A Survey of Authentication and Communications Security in Online Banking

SVEN KILJAN, NHL University of Applied Sciences, Open Universiteit, Radboud University
KOEN SIMOENS, Verizon Enterprise Solutions
DANNY DE COCK, KU Leuven
MARKO VAN EEKELEN and HARALD VRANKEN, Open Universiteit, Radboud University

A survey was conducted to provide a state of the art of online banking authentication and communications security implementations. Between global regions the applied (single or multifactor) authentication schemes differ greatly, as well as the security of SSL/TLS implementations. Three phases for online banking development are identified. It is predicted that mobile banking will enter a third phase, characterized by the use of standard web technologies to develop mobile banking applications for different platforms. This has the potential to make mobile banking a target for attacks in a similar manner that home banking currently is.

Categories and Subject Descriptors: K.4.4 [**Computers and Society**]: Electronic Commerce—*Security*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Authentication, invasive software, unauthorized access*

General Terms: Security

Additional Key Words and Phrases: Online banking, mobile banking, authentication, communications security, WWW security, mobile security, multifactor authentication

ACM Reference Format:
Sven Kiljan, Koen Simoens, Danny De Cock, Marko van Eekelen, and Harald Vranken. 2016. A survey of authentication and communications security in online banking. ACM Comput. Surv. 49, 4, Article 61 (December 2016), 35 pages.
DOI: http://dx.doi.org/10.1145/3002170

1. INTRODUCTION

An overview of the worldwide current state of online banking security was made in 2002 [Claessens et al. 2002]. It provided a state of the art that gave many researchers a base for their work. Since then, the adoption of online banking and the different ways to conduct it has changed quite a bit. We provide a new state of the art, based on a longer observation period between 2013 and 2015, and with a larger number of banks from different parts of the world. The scope of our work is authentication and

This work is a product of the Dutch Research Program on Safety and Security of Online Banking. The research program is funded by the Dutch banking sector (represented by the Dutch Banking Association), the Police Academy, and the Dutch National Police.
Authors' addresses: S. Kiljan and M. van Eekelen, Institute for Computing and Information Sciences - Digital Security, Radboud University, Postbus 9010, 6500GL Nijmegen, The Netherlands; emails: {s.kiljan, m.vaneekelen}@cs.ru.nl; K. Simoens, Verizon Enterprise Solutions, Culliganlaan 2E, 1831 Diegem, Belgium; email: koen@simi.be; D. De Cock, Department of Electrical Engineering - Computer Security and Industrial Cryptography, KU Leuven, Kasteelpark Arenberg 10, bus 2452, B-3001 Leuven-Heverlee, Belgium; email: decockd@esat.kuleuven.be; H. Vranken, Faculty of Management, Science and Technology, Open Universiteit, Postbus 2960, 6401DL Heerlen, The Netherlands; email: harald.vranken@ou.nl.

DOI: http://dx.doi.org/10.1145/3002170

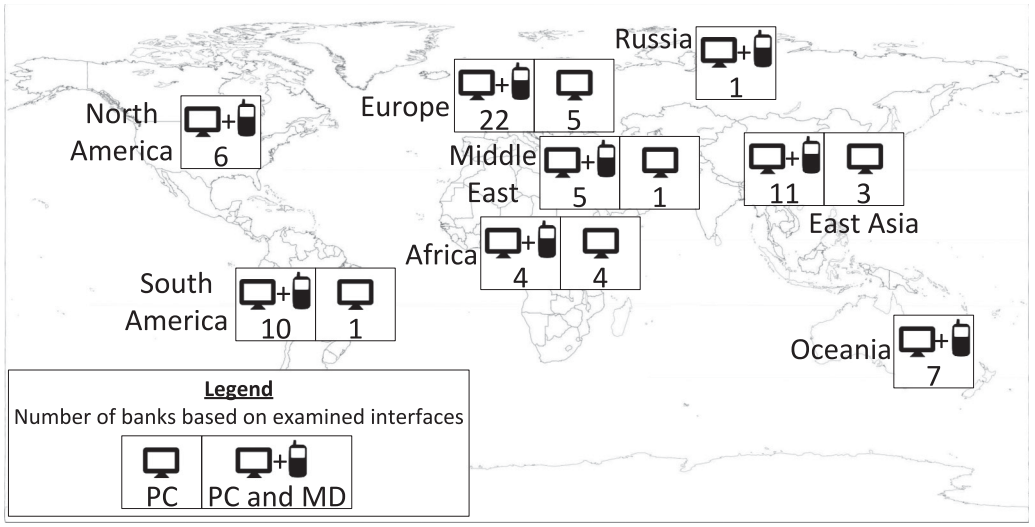

Fig. 1. Overview of worldwide surveyed banks.

communications security between banks and customers. These aspects were picked since they form a first line of defense against online banking fraud. Used information sources were the websites of banks and publicly available documentation.

In 2013, we examined 81 banks on SSL/TLS use and offered customer authentication methods. The resulting data was distributed in a technical report [Kiljan et al. 2014a]. 80 of the same banks were examined again by us in the first half of 2015 (the number of banks has been reduced by one since two European banks merged between 2013 and 2015). Search criteria for choosing the banks in 2013 were based on global representation and type of bank. The new data and comparisons with data from 2013 are included in this new article (see Figure 1 for an overview of the global distribution of the 80 surveyed banks between North and South America, Europe, the Middle East, Africa, Russia, East Asia, and Oceania).

The focus was on banks that provide account and payment services to consumers and small businesses (also referred to as "retail banks"). The assumption was made that retail banks with the most assets have the most customers. Having the most customers makes them represent how most people in their countries use online banking, and it also makes them a larger target for attacks conducted through customers. Random banks were picked for countries where the amounts of assets were closeer to each other or unclear. Language barriers were overcome by colleagues who translated critical information and by automated translation tools. We only examined publicly available documentation and software.

Due to technical, security, and usability differences between the different types of devices owned by banking customers, a distinction is made throughout this article between the use of Personal Computers (PCs) and Mobile Devices (MDs) for home banking and mobile banking, respectively. All banks were examined on how they facilitate home banking, while mobile banking services were examined at 66 banks.[1] Figure 1 makes a distinction between banks that were examined for the services they provide for both home and mobile banking, and for banks that were only examined for home banking.

[1]We could not find information about any offered mobile banking services for the other 14 banks.

The remainder of this article starts with Section 2, which opens with a short history of electronic banking and follows with an identified trend in the development of both home and mobile banking, based on both technological and sociological development.

The results of the conducted survey are split into two sections, based on the direction of the authentication process. In Section 3, the wide range of methods to authenticate users to banks are discussed for both home and mobile banking. Banks use the SSL/TLS protocol suite to authenticate to their users in the opposite direction and to provide communications security. Findings about how well banks implement SSL/TLS can be found in Section 4.

Section 5 reflects on the differences in uniformity between communications security and user authentication, and the limitations of our survey. It also provides some pointers for possible further research, based on the current development of online banking and the knowledge gained from the survey. Related work is mentioned in Section 6 and we give our concluding remarks in Section 7.

The first major contribution of this article consists of a mapping of online banking development phases based on technological and sociological developments, as well as an insight that describes the future adoption of web standard-based Hybrid Mobile Applications and how this development has the potential to make mobile banking a future target for exploitation by adversaries. This can be found in Section 2. Our second major contribution is the survey data and analyses of data from different time points in Section 3 for user authentication methods in home and mobile banking, and in Section 4 for communications security in home banking. Data is compared between 2013 and 2015. Additionally, for user authentication methods a comparison is made with data from 2002.

2. ONLINE AND MOBILE BANKING DEVELOPMENT

This section notes the history of electronic banking and an identified trend in the development of online and mobile banking platforms. Based on these observations, we note a number of security implications in the further development of mobile banking.

2.1. A Short History of Electronic Banking

The electronic transfer of money was already offered in 1871 as a service [Western Union 2012]*. However, transmitting money orders through a telegraph relied on operators to translate between human language and Morse code. It would take almost 110 years before banking customers could do something similar themselves from the comfort of their homes. Starting from the beginning of the 1980s, it became possible for customers to simply call the bank and talk to an employee through a telephone instead of visiting a branch office [Allchin 2012]*. Customers were capable of managing their account remotely. However, employing call operators to assist customers is expensive. Banks looked at ways to remove the bank employee from the process. The most obvious approach was to let customers interact with a bank computer.

Introduced in 1983, PRONTO was the first electronic banking system that did not rely on bank employees to be used by customers. Access to the system was possible with various types of home computers and a modem [Burns 1983]*. Similar systems soon followed. An example is Citibank's Direct Access, which could be accessed through a Commodore 64 or a phone with an embedded terminal [Moser 2012]*. These pioneers share a technical characteristic, which is that they all relied on proprietary terminal-based software. If a home computer was used, it was little more than a gateway to the user interface provided by the bank's computer.

This changed slowly at the end of the 1980s and during the 1990s. Having a continuous connection with a bank through a phone line to conduct banking business was expensive. To reduce costs (and with that, make it more accessible), so-called "home banking software" was developed. Utilizing the increase in processing power, memory,

and storage space, bank customers could now conduct their banking business offline for the most part. Only a brief modem connection with the bank was necessary to receive up-to-date account information, such as an account's transaction history and balance, and to transmit money transactions.

The Internet became more accessible at the end of the 1990s. Some banks updated their home banking software to support the use of the Internet to connect a customer's computer with the bank, instead of directly through a telephone line. Other banks saw potential in the World Wide Web (WWW), which offered a standardized way to present information to users and receive information from users through the Internet. A customer does not need any client-side software aside from a standard web browser when accessing a bank's website. When banks offer websites to conduct online banking, it saves them the effort of developing, maintaining, and distributing platform-specific client-side software. Banks either had a website for online banking, or soon provided one after the turn of the millennium. Home banking software was slowly being discontinued, and by 2013 most banks only provided a website for online banking on home computers [Kiljan et al. 2014a].

Mobile banking is online banking through a mobile device in a way that is more location independent compared to home banking. It started with the Wireless Application Protocol (WAP) in the period in which home banking was becoming more mature.[2] WAP can be described as a "light" version of the WWW and its underlying technologies. After it was introduced in 1997, banks started to offer mobile online banking services [ITavisen 1999]*. The use of WAP can be compared to the use of terminal-based electronic banking that was done on home computers at the beginning of the 1980s: it was revolutionary yet not user friendly, quite expensive, and accessible only by a limited user base.

The mobile operating systems Android and iOS became popular to develop online banking applications for after 2010. Developing and publishing applications for both platforms is relatively easy, and most banks provide applications for these mobile operating systems [Kiljan et al. 2014a]. Mobile banking is also widely being embraced by customers since that time. The number of mobile banking users has been growing substantially in Belgium since 2013 [Febelfin 2015]* and in the United States since 2011 [Board of Governors of the Federal Reserve System 2015]*. The number of mobile banking logins surpassed the number of site logins in the United Kingdom in 2015 [BBA 2015]*. In volume of transactions, most are performed through mobile banking for the majority of banks worldwide, and an exponential increase in the number of users is expected for the period 2020–2025. The highest adoption rates are in developing countries (such as China and India) [KPMG 2015]*. So far, the use of "traditional" home banking (using personal computers) is not declining. Mobile banking seems to be used in addition to home banking, not as a replacement [Board of Governors of the Federal Reserve System 2015; Cetera 2015]*.

Overall, online banking is very popular in different parts of the world. For 2014 in the United States, it was estimated that 74% of consumers with a bank account interacted with it through home banking while 35% did the same through mobile banking [Board of Governors of the Federal Reserve System 2015]*. For the same year in Europe, the estimation is that 44% of individuals aged 16 to 74 used home and mobile banking [Eurostat 2016]*. This varies for individual countries in Europe. Bulgaria and Romania had relatively low numbers of persons using online banking (4%–5%), while Iceland, Norway, and Finland had relatively high numbers (all above 85%). Separate home and mobile banking statistics are not available for the whole of Europe, but some individual countries release such numbers. For Ireland it was reported that in 2014

[2]We do note that SMS was used for mobile banking earlier and is still offered today by some banks, but elect to concentrate on online (Internet-based) banking instead.

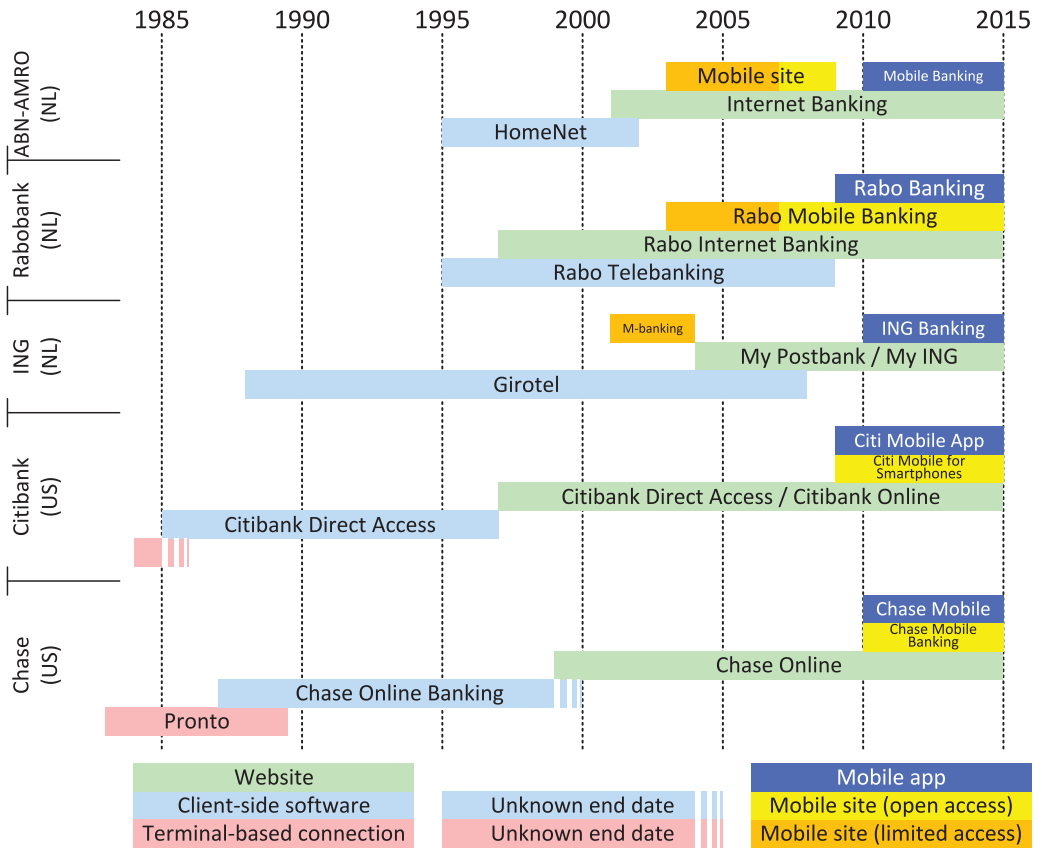

Fig. 2. Some examples of the development of online banking from the Netherlands (NL) and the United States (US).

home banking was used by 2.4 million users and mobile banking by 1.0 million users [Banking & Payments Federation Ireland 2015]*. Based on the last population count of 2011 [Ireland's Central Statistics Office 2012]*, Ireland's population of individuals aged 15 to 74 was 3.37 million. Therefore, the relative population in Ireland that used home and mobile banking can be estimated to be 71% and 29%, respectively. We can also make an estimation for China for 2013. Home banking was applied by 77.1% of the population that used the Internet, and the same value for mobile banking would be 44.6% [iResearch 2014]*. The total number of Internet users in China at the end of 2013 was 618 million [China Internet Network Information Center 2014]*. For the same year, the estimated population size of people aged 15 to 64 was 74% of the total population (estimated to be 1,357 million), so around 1,004 million [World Bank Open Data 2016]*. When assumed that only people aged 15 to 64 would use the Internet, it can be estimated that 47% of the Chinese population aged 15 to 64 used home banking in 2013. For the same year and the same population, the estimation would be 27% for mobile banking.

