Mobile Banking Security
Building and Maintaining Secure Mobile Apps

8 OF 10 MOBILE BANKING APPS CONTAIN SECURITY WEAKNESSES
EXECUTIVE SUMMARY

This study explores challenges faced by today’s megabanks, regional banks, and credit unions while building and maintaining secure mobile banking apps. Praetorian has identified build and configuration weaknesses in the overwhelming majority of mobile banking apps available on the App Store and Google Marketplace. While cursory, the results of the analysis indicate a need for continued improvement in mobile application security as the critical underpinnings of society become increasingly dependent on mobile technology.

Results suggest that environmental conditions have a direct impact on the quality and security of an institution’s mobile banking solution. Experience confirms that national banks tend to be the earliest adopters of security technology, in-source development efforts, and maintain mobile development projects over time. In contrast to this, regional banks and credit unions tend to reactively adopt new security technology, outsource development efforts, and maintain finite development cycles. While security weaknesses were identified across financial institutions of all asset sizes, the analysis shows a security gradient between national banks, regional banks, and credit unions, with build and configuration weaknesses being most prevalent in credit unions. This correlation suggests that the way in which mobile applications are developed may directly contribute to the outcomes of the study.

Recommendations

Incremental and rapid release cycles are driving the need for continuous and on-demand security evaluation to help address unique challenges encountered while building and maintaining secure mobile applications. More now than ever, organizations should engage in ongoing assessments as new features are released and code changes are made.

Mobile security solution providers need to play their part by equipping companies with the technology and service models they need to support continuous and on-demand security testing of mobile applications.
The goal of this study was to gain insight into mobile development practices among financial institutions by identifying build and configuration weaknesses in mobile banking applications developed and/or distributed by megabanks, regional banks, and credit unions. While this study is by no means comprehensive nor the test cases exhaustive, the issues identified do serve as indicators of the overall health and maintainability of these mobile applications.

The mobile applications collected for this assessment are freely distributed to the public by banking institutions with the intent to extend virtual branches with account management, bill pay, mobile remote deposit capture, and other such functionality that accesses sensitive information. End users of the mobile applications are primarily banking account holders and credit union members.

**CATEGORIES OF APPS TESTED**

- Top 50 Financial Orgs (Megabanks)
- 50 of the Largest Regional Banks
- Largest 50 U.S. Credit Unions

A list of financial institutions was compiled before collecting mobile applications from the App Store and Google Marketplace. Our list was composed of three categories, which included megabanks, regional banks, and credit unions.

Where available, both iOS and Android mobile applications—developed and/or distributed by the financial institutions on our list—were downloaded from the App Store and Android Marketplace on December 3, 2013. A total of 275 mobile banking apps were collected.

### Banking App Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>iOS</th>
<th>Android</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Unions</td>
<td>50</td>
<td>48</td>
<td>98</td>
</tr>
<tr>
<td>Regional Banks</td>
<td>47</td>
<td>46</td>
<td>93</td>
</tr>
<tr>
<td>Megabanks</td>
<td>44</td>
<td>40</td>
<td>84</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>141</td>
<td>134</td>
<td>275</td>
</tr>
</tbody>
</table>

Praetorian's Project Neptune

The mobile banking applications collected were then analyzed with Praetorian’s Project Neptune, a new mobile application security testing platform. This continuous and on-demand security testing platform helps mobile development teams address security challenges encountered while building and maintaining mobile apps.

The platform covers a broader suite of security verification and validation testing, including build management, configuration management, authentication, authorization, session and token management, data validation, data confidentiality, error and exception handling, and auditing and logging.

To learn more about Project Neptune, visit [https://neptune.praetorian.com](https://neptune.praetorian.com)
BUILD & CONFIGURATION TESTING

The scope of this study was limited to a small subset of the build and configuration management test capabilities offered by Project Neptune. The weaknesses tested are well-known and well-understood issues with mitigation strategies that have been available for some time. Several of the issues identified are addressed by simply updating to the latest mobile development environment or target software development kit (SDK).

The test cases selected were nonintrusive and focused on mobile application issues affecting the local device. Back-end web servers and services that mobile applications communicate with were not evaluated. Because 75% - 90% of the functionality of a mobile banking solution is on the back end, the results only represent a small fraction of the total attack surface of a mobile banking platform.

