Institution: University of Birmingham

Unit of Assessment: UoA11, Computer Science and Informatics

Title of case study: Securing Banking Infrastructure with a New Cryptographic Protocol Testing Tool

Period when the underpinning research was undertaken: 2014 to 2017

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
Dr Tom Chothia	Reader in Cyber Security	2007 to present
Prof. Flavio Garcia	Professor of Computer Security	2013 to present

Period when the claimed impact occurred: 2015 to 2018

Is this case study continued from a case study submitted in 2014? No

1. Summary of the impact

We achieved significant **commercial and economic impact** by directly enabling security updates to the mobile phone apps of some of the largest banks, and financial and VPN service providers in the world, including HSBC, Bank of America, [text removed for publication]. We developed a new methodology and an automated tool, Spinner, which **identified critical security vulnerabilities** in 28 apps (e.g., the ability to access PIN codes and usernames). Through our responsible disclosure of these vulnerabilities, the affected banks were able to swiftly patch their insecure software, thus **improving technology**, **mitigating against future losses** and **protecting tens of millions of users worldwide** from fraud. It also enabled the National Cyber Security Centre to push for a **coordinated vulnerability disclosure policy** within the banking sector.

2. Underpinning research

Transport Layer Security (TLS) is a cryptographic protocol that underpins the security of most online traffic, from Facebook to banking and critical infrastructure. To determine which cryptographic key should be used to talk to a specific server securely, TLS relies on public key certificates. These are public statements that bind the server's identity to its public key and are signed by a trusted party called a Certificate Authority (CA). Often, a chain of such certificates is used where the first one (called root CA) represents the ultimate trust anchor. But there are hundreds of CAs globally and, if a single one acts maliciously or is compromised (as DigiNotar was in 2011, for example), then the security of TLS is lost. To mitigate this, high-security applications use a technique called "certificate pinning" through which developers can choose to only accept certificates issued by a single, pre-arranged CA in their applications.

Most security-critical applications are tested for security vulnerabilities by a penetration testing (pentesting) company before deployment. One drawback of using certificate pinning is that traditional testing techniques require owning a certificate from the same CA (with accompanying ID checks and fees). This makes it difficult for pentesting companies to test the security of the TLS connection. Certificates are not only expensive, but some CAs only issue certificates to very large organisations and/or government, not to pentesting companies, thus preventing them from conducting proper TLS testing.

Between September 2014 and June 2017, we (Chothia and Garcia) researched a solution to the problems with existing pentesting processes. We developed a new methodology [R1] and a zero-cost, open-source, automated tool called Spinner [R2] which enables testing of TLS connections at scale, even when certificate pinning is being used. For this, we leveraged a large database of internet servers and the TLS certificates they use. By redirecting an app's traffic to a server using the same certificate as the one pinned by the app, we are able to conduct a thorough analysis of the encrypted traffic between the app and the server. The tool performs a series of tests and then pinpoints the exact step of the TLS handshake that fails. Based on this information, it detects a number of vulnerabilities such as the lack of proper hostname verification. This discovery that certificate pinning obscures the lack of proper hostname verification is termed **key finding 1** [KF1].

Using Spinner, we carried out an analysis of 400 Apple iOS and Android high-security applications including banking, stock trading, cryptocurrency and VPN apps. In this sample set, we identified 11 apps that were using certificate pinning but failed to perform hostname verification. A further 6 apps accepted self-signed certificates and another 9 did not verify the hostname correctly. These failures enabled adversaries to decrypt communications, retrieve users' credentials and perform operations as if they were customers. See Table 1, below, for an overview of the vulnerable apps found. The development of our new methodology that can perform pentesting without a certificate from the relevant host CA is termed **key finding 2** [KF2].

3. References to the research

R1. Tom Chothia, Flavio D. Garcia, Christopher Heppel, and Chris McMahon-Stone. 'Why banker Bob (still) can't get TLS right: A Security Analysis of TLS in Leading UK Banking Apps'. In *21st International Conference on Financial Cryptography and Data Security* (FC 2017). Lecture Notes in Computer Science, Vol. 10322. Springer, Cham. 2017. DOI: 10.1007/978-3-319-70972-7_33.

R2. Chris McMahon Stone, Tom Chothia and Flavio D. Garcia. 'Spinner: Semi-Automatic Detection of Pinning without Hostname Verification'. In *33rd Annual Computer Security Applications Conference* (ACSAC 2017). ACM. 2017. ACM, 2017. DOI: 10.1145/3134600.3134628.

4. Details of the impact

We have directly benefited global banks, stock traders, cryptocurrency and VPN service providers, and their millions of customers across four continents by developing an automated tool, Spinner, which detects cryptographic protocol failures in security applications. Spinner has significantly **mitigated against future losses by improving methods in security-critical applications and improving existing technology**. This **commercial and economic impact** is a consequence of the responsible disclosure we made to banks, with the support of the Government Communications Headquarters (GCHQ) and the Centre for the Protection of National Infrastructure (CPNI), of the vulnerabilities identified by the underpinning research [KF1, KF2].

Mitigation against future losses: Impact on security-critical applications

As we move towards a cashless society, the security of our internet banking infrastructure is becoming more critical. The magnitude and likelihood of potential losses due to security failures is enormous. In 2019, more than 25,000 incidents of internet banking fraud amounted to losses of over £111M in the UK alone [S1]. Besides the economic impact on the banks, there is also a socioeconomic aspect, as banks typically refuse to refund transactions where the right credentials have been input [S2]. We have shown that existing flaws in the banks' own apps enable fraud [KF1]. [text removed for publication] Our research and subsequent intervention prevented this negative impact and protected tens of millions of customers globally from falling victim to fraud.