2.2. Development and Acceptance of Online and Mobile Banking

Figure 2 illustrates when what kind of online services were offered by several banks in the United States and the Netherlands. This figure is used to show the similarities between the development of home banking and mobile banking. We chose these two countries because banks in the United States were among the early adopters to offer

home banking services, while the same is true for the banks in the Netherlands for mobile banking.

Three technological phases for the development and use of home banking are identified: early adoption, expansion, and exploitation. Some early adopters (both banks and customers in the United States) started with electronic banking using a terminal-based modem connection through a phone line. This evolved into intelligent client-side software that allowed connections with the bank either directly through a phone line or (later) through the Internet. It was this second phase that most banks in the United States and the Netherlands started to offer online banking services that were picked up by the masses, which is why we named it expansion. All banks continued with the exploitation phase and broke off the second phase around the turn of the century. Sites were preferred above client-side code, and eventually were the only way to conduct home banking.

The Technology Acceptance Model (TAM) can be applied to examine what motivates users to accept (intent to use) new technologies. TAM can also be applied to online banking [Lai and Li 2005]. The overlapping conclusions from research that applies TAM on home banking indicates that the most significant motivators are perceived usefulness and perceived credibility (trust) [Pikkarainen et al. 2004; Chong et al. 2010; Kesharwani and Bisht 2012]. Perceived ease of use has no direct significant effect on the intention to use online banking, although it can indirectly do so by affecting perceived usefulness.

For home banking in the early adoption phase, initially not many people had computers at home and hardware to make dial-up connections. The intent to use might have been there (if home banking would be perceived as useful and trustworthy at this time), but the ability to actually do so was simply missing. This changed in the expansion phase, in which more bank customers had access to computers at home and more banks started offering home banking. The idea that one could manage their bank affairs from the comfort of his or her home using a personal computer they already owned was considered useful and there was enough trust for users to intend to use it, which they did. Banks switched technologies in the exploitation phase from proprietary client-side code to open web standards by offering websites accessible through popular browsers. Adoption rates did not stall since the use of a browser instead of a bank's own application did not hamper the perceived usefulness and perceived credibility by bank customers.

The development of the technological phases of mobile banking and motivators to use it are similar. Expectations were high [van den Heuvel 2001]*, but the early adoption phase in the Netherlands was not successful [Houtman 2002; Tomesen 2006b]*. Early mobile sites used standardized technology for web page distribution (I-mode, WAP, or HTTP), but these sites could only be reached if the mobile provider allowed access to the site and if the mobile phone supported the necessary security features to access the site. Therefore, as with the early adoption phase of home banking, not all potential bank customers were able to use mobile banking. The expansion phase began in 2007, when providers started offering more open Internet access and affordable data subscription plans [Tomesen 2006a; Boogert 2008]*. All mobile sites were now easier to reach, including those of banks. It was also around this time that the mobile operating systems Apple iOS and Google Android were introduced to the market, which both offer a very developer- and user-friendly ecosystem. This made most banks release mobile applications around 2010, which were quickly accepted by their customers. Mobile banking is now offered by a large number of banks[3] and its adoption by customers is steadily climbing [Wilhelm 2014; Board of Governors of the Federal Reserve System 2015]*.

[3]Of the worldwide 80 banks examined in the survey for this article, at least 66 offer mobile services.

The TAM has also been used to examine which perceptions contribute most to the acceptance of mobile banking. As with home banking, perceived usefulness and trust are large motivators to accept (use) mobile banking. Unlike home banking, perceived ease of use also has a direct influence on the intent to use mobile banking [Luarn and Lin 2005; Gu et al. 2009]. One explanation for this is that most mobile banking users use mobile banking in addition to home banking, instead of replacing the latter with the former [Board of Governors of the Federal Reserve System 2015]*. The main (perceived) reasons to use mobile banking are the ability to access one's bank account from anywhere, that it saves time, and that it can be used without either using a home computer or visiting a bank. This is in contrast to home banking, where the main reasons also include managing household finances and financial tasks without visiting a bank [Cetera 2015]*. As mobile banking offers partially redundant functionality, perceived ease of use is also considered important. If it would not be (perceived to be) easy to use, users would be inclined to exclusively use home banking.

For mobile banking in its early adoption phase, the intent to use it was there for some part (as with home banking, due to the existing perceptions of usefulness and trustworthiness), but it was not perceived as being easy to use. Aesthetics play an important role in the adoption of mobile commerce, such as mobile banking [Cyr et al. 2006]. The displays of older phones did not have the capability to show an aesthetically pleasing user interface due to low resolutions and (in very old phones) the absence of color, which likely influenced the intent to use mobile banking negatively. The expansion phase began at the moment smartphones were introduced. Touch controls likely influenced the ease of use perception positively and the increase in technical capabilities of mobile device displays provided banks the opportunity to improve aesthetics.

2.3. Standardization: The Pressure to Go Multiplatform

When looking at the development of home banking, the transfer from the early adoption phase to the expansion phase was driven by the need for more users to use home banking. This is different from the transfer of the expansion phase to the exploitation phase, which seems to be driven more by banks to reduce costs and increase client-side interoperability. The perceptions that have the most influence on embracing home banking were positive in the expansion phase, and stayed positive after the transfer to the exploitation phase.

For mobile banking, the changes between phases were quite similar. The changes made during the transfer from the early adoption phase to the expansion phase were also due to the need for an increase in user acceptance. Unlike home banking, it seems that an exploitation phase (characterized by the use of open (web) technologies) has not been reached yet for mobile banking. Browser-independent mobile banking sites actually exist, but they are not offered by as many banks as mobile client-side applications. While we do not know the exact reasons used to rationalize the choice to offer mobile banking applications over mobile sites, we understand that there are enough possible arguments from many different perspectives for why applications are preferred. A technical reason for this might be that applications have a better integration with the underlying operating system and hardware, through which banks can gain more information (such as data from sensors, biometrics, etc.) compared to mobile browsers. As noted earlier, aesthetics are an important factor in the acceptance of mobile banking. A functional reason might be that an application integrates visually better with the operating system, creating a more consistent user experience. A usable security reason might be that it is not required to provide a client-side application with information (e.g., a URL) to reach the bank, which is both user friendly and which reduces the risk of visiting a wrong (and possibly fraudulent) website. Of course, the risk still exists that a user accidentally installs a malicious application instead of

code that legitimately comes from a bank, but that is a small risk that only applies to the initial installation of a mobile banking application, since future upgrades are automatically managed by the mobile platform.

The current situation of mobile banking can be compared to the end of the expansion phase of home banking: there are only a limited number of software platforms used for online banking (home banking in the 1990s: mostly DOS and Windows; mobile banking in 2015: mostly Android and iOS). At the time, banks slowly replaced their client-side applications with websites for online banking services, preferring the use of standardized technologies over custom client-side code. Ignoring the less often offered mobile banking sites, the current situation for mobile banking can be compared to the same time period for home banking. Mobile banking applications are currently written specifically for the most popular platforms of the moment (Android and iOS). There are several reasons for why this might change in the future.

The mobile landscape is still evolving. Standardization of technologies and device use seems to be a rising trend. Frameworks are available that allow developers to create Hybrid Mobile Applications (HMAs). An HMA is a mobile application of which the underlying code is largely written using web technologies, wrapped inside a native application that facilitates access to the mobile device's hardware, data sources, and native looks [Bristowe 2015]*. Use of HMAs can become attractive for banks in the future for reasons related to cost. First of all, using HMAs can reduce the amount of client-specific code to maintain between mobile platforms. Also, HMAs make it easier to support new mobile operating systems, because most code is platform independent. Different parties are currently developing platforms that seamlessly integrate desktop and mobile work environments [Collins 2013; Foley 2014]*. Another promising aspect of HMAs is that they can reduce the overhead of developing graphical user interfaces for different platforms and screen sizes.

Similar to the slow but steady move from client-side applications to websites for home banking in the exploitation phase, it can be expected that mobile banking will make a move from native client-side applications to a mix of easy to maintain native and web-based code.

2.4. Security Implications

The future use of standardized web technologies in mobile banking will likely be similar to that of home banking using browsers and websites, but not the same. The similarities and differences allow us to distill some implications.

What kept mobile banking relatively safe so far is a number of factors:

(1) Mobile banking is not as popular as home banking [iResearch 2014; Board of Governors of the Federal Reserve System 2015; Banking & Payments Federation Ireland 2015]*. It is logical that malware is written for the most popular platform for online banking, since more users equals more possible fraud victims.
(2) Home and mobile banking have an overlap in supported functions. If these functions are security critical (such as when transferring money), the mobile banking implementation is sometimes more limited compared to the home banking implementation by the same bank. Some banks in our survey only allow money transfers to previously used account numbers as destinations through mobile banking. Some others do allow first-time transfers to new accounts, but only with an extra authentication step or with a limit on the amount of money (which is sometimes adjustable by the user in the home banking environment).
(3) Malware aimed at home banking can be written once and customized for each targeted bank site to allow browser injection and hijacking, a modus operandi known as Man-in-the-Browser [Eisen 2010; Curran and Dougan 2012]. Malware

kits are developed as an open platform to be customized by an adversary for a specific target audience [Ollmann 2008; Alazab et al. 2012]. An example of such a malware kit is Zeus, which allows (silent) injection of data in a browser session on a Windows machine [IO Active 2012]*. Such easy customization is currently not possible in the ecosystem of mobile platforms, since banks tend to write their own platform-specific code for each supported mobile operating system. Individual mobile banking application can be written in an insecure manner [Fahl et al. 2012; Georgiev et al. 2012; Reaves et al. 2015], but these applications still have an inherent security advantage because the custom code base makes large-scale attacks on multiple banks difficult.

These factors slowly start to change in the evolving mobile landscape. It is claimed that the global number of mobile internet users surpassed the number of traditional desktop Internet users in 2014 [Bosomworth 2015]*, the popularity of mobile banking is increasing [Board of Governors of the Federal Reserve System 2014]*, and its growth is expected to continue [Cetera 2015]*. Banks have stated that customer loyalty is seen as critical in their mobile strategy. This might be seen as more important than security when it is considered that the latter has been neglected by a large number of banks during the development of their mobile applications [Sanchez 2014]*. The increase in popularity and the existence of vulnerabilities provide new fertile ground for adversaries, taking away the advantage which (1) provides.

Banks have been pushing their mobile services quite hard. When mobile banking replaces home banking further, banks could relax the restrictions placed on certain mobile banking functions. This could reduce the advantage that (2) brings. India provides an example where banks gained the freedom to do this. The government had a policy that stated that transactions initiated through mobile banking had an upper limit. This policy was removed to allow individual banks to set limits based on their own risk perception [Srivastava 2013]. In a market where mobile banking is becoming increasingly more popular [Business Standard News 2014]*, banks could be urged to relax their limits.

As noted earlier in Section 2.3, banks will likely be motivated to move toward a largely shared code base, based on standard web technologies. Factor (3) will therefore change, since it will be possible for malware manufacturers to create malware kits that are easy to adjust to the HMAs of different banks.

That personal computers by consumers are inherently insecure for home banking was noted in the expansion phase of home banking [Redhead and Povey 1998; Slewe and Hoogenboom 2004]. At the time, the notion that adoption was more important than security was accepted. Bank customers adopted a system that relies on an untrusted machine-in-the-middle, through which attacks are conducted to this day. Home banking communications rely on standard web technologies that make the alteration of the same attack to target different banks easy. Mobile banking is developing similarly to home banking. Adoption rates are high and a logical next step would be the reduction of operation costs, such as through shared code bases offered by HMAs. This presents a new opportunity for attacks on mobile banking that scale well to large numbers of banks.

3. CUSTOMER TO BANK AUTHENTICATION

Customers must perform authentication to prove their identity to a bank before a session is initiated in which bank account(s) can be managed. This is referred to as entity authentication. Furthermore, it is possible that an extra authentication step is required to authorize the transfer of money. This is defined as transaction authentication.

Entity authentication is mandatory, while transaction authentication is optional to implement [Claessens et al. 2002].

Several factors can be used in user authentication. These are knowledge (something the user knows), possession (something the user physically has), and biometrics (something the user physically is or does). The terms two- or multifactor authentication are used when at least two different factors need to be fulfilled to establish an authenticated session. Knowledge is mostly represented, followed by possession. Biometrics based on physical characteristics is rarely used, and was only observed in mobile banking.

We examined 80 home banking sites on the use of authentication methods for personal computers. The same was done for 60 mobile banking applications and 25 mobile banking sites. Not every bank that offers home banking offers mobile banking, which is why the numbers of the different types of examined online banking systems differ. Mobile banking applications seem to be far more popular compared to mobile banking sites, despite that the latter is more independent of the used platform. Also, for mobile banking we could not determine the used authentication methods for two applications and one site because we could not get the necessary information from the offered user interface or documentation. These are excluded from the 58 applications and 24 sites for which we could collect this information.