Testing of all 275 mobile banking apps was conducted on December 8, 2013. Build and configuration setting weaknesses in the Project Neptune security test cases included (see references section for more information on build and configuration weaknesses):

**iOS Build & Config Testing**
- Automatic Reference Counting (ARC) Not Enabled
- Position Independent Executable (PIE) Not Enabled
- Stack Protection Not Enabled

**Android Build & Config Testing**
- Android Targeting Old SDK
- Lack of Permission Hardening
- Android Debugging Enabled

TESTING NOTES:
Android applications that set "android:targetSdkVersion" to 13 and below were assigned the Android Targeting Old SDK weakness. This is the equivalent of targeting Android 3.2 (API level 13), which was released on July 15, 2011.

For the purposes of this study, Lack of Permission Hardening was assigned to Android applications that had more than 10 permissions. Some apps were found to have as much as 24 permissions set in the manifest.
MOBILE BANKING APP TEST RESULTS

Praetorian found that the overwhelming majority of mobile banking applications are affected by one or more of the security weaknesses tested. The outcome of the study is particularly noteworthy given the financial sector’s higher spend on information security when compared to most other industry verticals. While cursory, the results of the analysis indicate a need for continued improvement in mobile application security as the critical underpinnings of society become increasingly dependent on mobile technology.

The results also suggest that environmental conditions have a direct impact on the quality and security of an institution’s mobile banking solution. Experience confirms that national banks tend to be the earliest adopters of security technology, in-source development efforts, and maintain mobile development projects over time. In contrast to this, regional banks and credit unions tend to reactively adopt new security technology, outsource development efforts, and maintain finite development cycles. While security weaknesses were identified across financial institutions of all asset sizes, the analysis also shows a security gradient between national banks, regional banks, and credit unions, with build and configuration weaknesses being most prevalent in credit unions. The way in which mobile applications were developed may have directly contributed to the outcomes of the study.

Results reveal that 8 out of 10 mobile banking applications contain build and configuration setting weaknesses. While these findings are merely informational in terms of risk, they do provide insight into the state of mobile development practices among megabanks, regional banks, and credit unions.

As stated above, all weaknesses tested in this study are well-known and well-understood issues with mitigation strategies that have been available for some time. With that said, is it reasonable to conclude that the abundance of weaknesses identified suggest finite development cycles or insufficient maintenance provided to mobile banking apps over time? Further research is needed to adequately answer those questions, but it is important to highlight that build and configuration weaknesses were not found to be as prevalent in other app genres tested prior to this study.
REFERENCES FOR BUILD AND CONFIGURATION WEAKNESSES IDENTIFIED IN THIS STUDY

**iOS References**

- **Automatic Reference Counting (ARC) Not Enabled**

- **Position Independent Executable (PIE) Not Enabled**
  1. [http://cwe.mitre.org/data/definitions/119.html](http://cwe.mitre.org/data/definitions/119.html)

- **Stack Protection Not Enabled**

**Android References**

- **Android Targeting Old SDK**

- **Lack of Permission Hardening**

- **Android Debugging Enabled**

**Android Testing Notes:**

Android applications that set "android:targetSdkVersion" to 13 and below were assigned the Android Targeting Old SDK weakness. This is the equivalent of targeting Android 3.2 or earlier (API level 13), which was released on July 15, 2011.

For the purposes of this study, Lack of Permission Hardening was assigned to Android applications that had more than 10 permissions. Some apps were found to have as much as 24 permissions set in the manifest.

NEED MOBILE SECURITY HELP?

Contact us at 1 (800) 675-5152 to learn how Praetorian security services can help you accomplish your specific business and IT goals, or explore more by visiting:

www.praetorian.com

1 (800) 675-5152
www.praetorian.com
APPENDIX A: ABOUT THE DATASET

Financial Institutions Included in This Study
Mobile banking applications developed and/or distributed by the following financial institutions were the focus of this study. The mobile apps collected for this assessment are freely distributed to the public by banking institutions with the intent to extend virtual branches used by customers/members for account management, bill pay, mobile remote deposit capture, and other such functionality dealing with sensitive information.

Top 50 Financial Holding Companies (Megabanks)

» JP Morgan Chase  
» Bank of America  
» Citigroup  
» Well Fargo  
» Goldman Sachs  
» Morgan Stanley  
» American International Group  
» General Electric Capital  
» Bank of NY Mellon  
» US Bancorp  
» HSBC North American  
» PNC Financial Services  
» Capital One Financial  
» TD Bank  
» State Street Corporation  
» Principal Financial Group  
» BB&T Corporation  

» Suntrust Banks  
» Ally Financial  
» American Express Company  
» Charles Schwab Corporation  
» Fifth Third Bank  
» United Services Automobile Assoc  
» RBS Citizens  
» Regions Financial Corporation  
» BMO Financial Corp  
» Unionbancal Corporation  
» Northern Trust Corporation  
» Keycorp  
» M&T Bank Corporation  
» Bancwest Corporation  
» Santander Holdings  
» Discover Financial Services  
» BBVA Compass  

