Security In Mobile Bank Apps & TLS

by Steve Brown

A study by PwC finds 62% of companies surveyed expect cyber risk to cause disruption in the next 3Ys but only 9% say they have a high or very high cyber risk maturity. Clearly the data shows there is room to improve in this area and community banks are aggressively taking steps to do so as well.

Cybersecurity is often in the news. However, one of the latest issues to arise is somewhat new and concerns mobile banking apps. Cybersecurity experts have discovered vulnerabilities with the implementation of encryption connecting mobile phone apps to bank servers. This is concerning indeed as community banks increasingly look toward mobile banking as a way to hold onto and attract younger customers.

The experts say the issue lies in the Transport Layer Security (TLS). What is TLS? In a very simple explanation, TLS involves the secured communication between the mobile device and the bank server. A mobile user tries to logon to their bank's server via the bank app. When this happens, there needs to be a secure way for the client to validate the identity of the bank's server and send messages securely. This is done with a security certificate. Once the connection is authenticated by way of the certificate, the two sides exchange keys to allow encrypted communication between the mobile bank client and the bank server.

Unfortunately, some software app developers apparently aren't exactly getting the technology right. The result is that hackers have open pathways to decrypt a session on a customer's open app as it talks to a bank's servers. This is serious indeed.

Consulting firm Accenture and mobile-app security company NowSecure recently examined 15 North American financial companies' mobile apps. Their findings concluded that every app, whether on Android devices or iPhones, had a minimum of one security issue. They also reported that the bulk of the vulnerabilities were related to TLS issues.

The Accenture report also found that 80% of iPhone apps exposed "sensitive values" to possible interception by rogue hackers and 73% of Android apps were "vulnerable". Data that could be accessed included: username, password, GPS coordinates, Wi-Fi Address and phone number. The research warns developers to be shrewd to security issues, but the full extent of this problem may not rest solely with developers.

This flaw comes at a time when many banks are shoring up their TLS communication in what is called certificate pinning. While the intent is a good one - decrease the number of trusted certificates to access your site - it is not a TLS panacea. According to a security consultant at Synopsys, companies think that once they have certificate pinning in place, they are safe. But, as with all technology, you need to monitor your pins and renew the certificates regularly, so this is an ongoing process.

The gist for bankers is to take extra precautions when developing and managing mobile apps. Ask questions about any mobile security issues, including TLS connections. Have your IT specialists check the verification process of your bank's website for mobile users on an ongoing basis too and ensure your certificates are up to date. Lastly, it might make sense to bring in a top quality cybersecurity team to hunt for vulnerabilities you may not know about because they are always changing. Stay safe everyone and keep moving forward.

BANK NEWS

M&A Activity

1) Heritage Bank ($3.9B, WA) will acquire Puget Sound Bank ($567mm, WA) for about $126.1mm in stock (100%) or about 2.4x tangible book. 2) People's Intermountain Bank ($1.7B, UT) will acquire 7 branches from Banner Bank ($9.9B, WA) for an estimated $15.3mm deposit premium. People's gets $260mm in loans and $180mm in deposits with the transaction.

FDIC

The White House is reportedly considering nominating Fifth Third Bancorp's chief legal officer, Jelena McWilliams, to lead the FDIC. McWilliams was previously an attorney at the Fed and a Republican staffer on the Senate Banking Committee.

Loan Issues

A quick review of comments by bank CEOs from their Q2 earnings, finds many pointing to Washington DC gridlock as weighing negatively on loan demand. Let's hope politicians clean up their act soon.

Credit Cards

Uber will reportedly launch a credit card for its customers soon that will be issued by Barclaycard and carry the Visa brand.

Customer Initiatives

A Deloitte survey of global CIOs finds the top customer focused IT initiatives are: building technology platforms (59%), designing products (46%), delivering customer experience (45%), customer acquisition, retention and loyalty (44%), and analyzing customer data (38%).

Least Ready

Research by Cornerstone Advisors finds banks say they are not future-ready or are falling behind in the following areas: contact center (26%), analytics (22%), marketing (14%), branch delivery (13%) and payments (12%).

Home Spending

Harvard research finds that Americans will spend $316B remodeling their homes in 2017 vs. $296B in 2016. This also compares to a low of $222B (in 2009) and a high of $334B in 2006 (and adjusted for inflation).

More Spending

Research by Marsh & McLennan on cyber risks finds 86% of companies said they plan to increase spending on cybersecurity staffing in the next 12 months.

ON DEMAND HELP FOR COMMUNITY BANKERS

Community bankers face many difficult challenges every year, but you are not alone. Our experts stand ready to help you address a variety of issues. Go here to view options and opportunities.