nccgroup
freedom from doubt

RESEARCH INSIGHTS

Sector Focus: Financial Services

Author: Matt Lewis

December 2014

CONTENTS

AUTHOR

Matt Lewis

Matt is a Principal Security Consultant at NCC Group with over 12 years technical IT security experience. His specialisms include scenario-based penetration testing, vulnerability research, incident response and development of security testing tools. Matt's penetration testing and consultancy experience spans all manner of technologies across all sectors and many FTSE 100 and Forbes 2000 companies.

INTRODUCTION

At NCC Group we have the opportunity to get involved in a vast breadth and depth of security assurance activities on a regular basis. This provides visibility not only of which classes of vulnerability are most prevalent in different types of product and sector, but also through our Cyber Defence Operations, which vulnerabilities are actually being exploited.

This report provides some insight into what trends we are seeing in our industry, including how people are attacking systems, defensive measures that are being employed and how those within a specific market sector (financial services) are dealing with the current threats. The report concludes with some more general technology trends and threats.

Sector Focus
Financial Services

Phishing

During the past year the financial services sector has seen a staggering rise in targeted phishing attacks. The Anti-Phishing Working Group reported that in the last six months of 2013 that more than half of phishing attacks targeted financial services [1]. These statistics show a paradigm shift whereby attackers (most likely organised crime) are seeking to exploit actual financial institutions and their employees; different to the usual targeting of financial institution customers.

Phishing attacks exploit people, processes and technology. Any phishing attack success across financial services is therefore indicative of control failures across these three elements. Typically this is due to either a lack of user education, weak and ageing processes and legacy, or out-dated software.

From NCC Group's experience the common phishing attack vectors against financial institutions rely on tricking users to click on links or download and run executables either from:

- A crafted email
- Visiting a legitimate website that has been compromised
- Visiting an illegitimate website (e.g. domain squatting)
- Accessing removable media

Once tricked into performing actions NCC Group commonly sees examples of:

- Cross-Site Request Forgery (CSRF) attacks (User is tricked into clicking on a link which performs an action such as transferring funds.)
- Cross-Site Scripting (XSS) attacks (User is tricked into clicking on a link which steals their session cookies/tokens which can be used to hijack authenticated sessions on financial applications.)
- Malware Downloads (e.g. installation of a Remote Access Trojan such as Zeus)
- Browser Exploitation (e.g. 0-days in browsers or browser plugins such as Java, Flash etc.)

From the points above clearly there are many effective controls required to minimise the potential for phishing success. Fundamentally these controls need to be derived from robust Policy and Governance across financial institutions. In the short term it is certainly recommended that financial institutions revisit IT security policies and that these are updated to include and dictate the necessary controls for mitigating the risk of phishing.

Targeted Financial Malware and Remote Access Trojans (RATs)

Related to phishing is the recent increase in malware targeting financial institutions. Earlier this year cyber criminals drained over €500,000 from more than 190 customers at a European bank in the space of one week. [2]

RATs and Command & Control (C&C) botnet infrastructures, such as Zeus are still very much in operation across the Internet and continue to be developed and modified with functionality to exploit flaws in financial applications. If a customer is authenticated to a financial application and is unaware of malware running on their device (e.g. laptop) then that malware may be capable of performing authenticated transactions with the privileges of the authenticated victim, perhaps without the victim's knowledge.

[1] http://www.atmmarketplace.com/news/more-than-half-of-phishing-attacks-target-financial-services/
[2] http://www.computerweekly.com/news/2240223299/Cyber-thieves-tap-over-500000-from-European-bank

In recent times there has been a marked improvement in the exposure of vulnerabilities such as SQL injection and cross-site scripting.

A number of controls can be introduced within financial applications that will minimise the potential for unauthorised control by malware. Non-exhaustively these include:

- Use of anti-CSRF tokens across all web application requests
- Use of two-factor authentication to authenticate all transactions (and/or other challenge-response mechanisms)
- Secure cryptographic implementation (e.g. SSL/TLS) and where possible use of certificate pinning within client software

Financial Software Flaws

Recently a dive into financial software was performed by high-profile financial experts [3]. The article informs of "The terrible state of software code in elements of the financial industry, including at locations linked to major trading venues, is a plague to investors and remains a ticking time bomb ready to badly damage the wider economy."