» Deutsche Bank  
» Comerica  
» Huntington Bankshares  
» Zions Bancorporation  
» UTRECHT America  
» CIT GROUP  
» New York Community Bancorp  
» ETRADE Financial  
» Hudson City Bancorp  
» First Niagara Financial  
» Popular  
» John Deere Capital  
» Peoples United Financial  
» City National Corporation  
» BOK Financial Corporation  
» Synovus Financial Corp

50 of the Largest Regional Banks

» Associated BK NA  
» Bank Of Hawaii  
» Bank Of OK NA  
» Bancorpsouth BK  
» Cathay BK  

» Commerce BK NA  
» Frost NB  
» Comerica BK  
» Central Pacific BK  
» Citizens BK  

» Citizens Bus BK  
» City NB  
» East West BK  
» First BK  
» First Commonwealth BK
50 of the Largest Regional Banks (Continued)

» First-Citizens B&TC
» First Tennessee BK NA Mmphs
» First Midwest BK
» Firstmerit BK NA
» First NB Of Pa
» Fulton BK
» Huntington NB
» International BK Of Cmrc
» Mb Fncl BK NA
» M&I Marshall & Ilsley BK
» Manufacturers & Traders TC
» National Penn BK
» Old NB
» Pacific Cap BK NA
» Park NB
» Prosperity BK
» Privatebank & TC
» Regions Financial
» Signature BK
» Silicon Valley BK
» Columbus B&TC
» SterlingSvg BK
» Susquehanna BK
» TCF NB
» Trustmark NB
» Carolina First BK
» United Cmnty BK
» Umb BK NA
» Umpqua BK
» Valley NB
» Webster BK NA
» Wilmington TC
» Wesbanco BK
» Whitney NB
» Zions First N

Largest 50 U.S. Credit Unions

» Navy Federal Credit Union
» PenFed Federal Credit Union
» BECU
» Alliant Credit Union
» The Golden 1 Credit Union
» Security Service Federal Credit Union
» Star One Credit Union
» San Diego County Credit Union
» America First Credit Union
» First Technology Federal Credit Union
» American Airlines Federal Credit Union
» Randolph-Brooks Federal Credit Union
» Suncoast Schools Federal Credit Union
» Bethpage Federal Credit Union
» Alaska USA Federal Credit Union
» Citizens Equity First Credit Union
» Digital Federal Credit Union
» VyStar Credit Union
» Teachers Federal Credit Union
» Delta Community Credit Union
» ESL Federal Credit Union
» PSECU
» Police and Fire Federal Credit Union
» Patelco Credit Union
» Wings Financial Credit Union
» United Nations FCU
» Ent Federal Credit Union
» Hudson Valley Federal Credit Union
» Logix Federal Credit Union
» Mountain America Credit Union
» Redstone Federal Credit Union
» DFCU Financial
» OnPoint Community Credit Union
» Kinecta Federal Credit Union
» Desert Schools Federal Credit Union
» Visions Federal Credit Union
» Space Coast Credit Union
» Tinker Federal Credit Union
» SACU
» Lake Michigan Credit Union
» Eastman Credit Union
» SECU Credit Union
» SEFCU
» Tower Federal Credit Union
» Wright-Patt Credit Union
» Wescom Credit Union
» Northwest Federal Credit Union
» Veridian Credit Union
» Virginia Credit Union
» Michigan State University Federal Credit Union
App Names/Version Data
The following iOS and Android mobile banking apps were downloaded from the App Store and Google Marketplace on December 3, 2013. Readers will notice that some apps share similar and/or nondescript naming conventions. For example, “mBanking 1.3” and “mBanking 2.2” (found in the iOS Credit Union apps list) likely share a similar name because they were both built by the same third-party developer who then rebranded the app for each of its banking/financial institution customers. There are other examples in the list below where it may be difficult to connect the app name/version to its originating developer or financial institution.

