International Mobile Equipment Identity), Serial Number, and Phone Number. Sending sensitive data without certificate pinning creates higher risk as an attacker with network privileges, or who has compromised TLS, is better positioned to intercept data.

10. **App Transport Security**—App Transport Security (ATS) was new in iOS® 9, and provides secure connections between an app and the back-end server(s). It is on by default when an app is linked to iOS® 9.0 SDK (Software Development Kit) or later. With ATS-enabled, HTTP connections are forced to use HTTPS (TLS v1.2), and any attempts to connect using insecure HTTP will fail. It was found that 60% of tested banking apps running on iOS® OS had ATS globally disabled, which allows a connection regardless of HTTP or HTTPS configuration, connection to servers with lower TLS versions and a connection using cipher suites that do not support forward secrecy.

Table 1. Top Security Risks Identified in Vulnerability Assessment

	#	Analysis	Section	Issue	Impact	CVSS*	%
Android™	1	Dynamic	Permissions	World-Writable Files	High	7.7	33%
	2	Dynamic	Network	Broken SSL and Sensitive Data in Transit (with Encryption)	High	7.4	13%
	3	Dynamic	Permissions	Writable Executables	High	7.7	7%
	4	Static	Code	Obfuscation	Medium	N/A	60%
	5	Static	Code	SecureRandom	Medium	5.5	73%
	6	Static	Code	Dynamic Code Loading	Medium	4.3	33%
iOS®	7	Dynamic	Network	Cookie "HttpOnly" Tag	Medium	5.3	40%
	8	Dynamic	Network	Cookie "Secure" Tag	Medium	5.3	54%
	9	Dynamic	Network	TLS Traffic with Sensitive Data	Low	1.6	80%
	10	Static	Network	App Transport Security	Low	N/A	60%

*Common Vulnerability Scoring System

Source: NowSecure analysis completed in 2016

KEY VULNERABILITY THEMES

Based on the vulnerability assessments performed using the methodology and approach outlined in the "Assessment Scope and Methodology" section, we identified the key thematic elements that follow.

- All 30 banking apps that were analyzed had at least one known security risk identified. While not all vulnerabilities identified are classified as "high risk," organizations should have a defined process in place that requires the performance of an impact analysis with required actions for identified risks and proper governance and oversight through coordination across the three lines of defense. This process should promote informed risk-based decision making related to security.
- Based on current and historical assessment data spanning 2015 and 2016, banking institutions have been proactively remediating well-known critical security issues such as Heartbleed, MITM exposure and others. However, some mobile security vulnerabilities that pose significant security risks have gone un-remediated over that same time period, including Obfuscation, SecureRandom, World-Writeable, Broken SSL and Local Authentication.
- Industry standards and frameworks, such as the Federal Financial Institutions Examination Council (FFIEC) and the National Institute of Standards and Technology (NIST), provide guidance around employing multi-factor authentication to increase the security of mobile banking apps.[4] As a frame of reference, many of the banking institutions included in our assessment require multi-factor authentication for online banking (web) and have begun to adopt similar requirements for mobile, leveraging device capabilities, such as biometrics (TouchID, retina scan and facial recognition technology).

  Many financial institutions that require multi-factor authentication for customer-facing web-apps leverage SMS (Short Message Service) technology via out-of-band communication. SMS and other forms of out-of-band communication technology are inherently insecure and can be compromised by a skilled attacker.

  Based upon our analysis and observations, multi-factor authentication makes online banking more secure by reducing the exposure for the single greatest threat to account takeover, phishing and misappropriated account credentials.

Financial institutions need to carefully consider customers’ appetite for additional authentication measures in balancing security and user convenience but should work to follow industry and regulatory authentication guidance.

- Issues related to transport layer security are a recurring theme as 40% of security issues identified were mapped back to insecure communication. This recurring vulnerability suggests that security around the transfer of data across communication channels is a challenge for developers and that they may be placing too much confidence in secure end-user behavior and back-end server-side communications.

ALIGNMENT TO AN INDUSTRY FRAMEWORK

Mobile banking apps should, at a minimum, be developed with the same security standards as any other software asset.

Accenture has found that while secure development practices are often defined, communicated and reinforced through governance, policies and standards, and awareness and/or training initiatives, inconsistencies across dispersed development teams often lead to noncompliance with enterprise security standards. In addition, a constant push for innovation in the marketplace often outpaces security, which can lead to significant security gaps if an organization is not grounded in a well-established governance model.

A consistent approach to secure development, regardless of methodology or systems, can help financial institutions develop a robust threat modeling process that keeps pace with internal and external threats. A robust threat model can help inform security and development teams so that they can stay abreast of future attack vectors and proactively respond to attackers' evolving techniques. Threat modeling for mobile apps should focus on both the environment (app purpose and features) and the architecture, including back-end (app server, database) and runtime environments (OS version, MDM (Mobile Device Management), and rooted devices).

