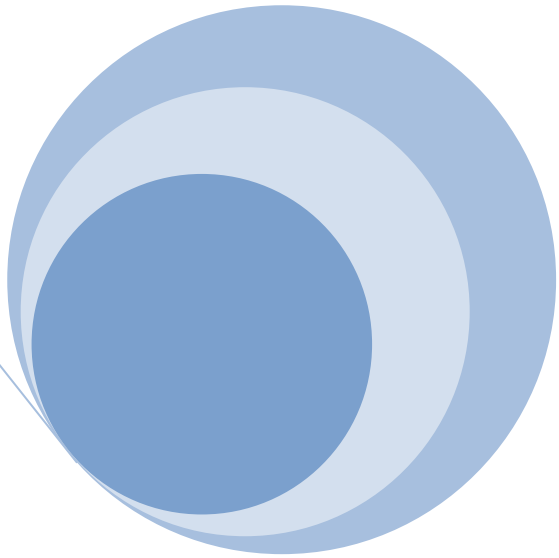
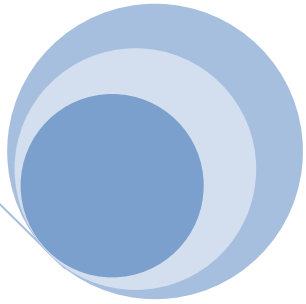
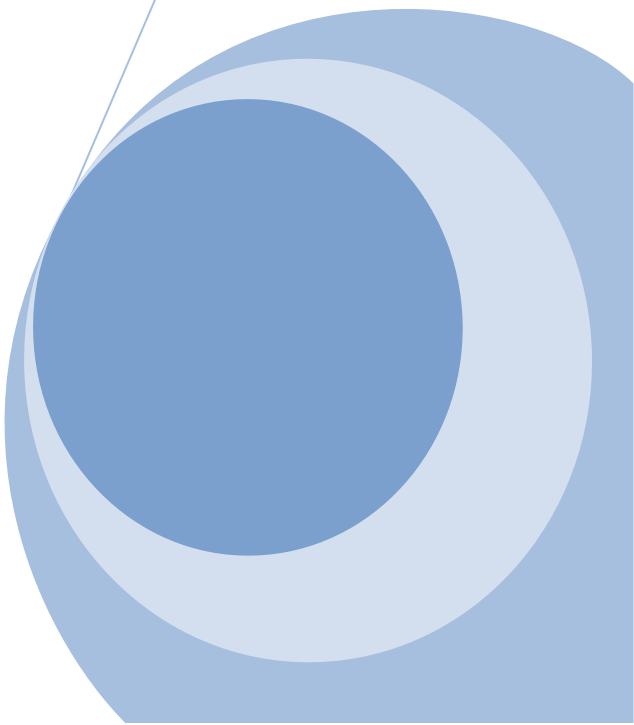




Credit cards vs iDeal a comparison of security issues

Mail ordering over the internet is a common way of doing business these days. Two ways of paying orders over The Internet are credit cards and iDeal – a Dutch online payment system. In this thesis, the relative security of both systems is put side-by-side.

P.M.A. van Leeuwen
14-12-2010



Contents

Abstract

Since the creation of the internet, the amount of online trade has reached great heights. There are several ways to carry out online transactions, two of them being iDeal and credit cards. Both have their advantages and disadvantages when it comes to security from the viewpoint of the customer. In this thesis, a comparison is made between iDeal and credit cards when it comes to security from a customer's viewpoint.

Fraud history
Currently, the rate of fraud with credit cards is staggering while I have been unable to find a single case of fraud with iDeal. The refunding policy of credit card companies greatly limits the damage for customers though.

Approach
The likelihood and impact of each possible attack on either system are determined to draw an overall conclusion about the security of both systems.

Conclusion
iDeal has superior technical security over credit cards. It is considerably easier to successfully carry out an attack on the credit card system than on iDeal. This is not surprising, since iDeal is built on top of existing online banking systems with built-in technical security. Credit cards, on the other hand, predate the creation of the internet with tens of years which takes its toll on their technical security. However, due to the generous refunding policy of credit card companies, the financial security of credit cards is actually higher despite the lower technical security.