Megabank App Names/Version (iOS)

- Ally Bank 2.2.2
- Amex 4.3.1
- Banking 5.0
- Bankwest 2.2.0
- BB&T 3.1.2
- BBVA US 3.0.0
- BMO 2.0
- BNY Mellon 1.1.8
- BofA 4.3.470
- Capital One 04.04.90
- Chase 2.310
- CIT Bank 2.7.11
- Citibank 5.2
- CN Mobile 201335218
- Comerica 1.1.5.77386
- Discover 12.1
- E_TRADE 4.0.2
- Fifth Third 2.1
- First Niagara 1.0.2
- HSBC 131122
- Huntington 1.5.15
- KeyBank 201335213
- LeasingSource for OI 1.2
- M&T Bank 1.3
- Meine Bank 1.9.2
- MS Matrix 2.0.7
- NorthernTrust 1.7.1
- PCB 201334825
- peoples.com 201334927
- PNC Mobile 201326610
- Popular BMB 201334854
- Principal 1.6
- Regions 4.0.1
- Santander 2.1
- Schwab 3.2.0.298
- SunTrust 2.1.1
- Synovus 1.0.4
- TD Bank (US) 3.0.1
- TransFund 1.0
- U.S. Bank 1.14.18
- UnionBank 2.8.0
- Visions Mobile
- VyStar Credit Union
- Wealth 1.3.1
- Wells Fargo 2.6.1
- Wells Fargo Mobile
- Wescom Credit Union Mobile
- Wings Mobile
- Wings Mobile 2.7.37
- WPCU HB 3.5.2.0
- WPCU Home Banking
- Zions Bank 2.5.3

Megabank App Names/Version (Android)

- Ally Mobile Banking
- Amex Mobile
- Bank of America
- Bank of Oklahoma Mobile
- Bank of the West Mobile
- BB&T Mobile Banking
- BBVA Provinet Movil
- BMO Harris Mobile Banking
- BNY Mellon Private Banking
- Capital One® Mobile
- Chase Mobile
- CIT Bank Mobile Banking
- Citi Mobile (SM)
- Citizens Bank Mobile Banking
- City National Bank Mobile
- Comerica Mobile Banking®
- Discover Mobile
- ETRADE Mobile
- Fifth Third Mobile Banking
- First Niagara Mobile Banking
- HSBC Mobile Banking
- Huntington Mobile
- KeyBank Mobile
- M&T Mobile
- People’s United Bank Mobile
- PNC Mobile
- Popular
- Principal® Mobile
- Private Passport Mobile
- Regions Bank
Megabank App Names/Version (Android) (Continued)

» Schwab Mobile
» State Street Bank Mobile
» SunTrust Mobile App
» Synovus Mobile Banking
» TD Bank (US)
» TFCU Home Branch Mobile
» Tower Federal Credit Union
» U.S. Bank
» UNFCU
» Union Bank Mobile Banking
» USAA Mobile
» VACU Mobile Banking
» Veridian Mobile Banking
» Visions Mobile
» VyStar Credit Union
» Wells Fargo Mobile
» Wescom Credit Union Mobile

» Wings Mobile
» Wings Mobile 2.7.37
» WPCU HB 3.5.2.0
» WPCU Home Banking

Largest Regional Bank App Names/Version (iOS)

» AB Mobile 2.0.2
» BancorpSouth 2.3.2
» Banking 2.7.5
» BMO Harris 201335101
» BOH 201334934
» BOK 1.7.1
» Cathay Bank 201335364
» Citizens Bank 2.20
» CN Mobile 201335218
» Comerica 1.1.5.77386
» Commerce 1.6
» CPB 2.0
» EastWestBank 3.5.2.1
» FCB 1.0.1
» First Bank 2.0.0
» FirstTenn 201335075
» FirstCitizens 1.0.1
» FirstMerit 1.3.3
» FirstMidwest 201326697
» FNB Mobile 3.5.2.0
» Frost 2.0.1
» Fulton Bank 3.5.1.2
» Huntington 1.5.15
» IBC Mobile 2.3.4
» M&T Bank 1.3
» MB Financial 1.1.0.102
» mBanking 1.0.1
» Mobile Bank 2.7.11
» Mobile Bank 201335750
» NP Mobile 2.6.8
» Park National 1.0.2
» PrivateBank 201335396

» Prosperity 2.6.3
» Regions 4.0.1
» Sterling 201335381
» SVB Mobile 2.2.0
» Synovus 1.0.4
» TCF Bank 4.10.053
» TD Bank (US) 3.0.1
» Trustmark 2.5
» UCBi Mobile 4.3.197
» Umpqua 1.1.2
» UnionBank 2.8.0
» Webster Bank 4.0.0
» WesBanco 2.6.0
» Whitney 2.3.5
» Zions Bank 2.5.3

Largest Regional Bank App Names/Version (Android)

