

A Proof of Concept Attack against Norwegian Internet Banking Systems

Yngve Espelid, Lars-Helge Netland, André N. Klingsheim, and Kjell J. Hole
{yngvee, larshn, klings, kjellh}@ii.uib.no

NoWires Research Group
Department of Informatics
University of Bergen, Norway
Short paper version, Feb. 21st, 2008

Abstract. The banking industry in Norway has developed a new security infrastructure for conducting commerce on the Internet. The initiative, called BankID, aims to become a national ID infrastructure supporting services such as authentication and digital signatures for the entire Norwegian population. This paper describes a practical man-in-the-middle attack against online banking applications using BankID. The attack gives an adversary access to customer bank accounts in two different online banking systems. Proof of concept code has been developed and executed to demonstrate the seriousness of the problem.

1 Introduction

The Norwegian banking community has created a new infrastructure for secure e-commerce, called BankID.¹ As of October 2007, BankID has more than 700,000 end-users. This number is expected to exceed 1.5 million come 2008. At the time of writing, the infrastructure is mainly used for authentication of Internet banking customers, but BankID is extending into other markets, such as the government sector and e-commerce in general. It has also been used in conjunction with e-voting in some companies. BankID won a European prize, namely the *ema Award for Excellence in Secure Electronic Business* in 2006. The system is modeled after a Public-Key Infrastructure (PKI), where the banks themselves own and operate the central infrastructure. Within a few years, the Norwegian banking industry wants BankID to become a nationwide identity system.

No publicly available independent third party evaluation of the system confirms that BankID meets a minimum of security and privacy requirements. This is worrisome for several reasons: Firstly, a report by the US National Research Council [1] states that public review is essential when developing a nationwide identity system. The social costs of a poorly thought-out system are simply too high to justify. Secondly, the banking industry both owns the BankID infrastructure and provides financial services on top of the framework. It is not clear how potential conflicts of interest, involving the bank as a service provider and

¹ Not to be confused with the Swedish BankID initiative.

PKI operator, will be resolved. Uncontested, the combination of no trusted third party and a security-through-secrecy policy could undermine the legal protection of Norwegian bank customers. This issue was explored in depth in a previous report that performed a risk analysis of the BankID infrastructure [2]. Our work was done in parallel with the mentioned evaluation, and examines the therein suggested Man-in-the-Middle (MitM) attack in detail.

This paper is organized as follows: Section 2 looks at BankID from the attacker's point of view and describes a MitM attack against Norwegian online banks that use the security infrastructure; Section 3 provides improvement suggestions for BankID; Section 4 comments on related work; while Sect. 5 concludes the paper.

2 BankID through Adversarial Eyes

A rough sketch of BankID can be drawn after inspecting a white paper released by the BankID project [3]. The system is built around three entities: a central *infrastructure*, *customers*, and online *merchants*. Private keys and the corresponding public-key certificates issued to customers are stored and used by the central infrastructure. This design differs from a typical X.509 PKI, which requires private keys to be solely available to the entity identified in the matching certificate [4]. As a consequence, all customer authentication and digital signature services with PKI credentials are executed by the infrastructure. Merchants control their own cryptographic keys and rely on server software distributed by the BankID project.

A Java applet is central in the authentication procedure. The applet is readily available from the central infrastructure, and is provided to end-users by all affiliated merchants. This makes it a natural target for uncovering technical details about BankID.

2.1 Reverse Engineering

A common technique to understand undocumented software is *reverse engineering* [5]. The information gathered from public written sources was insufficient to understand the inner-workings of BankID protocols involving customers. Hence, we reverse engineered the applet to study the protocols in more detail. The process included studying input and output data, the communication flow, and representing the application as human-readable source code.

By inspecting merchant web pages we discovered that the applet is controlled through HTML parameters. Two parameters specify addresses to the infrastructure server running a two-factor authentication procedure and the merchant server carrying out a challenge-response protocol. Consequently, all merchants can use the same applet by configuring these initialization parameters.

2.2 The Attack

By changing the two parameters to the applet, it willingly communicates—over either HTTP or HTTPS—with the MitM proxy depicted in Fig. 1. We choose HTTP to avoid having to install a certificate on the MitM proxy. The decision to store the customers' cryptographic keys at the infrastructure results in a complex authentication protocol:

- The customer presents her birth number, one-time password (OTP), and fixed password to the central infrastructure. This action unlocks PKI functionality.
- The customer engages in a challenge-response protocol with the merchant. The infrastructure handles all PKI operations on behalf of the user.

The proxy learns the communication between the applet and the merchant, which is sufficient to obtain an authorized session to the merchant. However, the information flow between the customer and the infrastructure is encrypted, preventing the proxy from obtaining the customer credentials. The attack is carried out through the following steps:

1. Trick the user into visiting a webpage on the proxy, initializing the applet with malicious parameters.
2. Start the HTTPS session between the MitM proxy and the merchant to obtain session IDs.
3. Relay the traffic until the authentication completes.
4. Seize the HTTPS session to the merchant after the authentication is completed.