Credit cards are especially vulnerable to a data gathering attack, since the system cannot function if the merchant does not receive a credit card number and other required data. Besides, credit cards are susceptible to key logger attacks and man-in-the-browser attacks. iDeal is impervious to key logger attacks and data gathering attacks and well-protected – though not immune – against man-in-the-browser attacks.

A customer has the option to opt for iDeal – smaller chance of a successful attack but worse impact if it happens – or for credit cards – bigger chance of a successful attack but considerably lower impact.

Suggestions for future research
The academic community should create measurement standards to measure 'security', other systems can be compared next to iDeal and credit cards, other viewpoints may be included in the conclusion and the security of iDeal can be compared with regular online banking.

Disclaimer

This document considers the state of affairs till May 2009 and hence disregards Mastercard SecureCode and Verified by Visa, as well as other security methods deployed after May 2009.

1 Introduction

This chapter provides an introduction to the information age and two different methods of online payment, credit cards and iDeal.

1.1 The information age

Since the rise of the Internet in the nineties and further thereafter, the world of business and private lives have changed dramatically. Some scientists even talk about the information age. Mail ordering on the Internet is now as common as mail ordering through catalogues in the age preceding the information age. Next to the rise of business on the Internet, ways of placing orders by customers were invented. Some of them are clearly spin-offs of already existing methods, others however would hardly be possible without the Internet.

The business partner usually does not see a person in real life when he orders commodities or even just information by mail order. All contact takes place on some kind of network system, usually the Internet. This creates several security issues, which will be explored in detail in this paper.

1.2 Credit card

A common way for a customer to pay an order is using a credit card. By recording the credit card number and – usually – the expiration date by the customer, the merchant is able to collect the money from the customer's bank account. Credit cards have turned out to be perfectly applicable for Internet transactions for several reasons. They have their drawbacks as well, when it comes to security.

Credit card fraud is widespread. For example, according to [1] the rate of fraud in the UK in 2006 was £428.0 million which, according to the current exchange rate, equals €601 million. Estimates for the US are hard to find, but as credit card use is more widespread in the US the amount of fraud must be even higher.[1] Credit card companies pay large amounts of money to compensate victims of fraud. To gain widespread acceptance, a credit card must be easy to use which has its drawbacks on security measures. Obviously, credit card companies rather choose to have a system with a minimum of inconvenience – a credit card transaction can take place in a minute – rather than a system with more security, as long as the additional revenue of more transactions outweighs the cost of repaying victims of fraud.

[1] According to [7], there are 65,368,000 credit cards in the UK and according to [8] there are 640 million in the US. This means there are approximately one credit card for each UK resident and approximately two for each US resident.

1.3 iDeal

iDeal is a Dutch system and is only available in The Netherlands, which means that customers and merchants must have an account at a Dutch bank. Currently, ABN AMRO, Postbank, SNS Bank, Rabobank and Fortis Bank support iDeal. iDeal works in a way similar to the deposit-transfer card[2] system. A merchant can send a deposit-transfer card to a customer, which the customer has to sign and return to the bank, either by delivering it there personally or by sending it by snail mail. Another way of paying a deposit-transfer is using an internet banking system to make a transfer to the required bank account with the required sum. iDeal is similar in the way that it presents the user with a form which shows the total amount to pay, which must be authorized by the customer.

iDeal is designed to make use of the internet banking infrastructure of the supporting banks. When a customer chooses to pay an order using iDeal, he is redirected to the website of the bank he wishes to use. Obviously, the customer is required to have an account at the chosen bank. Instead of filling in the transfer form completely, as he would normally do if he made a transfer, the required bank account number of the merchant and the right amount of money are already prefilled. Actually, this is all iDeal does: redirecting the customer to the website of his bank and prefilling the form with the desired values. This makes iDeal essentially a very simple system.

The customer has to sign the order in the same way as he would normally do when he uses internet banking. This means that customers do not need to learn a new system but can use their old and trusted systems. Besides, most internet banking systems have been in use for years and are supposed to be safe at this moment, which is much harder to ensure with a new system.

A demonstration which shows how iDeal works can be found at [10].

[2] An acceptgiro in Dutch

2 About this document

This document describes the research which has been carried out to compare the 'security' of iDeal (see 1.3) on one side and credit cards (see 1.2) on the other side when it comes to paying online orders.

This thesis contains the following sections:

2.1 Fraud History

At first, an introduction is provided of the current known fraud history of credit cards and iDeal. Since information is not always readily available, estimates have been made as accurately as possible.