We also compare our findings with our research data from 2013. At the time, we examined 81 home banking sites, 45 mobile applications, and 19 mobile sites. For one home banking site, it was in 2013 not possible to determine what kind of authentication method they used since a customer number had to be entered first before any information about authentication options were given [Kiljan et al. 2014a]. Therefore, for user authentication, only 80 banks home banking sites are considered for 2013, the same number of home banking sites as were examined in 2015.

First, we will present our findings concerning the combinations of factors (knowledge, possession, biometrics). After that, each factor will be discussed in more detail. We close with a comparison of data from 2002, 2013, and 2015.

3.1. Single or Multifactor?

Factors concern the difference in the amount of resources required by users and by adversaries to use a system. Resources can be in the form of secret knowledge possessed by the user that nobody else is supposed to know, something the user has in his or her possession that is hard to duplicate, and something that only the user is or does and that can be measured using biometrics. The three factors (knowledge, possession, and biometrics) can be combined to increase the amount of effort required by an adversary to commit successful identity fraud.

While multiple factors do provide protection against long-term credential stealing attacks, they are not the holy grail of information security. Multifactor authentication does not protect against social (e.g., phishing) or various technical attacks (e.g., session hijacking/injection attacks) [Schneier 2005]. There are also various technological, economical, and usability limitations that delayed sector-wide acceptance of multifactor authentication [Herley et al. 2009].

We will take a look at how factors are used and combined in home and mobile banking. More detailed information about individual authentication methods is given in Section 3.2 for knowledge, Section 3.3 for possession, and Section 3.4 for biometrics.

3.1.1. Home Banking. Figure 3 shows a comparison of the use of multifactor authentication in 2013 and 2015. Not a lot has changed. Banks that applied multifactor authentication still do so, and most banks that opted to use only knowledge have not gone back on this decision. Only a small number of banks that previously only relied on a password and/or PIN have changed their authentication methods to multifactor.

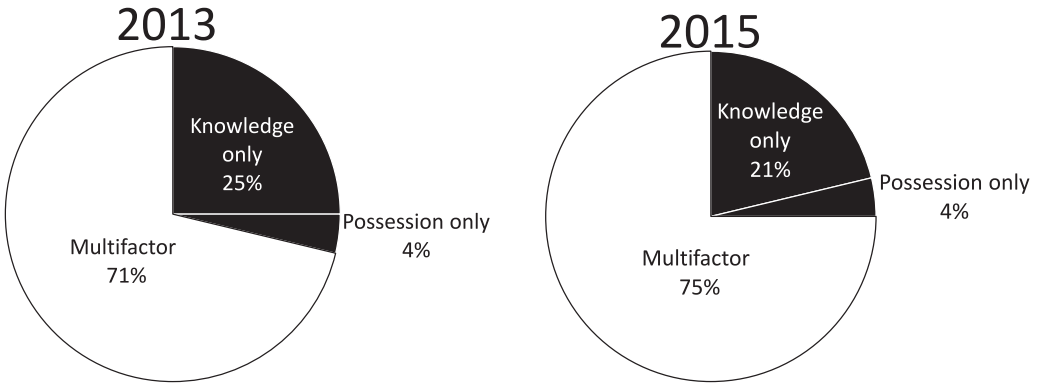

Fig. 3. The use of multifactor in home banking, 2013 and 2015 compared.

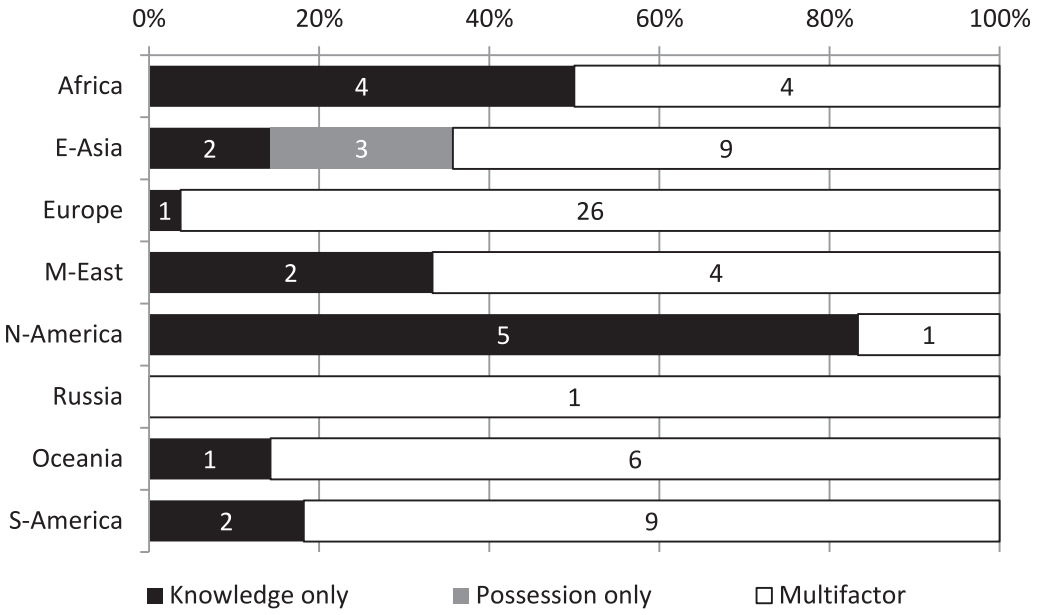

Fig. 4. Authentication factors used in online banking on PCs in different regions in 2015.

A separation of authentication factors based on region is shown in Figure 4. Most banks in Europe, South America, and Oceania require the use of multiple factors, while most other regions seem to be more divided.

Banks that offer multifactor authentication are rare in North America compared to other parts of the world. An explanation for this could be that people in this region are reluctant to embrace the use of multiple factors to protect financial assets. For example, the United States has only recently started to widely implement smart card-based payment cards that require a PIN [Scott 2014]*. Before that, shoppers were often able to electronically pay with a credit card using its magnetic stripe without using a PIN.

East Asia is quite exceptional, since some banks there allow users to log in using only the possession factor. This is achieved by making users log in using digital certificates

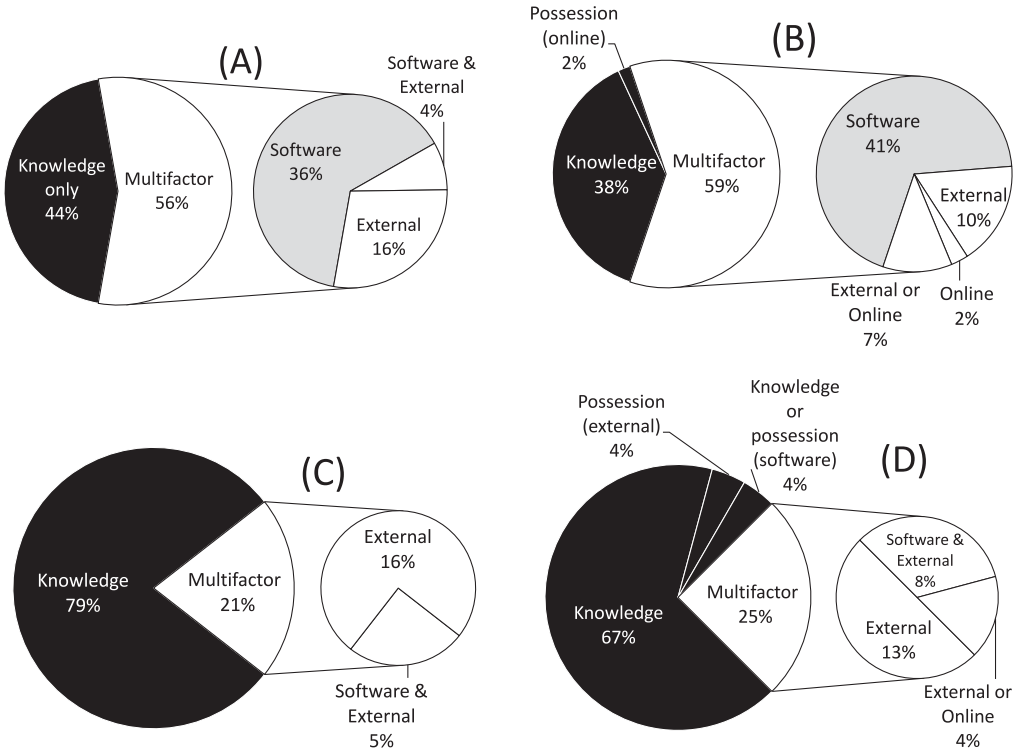

Fig. 5. Knowledge and possession factor use in mobile banking. (A) Applications in 2013 (based on 56 examined banks), (B) applications in 2015 (58 banks), (C) sites in 2013 (22 banks), and (D) sites in 2015 (25 banks).

without any PIN or password validation. More information about the use of certificates can be found in Section 3.3.

3.1.2. Mobile Banking. Figure 5 shows the use of knowledge and possession authentication factors by mobile banking applications and sites in 2013 and 2015.

We made categories for the possession factor since they vary greatly. These categories are as follows:

—Software indicates that supporting information for a possession factor is stored in the main memory of the mobile device that runs the banking application. Examples include a piece of information that binds the mobile device to a specific user's bank account(s), and the use of another mobile application that generates one-time passwords based on a secret key stored on the device itself.

—Online requires some kind of mobile connection to retrieve authentication credentials such as One-Time Passwords (OTPs). The end-point of the connection on the receiving device used by the user acts as a possession factor, since it is assumed that adversaries do not have access to transferred information and that they do not have the ability to change the end-point of the connection.

Examples include the use of Short Message Service (SMS) text messages and of other mobile banking applications that receive OTPs from banks using an internet connection. The use of an online connection can be almost the same as software if the mobile device used to receive the one-time password is also the same device used for mobile banking, such as with a smartphone. However, it can also be that a

second mobile device is used to receive OTPs, such as with a tablet (to use the mobile banking application on) and a mobile phone (to receive SMS text messages). Both options are supported and it is up to the user which is chosen.

—External means that the possession factor is a separate item issued by the bank to the user. Examples include physical paper or plastic cards from which OTPs can be read or derived, and electronic tokens (either stand-alone or using the user's bank card) that can generate OTPs.

More details about authentication methods from each category are given in Section 3.3.

As Figure 5 shows, there is not much change in the overall use of knowledge and possession factors in both mobile applications and sites between 2013 and 2015. The only unusual sight is the introduction of possession only authentication in 2015 by a handful of banks. This concerns a single bank for mobile applications (using OTPs received by SMS) and a single bank for mobile sites (using OTPs from an external physical card).

For multifactor authentication, the number of banks that apply an external possession factor stayed almost the same between 2013 and 2015. However, several banks started to offer an online possession factor as an alternative in 2015. A possible reason for this could be the inconvenience of carrying an additional device around, since the mobile device used for banking can also act as the possession factor. The online possession factor was not encountered in 2013, but was used compulsorily or offered as a choice in 2015.

The use of a software possession factor stayed more or less the same. Similar to the online possession factor, the used mobile device for banking can also provide the possession factor if it is kept in software.

We noticed in 2013 a few mobile banking applications of which their use required both registration of the bank account to the user's phone and an additional authentication device (accounting for "Software & External" in the graph). This combination of different possession factors is something we did not encounter anymore in 2015 for applications. However, it was used by a few mobile banking sites in 2013 and 2015.

It is interesting to note that most banks that offer a mobile site and that apply multiple factors require the use of an external possession factor. This implies that banks trust the user's device less for their mobile sites compared to their mobile applications. A possible explanation for this is that mobile sites are also usable on PCs with only a browser, which are less trusted by banks due to the higher risk of malware attacks.

Aside from knowledge and possession, there is also the biometrics factor (not shown in Figure 5). Its use was not observed in 2013, but in our survey for 2015 a few banks offer the use of a mobile device's fingerprint scanner as an alternative authentication scheme. More detailed information about biometrics is given in Section 3.4.

3.2. Knowledge: Passwords and PINs

Text-based passwords and PINs were the only encountered implementations of knowledge-based factors. Other knowledge-based schemes have been proposed in the past, such as cognitive and graphical passwords [Zviran and Haga 1990; Suo et al. 2005], but none of them are used by the banks examined in the survey.

Using knowledge as a single factor for authentication is quite unsafe. Passwords and PINs are often kept static for longer periods of time to keep them memorable. As long-term secrets, passwords and PINs entered as plain text on a user's computer can be collected by software-based keyloggers, to be used instantly in subsequent attacks [Mannan and Van Oorschot 2007]. Despite this vulnerability and as shown in Table I, a relatively large number of banks still use passwords or PINs exclusively in home and

Table I. Knowledge Authentication Factor Use in Online Banking in 2015

Knowledge factor ↓	Possession factor					
	Regular sites (80)		Mobile apps (60)		Mobile sites (25)	
	None	Present	None	Present	None	Present
Password	14	32	16	14	13	4
PIN	2	17	5	20	2	3
Password and PIN	1	6	1	0	1	0
Password or PIN	0	3	0	1	0	0
Password and/or PIN	0	2	0	0	0	0
None	N/A	3	N/A	1	N/A	1
Unknown	0		2		1	

mobile banking (20% for home banking, 35% and 60% for mobile banking applications and sites, respectively).

The "Password and/or PIN" knowledge factor in Table I requires some explanation. It relates to banks that offer different combinations of authentication options that support either passwords, passwords and PINs, or PINs only. This is because they offer different physical or electronic authentication devices, each with its own set of knowledge factors. For example, a bank can require a password to log in, and either physical paper or an electronic device to derive one-time passwords from for transaction authorization. The electronic device requires a PIN to be accessible, while a PIN is not necessary for the physical paper.

Passwords are popular in both situations where knowledge is used as a single factor and when a possession factor is used. PINs are only popular in combination with a possession factor. If the only factor is knowledge, it is logical that passwords are preferred above PINs, since passwords offer more security due to their higher complexity, making them harder to guess. An explanation for why PINs are still quite popular in multi-factor scenarios is that they are often an intrinsic part of the authentication method. For instance, some OTP generators require the use of some knowledge to unlock their functionality. If the knowledge has to be provided on the (often relatively small) device itself, a PIN would be the most practical way since its entry requires less buttons and button presses compared to a password.