Accenture has identified key principles to help organizations develop a comprehensive program for embedding security throughout the enterprise's mobile lifecycle with a strategy that addresses security and promotes informed decisions around security risks, across 6 key components:

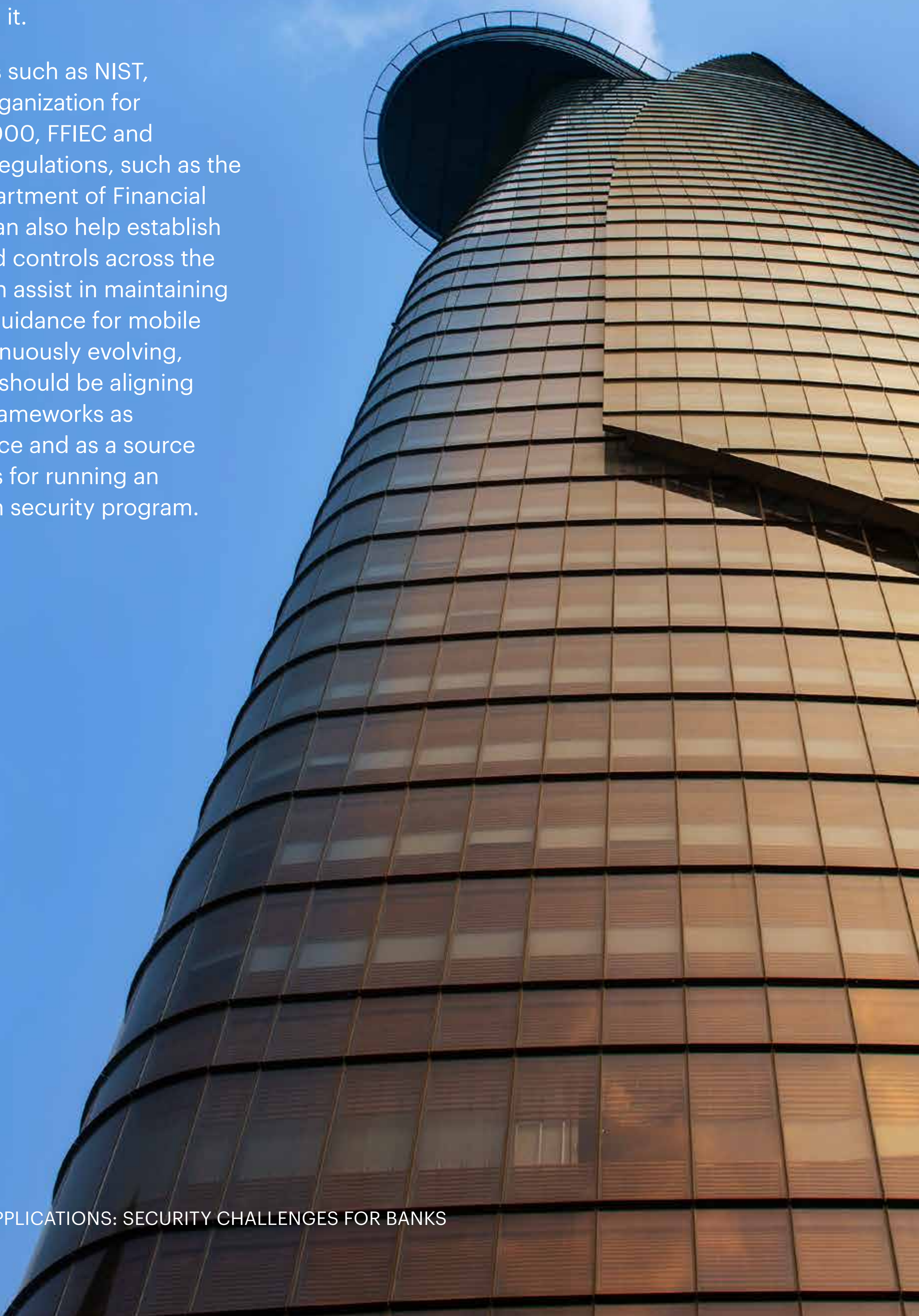
1. **Device**
2. **Network**
3. **Data**
4. **Application**
5. **User Access**
6. **Governance and Compliance**

Leading organizations recognize the expansion of mobile technologies within their enterprise and seek ways to securely integrate them to further enable their workforce and achieve business goals by:

- Developing a mobile security strategy to properly integrate with the overall security and business strategy.
- Identifying the resources and systems that are affected by the introduction of mobile technologies.

- Selecting the technologies and implementing controls to meet requirements defined by business needs as well as compliance requirements.
- Understanding the impact across the organization and the processes needed to support it.