2.2 Protocols

To get a better understanding of how an attack interferes with the standard procedures of iDeal and credit cards, the protocols are provided in chapter 4.

2.3 Assets

Mallory does not need to carry out an attack if there are no valuables to obtain. This does not mean only physical valuables like money or commodities. A credit card number might be an asset in itself.

A list of assets Mallory can threaten is, therefore, provided in chapter 4.

2.4 Operationalisation

The definitions of the 'likelihood' and 'impact' of an attack as well as the definitions of the various viewpoints to look at 'security' is provided in chapter 6.

2.5 Attacks

To determine the security levels of both payment systems, the security attacks as known from the literature will be taken as the basis, not the security measures which are used for protection. Therefore, in chapter 7, an overview of the attacks will be provided. Each subsection of chapter 7 will describe one specific kind of attack, e.g. the man-in-the-middle attack, the key logger attack etc. The subsections start with an introduction to the specific attack, describing the attack in general. There may be several subsections for each attack, each describing the attack under different circumstances or with certain security methods in place.

Then, each subsection is split in two sections, one for iDeal and one for credit cards. A short summary is provided, describing the assets at stake and the risk that those assets are compromised by that specific attack. The summary is based on the findings of the research and do not have any external source. Each subsection has a conclusion, on which the summary is based. Those summaries are the foundation of the final conclusion of the thesis.

2.6 Countermeasures

As certain attacks can be prevented by countermeasures – for example, a hardware key logger attack can be prevented by regularly checking keyboards for alien devices -, the specific countermeasures against a certain attack are taken into consideration. Those countermeasures are specifically described in the subsections. The 'general' counter measures which can be used for protection against multiple of attacks are described in chapter 8.

2.7 Conclusion

The final conclusion of the research is presented in chapter 9. The conclusion is based on the summaries which are present in the subsections of the attacks. Likelihood and impact are known from the summaries and they are grouped together in several ways to present the conclusion from three different viewpoints: "technical, financial and overall'.

3 Fraud history

This chapter describes the history of fraud with online payments using a credit card or iDeal. It must be noted that credit cards are nearly a century old, whereas iDeal was created 2005.

According to [5], fraud with Internet banking is 'negligible'. This, however, is a claim of the banks themselves which raises questions about the reliability of the claim.

3.1 iDeal

Some ways to commit fraud with iDeal have little to do with iDeal itself, but rather with iDeal modules created by third parties. Such a module makes it possible for a merchant to make use of iDeal without creating an account first. The actual account used resides with a third party who provides this as a service.

An example of such a third party module is 'Idealm' of the company Oscommerce. Due to a programming error – uncritically trusting a $_POST variable in PHP – it was possible for a fraudulent customer to lower the amount he had to pay while still authorizing the payment. Oscommerce quickly patched the erroneous code and reported fraud was very low. More about this security breach can be found in [9]. Surprisingly, the erroneous code had been in the module for years without anybody noticing it and exploiting it.

I have not been able to find an actual case of iDeal fraud. I have only found one person on a message board who complained about being robbed with iDeal, even though I thoroughly checked on Google and AltaVista. The specific case I found, however, most certainly had nothing to do with iDeal itself and the victim simply transferred too much money to a fraudulent merchant which in his case was a web cam girl.

3.2 Credit cards

Fraud is not uncommon with credit cards. Because the system must be easy to use, security measures cannot be extremely strict. Accurate numbers are hard to find for the US or The Netherlands but if the UK is taken as an example, according to [1] it is clear that fraud is rampant[3]. Usually, in the last analysis, the victim is not the customer but the credit card company, which repays fraudulent transactions.

[3] According to The International Herald Tribune, "an FBI report from 2005 indicated that credit cards represented the majority of the total $315 billion U.S. financial fraud loss for that year, while a recent European study found that more than 22 million adults fell victim to credit card scams in 2006. Figures from the Banque de France, the country's central bank, showed a credit card fraud loss of €236 million, or $319 million, for 2005." [18]

4 Protocols

The following chapter describes the protocols as used by online credit card transactions and iDeal transactions.