Some banks provide additional proprietary software to detect or protect against passive password or PIN sniffing attacks against home banking. The use of this software is mandatory at eight banks and optional at one bank. We did not study this software in depth on how passwords are protected, but it is implied by documentation that some possible offered features include a scanner for malware-based sniffers and an overlay for password and PIN fields that offers a randomized keyboard to be used with a pointer device, such as a mouse.

Another security enhancing feature is the use of an on-screen keyboard with randomly placed buttons, offered for home banking on a bank site and not through software. Passive sniffing of keyboard and mouse data will not gain passwords or PINs in an attack if this feature is used. Two banks offer this through their sites for password entry and one bank offers this for PIN entry.

In addition to using a password, one bank implemented a system that relies on questions answerable by the user. Upon registration, the user creates three pairs of questions and answers. Whenever the user wants to log in, the bank asks for the password and one of the user-chosen questions. The user has to enter specific letters (chosen by the bank) of the answer and not the entire answer. This ensures that all secret knowledge cannot be gained in a single password sniffing attack. However, it does not protect against long-term repeated passive attacks, or against active and social engineering attacks.

3.3. Possession: Physical and Digital

The possession factor is often used in multifactor authentication but rarely as a single factor. Exact numbers of banks that apply possession as a single factor are shown in Table I (under the knowledge factor label "None" and possession factor label "Present").

There are many different types of possession factors banks can accept. We note the different types based on the earlier made separation between software, online, and external possession factors.

3.3.1. Software. Software as a possession factor uses information to present some kind of proof that the user is in possession of said information. The information is stored and processed on a device owned by the user.

There are two authentication methods that use this in home banking:

—Software certificates
If the private key of a certificate is not stored in a secure hardware device, it must be stored and processed in software. Five banks (all in the East Asian territory) apply this. Of these, four use proprietary software in the form of browser plugins for key management and signature handling. A single bank relies on the browser's own certificate management system. Potentially, users could also use a hardware device for this single bank if it is supported by the browser. Of the four banks, one also optionally supports proprietary hardware devices for key storage through the provided software.

The popularity of this software-based possession factor is slowly decreasing. In 2013, seven banks in East Asia applied software certificates, of which four also offered hardware certificates as an option.

—File-based
One observed method is where a bank provides a file to be stored on a user's home computer. Whenever the user initiates an action that requires extra security (such as the transfer of money to a third party), the site requests the file. If the file is provided by the user, the operation is permitted and a new file is provided for the next action. The file can be stored on the user's computer itself or on removable media. A single bank used this in 2013 and still does so in 2015.

Software as a possession factor is not popular in home banking. However, the use of data stored in software as a possession factor is the most applied type of possession factor in mobile banking applications, as can be seen in Figure 5. Twenty-four of the 58 mobile banking applications (41.4%) for which we were able to document authentication factors in 2015 use software as a possession factor in a multifactor authentication scheme. To be able to use mobile banking with one of these applications, a user must register his/her bank account through the application and bind its use to the mobile device. Once registered, the application only works for that specific user's account at the bank. The registered mobile device represents the possession factor. We did not analyze the internal workings of the applications, but it can be assumed that registration of a user's bank account on a mobile device results in a possession factor based on one or more identifiers from that device.

Software possession factors are stored and processed on user-owned devices. We marked the exclusive use of software factors gray in Figure 5 since using these introduces a security risk. The possession factor is represented by the mobile device itself in an untrusted digital environment, which makes it possible for an adversary to copy the possession factor in a malware attack. Combined with retrieval of the knowledge factor, every used authentication factor can be retrieved from the same mobile device in a single attack.

3.3.2. Online. Online is a type of possession factor where the end-point of a network connection represents the possession factor. Every method that applies this relies on the ability to authenticate or receive messages through an online connection.

For home banking on PCs, the most popular online possession factor is the use of SMS text messages to send OTPs to the user, used by 21 out of 80 banks (26.3%) in 2013 and 25 of the same 80 banks (31.3%) in 2015. In this case, SMS uses an out-of-band channel and the user's mobile phone represents the possession factor. The use of SMS to provide a user with OTPs is also proposed in literature, such as by Aloul et al. [2009], Hisamatsu et al. [2010], and Weigold and Hiltgen [2011]. A less popular variant is the use of a mobile application to receive OTPs from the bank through the Internet. We did not encounter this in 2013, but 11 of the 80 banks (13.8%) offered this as an alternative authentication method in 2015. We also encountered a rare variant that uses email instead of SMS to send transaction data and an OTP to the user, only observed in 2015 and used by two out of 80 banks (2.5%) for home banking authentication.

Home banking can alternatively use other connected devices as a possession factor to authenticate to the bank. Two types of such devices can be distinguished:

—Hardware certificates
Similar to software certificates, this can be used for signature-based authentication. The only difference is that secret key material is stored in an external device, protecting it against authentication credential stealing through malware attacks. With hardware certificates, the device that has the secret keys represents the possession factor. Seven out of 80 banks (8.8%) use hardware certificates to let their users authenticate in 2015, of which four require the use of proprietary software to support the hardware. Six out of 80 banks (7.5%) supported hardware certificates in 2013. We did not encounter the use of hardware certificates in mobile banking in 2013 or 2015.

—Connected hardware tokens
A significant difference between hardware certificates and connected hardware tokens is the amount of user interaction with the device. Hardware certificates are only connected by the user to the computer used for home banking. Connected hardware tokens expect more user interaction with the device itself, such as PIN entry and information verification. Three of 80 banks (3.8%) from our 2015 survey offer connected hardware tokens for home banking (all connected through USB). Of these, two banks use these devices to make the user verify transaction data and they protect these devices with a PIN, while the last one only lets a user verify the entered name and account number of new beneficiaries, without the necessity to enter a PIN on the device itself.

A rare example of a connected hardware token used in mobile banking has been observed in our 2015 survey. A small token can use a two-way connection using Near-Field Communication (NFC) to communicate with a mobile banking application on the phone. Critical transaction details can be verified and accepted or rejected by the user on the token.

A few other possession factors that are classified as online have also been observed in our 2015 survey for mobile banking. Four out of 58 mobile bank applications (6.9%) use OTPs received by SMS on either the same or another mobile device. A single bank does something similar, but relies on a mobile application to receive the OTP. Another bank uses challenge-response authentication using QR-like codes, which are shown on the first mobile device (used for mobile banking) to be scanned by a second mobile device. The entered transactions and a response code are shown on the screen of the second

mobile device. The user is expected to verify the transactions and enter the response code for confirmation.[4]

Depending on the kind of authentication method used, an online possession factor can be as insecure as a software possession factor or as secure as an external possession factor. It is insecure if the factor is effectively represented by the user's mobile device, since its untrusted environment is vulnerable to malware. It is also insecure if the transportation channel of information cannot be trusted, such as with SMS (which is vulnerable to SIM swap scams [Nedbank 2011]*). However, as a connected external device, an authentication method can be secure if it offers a trusted environment separate from the untrusted environment of the user's mobile device, and if it does not rely on the security of the communication channel between an untrusted device and the bank.

3.3.3. External. Some trusted devices have earlier been described under 'Online." These concern devices that rely on a network connection (hence the name). An "External" possession factor relies on a bank-issued authentication device that does not use an electronic connection with other devices. There are a few variations that are either low-tech or high-tech.

—OTPs on paper/plastic

This is the simplest form of a possession factor. It consists of an indexed list of OTPs on paper or an indexed grid of characters on a small plastic card. A user derives an OTP from one of these when the bank requests it. The bank specifies which OTP it wants by referring to one or more index numbers. The physical paper or plastic represents the possession factor. Advantages are that it is easy to use and that it is protected against malware-based attacks, like all external possession factors. A disadvantage is that a physical medium with written text is easy to copy. A picture of the page or card made by a camera already represents a copy of the possession factor that is usable by an adversary.

We observed that 16 out of 80 banks (20%) let users authenticate with OTPs from paper or plastic in 2015. Of these 16 banks, five (31.3%) do not give the user an alternative choice for the possession factor. Most of the 16 banks are located in Europe and South America, where this method seems to be more popular compared to other regions. Paper and plastic OTPs have become more popular since 2013, when only 13 banks (16.3%) applied it for home banking. At that time, eight of the 13 banks (61.5%) required the use of a physical page or card to get OTPs from and an alternative was not available. This implies that this representation of the possession factor became more popular as an alternative authentication scheme instead of as the only (mandatory) option.

OTPs from a physical medium are used for authentication in six of 58 examined mobile applications (10.3%), and in four out of 24 mobile sites (16.7%) in 2015. The same numbers for 2013 were three out of 45 (6.7%) and zero out of 19 (0%), respectively.

—Offline electronic tokens

We added the "offline" keyword to the description of these kind of tokens to distinguish them from online hardware tokens. These tokens do not have an electronic connection with any other device, but rely on their own battery as a power source and nonelectronic methods for information transfer. There are different types of tokens, ranging in functionality and offered user interface.

[4]We did not examine these secondary mobile banking applications (one which generates an OTP, one which scans QR-like codes) on a technical level and assume that they require an online connection to receive OTPs or response codes.

Table II. Offline Tokens Used for Home Banking at 31 Out of 80 Banks (38.8%). One Bank Implemented Two Different Kinds of Devices, Resulting in a Total Value of 32. Numbers in Parentheses Represent Banks from the same Group which also Use Tokens for Mobile Banking

	Authentication method			
Device(s) and optional knowledge factor	OTP	CR	OTP & CR	WYSIWYS
Stand-alone token	8 (1)	0	0	2
Stand-alone token with PIN	10	0	3	0
Smart card, token and PIN	1	2	5 (1)	1

The simplest token consists of a single button and a small display. When the button is pushed, the display shows a single OTP. Eight out of 80 (10%) observed home banking sites applied such a token in 2015 and seven out of the same number of observed banks (8.8%) did so for home banking in 2013.

A slightly more complex token consists of a display, a number of function buttons, and possibly a keypad. These tokens work stand-alone or rely on an inserted bank card to provide cryptographic credentials. The functions of some of these tokens are only usable after it is unlocked by a PIN (associated either with the device itself or with a smart card). There are several functions that can be supported by different kinds of tokens:

—Generate OTPs. Like the one-button tokens, OTPs can be generated after entering a PIN. Offering the OTP to the bank proves that the user is in possession of the device used to create the OTP and (indirectly) of the PIN required to operate the device.

—Generate responses for Challenge-Response (CR) authentication. After entering the PIN, the user must enter a challenge (given by the bank), after which the token will generate a response for the user to enter in the online banking site. Receiving the expected response to the sent challenge is an indication for the bank that the user is in possession of what is needed to generate the response (a specific token or bank card and a PIN).

—Show critical transaction information and confirmation codes. The information is received through a nonelectronic one-way connection between the token and the user's device. We only observed this new authentication method in our 2015 survey. The one-way information transfer is facilitated by an optical sensor, which scans QR-like codes from the monitor of a user's device.

Table II provides an overview of the types and numbers of offline electronic tokens we encountered in our 2015 survey.

3.3.4. Most Often Applied Possession Factors by Region. There are many different possession factors employed in the online banking world. Table III shows for each region which possession factors are most often applied according to the survey data. A value of "none" indicates that most banks do not prefer to use a possession factor at all. The numbers of observed banks are included for reference.

3.4. Biometrics and Behavior Anomaly Detection

Biometrics is also known as the inherence factor in user authentication. Unlike the other factors, it does not concern something that the user should know or have. Instead, this factor focuses on what the user is or does to ensure the user's identity. Physical biometrics measure the presence of physical characteristics of the user. Absence of such physical characteristics can be considered suspicious and a reason for the system to ask for alternative authentication credentials. Behavior anomaly detection concerns the use of user behavior data to, after a user action has been taken, detect deviations from a previously established baseline. Therefore, afterwards it can be said whether

Table III. Most Applied Possession Factor in Different Regions and Online Banking Environments

Region	Home banking	Mobile banking	
		App	Site
Africa	(8) Offline electronic tokens (OTP)	(3) None	(1) None
Asia	(14) Hardware & Software Certificates	(8) Software	(6) None, physical tokens (OTP)
Europe	(27) Offl. elect. tokens (OTP, CR, WYSIWYS)	(22) Software	(7) Mixed OTP
M-East	(6) SMS (OTP)	(5) None	(0) N/A
N-America	(6) None	(5) None	(6) None
Oceania	(7) Offl. electr. tokens (OTP)	(7) Software	(3) Offline electronic token (OTP)
Russia	(1) Mixed (OTP)	(1) Software	(0) N/A
S-America	(11) Physical tokens (OTP)	(9) Software	(2) None

a user behaved as expected or not. Abnormal user behavior can be an indication of identity fraud, where an adversary has (direct or indirect) access to all authentication credentials.

3.4.1. Physical Biometrics. Biometrics based on physical characteristics can be used as an additional or alternative authentication factor for user authentication. An advantage it has is that it generally is quite usable. Disadvantages include the unwillingness of some people to use them due to social stigmas and the limited number of nonreplaceable characteristics (which can be zero for users with disabilities). These disadvantages limit biometrics for user authentication to users who want and can use them, which is why an alternative authentication method (based on the other two factors) has to be available.

Physical characteristics were not used for user authentication by any of the surveyed banks in 2013. Registering these characteristics requires specialized sensors. These sensors were not widely integrated in user equipment at the time. While banks could opt to distribute needed equipment, it would be very expensive to support an authentication method for which an alternative must always be available.

The use of physical characteristics has been observed in our 2015 survey for a limited number of mobile banking applications. Two banks support Apple TouchID, which consists of a fingerprint sensor, operating system support, and an application programming interface. The fingerprint is used as an alternative to providing a PIN, while the applied possession factor remains the same. Enrollment is performed by the operating system and not by the mobile banking application.

More banks have indicated that they will support Apple TouchID in the future [Rawlinson 2015]*, despite that it is possible to spoof fingerprints [Chaos Computer Club 2013]*.