From NCC Group's recent experience of testing financial system software in recent times there has been a marked improvement in the exposure of vulnerabilities such as SQL injection and cross-site scripting. What NCC Group has been seeing which is directly impacting on financial systems is:

- Processing of exponents in some languages leading to DoS. e.g. financial packages for Java can cause a DoS via memory exhaustion if given a large enough number such as 9E1000000000.
- Race conditions – non-deterministic results when performing the same transaction more than once and at the same time.

Race Conditions, or Time of Check, Time of Use (TOCTOU) vulnerabilities in financial software, which are commonly overlooked during functional and security testing are regularly identified by NCC Group. Time and order sequence is crucial to correct financial software operation. Many financial transactions rely on checking balances and values (sometimes in real-time) before processing. If there is latency or delays between these checks and/or if lack of resource coordination is implemented around multi-threaded solutions then there may be scope for manipulating application logic, perhaps for financial gain.

Consider the following example commonly seen by NCC Group. A user is authenticated to a financial application concurrently from two different devices (but with the same session). A transaction is performed seeking to transfer money from account number 1019 to account number 9823 for the amount of £100.

Suppose the server-side code is as follows and that the user's account balance is £100:

```
1: if (amount <= account_balance) {
2:      account_balance = account_balance – amount
3: }
```

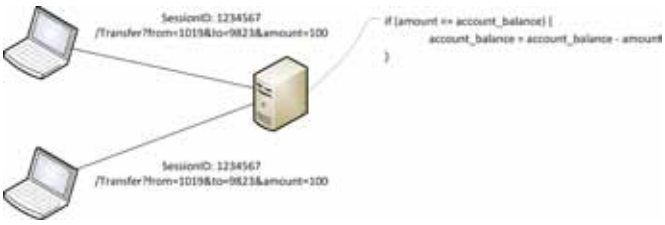

Figure 1 - Concurrent sessions can lead to Race Conditions

[3] http://www.forbes.com/sites/leoking/2014/06/07/terrible-state-of-financial-software-code-plagues-investors/

Sector Focus
Financial Services cont...

If the same transfer request can be fired into the web application at the same time then there is the potential that line 1 in the code is executed twice (e.g. multi-threaded) before line 2 is executed. If this occurs, then the first check that £100 is <= £100 holds true twice and so when the if statement block executes, the account_balance value is decremented by £100 twice, meaning that the user has been able to transfer more money than allowed (as dictated by the if statement in the source code).

NCC Group has tested the above using two or more devices running the same application session across many financial applications and has been able to demonstrate use of funds not allowed by the presumed application logic. The implications of this could be severe depending on the nature of the application as it opens up the potential for theft and/or use of unauthorised amounts of money and provides a potential mechanism for fraud and other laundering activities.

In terms of mitigation, the application logic for financial applications needs to be properly designed, tested and implemented. Where necessary, resource locks should be placed on critical components and/or batch processing used to implement a more linear and deterministic set of transactions to be processed. Transaction auditing is also crucial in this domain as such logs could prove valuable insight into potential abuse in these areas.

Legacy Issues

As with most sectors, financial services are still largely affected by legacy issues – i.e. use of out-dated and unsupported software. For backend systems this is not necessarily surprising as financial systems are often revenue-generating or financial processing 24/7, meaning that downtime for those systems for updating or maintenance, even for just a few seconds might not be an option. In these situations key to protection is proper segmentation (firewalling and limiting access to critical backend systems) and ensuring that endpoint security (i.e. laptops and desktops) is maintained to high standards. On top of all of this is authentication and passwords. We are still seeing "Password1" protecting access to financial systems in 2014. As mentioned earlier in this briefing, such an observation hints to likely poor or lack of robust Policy and Governance at some financial institutions.

Application Layer (DoS)

A relatively recent concern regarding Internet-facing financial systems has been application-layer DoS attacks [4].

This is where software flaws at the application-layer might be invoked to perform a DoS attack against a server. Whereas traditional DoS or DDoS attacks might require tens or hundreds of thousands of hosts attacking a server at the same time; an application-layer DoS flaw could be exploited by one host only and would not be detected or blocked by traditional DDoS protection mechanisms. Examples seen by NCC Group from testing around this issue over the past year include:

- Invoking complex database queries - either through SQL injection or implementation of inefficient stored procedures
- File create/write operations – resource exhaustion
- Parsing and recursive functions – e.g. flaws in XML and regular expression processing
- Large object instantiation – e.g. large Java/.NET objects created at runtime
- Large memory allocations
- Infinite loops (intentional or unintentional)
- Cryptographic and hashing functions (e.g. web applications performing thousands of iterations of hash functions for password hashing)
- Flaws in email and registration functions

[4] https://www.nccgroup.com/media/481243/the-new-ddos-battleground-white-paper-final.pdf

As with most sectors, financial services are still largely affected by legacy issues

The main mitigation to these flaws is focused source code review around potentially vulnerable areas in conjunction with active testing for these flaws (in non-production environments).

