Diploma Programme
Programme du diplôme
Programa del Diploma

Computer science
Case study: electronic banking

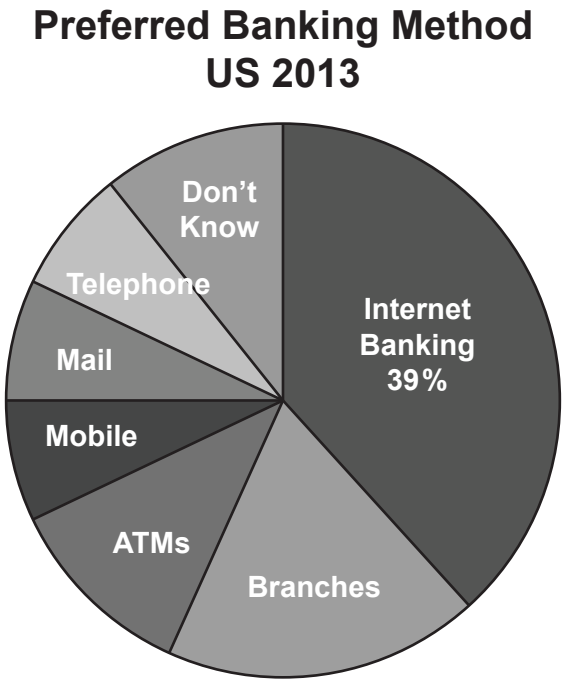
For use in May 2015 and November 2015

Instructions to candidates

- Case study booklet required for higher level paper 3.

Introduction

Banking in the modern sense began in Italy in the 14th century when farmers borrowed money in order to finance the sowing of their crops, with the value of their crops being held against the loan. The people arranging these credits carried out their business on benches in the agricultural markets – the word "bank" derives from *banca*, the Italian word for "bench". Similar banking practices spread throughout Europe with the banks taking up residence in more permanent establishments, where they have since become the central pillar underpinning financial transactions, first between businesses, and then individuals.



The last twenty years have seen a dramatic change in the way that banks interact with their customers, with the advent of online banking made possible by the development of the internet.

The consequence is that banks are gradually moving their business transactions from the physical world of their city branches to the virtual world[1]. The innovations in technology have revolutionized the banking industry with transactions now being made almost instantaneously from any point on Earth that is within reach of an internet connection.

The cost advantages for the banks and the convenience factors for the customers are clear, but there is a downside to this. Security and authenticity are the fundamental cornerstones of all financial transactions and the entire banking system is dependent upon the secure transmission of data. Revelations reported by *The Guardian* newspaper in September 2013 that the encryption standards used for these transactions may no longer be safe are therefore a cause for considerable concern[2].

The last few years have seen further changes with a strong move towards mobile banking and mobile payments as the ownership of smartphones and tablets has increased. Customers using these devices expect their banking services to be available when they are on the move, demanding both security and ease of use; a difficult compromise for the IT personnel at these banks.

This Case Study looks at the operations of the fictious bank, *TransEuropa*. The focus is on the computer science underpinning both the operations and the security aspects of banking transactions.

---

1 http://www.aba.com
2 http://www.theguardian.com/…/nsa-gchq-encryption-codes-security

TransEuropa

TransEuropa is based in a European country where it has been established for many years. It also has a presence in some developing countries where its branches are confined to the major cities.

In an interview with Michael, the Head of IT Operations, he explained how security was a top priority in their banking operations. He described some of the procedures currently in place.

> "Even though our internet banking operations in Europe have been in place for several years, we continually have to address the security issues surrounding our operations. For customers to have confidence in our company, it is essential that they are satisfied that the possibility of fraud is minimized.
>
> "Two main areas of attention are authentication and secure transmission of data. Our login process used to be based on the entry of a username and password, but this has been changed to 2-factor authentication. Now the customer replies to a security question and then enters a TAN (transaction authentication number), which is a type of one-time password. Each of our online customers has been sent a special keypad device which is able to generate the TAN, after the user has typed in a code known only to themselves and the bank. They are able to continue with their transaction or enquiry only after the answer to the security question and the TAN have been verified by the bank's server."

Michael then addressed the security of transmissions. He explained that, as the online operations are carried out over the internet, the security was based on the SSL protocol, which makes use of both asymmetric and symmetric encryption. An extended validation digital certificate issued by a Certificate Agency is sent from the bank's server to the client's computer.

Recent developments have suggested that this encryption can in fact be broken, which is of great significance to any business wishing their data transmissions to be secure. Michael questioned whether the current encryption key length of 2048 bits might now be breakable by brute-force decryption methods or whether certain agencies had made use of backdoor methods in decrypting the transmissions[3]. Either way, he said, there was a constant need to review the bank's security procedures.

Threats from malware are also a permanent concern to the banking industry. Michael highlighted both phishing exploits and the Man-in-the-Browser Trojan as particular dangers that customers should be aware of. He suggested that further measures would be considered by the bank, such as out-of-band verification, to minimize the risks posed by these threats.

---

[3] http://www.computerweekly.com/news/…/US-acts-to-restore-...

Mobile Banking

Internet banking was originally restricted to personal computers, but the explosion in mobile technology and the ability of smartphones and tablets to access the internet has led to an increasing demand for mobile banking.