3.4.2. Detection of Behavior Anomalies. Behavior anomaly detection monitors the user's behavior to detect whether a transaction is possibly made by a fraudulent party. The identity of the user can only be ascertained after the user's behavioral patterns have been registered and compared to a past baseline. Since the user is required to do something before there is some certainty of the user's identity, anomaly detection based on behavior is unsuitable for user authentication (at the beginning of a session, before a user has performed any actions), but can be used to provide some certainty about the user's identity and the validity of a user's action afterwards. The origin of the data can come from user actions (such as at what time of the day a user performs an action and the user's data entry speed) and from the environment in which the user's device operates (such as the geographical location and local temperature). The used methods can be compared to those of data leakage detection systems used to spot anomalies in

Table IV. Overview of Similarities and Differences in Basic Authentication Methods for Online Banking Using a PC as Observed in 2002, 2013, and 2015

Method	2002	2013	2015
Password/PIN-only	✓(66.7%)	✓(23.8% + 13.8%)	✓(21.3% + 15%)
OTP (paper/plastic)	✓(6.7%)	✓(16.3%)	✓(20%)
OTP (offline electronic tokens)	✓	✓(13.8%)	✓(33.8%)
OTP (SMS)		✓(26.3%)	✓(31.2%)
Challenge-response (offline electronic tokens)	✓	✓(13.8%)	✓(12.5%)
Certificate-based	✓(14.3%)	✓(3.8% + 2.5% + 5%)	✓(3.8% + 6.3% + 2.5%)

Note: Percentages represent the relative amount of observed banks that apply a method in a specific year. Observations can be compared between years (columns) but not between methods (rows) because some banks in our survey are counted multiple times when they offer multiple methods (which is why the percentages can exceed 100% when summed).

data transactions (such as proposed by Constante et al. [2014]). Several examples of implemented fraud detection techniques are given by Kou et al. [2004], and Quah and Sriganesh [2007] provide an example of a proposal for a system that recognizes fraud.

Since user behavior anomalies are registered by the back-end technical infrastructure of banks, it cannot be said with full certainty how many of the banks in our 2013 and 2015 surveys apply this and to what extent. However, some banks state that they do use monitoring services for financial transactions [Ally Bank 2010; Bank of America 2013; Barclays 2014]*. It has also been claimed that some banks profile low-level user actions through mobile applications [Matthews 2012]*.

3.5. Comparing 2002, 2013, and 2015

Table IV gives an overview of observed basic authentication methods used for home banking in 2002 by Claessens et al. in 2002 and by us in 2013 and 2015. Check marks indicate that a method was observed and percentages (if the required information is available to produce them) indicate the relative number of banks that apply the methods in the survey for a specific year. Note that all methods except "Password/PIN-only" are not exclusive. For example, a bank that applies OTP authentication in any way can still require an additional password or PIN from the user. A bank that applies OTP authentication using a bank-issued device for entity authentication can also apply CR authentication for transaction authentication.

For Password/PIN-only, two percentages are given for our work. These stand, respectively, for the percentage of banks that offer Password/PIN-only based authentication without and with a multifactor based alternative. For certificate-based authentication, our percentages relate, respectively, to the relative number of banks that offer this type of authentication with the private key stored in software only, in hardware only, and for the banks which give this as a choice to the user (by supporting both hard- and software storage of the private key).

We excluded the exceptional methods found in our survey to keep the table easy to read. While the often used basic authentication mechanisms show little difference, the ratios in which they are implemented differ significantly between 2002 and 2013 and moderately between 2013 and 2015. Claessens et al. [2002] conclude that in their survey passwords and PINs as a single factor were most widely used to authenticate users. Today, most banks offer multifactor authentication. Since 2002, a large number of online banks have migrated to methods that are safer but also have been available for quite some time. The only method that is popular now that was not discussed by Claessens et al. in 2002 is the use of text messages to send OTPs to users.

4. BANK TO CUSTOMER AUTHENTICATION AND COMMUNICATIONS SECURITY

This section describes the observations from our surveys concerning authentication by the bank to the user. Data from 2013 and 2015 is compared.

In 2002, the standard solutions for communications security with online banking was Secure Sockets Layer/Transport Layer Security (SSL/TLS) for PCs and Wireless Transport Layer Security (WTLS) for MDs. Claessens et al. [2002] describe the various versions of SSL/TLS up to SSL 3.0 and TLS 1.0 [Freier et al. 2011; Dierks and Allen 1999]*. Since then, several weaknesses in both SSL/TLS standards and implementations have been discovered, and TLS 1.1 and 1.2 have been developed [Dierks and Rescorla 2006, 2008]*. An update was also released for all TLS versions that breaks backwards compatibility of TLS with SSL 2.0 [Turner and Polk 2011]*. WTLS has not seen a newer version since 2001 [Wireless Application Protocol Forum 2001]*, which is most likely caused by the decline of WAP in favor of SSL/TLS on MDs.

The use of SSL/TLS by home banking sites was examined in the survey. Due to the large number of banks, the analysis was narrowed down to the use of SSL/TLS to secure communication between home banking sites and web browsers (HTTPS). The use of SSL/TLS in mobile banking was not examined due to it requiring a more specialized approach that takes more time. Examples of research in SSL/TLS use by mobile applications, including bank applications, are given in Section 6. We did not examine SSL/TLS for mobile banking sites since most sites are hosted by the same server or SSL/TLS front-end, which would provide the same results as the examined regular sites. Also, SSL/TLS as possibly used by other services hosted by the bank (such as email and VPN for their employers) was not examined since these services are not meant for customer-bank interaction. From a technical perspective, the information required to connect with such services are time-consuming to find and not all banks will offer such services uniformly, making useful comparisons harder.

The authors of this article do not have accounts at most banks, which is why SSL/TLS-usage was examined using login pages. All 80 surveyed online banking sites rely on SSL/TLS for both server authentication and secure communication. Used cryptographic algorithms, vulnerabilities, and optional TLS functions were examined.

In an earlier technical report [Kiljan et al. 2014a], bank sites were examined using Qualys SSL Labs SSL Server Test.[5] The test by Qualys was chosen since it was the most expanded test available online. Alternative approaches were considered, such as using self-hosted security and vulnerability scanners. An example is Nmap,[6] which has the potency to provide more information about scanned sites, but a disadvantage is that its scans can be quite intrusive. Whereas Qualys uses standard site requests (like a browser would when setting up a connection) and analyzes the responses, other scanners have capabilities to scan deeper by sending nonstandard requests that could be interpreted as malicious, which in some countries could result in legal issues. The intrusive scans might be disabled, but then the retrieved relevant information would be the same or less than what Qualys collects. It was also considered to forego scanning entirely and instead use data collected by the Internet-Wide Scan Data Repository,[7] which uses ZMap[8] to scan all possible IPv4 hosts. Unfortunately, the data provided by this repository is wide but shallow. Data is only collected based on the connection the ZMap scanner negotiates. Unlike Qualys, it does not make an attempt to find out which weaker versions of SSL/TLS are supported, whether vulnerabilities are present, and whether the site supports additional TLS functions that can improve security. Therefore, Qualys' scanner was used instead.

[5]Qualys SSL Labs SSL Server Test: https://www.ssllabs.com/ssltest/.
[6]Nmap: https://nmap.org/.
[7]Internet-Wide Scan Data Repository: https://scans.io/.
[8]ZMap - The Internet Scanner: https://zmap.io/.

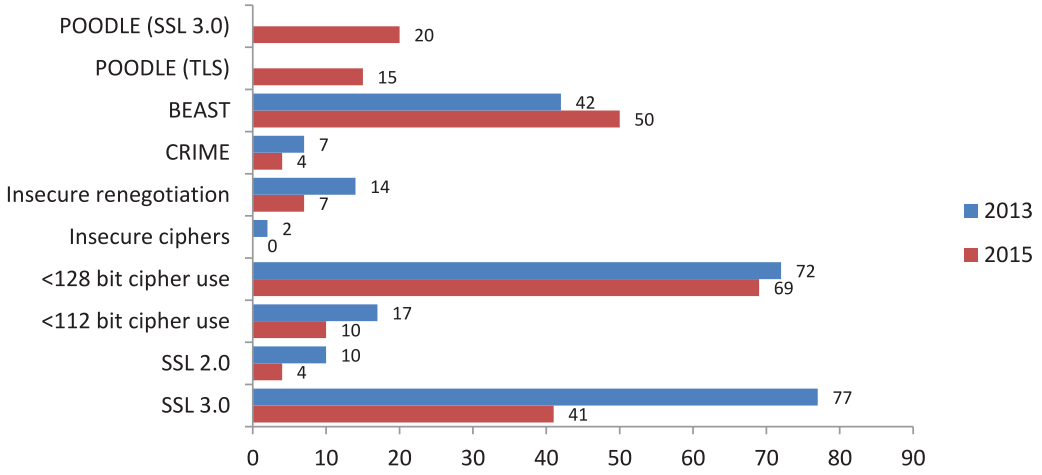

Fig. 6. An overview of the encountered SSL/TLS vulnerabilities.

4.1. Vulnerabilities

Figure 6 shows an overview of the vulnerabilities and how often we encountered them among the 80 surveyed banks. Each vulnerability is discussed briefly.

At the end of 2014, a successful attack was made against SSL 3.0 and TLS 1.0 when block ciphers are used. An adversary manipulates a user's browser to send requests to a site using SSL/TLS where the user is logged in. Important information can be derived by observing the cipher text, such as session cookies that can be used to hijack sessions. This attack was named POODLE [Möller et al. 2014; Langley 2014]*. Vulnerabilities to POODLE are only noted for 2015 since the attack was not yet known in 2013. For SSL 3.0, the only way to protect against POODLE is by disabling cipher suites that use block ciphers. POODLE also works with some web servers that implement padding in TLS 1.0 incorrectly, which updates to the web server software might be able to solve. Figure 6 shows the number of banks that are vulnerable to POODLE with either SSL 3.0 or TLS. Five banks overlap, and are vulnerable to POODLE attacks with both protocol versions. Therefore, 30 out of 80 banks in our survey are vulnerable to POODLE attacks.

Within the SSL/TLS protocol suite (up to versions 3.0/1.0, respectively), one method to encrypt data is with block ciphers used in Cipher-Block Chaining (CBC) mode. The SSL/TLS standard mandates that chained Initialization Vectors (IVs) are used with CBC mode encryption. With chained initialization vectors, the last block of the previous ciphertext is used as an IV for the next message. This presents a vulnerability that can be exploited using a Blockwise Chosen-Boundary Attack (BCBA) [Duong and Rizzo 2011]*. A BCBA applied on a HTTPS session is known as a BEAST attack [National Institute of Standards and Technology 2011]*. BEAST can be mitigated by letting servers only allow connections exclusively using TLS 1.1 or 1.2. Figure 6 shows that between 2013 and 2015 the number of banks that are vulnerable to BEAST attacks has increased. An explanation for this is that banks that became vulnerable at one point in time stopped supporting RC4, the only streaming cipher supported by SSL/TLS, since it is vulnerable to attacks [AlFardan et al. 2013]. The only alternative without disabling support for the older SSL 3.0 and TLS 1.0 protocol versions were cipher suites that applied CBC, and by implementing those the relevant banks became vulnerable to BEAST. This is likely seen as the preferable alternative, since the BEAST attack

can be mitigated by browsers by implementing 1/n−1 record splitting as a workaround [Langley 2012; Ristic 2013]*.

If an attacker can observe network traffic and manipulate a victim's browser to submit requests to a target site, it is possible to retrieve data from the TLS stream when DEFLATE compression is used. An attacker can steal session cookies with CRIME, which makes it possible to hijack a session [Ristic 2012]*. While this attack is easier to execute compared to BEAST, it is also easier to defend against by disabling TLS compression. This can be done server- or client-side. The vulnerability is only exploitable when both server and client support and use TLS compression when a session is established. In 2013 only seven banks supported TLS compression, which after 2 years was reduced to four banks.

SSL/TLS renegotiation makes it possible to use the same data session over multiple connections. Originally, the SSL and TLS protocols did not consider that different parties can use the same data session due to renegotiation, where one party has control of the connection before renegotiation, and the other afterwards. This allows a man-in-the-middle to inject plain text in an established session with a web server before the web server is reconnected with the user's browser through renegotiation [Ristic 2009]*. As a response, some sites disabled the renegotiation feature [Ristic 2010]*, while others implemented an extension which fixed the problem [Rescorla et al. 2010]*. Renegotiating is cryptographically protected when both the server and the browser support the extension, thereby preventing the same data session to be shared between an end-user and a man-in-the-middle. Half of the banks that were vulnerable in 2013 fixed the issue in the following 2 years.

SSL/TLS supports a number of cipher suites with different key sizes to support the confidentiality and integrity of an established session. Some of these cipher suites are merely meant for testing and unlike regular cipher suites, they do not offer either authenticity of the server's identity (such as with anonymous (Elliptic curve) Diffie-Hellman) or encryption, due to the lack of required algorithms in the suite. To prevent this, insecure cipher suites should be disabled. Only two sites from our survey supported insecure ciphers in 2013, which have since then fixed this issue.

The SSL Server Test from Qualys designates all cipher suites that are less than 112 bits as "weak." If the assumption is made that data has to stay confidential and its integrity safeguarded against eavesdroppers for the period "2031 and Beyond," a minimum of 128 bits conforms with recommendations by NIST [Barker et al. 2012]*. This is why any applied cipher suite with a symmetrical key length of less than 128 bits is considered vulnerable. However, there are a large number of sites that deploy cipher suites of which the shortest key length is 112 bits. These sites are noted separately in Figure 6 to distinguish sites that slightly deviate from NIST recommendations (less than 128 bits but at least 112 bits) and those which deviate significantly (less than 112 bits, i.e., 40 or 56 bits). Not much has changed since 2013. The most significant change was a moderate reduction in banks that supported very weak ciphers (from 17 to 10 banks). These banks disabled the weaker cipher suites in their web server configurations, forcing clients to use the stronger alternatives.

Support for SSL 2.0 (with cipher suites enabled) or SSL 3.0 is considered a vulnerability. SSL 2.0 has a number of flaws that were already acknowledged by Claessens et al. [2002]. These are the use of the same cryptographic keys for message authentication and for encryption (which makes the security of Message Authentication Codes (MACs) unnecessarily weak when encryption key size is limited due to export restrictions), the sole dependence on MD5 as a vulnerable hash function to construct MACs, the lack of handshake protection, and the possibility to truncate a connection due to relying on the closure of the TCP connection. SSL 3.0 is also considered insecure since all available cipher suites for that protocol version are vulnerable. Cipher suites using

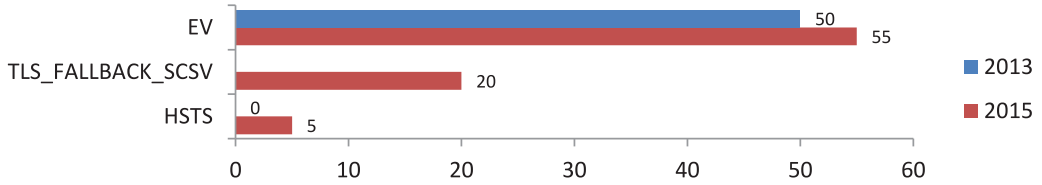

Fig. 7. An overview of additional SSL/TLS functions supported by bank sites.