Cloud and Data Management

This year NCC Group surveyed CIOs from financial services companies with over 1,000 employees and found that less than half of those questioned carry out third party audits of prospective cloud providers prior to engagement, and over 60 per cent say that they do not have any contractual protection in place if their cloud provider fails.

The use of cloud for financial services has raised many questions and issues which are not properly addressed and understood These include:

- Data management – where is corporate and customer data stored (logically and physically)?
- How easy is it to delete data (e.g. across multiple load-balanced and redundant/elastic systems)?
- How can it be proved that deletion of data is comprehensive (from memory and disk)?
- What are the data protection laws in the respective countries of where cloud data is held?
- How are any offsite backup tapes protected?

The many layers of abstraction offered by cloud providers does therefore drastically reduce the grasp of auditing across systems hosted by those cloud providers. For financial services (a highly regulated industry) there is therefore an open question as to whether cloud services can meet the audit requirements and demands of regulating bodies from internal audit to entities such as the Financial Conduct Authority (FCA)?

Industry Change - CBEST

A major drive is afoot within the financial services industry to improve security through better intelligence sharing. It has been recognised that penetration testing has become compartmentalised, only looking at small systems in isolation. Additionally the financial sector has traditionally been reluctant to test critical systems. As a result a new framework to deliver controlled, bespoke intelligence-led cyber security tests has been introduced: Central Bank Ethical Security Test (CBEST) [5].

The aim of CBEST is for:

- Testing to replicate behaviours of real-world threat actors
- Obtaining closer synergy with intelligence providers and agencies
- Testing security posture and proactive and reactive incident response procedures

CBEST will therefore offer much more than traditional bespoke penetration tests against systems in isolation. Organisations should be aware that in order to be effective, CBEST will require detailed planning, meetings with a number of different stakeholders (BoE, threat intelligence providers, SIROs, CBEST-accredited testing company etc.) with a clear view to development of an improvement strategy, this will provide organisations with a view of failures in people, process and technology such that adequate training, policy and technology change can be implemented or improved to minimise the potential for cyber attack against financial organisations.

[5] http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

CONTACT US

+44 161 209 5200
response@nccgroup.trust
@nccgroupplc
www.nccgroup.trust

United Kingdom

Manchester - Head office
Manchester Technology Centre
Oxford Road
Manchester
M1 7EF

Cheltenham
Eagle Tower
Montpellier Drive
Cheltenham
GL50 1TA

Milton Keynes
Suite 526-528
Elder House
Eldergate
Milton Keynes
MK9 1LR

Edinburgh
37 York Place
Edinburgh
EH1 3HP

Leatherhead
Kings Court
Kingston Road
Leatherhead
KT22 7SL

Glasgow
The Beacon
176 St Vincent Street
Glasgow
G2 5SG

London
Floor 4
Tavistock House North
London
WC1H 9HR

Europe

NCC Group - Switzerland
Ibelweg 18A
CH-6300 Zug
Switzerland

NCC Group - The Netherlands
Veemkade 396
1019 HE Amsterdam
The Netherlands

NCC Group GmbH - Germany
Heimeranstrasse 37
D-80339 Munchen
Germany

FortConsult - Denmark
Tranevej 16-18
DK-2400 Kobehavn NV
Copenhagen
Denmark

North America

iSEC Partners
Suite 1020
123 Mission Street
San Francisco
CA 94105

iSEC Partners & NGS
4029 South Capital of Texas Hwy
Suite 100
Austin, TX 78704

Matasano
39 W. 14th St.
Suite 202
New York
NY 10011

Matasano
53 W.Jackson
Suite 464
Chicago, IL 60604
USA

iSEC Partners - Seattle
720 3rd Avenue
Suite 2101
Seattle

Asia Pacific

NCC Group - Australia
2.08/56 Bowman street
Pyrmont NSW 2009
Australia

www.nccgroup.trust
@nccgroupplc