Improved technology: Impact on existing products resulting in improved security

Table 1 shows the apps that we identified as vulnerable in the underpinning research [KF2] together with their respective numbers of users. They all had insecure TLS connections that exposed their users' credentials, and therefore their bank accounts, to attackers and fraudsters.

Table 1: Vulnerable banking apps identified by the underpinning research

App name	Vulnerability	OS	No. of installs
[text removed for publication]	Pinning w/o hostname verification	Android	100k–500k
[text removed for publication]	Pinning w/o hostname verification	Android	5M–10M
HSBC	Pinning w/o hostname verification	iOS	5M–10M
HSBC Business	Pinning w/o hostname verification	iOS	10k–50k
HSBC Identity	Pinning w/o hostname verification	iOS	10k–50k
HSBCnet	Pinning w/o hostname verification	iOS	10k–50k
HSBC Private	Pinning w/o hostname verification	iOS	10k–50k
Bank of America Health	Pinning w/o hostname verification	Android	100k–500k
Meezan Bank	Pinning w/o hostname verification	Android	10k–50k
Smile - the internet bank	Pinning w/o hostname verification	Android	10k–50k
TunnelBear VPN	Pinning w/o hostname verification	Android	1M–5M
Emirates NBD	Accepts self-signed certificates	iOS	n/a
Kotak Bank	Accepts self-signed certificates	iOS	n/a
Al Rajhi Bank	Accepts self-signed certificates	iOS	n/a
Britline	Accepts self-signed certificates	Android	1k–5k
Opal Transfer	Accepts self-signed certificates	Android	100k–500k
Aman Bank	Accepts self-signed certificates	Android	10k–50k
Santander UK	No hostname verification	iOS	n/a
CommBank Property	No hostname verification	iOS	n/a
American Bank of Sydney	No hostname verification	Android	<1k
Ulster Bank NI	No hostname verification	Android	100k–500k
Ulster Bank RI	No hostname verification	Android	100k–500k
BofAML Research Library	No hostname verification	Android	10k–50k
First Financial Bank	No hostname verification	Android	10k–50k
ACU Mobile	No hostname verification	Android	5k–10k
Bitcoin.co.id	No hostname verification	Android	100k–500k

After identifying these flaws, we initiated a process of responsible disclosure that **directly led to changes in existing technologies** (the apps) **and the adoption of improved security methods**. Using the knowledge and recommendations we provided to them, financial and VPN service providers were able to patch their software.

We first informed [text removed for publication] on 27 February 2015 of the vulnerabilities in their app. These vulnerabilities, identified using Spinner [KF2], had been missed by two pentesting companies. One week later, [text removed for publication] pushed a fix. Afterwards, a similar process was carried out with [text removed for publication]. After these disclosures, it was evident that a more scalable approach to vulnerability disclosure was needed. [text removed for publication]

The reach and significance of our work is attested by improvements across global banking and financial service providers and by the stimulation of policy debate between [text removed for publication] and the UK financial sector on responsible disclosure. [text removed for publication]

As a result of our disclosures, **all of the affected apps have been fixed**, to the benefit of both the respective banks and their customers. Some of the largest affected banks have made public statements acknowledging our contribution to fixing their apps, including HSBC: 'We thank the University of Birmingham for the opportunity to work together, and we have already taken steps to address this' [S4] and Bank of America: 'The vulnerability identified in this report [R1] was resolved in Bank of America's health app in January 2016' [S4].

To ensure the continued impact of our research, we released the Spinner tool as **open source** in December 2017 so that pentesting **companies are free to use it**. Spinner's availability and a wide range of national media coverage in late 2017 [S5, S6, S7, S8, S9], led to international recognition of the importance of our research and impact. [text removed for publication]

Taken together, we have **improved the security of mobile apps across the sector**, benefiting companies, customers and the economy more broadly. A measurement study of 20 banking apps conducted by one of our students shows a sharp increase in the prevalence of certificate pinning [S10, section 3.2.2]. Significantly, the study quantifies the impact by showing that each of the banking apps using certificate pinning in 2019 does so correctly and securely [S10, section 3.4].

5. Sources to corroborate the impact

S1. UK Finance, Fraud - The Facts 2020: The definitive overview of payment industry fraud, [accessed 20/8/2020].

S2. 'Disputed Transactions', *Ombudsman News*, March/April 2014 [accessed 20/8/2020].

[text removed for publication]

S4. Maria LaMagna, 'The apps of these major banks were found to have security flaws', MarketWatch, 2017 [accessed 13/7/2020].

S5. 'Flaw discovered in banking apps leaving millions vulnerable to hack', *The Telegraph*, 2017 [accessed 10/7/2020].

S6. 'Newly created tool spots TLS vulnerability in major banking and VPN apps', *SC Magazine*, 2017 [accessed 13/7/2020].

S7. 'Security flaw puts 10 million banking app users at risk', *SC Magazine*, 2017, [accessed 13/7/2020].

S8. 'Man-in-the-middle flaw left smartphone banking apps vulnerable', *ZDNet*, 2017, [accessed 13/7/2020].

S9. 'Security Flaw In Banking Apps Make Millions Of Users Vulnerable', *International Business Times*, 2017 [accessed 13/7/2020].

S10. Andreea Gabriela Petcu, 'Security Analysis of TLS in Android Banking Applications', Final Year Project, University of Birmingham, 2019.