CBC are vulnerable to the earlier discussed POODLE attack due to an inherent flaw in the SSL 3.0 protocol itself, while the only supported streaming cipher is the RC4 algorithm, which is prone to attacks [AlFardan et al. 2013]. To mitigate these vulnerabilities, it is enough to simply disable SSL 2.0 and 3.0 support on the server. While support for SSL 2.0 and 3.0 has dropped by almost half of the banks that supported it in 2013, there still are a surprising number of banks that support these older versions.

It must be noted that modern browsers can mitigate some of the vulnerabilities as discussed in this section. SSL 2.0 support has been disabled in modern browsers for quite a while. Examples include Microsoft Internet Explorer, Mozilla Firefox, and Opera [Lawrence 2005; Mozilla 2006; Opera Software 2008]*. Support for SSL 3.0 in these browsers was disabled more recently [Molland 2014; Mozilla 2014; Microsoft 2015]*. When such browsers are used to connect to a site, they are not vulnerable to the protocol vulnerabilities of SSL 2.0 or 3.0 since a higher protocol version must be negotiated with the server. If the server does not support a higher protocol version, the connection will simply fail. Users with older browsers are still vulnerable.

4.2. Additional TLS Functions

There are several optional functions in TLS that can be used to increase security. These have to be implemented server-side. Figure 7 shows the support of several of these functions between 2013 and 2015 by the surveyed banking sites.

The functions found in the survey and some missing functions are each described briefly.

4.2.1. Extended Validation (EV). We tested the availability of the EV attribute in certificates offered by bank sites, which notifies the user in various ways (depending on the used browser) that a more thorough identification process was followed before the certificate was issued. The expected procedures are noted in guidelines as published by the CA/Browser forum.[9] EV depends on the capabilities and willingness of users to recognize the difference between basic certificates and EV certificates. Whether EV provides any benefit is disputed. Without training or guidance, a considerable number of users do not notice the differences between offered basic and EV certificates in web browsers [Jackson et al. 2007; Sobey et al. 2008; Biddle et al. 2009]. As shown in Figure 7, EV was already quite popular in 2013, but its popularity only increased marginally between then and 2015.

4.2.2. TLS Fallback Signaling Cipher Suite Value (TLS_FALLBACK_SCSV). When a browser and server negotiate which SSL/TLS versions and cipher suites will be used, a fallback mechanism exists in case the handshake fails. If a connection on a higher protocol version fails, the default policy is to try one lower protocol version since it is assumed that the other party does not support the higher version. This fallback mechanism sometimes is used incorrectly in a situation where both parties actually do support a higher

[9]The latest version of the Guidelines for the Issuance and Management of Extended Validation Certificates can be obtained from https://cabforum.org/documents/.

version. For example, a browser will try to reconnect with a server using a lower protocol version even though both browser and server support a higher version. Reasons for failure can simply be a network disruption the first time a browser attempts to connect, but an adversary can also use this flaw to force a downgrade of the protocol (also known as a downgrade attack) to an exploitable version by influencing the availability of a connection between browser and server. TLS Fallback Signaling Cipher Suite Value (also known by its TLS cipher suite value: TLS_FALLBACK_SCSV) is an extension for TLS that prevents the use of a lower version protocol in scenarios where the initial handshake for protocols to use between browser and server fails [Moeller and Langley 2015]*. The extension is added to any reconnection attempt by the browser, so the server knows that a downgrade was performed. If the downgrade was unjustified (both the browser and server support a higher protocol version), the server refuses the connection. Support for TLS_FALLBACK_SCSV requires up-to-date web server software and SSL/TLS libraries. This extension is relatively new since it was proposed in 2014, yet a quarter of the banks that we examined already implemented it 1 year later.

4.2.3. HTTP Strict Transport Security (HSTS). When a user enters a website name without specifying the protocol the insecure "http" protocol will be used by default, even if SSL/TLS (through the "https" protocol identifier) is available. A man-in-the-middle who has control of the connection between the user's computer and the bank can prevent a user from ever connecting to the secure site by manipulating all replies from the bank [Marlinspike 2009]*. HTTP Strict Transport Security (HSTS) provides protection against man-in-the-middle attacks that exploit this initial insecure connection by implementing an additional HTTP response header [Hodges et al. 2012]*. This header instructs browsers that for future visits within a specific time frame only secure connections through SSL/TLS ("https") should be allowed. To also protect the first visit, browser updates include a list of sites that should only be visited securely. (Retro)fitting web servers with HSTS support is quite simple, since only a HTTP response header has to be added to its existing configuration. An example that states that only secure connections should be allowed for a year would be `Strict-Transport-Security: max-age=31536000`. Note that this yearly counter is updated every time the user visits the site, making it unlikely that it would ever expire if the user visits the site regularly. Despite its simplicity, HSTS is only implemented by a few banks in our survey.

4.2.4. HTTP Public Key Pinning (HPKP). A similar useful HTTP response header is HTTP Public Key Pinning (HPKP), which allows browsers to detect fraudulently issued certificates from trusted certificate authorities [Evans et al. 2015]*. On the first visit to a site that supports HPKP, the site tells the browser that at least one certificate in the trust chain should contain a specific public key for subsequent visits in a certain time frame. If within this time frame the site is revisited and a valid certificate chain is offered that does not contain one of the earlier registered public keys, the browser refuses to connect. This protects against trusted but fraudulent certificate authorities who issue valid certificates of sites for adversaries. If in a subsequent visit the certificate chain has been changed in such a way that the HPKP policy is violated, it indicates that a wrongfully issued certificate is being offered, possibly as part of a man-in-the-middle attack. HPKP requires that two public keys are specified. If the primary public key is compromised (such as when an adversary obtains the paired private key) and revoked, the backup public key can be used to replace the lost part of the certificate chain. This avoids the situation where the security measures of a browser prevent access to the site with a new legitimate certificate chain. It is recommended that a backup private key and backup certificate are kept on an offline medium for safekeeping, since they can be used for undetectable man-in-the-middle attacks if compromised. An example of an HPKP HTTP response

Table V. Geographical Distribution of Important SSL/TLS Functions and Vulnerabilities in 2015

Region	Africa	Asia	Europe	M-East	N-America	Russia	Oceania	S-America
# banks	8	14	27	6	6	1	7	11
Extended validation	3	12	19	4	4	1	7	5
TLS Fallback Sign.	0	0	14	1	4	0	1	0
HSTS	0	0	5	0	0	0	0	0
POODLE (SSL 3.0)	6	4	7	0	1	0	1	1
POODLE (TLS 1.0)	1	5	3	1	0	0	2	3
BEAST	7	6	19	4	4	1	5	4
CRIME	2	1	1	0	0	0	0	0
Insecure reneg.	1	0	1	1	1	0	0	3
<112 bit ciphers	3	2	1	1	1	0	0	2
SSL 2.0	2	0	0	0	0	0	0	2
SSL 3.0	7	11	13	1	1	0	3	5
Function support	13%	29%	47%	28%	44%	33%	38%	15%
Vulnerability	45%	26%	21%	17%	17%	13%	20%	23%

header that would pin two public keys for 2 months on each visit of the site and any of its subdomains would be `Public-Key-Pins: pin-sha256="ABCxyz123+(...)";pin-sha256="XYZabc987+(...)";max-age=5184000; includeSubDomains`. Note that for the example the PINs (encoded in Base64 SHA-256 hash values of public keys) have been shortened for readability.

This extension was not used by any of the banks at the time the survey was conducted, which is why it is absent in the graph shown in Figure 7.

4.2.5. Other non-SSL/TLS Related Response Headers. There are several HTTP response headers that increase security, but that do not relate to SSL/TLS. Examples focus on preventing cross-site interaction that can be insecure, such as through frames (the `X-Frame-Options` header [Ross et al. 2015]*) and scripting (the `X-WebKit-CSP` header [W3C 2015]*). These response headers were excluded from the survey both due to limited time, and because they have not (yet) been accepted as standards (`X-WebKit-CSP`) or have been obsoleted without a replacement being available (`X-Frame-Options`).

4.3. Geographical Spread of Vulnerabilities and Functions

The data in Table V shows the global distribution of important SSL/TLS functions and vulnerabilities according to our survey data.

As noted in Section 1, we believe that our set of banks is representative for banking worldwide. However, there is room for variance due to the limited number of observed banks in some regions. Comparisons using the final percentages should therefore be made with care. The most obvious case is Russia, for which only a single bank was examined that neither supports any of the listed functions and that has none of the listed vulnerabilities. We therefore only make conclusions based on the other regions.

Europe and North America seem to be quite active in supporting new SSL/TLS functions, followed by Oceania, East-Asia, and the Middle East. Other regions do not seem to give any priority to the support of additional secure functions of SSL/TLS. SSL/TLS vulnerabilities in banking sites were observed mostly in Africa, while the presence of such vulnerabilities seems to be less in other regions.

4.4. SSL/TLS Overall Observations

It is a positive development that most banks see SSL/TLS as something that should not be configured once and then be left alone. Examining Figure 6 shows that the number of occurrences for most vulnerabilities dropped between 2013 and 2015 (ignoring BEAST,

which can be considered a nonissue if an updated browser is used). Unfortunately, there still are a large number of banks (10 out of 80, or 12.5%) that support insecure cipher suites with 40 or 56 bit key sizes.

Optional security-enhancing SSL/TLS functions became slightly more popular, as shown by Figure 7. EV is already widely implemented, and saw a slight increase. The TLS Fallback Signaling Cipher Suite Value was implemented by 25% of the examined bank sites between its introduction and the 2015 survey. HSTS is a bit of an exception. Of all the optional functions that we examined, it has the lowest technical threshold to implement. Considering that HSTS was already available before the 2013 survey, it is not known why there are only a few bank sites that implemented it.

Mobile banking and payment applications are prone to implementing communications security incorrectly, resulting in large security gaps [Georgiev et al. 2012; Fahl et al. 2012; Reaves et al. 2015]. Online banking sites have the advantage that they rely on browsers to implement SSL/TLS correctly client-side, which reduces the development area of banks in which mistakes can be made. Therefore, the work for banks is to keep their server-side implementations as secure as possible. From the data in the survey, it can be concluded that most banks do it well, but there are some sites that are still vulnerable in ways that were considered old a decade ago.

5. DISCUSSION, LIMITATIONS, AND FURTHER RESEARCH

Of 81 banks in 2013 and 80 banks in 2015, the user authentication methods were examined in Section 3 and the communications security implementations for home banking were examined in Section 4. When the conclusions are compared, a difference in uniformity is quite clear. All banks rely on SSL/TLS for communications security in home banking. There is some variety in how well SSL/TLS is implemented, but all banks chose to use parts from a single, standardized protocol suite. This is in sharp contrast to the methods applied for user authentication, which vary greatly. Most likely, SSL/TLS provides "good enough" communications security, while there are several factors for why banks cannot agree on a single user authentication method. Such factors can include demographic differences in which methods are accepted by bank customers. For example, in the United States bank card or credit card payments are often conducted without requiring a PIN [Scott 2014]*. Instead, a physical signature (easy to forge, and easy to forget to check) is asked from the person who uses the card. One reason why issuers hesitate to introduce PINs to cards is that they do not want to have a card in the user's wallet that is more difficult to use compared to cards from competitors [Krebs 2014]*. Such differences exist as well in online banking user authentication methods in different regions, as shown by the survey data in Section 3. Further research that examines online banking should also focus on whether communications security is correctly implemented. However, the area with the most work for further research seems to be user authentication and transaction authorization, for which the industry does not have a unified answer.

A limitation of the survey related to communications security is that it was examined for home banking, but not for mobile banking. Whenever a browser is not used, banks must implement SSL/TLS in their mobile applications themselves. These implementations are not always secure [Fahl et al. 2012; Georgiev et al. 2012; Onwuzurike and De Cristofaro 2015; Reaves et al. 2015]. Aside from client-side, there can be server-side issues. The survey in this article has shown that for home banking, servers can have vulnerabilities that potentially weaken communications security. The same could be true for servers used by mobile banking applications. More research in both can provide a more complete overview on how well SSL/TLS is used client- and server-side for mobile banking.

Another limitation is that authentication methods were only examined from an external perspective, using login pages and documentation. For example, for the discussed password and PIN implementations in Section 3.2, we were unable to get additional details concerning password policies that could influence security and usability. Letting the user choose a password, having relaxed rules about the length and complexity of the password, and not requiring the user to renew passwords on a regular basis all increase usability but potentially decrease security, and vice versa. Most banks do not publish their password policies, which is why this was excluded from the survey. Examining such policies would give more insight into the overall security concerning the often applied knowledge factor (either by itself, or in combination with a possession factor) but would require accounts at most banks, since it is quite rare that password policies are public. Gaining such detailed information could be done in further research. One approach would be by letting researchers around the world cooperate by sharing information about security systems from the banks where they are customers. The same further research could also expand on the 80 chosen banks and provide a better geographical distribution of examined banks. Examining home and mobile banking qualitatively and quantifying the results takes a lot of effort. This is especially true for the collection of information concerning authentication methods, since it requires the examination of documentation login pages and mobile banking software, all in many different languages. 80 banks worldwide is a small number, but it takes a large amount of time to examine them and it could be that some of the finer points of their authentication methods were missed.

In Section 4.3, some observations were made about the geographical distribution of SSL/TLS vulnerabilities and optional functions. Due to the somewhat limited sample size, these observations are solely based on the impressions that the survey gives and not on a statistical foundation. The same is true for other sections in which different regions are compared.

A question not answered by our survey is what influences the observed regional differences. The results suggest that there are differences in how regions implement user authentication methods and SSL/TLS, as shown by Figure 4, Table III, and Table V. Answering this question could give more insight into which motivators (e.g., regulations) drive banks and users to adopt more secure implementations and methods.

6. RELATED WORK

The primary focus of this work is on the development of online banking in general and the security in online banking in particular. Security in online banking has been an active research subject for many years. This section notes related work.

Several references are made in Section 2.1 to work that examines what makes users accept online banking, based on the technology acceptance model. Two other models that are also used to examine the acceptance of technology are the theory of reasoned action and the theory of planned behavior. All three models have been examined in an online banking context. The technology acceptance model has the best fit to determine what makes online banking acceptable [Yousafzai et al. 2010].