Industry frameworks such as NIST, ISO (International Organization for Standardization) 27000, FFIEC and forthcoming cyber regulations, such as the New York State Department of Financial Services (NYDFS), can also help establish secure practices and controls across the organization and can assist in maintaining compliance. While guidance for mobile app security is continuously evolving, banking institutions should be aligning to these or similar frameworks as foundational guidance and as a source of guiding principles for running an effective information security program.



CONCLUSION

Banks need to balance innovation and security, bringing each into alignment with their organization’s risk appetite and threshold levels.

This means that development teams should strive to embed security within the end-to-end mobile SDLC (Systems Development Life Cycle), with proper security governance and oversight supported by recurring developer training and awareness and testing. While banks’ security capabilities are evolving, attackers continue to explore new avenues—including mobile devices—to commit malicious activities such as sensitive data exfiltration or fraud.

Organizations should also have a strategy for performing regular vulnerability and/or configuration assessments, complemented by penetration testing, app fuzzing, and source code reviews, to obtain a comprehensive understanding of the mobile security environment across the entire mobile deployment stack. This hybrid approach relies on a known list of vulnerabilities for scanning purposes complemented by pen-testing and code reviews which help determine the exploitability of vulnerabilities (both known and unknown), and provide an accurate view of the effectiveness of security controls. This approach can help drive risk-based prioritization and funding to remediate any vulnerabilities and/or control weaknesses identified.

The vulnerability assessment results suggest that, despite an increased focus on security, banking institutions continue to encounter challenges related to secure mobile app design. These challenges should be addressed holistically across people, process and technology, with a focus on aligning the development organization to an industry framework and approach, defining enterprise security development policies, embedding a consistent and secure culture within the development teams through training and awareness initiatives, and enforcement of policies through regular testing.

About the Authors

Chris Thompson

Chris Thompson is a Senior Managing Director, based in New York and leading the Accenture global Financial Services Security and Resilience practice. The Security and Resilience practice helps clients manage cyber risk: the subversion of information risk controls for the agenda of the perpetrator. It unifies security, operational risk, fraud and financial crime and provides end-to-end services across strategy, simulated attacks, consulting and managed service delivery. Chris has over 20 years of experience in large-scale change programs, working with some of the world's leading retail, commercial and investment banks.

Ryan Leininger

Ryan Leininger is a Manager in the Accenture Cyber Risk & Resilience practice. Based in New York, Ryan specializes in cybersecurity strategy, enterprise risk management, security risk and maturity assessments, incident response and regulatory compliance. He works with global banking and insurance firms to navigate the dynamic complexities associated with cybersecurity, information security and operational risk while helping to mitigate risk and improve organizational security posture.

Roshani Bhatt

Roshani Bhatt is a Managing Director, Accenture Digital. Based in New York, Roshani specializes in the delivery of large-scale complex transformational IT and risk programs. She brings over 18 years of broad-based experience in analytics, data management, cyber risk, resilience and security and has helped global financial services organizations address cyber business process and infrastructure resilience issues. Her recent focus has included transforming IT risk management capabilities into drivers of value and sustainability, strengthening organizations by identifying and reducing cyber risk, increasing data security, and deriving strategic management insights by leveraging big data technology.

REFERENCES

1 Secure Mobile Development Best Practices," NowSecure. Access at: https://www.nowsecure.com/ebooks/secure-mobile-development-best-practices/.

2 IOS is a trademark or registered trademark of Cisco Systems, Inc. in the US and other countries and is used under license by Apple Inc.

3 "Welcome to OWASP." Access at: https://www.owasp.org/index.php/Main_Page.

4 "Authenticating E-Banking Customers," FFIEC IT Examination HandBook InfoBase," Access at: http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/information-security-program/authenticating-e-banking-customers.aspx. "Appendix E: Mobile Financial Services," FFIEC IT Examination HandBook InfoBase. Access at: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-e-mobile-financial-services.aspx. "Security and Privacy Controls for Federal Information Systems and Organizations [including updates as of 1/22/2015]," NIST, January 22, 2015. Access at: https://www.nist.gov/node/557861.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 401,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT NOWSECURE, INC.

NowSecure is a mobile application security technology company. NowSecure focuses exclusively on meeting the needs of enterprises with mobile-centric workforces using dual-use devices and delivering secure user experiences to their customers through mobile apps. NowSecure delivers mobile app security testing, endpoint risk, incident response, and compliance solutions. Visit us at www.nowsecure.com.

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

STAY CONNECTED

Accenture Finance and Risk
www.accenture.com/financeandrisk

Accenture Security
www.accenture.com/us-en/security-index

Finance and Risk Blog
financeandriskblog.accenture.com/

Connect With Us
www.linkedin.com/groups?gid=3753715

Join Us
www.facebook.com/accenture

Follow Us
https://twitter.com/accenture
www.twitter.com/AccentureSecure

Watch Us
www.youtube.com/accenture

1 2 4 6 0 5 0 3

171549