www.pwc.com

Mobile banking security - a long way to go

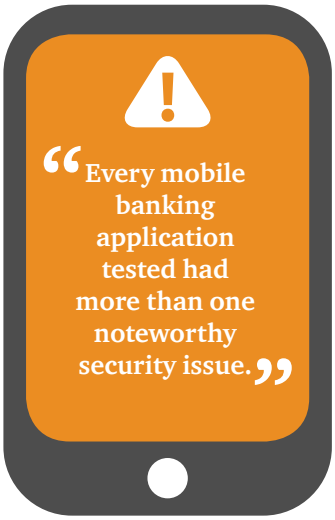
Research report on security of mobile banking applications in India.

Research report.
September 2016

pwc

Mobile application use has grown dramatically over the last five years. In September 2012, Google announced that over 25 billion apps had been downloaded from its app store and the last reported figures from May 2016 showed that 65 billion apps had been downloaded from Google Play.[1] Keeping up with this trend, all major banks in India have developed and are promoting mobile banking using mobile banking applications.

Most banks today are in a race to introduce innovative features for their customers using mobile applications. The question we asked ourselves was, 'Are banks considering adequate security measures, especially considering the risks of an open operating system such as Android?' Our security research team looked at top mobile banking applications in India built for the Android platform and assessed their security framework. The team focused on flaws in the mobile banking application due to internal programmatic and integration issues. For this research, we ignored the flaws with business logic and authentication mechanisms, which may be a topic for further research.



Our team focused on fundamental problems which might be applicable across a range of mobile banking applications. The research examined three primary security parameters: cryptographic controls, data security and insecure implementation.

Every mobile banking application tested had at least one security issue which may be potentially exploited in the near future. We also observed that the data security controls were weak across the spectrum of mobile banking applications. Considering the plethora of security issues across the mobile banking applications, there exists a serious risk of security breaches occurring.

Some of the major issues which we observed are explained below.

Cryptographic controls

Cryptography is the cornerstone of cyber security. A large part of the trust in digital systems is on account of strong cryptography which allows us to store and exchange data securely and ensure counterparty identification and non-repudiation of transactions. Three important aspects determine if the cryptographic controls will be able to achieve the said objectives: algorithms used, secure keys management, and implementation or programmatic realisation of the cryptographic control.

We observed that 96% of the tested mobile applications used SSL v3 instead of TLS v1.x. The SSL V3 protocol has been demonstrated to be insecure and vulnerable to attacks such as POODLE and BEAST. Thus, the use or support of this protocol can lead to theft of potentially sensitive information. Even before the discovery of the POODLE vulnerability, the US Government had mandated the use of TLS v1.0 for sensitive government communication.[2]

In addition, we observed that 65% of the mobile banking apps used SHA1 as part of the protocol implementation. SHA1 has been demonstrated to be vulnerable to compromise through a collision attack with minimal hardware requirements—as low as a 16-node cluster of graphics card. With the advent of cloud computing, such computing power can be rented anonymously on a trial basis with many service providers. Currently, the recommended cryptographic standard is SHA256.

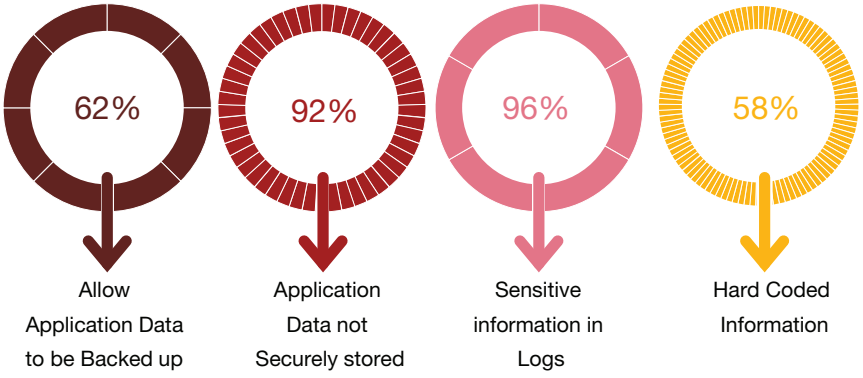
SSL or TLS connections between two machines are initiated by identifying the server by its digital certificate. The certificate issued by a certifying authority provides a proof of identity of the server being accessed. When a secure connection is established between the server and the application, the application can verify if it is connecting to the correct server or if the connection has been compromised using a proxy or other man-in-the-middle attacks. We observed that 12% of the mobile banking applications did not validate server certificates. This means that a user can be subject to man-in-the-middle attacks which can lead to theft of mobile banking credentials and fraudulent transactions.

[1] https://techcrunch.com/2016/05/18/google-play-installs-reached-65-billion-last-year/
[2] NIST Special Publication 800-52, Revision 1

Data security

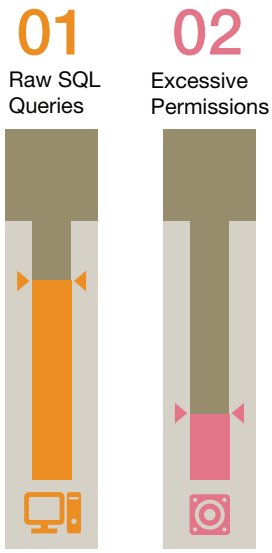
Mobile applications are client server applications and a significant portion of data is processed at the client end—basically mobile handsets. If this data is not secured appropriately, loss, theft or unauthorised access to the handset, either physically or through a malicious application/malware, can result in a security compromise.

One of the greatest risks we uncovered was that 92% of mobile banking applications store application logs on the handset. These logs contain error details, system information, version information and other information which may be used by an attacker to compromise the security of a mobile banking application. Over 62% of the mobile applications created local temporary files and many of these (92%) did not encrypt the data using secure encryption techniques. This makes the data vulnerable to theft and compromise. Some of the applications (58%) used hard-coded information, including hard-coded references, hashes and keys. Often, such information can be sensitive and be used in numerous replay attacks, authentication compromise attacks and phishing attacks.



Insecure implementation

Mobile applications have to query databases to fetch or update data. We observed that 77% of the mobile banking applications used raw SQL queries. This means that the queries were visible and possibly provided information to a potential attacker which could be used to manipulate the queries and lead to attacks such as SQL injection. We also observed that 15% of the mobile banking applications used more permissions than required to effectively operate a mobile banking application. Excessive permissions provide the application with more control over the end point than necessary. A malicious code injection or an exploit affecting the application can compromise the end user device. Any transaction occurring over a compromised end point can lead to major security breaches.



Conclusion

Mobile applications are going beyond just a 'view only' banking channel to becoming the primary channel for many banks. This changes the paradigm of security for mobile banking applications. With insecure end point devices, a highly diverse ecosystem and a combination of a variety of technologies, mobile banking is set to become one of the highest risk channels for banks.

Banks today need to look beyond just cookie-cutter testing of mobile banking applications. They should look at the possibilities which can be exploited by an attacker seeking to take advantage of an insecure operating system and uninformed users. The security approach should start with threat modelling, secure development life cycle and integrated testing of the applications. With mobile banking offering advanced features, this is the right time for banks to explore cross-channel fraud detection systems.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

For more information, contact:

Sivarama Krishnan
Leader, Cyber Security
+91 9650788787
sivarama.krishnan@in.pwc.com

Sangram Gayal
Director
+91 9819197716
sangram.gayal@in.pwc.com

pwc.in

MJ/October2016-7589