Data was collected for the survey about methods used by banks to authenticate customers, which are discussed in Section 3. Many of these methods have also previously been examined and proposed in the academic field. AlZomai et al. investigated the effectiveness of an information scheme that makes the customer verify transactions securely and also proposed a method that implemented such a scheme [AlZomai et al. 2008, 2010]. This scheme is known as What You See Is What You Sign (WYSIWYS). Weigold and Hiltgen proposed several methods that use WYSIWYS [Weigold and Hiltgen 2011]. An alternative to WYSIWYS was proposed by several

authors of this article under the name What You Enter Is What You Sign [Kiljan et al. 2014b].

Section 4 is dedicated to the use of SSL/TLS by bank sites and browsers, which authenticates the bank to the customer and provides confidentiality and integrity. When this protocol is used by a browser to conduct online banking, it relies on the perception of the customer to see if it is used and whether it is offered in a secure manner, based on several visual security indicators. The availability and effectiveness of these browser security indicators have been examined to a great extent [Dhamija et al. 2006; Oghenerukeybe 2009; Amrutkar et al. 2012].

SSL/TLS is used for more than just browser-server traffic. Several authors have examined SSL/TLS implementations used for (among others) mobile banking applications [Georgiev et al. 2012; Fahl et al. 2012; Reaves et al. 2015].

Of course, security in online banking is more than authentication and communications security. One example is the detection of fraudulent transactions by banks, based on characteristics of the transaction itself and on customer behavior (also briefly discussed in Section 3.4.2). Academic proposals for such systems have also been made [Aggelis 2006; Wei et al. 2013].

7. CONCLUDING REMARKS

We identified a pattern in the development of online banking that seems to rely on three phases, each relating to both technological and adoption trends. In the early adoption phase, banks offer a technologically crude way to conduct online banking that is expensive and not available for everyone. Availability and popularity of online banking increase in the following expansion phase, in which users start to accept online banking because critical aspects are perceived as being satisfactory. Finally, the exploitation phase relies on standardized technologies to make online banking available to almost anyone. The three phases are identified in the development of home banking (using a "desktop" computer), and the first two phases can also be identified in the development of mobile banking (using a mobile device anywhere an internet connection is available). Based on the identified trend, we predict that mobile banking has yet to enter the exploitation phase. In this predicted third phase, Hybrid Mobile Applications that are based mostly on standard web technologies will likely be introduced to reduce the costs of supporting multiple platforms and form factors. For mobile banking, this opens up opportunities for new kinds of scalable malware attacks that are similar to attacks made against home banking.

Security is an important aspect in online banking. For home banking, we examined 80 banks worldwide on how they authenticate their customers and how they implemented communications security. We also examined the implemented authentication methods for mobile banking at 66 banks.

For user to bank authentication, 75% of the banks offer an authentication method that relies on multiple factors (what the user knows and possesses) for home banking. The possible use of multiple factors was found in 59% of mobile applications and 25% of mobile sites. The adoption of multifactor authentication in both home and mobile banking increased slightly in a 2 year period, and seems to be most absent in North America. While there is not much diversity in the used knowledge factor (either password or PIN), different regions have different preferences for the possession factor. Noteworthy are the wide embrace of offline electronic devices used to generate login credentials in Africa, Europe, and Oceania, and the popularity of a one-time password distributed on paper or plastic in South America. Different possession factors are also used in mobile banking. Use of the mobile device itself as the possession factor is overall most favored. A recent development in mobile banking is that fingerprint-based

biometrics are slowly starting to be offered in alternative authentication schemes, despite that it is trivial to spoof fingerprint sensors embedded in user devices.

Whereas authentication from customer to bank is quite varied, the opposite is true for bank to customer authentication. The SSL/TLS protocol suite is used for communications security in home banking by all examined banks. All banks apply ciphers that provide confidentiality and integrity, but 12.5% of the banks support ciphers that provide an amount of protection that is far below NIST recommendations. The server-side implementation of SSL/TLS can also present several vulnerabilities that endanger the communication between bank and customer to eavesdropping and man-in-the-middle attacks. We found most of these vulnerabilities at banks in Africa. Support for optional SSL/TLS functions that increase security is mostly found in Europe and North America. Most banks have an implementation that is adequate to protect against man-in-the-middle attacks, but there are some sites that still present vulnerabilities that could have been solved more than a decade ago.

It is important to note that the survey does not look at all security aspects of online banking. For example, banks can implement behavior anomaly detection, used to detect financial transactions that are made under suspicious circumstances. While there are indications that some banks implement such in-house systems, they are hard to examine from an outside perspective.

ACKNOWLEDGMENTS

We thank the anonymous reviewers who were asked by ACM Computing Surveys to review this article, as well as the editor. They provided constructive feedback that was used to expand our research and improve this article extensively.

This article is a product of the Dutch Research Program on Safety and Security of Online Banking.

ACADEMIC REFERENCES

Vasilis Aggelis. 2006. Offline internet banking fraud detection. In *Proceedings of the the 1st International Conference on Availability, Reliability and Security (ARES'06)*. 2 pp-. DOI: http://dx.doi.org/10.1109/ARES.2006.89

Mamoun Alazab, Sitalakshmi Venkatraman, Paul Watters, Moutaz Alazab, and Ammar Alazab. 2012. Cybercrime: The case of obfuscated malware. In *Global Security, Safety and Sustainability & e-Democracy*, Christos K. Georgiadis, Hamid Jahankhani, Elias Pimenidis, Rabih Bashroush, and Ameer Al-Nemrat (Eds.). Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 99. Springer, Berlin, 204–211. DOI: http://dx.doi.org/10.1007/978-3-642-33448-1_28

Nadhem J. AlFardan, Daniel J. Bernstein, Kenneth G. Paterson, Bertram Poettering, and Jacob C. N. Schuldt. 2013. On the security of RC4 in TLS. In *Proceedings of the 22nd USENIX Conference on Security (SEC'13)*. USENIX Association, Berkeley, CA, 305–320.

Fadi Aloul, Syed Zahidi, and Wassim El-Hajj. 2009. Two factor authentication using mobile phones. In *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications (AICCSA'09)*. 641–644. DOI: http://dx.doi.org/10.1109/AICCSA.2009.5069395

Mohammed AlZomai, Bander AlFayyadh, and Jøsang. 2010. Display security for online transactions: SMS-based authentication scheme. In *Proceedings of the 2010 International Conference for Internet Technology and Secured Transactions (ICITST)*. 1–7.

Mohammed AlZomai, Bander AlFayyadh, Audun Jøsang, and Adrian McCullagh. 2008. An exprimental investigation of the usability of transaction authorization in online bank security systems. In *Proceedings of the 6th Australasian Conference on Information Security-Volume 81*. Australian Computer Society, Inc., 65–73.

Chaitrali Amrutkar, Patrick Traynor, and Paul C. Van Oorschot. 2012. Measuring SSL indicators on mobile browsers: Extended life, or end of the road? In *Information Security*, Dieter Gollmann and Felix C. Freiling (Eds.). Lecture Notes in Computer Science, Vol. 7483. Springer, Berlin, 86–103. DOI: http://dx.doi.org/10.1007/978-3-642-33383-5_6

Robert Biddle, Paul C. Van Oorschot, Andrew Patrick, Jennifer Sobey, and Tara Whalen. 2009. Browser interfaces and extended validation SSL certificates: An empirical study. In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*. ACM, 19–30.

Alain Yee-Loong Chong, Keng-Boon Ooi, Binshan Lin, and Boon-In Tan. 2010. Online banking adoption: An empirical analysis. *International Journal of Bank Marketing* 28, 4 (2010), 267–287. DOI: http://dx.doi.org/10.1108/02652321011054963

Joris Claessens, Valentin Dem, Danny De Cock, Bart Preneel, and Joos Vandewalle. 2002. On the security of today's online electronic banking systems. *Computers and Security* 21, 3 (June 2002), 253–265. DOI: http://dx.doi.org/10.1016/S0167-4048(02)00312-7

Elisa Constante, Jerry I. den Hartog, Milan Petkovic, Sandro Etalle, and Mykola Pechenizkiy. 2014. Hunting the unknown. http://eprints.eemcs.utwente.nl/25142/. In *Proceedings of the 28th Annual IFIP WG 11.3 Working Conference Data and Applications Security and Privacy (DBSec)*, Lecture Notes in Computer Science, Vol. 8566. Springer, Berlin, 243–259.

Kevin Curran and Timothy Dougan. 2012. Man in the browser attacks. *International Journal of Ambient Computing and Intelligence* 4, 1 (Jan. 2012), 29–39. DOI: http://dx.doi.org/10.4018/jaci.2012010103

Dianne Cyr, Milena Head, and Alex Ivanov. 2006. Design aesthetics leading to m-loyalty in mobile commerce. *Information & Management* 43, 8 (2006), 950–963. DOI: http://dx.doi.org/10.1016/j.im.2006.08.009

Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'06)*. ACM, New York, NY, 581–590. DOI: http://dx.doi.org/10.1145/1124772.1124861

Ori Eisen. 2010. Catching the fraudulent man-in-the-middle and man-in-the-browser. *Network Security* 2010, 4 (2010), 11–12. DOI: http://dx.doi.org/10.1016/S1353-4858(10)70046-5

Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith. 2012. Why eve and mallory love android: An analysis of android SSL (in)security. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS'12)*. ACM, New York, NY, 50–61. DOI: http://dx.doi.org/10.1145/2382196.2382205

Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov. 2012. The most dangerous code in the world: Validating SSL certificates in non-browser software. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS'12)*. ACM, New York, NY, 38–49. DOI: http://dx.doi.org/10.1145/2382196.2382204

Ja-Chul Gu, Sang-Chul Lee, and Yung-Ho Suh. 2009. Determinants of behavioral intention to mobile banking. *Expert Systems with Applications* 36, 9 (2009), 11605–11616. DOI: http://dx.doi.org/10.1016/j.eswa.2009.03.024

Cormac Herley, Paul C. Van Oorschot, and Andrew S. Patrick. 2009. Passwords: If we're so smart, why are we still using them? In *Financial Cryptography and Data Security*, Roger Dingledine and Philippe Golle (Eds.). Lecture Notes in Computer Science, Vol. 5628. Springer, Berlin, 230–237. DOI: http://dx.doi.org/10.1007/978-3-642-03549-4_14

A. Hisamatsu, Davar Pishva, and G. G. D. Nishantha. 2010. Online banking and modern approaches toward its enhanced security. In *Proceedings of the 2010 12th International Conference on Advanced Communication Technology (ICACT)*, Vol. 2. 1459–1463.

Collin Jackson, Daniel R. Simon, Desney Tan, and Adam Barth. 2007. An evaluation of extended validation and picture-in-picture phishing attacks. In *Financial Cryptography and Data Security*. Springer, 281–293.

Ankit Kesharwani and Shailendra Singh Bisht. 2012. The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model. *International Journal of Bank Marketing* 30, 4 (2012), 303–322. DOI: http://dx.doi.org/10.1108/02652321211236923

Sven Kiljan, Koen Simoens, Danny De Cock, Marko van Eekelen, and Harald Vranken. 2014a. *Security of Online Banking Systems*. Technical Report TR-OU-INF-2014-01 (Open Universiteit). Retrieved from http://portal.ou.nl/documents/114964/523334/TR-OU-INF-2014-01.pdf.

Sven Kiljan, Harald Vranken, and Marko van Eekelen. 2014b. What you enter is what you sign: Input integrity in an online banking environment. In *Proceedings of the 2014 Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. 40–47. DOI: http://dx.doi.org/10.1109/STAST.2014.14

Yufeng Kou, Chang-Tien Lu, S. Sirwongwattana, and Yo-Ping Huang. 2004. Survey of fraud detection techniques. In *Proceedings of the 2004 IEEE International Conference on Networking, Sensing and Control*, Vol. 2. 749–754. DOI: http://dx.doi.org/10.1109/ICNSC.2004.1297040

Vincent S. Lai and Honglei Li. 2005. Technology acceptance model for internet banking: An invariance analysis. *Information Management* 42, 2 (Jan. 2005), 373–386. DOI: http://dx.doi.org/10.1016/j.im.2004.01.007

Pin Luarn and Hsin-Hui Lin. 2005. Toward an understanding of the behavioral intention to use mobile banking. *Computers in Human Behavior* 21, 6 (2005), 873–891. DOI: http://dx.doi.org/10.1016/j.chb.2004.03.003

Mohammad Mannan and Paul C. Van Oorschot. 2007. Using a personal device to strengthen password authentication from an untrusted computer. In *Financial Cryptography and Data Security*, Sven Dietrich

and Rachna Dhamija (Eds.). Lecture Notes in Computer Science, Vol. 4886. Springer, Berlin, 88–103. DOI: http://dx.doi.org/10.1007/978-3-540-77366-5_11

Egwali Annie Oghenerukeybe. 2009. Customers perception of security indicators in online banking sites in Nigeria. *Journal of Internet Banking and Commerce* 14, 1 (2009), 1–15.

Gunter Ollmann. 2008. The evolution of commercial malware development kits and colour-by-numbers custom malware. *Computer Fraud & Security* 2008, 9 (2008), 4–7. DOI: http://dx.doi.org/10.1016/S1361-3723(08)70135-0

Lucky Onwuzurike and Emiliano De Cristofaro. 2015. Danger is my middle name: Experimenting with SSL vulnerabilities in android apps. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec'15)*. ACM, New York, NY, Article 15, 6 pages. DOI: http://dx.doi.org/10.1145/2766498.2766522

Tero Pikkarainen, Kari Pikkarainen, Heikki Karjaluoto, and Seppo Pahnila. 2004. Consumer acceptance of online banking: An extension of the technology acceptance model. *Internet Research* 14, 3 (2004), 224–235. DOI: http://dx.doi.org/10.1108/10662240410542652

Jon T. S. Quah and M. Sriganesh. 2007. Real time credit card fraud detection using computational intelligence. In *Proceedings of the International Joint Conference on Neural Networks (IJCNN 2007)*. 863–868. DOI: http://dx.doi.org/10.1109/IJCNN.2007.4371071

Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin R. B. Butler. 2015. Mo(bile) money, mo(bile) problems: Analysis of branchless banking applications in the developing world. In *Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15)*. USENIX Association, Berkeley, CA, 17–32.