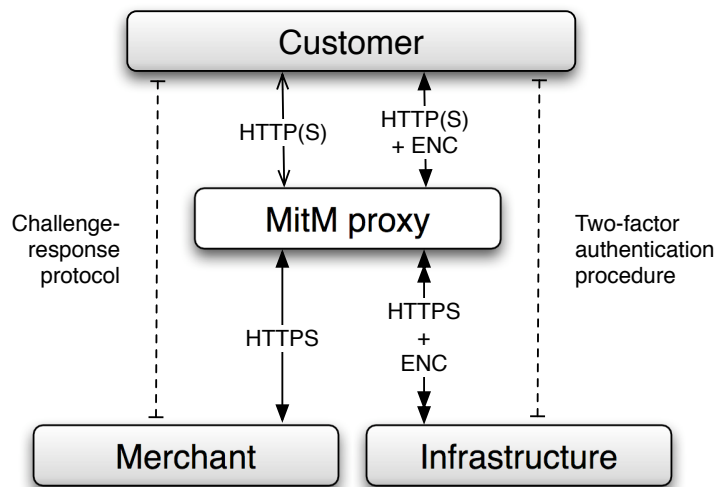


Fig. 1. The MitM proxy in the authentication protocol

Norwegian banks currently use OTPs and fixed passwords to authorize transactions. Therefore, the attacker must collect at least one OTP and the password to transfer money out of the account. This can be achieved by alerting the user at the end of the log-in procedure that the previously entered fixed password and OTP were incorrect, after which the attacker asks for them again.

Proof of Concept. The attack was tested against two randomly chosen Norwegian online banking systems. Both attempts gave access to a customer account in these banks. The vulnerability was first identified and tested in March 2007. The BankID community claims to have fixed the problem in November 2007.

3 Possible BankID Improvements

The MitM attack described herein must be addressed by the BankID community. The applet needs to properly authenticate its communication peers, enabling it to detect a MitM proxy. Also, the applet must require end-to-end encryption when communicating with both the infrastructure and the merchant.

In the long-term, the BankID community should evaluate the implications of moving to a traditional PKI where the clients possess their own credentials. This would improve the strength of the authentication, and yield a simpler design. Of course, such a change comes with a cost. However, a national security infrastructure must fulfill minimum security requirements, including resistance to MitM attacks.

As the system is now gaining serious momentum in Norway, its users need a better perception of the true level of security. In light of our attack, and the findings in [2], a thorough analysis of BankID is called for. The infrastructure and its documentation should be scrutinized by independent security experts to detect and resolve problems. This could increase the trustworthiness of BankID in the long run.

4 Related Work

A series of three articles analyze Norwegian banking systems [6,7,2]. Our attack builds on the above-mentioned article series and zooms in on weaknesses touched upon in the risk analysis of BankID [2]. In particular, our work further testifies to the inefficacy of the banks' security-through-secrecy policy.

In [8], Anderson argues that a false threat model was accepted, due to the lack of feedback on why British retail banking systems failed. In doing so, the financial industry developed increasingly complex systems to protect against cryptanalysis and technical attacks, when it would have been wiser to focus on implementation and managerial failures. Analyses of banking systems published after Anderson's initial paper underscore the observation that systems fail not because of inadequate cryptographic primitives, but rather design flaws and implementation errors [9,10].

5 Conclusion

The new national security infrastructure for e-commerce in Norway, BankID, was vulnerable to a MitM attack in 2007. By changing initialization parameters to the BankID applet, an adversary could insert a proxy between a customer and a merchant. When BankID was used in Internet banking, an attacker could let a customer complete authentication, and later take over the banking session. The attack did not depend on malicious software being installed on the victim's computer. Proof of concept code was developed to demonstrate the attack.

The MitM vulnerability in BankID calls for immediate attention. The banks claim to have fixed the problem in November 2007. In the long run, the banks should carefully evaluate their development process, as their current methodology results in software that contradicts advice given in well-known security textbooks.

5.1 Final Remark

We would like to emphasize that *only* BankID accounts belonging to members of the NoWires Research Group were used to develop and demonstrate the MitM attack. No accounts belonging to others were involved in any way during our work with this paper.

References

1. Kent, S.T., Millett, L.I., eds.: IDs—Not That Easy: Questions About Nationwide Identity Systems. The National Academies Press (2002)
2. Hole, K.J., Tjøstheim, T., Moen, V., Netland, L., Espelid, Y., Klingsheim, A.N.: Next generation internet banking in Norway. submitted to IEEE Security & Privacy (2007) Available at: <http://www.nowires.org/Papers-PDF/BankIDevaluation.pdf>.
3. The Norwegian Banks' Payment and Clearing Centre: BankID FOI white paper. (Release 2.0.0) (2006) (in Norwegian)
4. Adams, C., Lloyd, S.: Understanding PKI—Concepts, Standards, and Deployment Considerations. 2nd edn. Addison-Wesley (2003)
5. Chikofsky, E.J., Cross II, J.H.: Reverse engineering and design recovery: A taxonomy. IEEE Software **7**(1) (1990) 13–17
6. Hole, K.J., Moen, V., Tjøstheim, T.: Case study: Online banking security. IEEE Security & Privacy **4**(2) (2006) 14–20
7. Hole, K.J., Moen, V., Klingsheim, A.N., Tande, K.M.: Lessons from the Norwegian ATM system. IEEE Security & Privacy **5**(6) (2007) 25–31
8. Anderson, R.: Why cryptosystems fail. In: ACM 1st Conference on Computer and Communication Security, Fairfax, VA, USA (1993)
9. Berkman, O., Ostrovsky, O.M.: The unbearable lightness of pin cracking. In: Financial Cryptography and Data Security (FC), Lowlands, Scarborough, Trinidad/Tobago (2007)
10. Anderson, R., Bond, M., Clulow, J., Skorobogatov, S.: Cryptographic processors—a survey. Technical Report 641, University of Cambridge (2005)