» Associated Mobile Banking
» BancorpSouth
» Bank of Oklahoma Mobile
» Banking
» BMO Harris Mobile Banking
» BOH Mobile Banking
» Cathay Bank
» Central Pacific Bank
» Citizens Bank Mobile Banking
» City National Bank Mobile
» Comerica Mobile Banking®
» Commerce Bank for Android
Largest Regional Bank App Names/Version (Android) (Continued)

» East West Bank Mobile Banking
» FCB Mobile Deposit
» First Banks Mobile
» First Citizens Mobile Banking
» First Midwest Mobile
» First Tennessee Mobile Banking
» FirstMerit Mobile Banking
» FNB Banking App
» Frost

» Fulton Bank Mobile Banking
» Huntington Mobile
» IBC Mobile
» M&T Mobile
» MB Financial Bank
» National Penn Mobile
» Old National Mobile Bank
» Park National Bank
» Prosperity Bank
» Regions Bank

» Signature Bank Mobile Banking
» Sterling Bank Mobile
» SVB Mobile Banking
» Synovus Mobile Banking
» TCF Bank Mobile
» TD Bank (US)
» The PrivateBank Mobile Banking
» UCB Mobile Banking
» UMB Mobile Banking

» Umpqua Mobile Banking
» Union Bank Mobile Banking
» Webster Bank® Mobile
» WesBanco Mobile Banking
» Whitney Bank Mobile Banking
» Zions Bank Mobile Banking

Largest U.S. Credit Union App Names/Version (iOS)

» AAFCU 1.8
» AFCU 2.0.1
» Alaska USA 45427
» Alliant 2.3.30307
» BECU 5.0.1
» CEFCU 1.0
» DCCU 2.0.1
» DCU 1.5
» DFCU Mobile 1.1
» DS Banking 1.1.0
» ECU Mobile 3.5.2.3
» Ent Mobile 2.1.0
» ESL Mobile 3.5.2.0
» First Tech 2.2.0
» Golden 1 2.5.2
» HVFCU Mobile 3.5.2.1
» Kinecta 2.7.38

» LMCU 2.7.17
» Logix Mobile 1.7
» MACU 2.7.38
» mBanking 1.3
» mBanking 2.2
» MSUFCU 1.2
» myBranch 7.74.00108
» Navy Federal 3.0.1
» NWFCU 2.7.37
» OnPoint 8.0.2
» PatelcoCU 2.9
» PenFed 1.2
» PFFCU 1.19
» PSECU 1.6
» RBFCU 3.0.1
» RFCU Mobile 3.5.2.2
» SACU 2.3.10008

» SCCU 1.4
» SDCCU 4.4.9
» SEFCU 3.5.2.5
» StarOne 7.73.00095
» Suncoast 2.3.0
» TFCU 2.7.38
» TFCU Mobile 1.5
» Tower FCU 3.5.2.1
» UNFCU Mobile 20135073
» VACU 3.1.16
» Veridian 4.2
» Visions FCU 2.8
» VyStar Mobile 3.5.1.0
» Wescom 2.4.11007
» Wings Mobile 2.7.37
» WPCU HB 3.5.2.0
Largest U.S. Credit Union App Names/Version (Android)

- AAFCU
- Alaska USA
- Alliant Mobile Banking
- America First Mobile Banking
- BECU Mobile Banking
- Bethpage Mobile Banking
- Delta Community Mobile Banking
- Desert Schools Mobile Banking
- DFCU Mobile
- Eastman Credit Union Mobile
- Ent Mobile Banking
- ESL Mobile Banking
- First Tech
- GO the mobile app from SACU
- Golden 1 Mobile
- Hudson Valley FCU Mobile
- Kinecta Direct Mobile Banking
- LMCU Mobile Banking
- Logix Mobile
- Mountain America Credit Union
- MSUFCU Mobile
- Navy Federal Credit Union
- NWFCU
- OnPoint Mobile
- Patelco
- Police and Fire Federal Credit
- PSECU Mobile+
- RBFCU Mobile
- Redstone Federal Credit Union
- SchoolsFirst FCU Mobile
- SDCCU Mobile Banking
- SECU Mobile
- Security Service myBranch App
- SEFCU Mobile Banking
- Space Coast CU Mobile
- Star One Mobile Banking
- Suncoast Schools SunMobile
- Teachers Federal Credit Union
- TFCU Home Branch Mobile
- Tower Federal Credit Union
- UNFCU
- VACU Mobile Banking
- Veridian Mobile Banking
- Visions Mobile
- VyStar Credit Union
- Wescom Credit Union Mobile
- Wings Mobile
- Wings Mobile 2.7.37
- WPCU HB 3.5.2.0
- WPCU Home Banking