Tim Redhead and Dean Povey. 1998. The problems with secure on-line banking. *Proceedings of the 17th Annual South East Asia Regional Conference (SEARCC'98)*.

Bruce Schneier. 2005. Two-factor authentication: Too little, too late. *Communications of the ACM* 48, 4 (April 2005), 136–136. DOI: http://dx.doi.org/10.1145/1053291.1053327

Ton Slewe and Mark Hoogenboom. 2004. Who will rob you on the digital highway? *Communications of the ACM* 47, 5 (May 2004), 56–60. DOI: http://dx.doi.org/10.1145/986213.986240

Jennifer Sobey, Robert Biddle, Paul C. Van Oorschot, and Andrew Patrick. 2008. Exploring user reactions to new browser cues for extended validation certificates. In *Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security (ESORICS'08)*. Springer-Verlag, Berlin, 411–427. DOI: http://dx.doi.org/10.1007/978-3-540-88313-5_27

Atul Srivastava. 2013. Mobile banking and sustainable growth. *American Journal of Economics and Business Administration* 5, 3 (2013), 89–94. DOI: http://dx.doi.org/10.3844/ajebasp.2013.89.94

Xiaoyuan Suo, Ying Zhu, and G. S. Owen. 2005. Graphical passwords: A survey. In *Proceedings of the 21st Annual Computer Security Applications Conference*. 463–472. DOI: http://dx.doi.org/10.1109/CSAC.2005.27

Wei Wei, Jinjiu Li, Longbing Cao, Yuming Ou, and Jiahang Chen. 2013. Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web* 16, 4 (2013), 449–475. DOI: http://dx.doi.org/10.1007/s11280-012-0178-0

T. Weigold and A. Hiltgen. 2011. Secure confirmation of sensitive transaction data in modern internet banking services. In *Proceedings of the 2011 World Congress on Internet Security (WorldCIS'11)*. 125–132.

Shumaila Y. Yousafzai, Gordon R. Foxall, and John G. Pallister. 2010. Explaining internet banking behavior: Theory of reasoned action, theory of planned behavior, or technology acceptance model? *Journal of Applied Social Psychology* 40, 5 (2010), 1172–1202. DOI: http://dx.doi.org/10.1111/j.1559-1816.2010.00615.x

Moshe Zviran and William J. Haga. 1990. Cognitive passwords: The key to easy access control. *Computers & Security* 9, 8 (1990), 723–736. DOI: http://dx.doi.org/10.1016/0167-4048(90)90115-A

NONACADEMIC AND WEB REFERENCES*

Josie Allchin. 2012. A history of innovation in payments. Retrieved from http://www.marketingweek.com/2012/11/28/a-history-of-innovation-in-payments/.

Ally Bank. 2010. How We Protect You. Retrieved from http://www.ally.com/security/.

Bank of America. 2013. Online Banking Security from Bank of America. Retrieved from https://www.bankofamerica.com/privacy/online-mobile-banking-privacy/online-banking-security.go.

Banking & Payments Federation Ireland. 2015. Online and Mobile Banking Report—Full Year 2014 and Q4 2014. Retrieved from http://www.bpfi.ie/wp-content/uploads/2015/05/BPFI-Online-and-Mobile-Banking-Q4-2014-FINAL.pdf.

Barclays. 2014. What we're doing to protect your account. Retrieved from http://www.barclays.co.uk/Helpsupport/Whatweredoingtoprotectyou/P1242560037946#Fraudmonitoring.

Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid. 2012. Transitions: Recommendation for key management—Part 1: General (revision 3). *NIST Special Publication* 800 (2012), 57.

BBA. 2015. The Way We Bank Now: World of Change. Retrieved from https://www.bba.org.uk/publication/bba-reports/world-of-change-2/.

Board of Governors of the Federal Reserve System. 2014. Consumers and Mobile Financial Services 2014. Retrieved from http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf.

Board of Governors of the Federal Reserve System. 2015. Consumers and Mobile Financial Services 2015. Retrieved from http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf.

Erwin Boogert. 2008. Mobiel internet groeide 30 procent in 2007. Retrieved from http://www.emerce.nl/nieuws/mobiel-internet-groeide-30-procent-in-2007.

Danyl Bosomworth. 2015. Statistics on mobile usage and adoption to inform your mobile marketing strategy. Retrieved from http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/.

John Bristowe. 2015. What is a Hybrid Mobile App? Retrieved from http://developer.telerik.com/featured/what-is-a-hybrid-mobile-app/.

Deborah Burns. 1983. PRONTO: Bank on your atari. *Antic* 1, 6 (February 1983). Retrieved from http://www.atarimagazines.com/v1n6/pronto.html.

Business Standard News. 2014. Mobile banking zooms as India gets smarter. Retrieved from http://www.business-standard.com/article/finance/mobile-banking-zooms-as-india-gets-smarter-114081100826_1.html.

Mike Cetera. 2015. Online banking vs. mobile banking. Retrieved from http://www.bankrate.com/financing/mobile-finance/online-banking-vs-mobile-banking/.

Chaos Computer Club. 2013. Chaos Computer Club Breaks Apple TouchID. Retrieved from http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid.

China Internet Network Information Center. 2014. Statistical Report on Internet Development in China (Jan. 2014). Retrieved from http://www1.cnnic.cn/IDR/ReportDownloads/201404/U020140417607531610855.pdf.

Richard Collins. 2013. Get the FAQs about Ubuntu on Smartphones. Retrieved from https://insights.ubuntu.com/2013/02/15/get-the-faqs-about-ubuntu-on-smartphones/.

Tim Dierks and Christopher Allen. 1999. RFC 2246—The TLS Protocol Version 1.0. Retrieved from http://tools.ietf.org/html/rfc2246.

Tim Dierks and Eric Rescorla. 2006. RFC 4346—The Transport Layer Security (TLS) Protocol Version 1.1. Retrieved from http://tools.ietf.org/html/rfc4346.

Tim Dierks and Eric Rescorla. 2008. RFC 5246—The Transport Layer Security (TLS) Protocol Version 1.2. Retrieved from http://tools.ietf.org/html/rfc5246.

Thai Duong and Juliano Rizzo. 2011. Here Come The ⊕ Ninjas. Unpublished manuscript. Retrieved from http://netifera.com/research/beast/beast_DRAFT_0621.pdf.

Eurostat. 2016. Individuals Using the Internet for Internet Banking. Retrieved from http://ec.europa.eu/eurostat/tgm/table.do?tab=table&plugin=1&language=en&pcode=tin00099.

Chris Evans, Chris Palmer, and Ryan Sleevi. 2015. RFC 7469—Public Key Pinning Extension for HTTP. Retrieved from https://tools.ietf.org/html/rfc7469.

Febelfin. 2015. Cijfers—Succes internetbankieren. Retrieved from https://www.safeinternetbanking.be/nl/cijfers-internetbankieren.

Mary Jo Foley. 2014. Microsoft to Bring Back Start Menu, Windowed Apps to Windows. Retrieved from http://www.zdnet.com/article/microsoft-to-bring-back-start-menu-windowed-apps-to-windows/.

Alan Freier, Philip Karlton, and Paul Kocher. 2011. RFC 6101—The Secure Sockets Layer (SSL) Protocol Version 3.0. Retrieved from http://tools.ietf.org/html/rfc6101.

Jeff Hodges, Collin Jackson, and Adam Barth. 2012. RFC 6797—HTTP Strict Transport Security (HSTS). Retrieved from https://tools.ietf.org/html/rfc6797.

Jasper Houtman. 2002. Postbank: 40 procent bankiert met mobiel toestel. Retrieved from http://www.emerce.nl/nieuws/postbank-40-procent-bankiert-met-mobiel-toestel.

IO Active. 2012. Reversal and Analysis of Zeus and SpyEye Banking Trojans. Retrieved from http://www.ioactive.com/pdfs/ZeusSpyEyeBankingTrojanAnalysis.pdf.

Ireland's Central Statistics Office. 2012. Population and Migration Estimates - April 2012. Retrieved from http://www.cso.ie/en/media/csoie/releasespublications/documents/population/2012/popmig_2012.pdf.

iResearch. 2014. Mobile Finance Becomes the Trend of Future Banking. Retrieved from http://www.iresearchchina.com/content/details7_18315.html.

ITavisen. 1999. Verdens frste WAP-bank fra Norge. Retrieved from http://www.itavisen.no/nyheter/verdens-f%C3%B8rste-wap-bank-fra-norge-41812.

KPMG. 2015. Mobile Banking 2015. Retrieved from http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/mobile-banking-report-2015.pdf.

Brian Krebs. 2014. Chip & PIN vs. Chip & Signature. Retrieved from http://krebsonsecurity.com/2014/10/chip-pin-vs-chip-signature/.

Adam Langley. 2012. BEAST Followup. Retrieved from https://www.imperialviolet.org/2012/01/15/beastfollowup.html.

Adam Langley. 2014. The POODLE Bites Again. Retrieved from https://www.imperialviolet.org/2014/12/08/poodleagain.html.

Eric Lawrence. 2005. Upcoming HTTPS Improvements in Internet Explorer 7 Beta 2. Retrieved from http://blogs.msdn.com/b/ie/archive/2005/10/22/483795.aspx.

Moxie Marlinspike. 2009. New tricks for defeating SSL in practice. Black Hat DC, Washington D.C. (2009). Retrieved from https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf.

Tim Matthews. 2012. Don't Be Afraid of Mobile Banking Apps. Retrieved from http://www.banktech.com/channels/dont-be-afraid-of-mobile-banking-apps/a/d-id/1295727.

Microsoft. 2015. Security Bulletin MS15-032—Cumulative Security Update for Internet Explorer (3038314). Retrieved from https://technet.microsoft.com/en-us/library/security/MS15-032.

Bodo Moeller and Adam Langley. 2015. RFC 7507—TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks. Retrieved from https://tools.ietf.org/html/rfc7507.

Håvard Molland. 2014. Security changes in Opera 25; the poodle attacks. Retrieved from http://www.opera.com/blogs/security/2014/10/security-changes-opera-25-poodle-attacks/.

Bodo Möller, Thai Duong, and Krzysztof Kotowicz. 2014. This POODLE Bites: Exploiting The SSL 3.0 Fallback. Retrieved from https://www.openssl.org/~bodo/ssl-poodle.pdf.

Kim Moser. 2012. Computer History—Citibank Direct Access and the Enhanced Telephone. Retrieved from http://www.kmoser.com/computerhistory/?id=citibank.

Mozilla. 2006. Bug 236933—Disable SSL2 and other weak ciphers. Retrieved from https://bugzilla.mozilla.org/show_bug.cgi?id=236933.

Mozilla. 2014. Firefox—Notes (34.0). (2014). https://www.mozilla.org/en-US/firefox/34.0/releasenotes/.

National Institute of Standards and Technology. 2011. Vulnerability Summary for CVE-2011-3389. Retrieved from http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3389.

Nedbank. 2011. SIM Swap Scam. Retrieved from http://www.nedbank.co.za/website/content/Security/sim.asp.

Opera Software. 2008. Opera 9.5 for Windows Changelog. Retrieved from http://www.opera.com/docs/changelogs/windows/950/.

Kevin Rawlinson. 2015. Banks to Allow Account Access Using Fingerprint Tech. Retrieved from http://www.bbc.com/news/technology-31508932.

Eric Rescorla, Marsh Ray, Steve Dispensa, and Nasko Oskov. Retrieved from RFC 5746—Transport Layer Security (TLS) Renegotiation Indication Extension. (2010). https://tools.ietf.org/html/rfc5746.

Ivan Ristic. 2009. SSL and TLS Authentication Gap Vulnerability Discovered. Retrieved from https://community.qualys.com/blogs/securitylabs/2009/11/05/ssl-and-tls-authentication-gap-vulnerability-discovered.

Ivan Ristic. 2010. Disabling SSL Renegotiation is a Crutch, Not a Fix. (2010). https://community.qualys.com/blogs/securitylabs/2010/10/06/disabling-ssl-renegotiation-is-a-crutch-not-a-fix.

Ivan Ristic. 2012. CRIME: Information Leakage Attack against SSL/TLS. (2012). https://community.qualys.com/blogs/securitylabs/2012/09/14/crime-information-leakage-attack-against-ssltls.

Ivan Ristic. 2013. Is BEAST Still a Threat? Retrieved from https://community.qualys.com/blogs/securitylabs/2013/09/10/is-beast-still-a-threat.

David Ross, Tobias Gondrom, and Thames Stanley. 2015. RFC 7034—HTTP Header Field X-Frame-Options. Retrieved from https://tools.ietf.org/html/rfc7034.

Ariel Sanchez. 2014. Personal banking apps leak info through phone. (2014). http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html.

Mark Scott. 2014. Preparing for Chip-and-PIN Cards in the United States. Retrieved from http://bits.blogs.nytimes.com/2014/12/02/preparing-for-chip-and-pin-cards-in-the-united-states/.

Remco Tomesen. 2006a. Grote merken willen beter mobiel internet. Retrieved from http://www.emerce.nl/nieuws/grote-merken-willen-beter-mobiel-internet.

Remco Tomesen. 2006b. Rabobank ontevreden over gebruik mobiel bankieren. Retrieved from http://www.emerce.nl/nieuws/rabobank-ontevreden-over-gebruik-mobiel-bankieren.

Sean Turner and Tim Polk. 2011. RFC 6176—Prohibiting Secure Sockets Layer (SSL) Version 2.0. Retrieved from http://tools.ietf.org/html/rfc6176.

Monique van den Heuvel. 2001. Het mobieltje van Postbank. Retrieved from http://www.mt.nl/1/1727/home/het-mobieltje-van-postbank.html.

W3C. 2015. Content Security Policy Level 2. Retrieved from https://www.w3.org/TR/CSP2/.

Western Union. 2012. History of Western Union. Retrieved from https://www.westernunionbank.com/en/history/.

Colin Wilhelm. 2014. Mobile Banking Deployment Widespread. Next Challenge: Adoption. Retrieved from http://www.americanbanker.com/issues/179_209/1070929-1.html.

Wireless Application Protocol Forum. 2001. Wireless Transport Layer Security - Version 06-Apr-2001. (2001). http://technical.openmobilealliance.org/tech/affiliates/wap/wap-261-wtls-20010406-a.pdf.

World Bank Open Data. 2016. Data Related to China. Retrieved from http://data.worldbank.org/country/china.

Received July 2015; revised August 2016; accepted September 2016