This increase is shown by the following statistics which were taken from the 2013 Annual Mobile Banking and Commerce Summit[4]:

- This year, 590 million mobile phone users globally will use their device for banking purposes. In 2017, that number will exceed 1 billion.
- Worldwide, banks will spend $118 billion on technology and mobile banking in 2013.
- 81 of the top 100 US financial institutions currently offer some form of mobile banking.

TransEuropa has already taken two different approaches to this area. When questioned on this topic, Michael explained that the approach in the developing countries differed from that used in Europe due to the differences in the available technology of the customer base. He went on:

> "In Europe, we want to offer our mobile customers the same range of services available to our PC users. However, mobile devices come in all shapes, sizes and specifications, so we need to try to tailor the content to the specific device. To achieve this, we employ mobile device detection technology to the HTTP requests arriving at our servers. This detection is based on reading the user agent header field and correlating the data held there with the different models described in the Device Description Repositories. We provide a combination of push and pull technologies and try to persuade our customers to download apps that are specific to their device. We also offer certain SMS banking facilities."

He went on to describe how the level of security of mobile phone transmissions varied depending upon the type of connection.

> "Customers may be using WiFi, where the connection might be controlled by either WPA or WEP protocols, or they might be using an unsecured service. If they were connected through their phone company they would be using GSM protocols."

He continued by explaining that mobile banking in the developing world has taken a radically different approach.

> "Our customer base in our European operation is completely different from that in the developing countries. In Europe, most of our customers are connected to the internet and require internet banking facilities. They expect to be able to conduct all of their financial operations online. Compare that to the developing countries where our operations are limited to cities and where most customers still physically come to the bank to conduct their business. The majority of the rural population don't have access to the internet. In fact, the majority don't have a bank account. However, the majority do own mobile phones."

---

[4] https://blog.compete.com/…/mobile-banking-today-highlights-from-mcs2013/

He went on to explain how *TransEuropa* had entered into a partnership with a local telecommunications company in one of the developing countries in order to provide basic financial services to the rural population, even though they had no bank accounts. They were basing their operations on the success of the M-PESA system in Kenya, where mobile phone owners are able to make certain payments, either for services, such as utility bills, or to transfer money to another person or even between countries. Credit can be added to each phone (or cashed in) at any of the mobile phone operators' offices which are scattered throughout the country.

"People are able to use their air-time credit as a mobile bank account", continued Michael. "It works because the majority of the adult population own mobile phones which can send SMS messages. Part of our role is to develop the STK (SIM Application Toolkit), which provides the interface with the user."

New Developments

The first was the development of a Mobile Wallet app which the bank's customers could download onto their smartphones. This app would allow them to use their smartphones to pay for goods with either store cards or with credit/debit cards at stores that had the necessary technology installed. Michael referred to *Starbucks* as a chain in which a significant percentage of sales were conducted in this way, and to *Pingit* and *Zapp* as two mobile payment services that were already in operation with other companies. The same app would also allow customers to access ATMs without the need for a bank card.

> "This idea of a Mobile Wallet is one which we expect most of our customers to eventually embrace, as people look for quicker and easier ways of making their purchases. We believe that it is a market we should enter, as customers are more likely to trust technology that is provided by the banks. The choice we have is to either make use of 'contactless' technology using NFC or to use QR codes as part of the payment process. In either case the safeguarding of sensitive information will be a priority."

He pointed out that *Visa Europe* predicts that, by 2020, more than half of its transactions will be carried out on a mobile device[5].

The second development was the investigation into the use of biometrics in providing even more secure authentication and verification. Biometrics has been used as part of multi-factor authentication in areas such as immigration for some time, but for various reasons its incorporation into banking services has been slower.

Michael concluded by summarizing the main issues concerning modern banking from the technology point of view with a look towards the future.

> "The main areas that are essential for maintaining and increasing our customer base are authentication, data security and user interface. For authentication, we will increasingly be looking towards the use of biometrics. For data security, we will need to continuously monitor the encryption standards used on the internet (SSL/TLS) and for mobile phone transmissions (WiFi and GSM protocols). Although some traditional services will have to be maintained, the majority of our customers increasingly want services such as internet banking and mobile payments to be a seamless part of normal life where the quality of the service is often more important than the provider. If we are to survive we must adapt to the ever-changing landscape."

---

[5] http://www.bankingtech.com/...-payments-play-with-first-data/...

Challenges Faced

Michael and *TransEuropa's* challenges for the immediate future are:

- to prepare a report on the different encryption protocols currently being used and how they might change in the future;
- to design the user interface that will work with the STK for their developing world mobile project;
- to complete the research necessary for developing the Mobile Wallet project;
- to review the authentication procedures in order to increase the security of banking operations.

Additional Terminology To The Guide

Apps
Asymmetric / symmetric encryption
Authentication / 2-factor / multi-factor authentication
Backdoor methods
Brute-force decryption
Contactless technology
Device Description Repository (DDR)
Extended validation digital certificate
Global System for Mobile communication (GSM)
HTTP(S)
Man-in-the-Browser (MitB) Trojan
Mobile Wallet
M-PESA
NFC
One-time password
Out-of-band verification
Phishing
Pingit
Push / Pull technology
QR codes
SMS
SSL/TLS
STK (SIM Application Toolkit)
Transaction authentication number (TAN)
Trojan
User agent header field
WEP
WPA
Zapp

Some companies, products, or individuals named in this case study are fictitious and any similarities with actual entities are purely coincidental.