4.1 Credit card transactions

4.1.1 Summary

1. The customer places an order with a certain amount at a merchant's website.
2. The merchant checks the validity of the credit card as far as is possible with a CNP (card not present) transaction. Next to that, he can check if the customer has enough money or credit on his account to afford the transaction.
3. If the merchant gets a positive result from the checks in step 3, he will deliver the order.
4. Later, the merchant receives the money from the credit card company, rather than directly from the customer.

4.1.2 Detailed

	Customer	*Merchant*	*credit card comp*
1	*Order Details* →		
2	*Credit Card details* →		
3		*Ack request* →	
4		← *Ack*	

4.2 iDeal transactions

4.2.1 Summary

1. The customer places an order for a certain amount at a merchant's website.
2. Upon checkout, the customer opts to pay using iDeal.
3. The customer chooses his bank.
4. In the background and invisible to the user, the transaction is prepared at the bank.
5. The user is redirected to the website of the bank, where he will find his prepared order.
6. The user carries out the transaction as he would normally carry out any bank transfer, using Internet banking.

4.2.2 Detailed

Normally, if no attack takes place, the protocol would be as follows. Note that if the Postbank is used, the protocol is a little different. The individual steps are explained in more detail below the table.

	Customer	Merchant	Bank	
1	iDeal, Bank →			
2		OrderDetails, OrderId →		
3	← Red, OrderId			
4	(customer is redirected to bank website)			
5	← Challenge			
6	$[Challenge]_{key}$ →			
7		← Ack		

8	← Red	
9	(customer is redirected back to the merchant's website)	

If the Postbank is used, steps 5 and 6 are different. Instead of sending a challenge to the customer, the user must provide a so-called TAN-code. The TAN-code can be sent to the user by an SMS or taken from a list of 100 TAN-codes. The list of codes varies from user to user. The bank provided an index number and the customer provides the right TAN-code according to the index number.

1 The customer, on the website of the merchant, chooses to pay using iDeal and he selects his bank.
2 The merchant prepares the order at the bank. This requires a unique order ID.
3 The merchant redirects the customer to the bank's website. The order ID is included so the customer sees his order prepared after he is redirected to the bank.
4 The customer now sees the website of his bank, with the order prepared.
5 The bank sends a challenge to the customer. See Figure 1. The challenge is the number '36572 86140'.
6 The user signs the challenge with a certain key only he can create[4]. To accomplish this, the user uses a device called a 'token'. Besides, he needs the bank card and the PIN-code to ensure only the genuine customer can sign the challenge. It is assumed is that Mallory is unable to sign the challenge. The signed challenge is sent to the bank, so the bank can authenticate the user.
7 After the order has been paid, the bank informs the Merchant about this.
8 A redirection link is sent to the customer, so his browser can redirect him.
9 The customer is redirected to the website of the merchant and informed that the order has been paid.

[4] Signing the challenge requires the bank card of the customer as well as his PIN.

Figure 1: Screenshot iDeal challenge, example taken from a Rabobank transaction ([10])

5 Assets

This chapter describes the various assets which might be of value to a customer and which therefore are required to be safe. The assets are grouped in four different kinds.

Essentially, if a hacker tries to place an attack, it must be targeted at one or more of the following assets.

5.1 Confidentiality

- Transactions (transaction details, number of transactions)
- Credit card number (not the case when using iDeal)

5.2 Entity Authentication

- Authentication of the merchant by customer
- Authentication of the bank (only an issue of iDeal)

5.3 Data Authentication (a.k.a. integrity)

- Order details (including payment details)
- Transaction details

5.4 Non-repudiation

- Transaction by merchant [5]
- Payment by merchant (merchant tries to deny he received money)
- Order by customer (customer wants to deny he actually placed an order)

[5] There are several reasons why a merchant might want to deny he agreed on a certain transaction. For example, if the price of a certain commodity increases sharply after a customer placed an order, the merchant might want to deny he agreed to the transaction. This might be especially a concern with commodities with high price fluctuations like stocks or foreign currencies.

6 Operationalisation

The main subject of research is *security* of credit cards and iDeal under specific circumstances. 'Security' however is an extremely wide subject.

To make it possible to make statements about various aspects of computer security - confidentiality, data authentication, entity authentication and non-repudiation -, these aspects will be researched separately. Vulnerability and threats might apply to more than aspect.

Many aspects will not be entirely the same either system, iDeal and credit cards. For example, in the case of entity authentication, a user of iDeal must authenticate a merchant as well as a bank, while in the case of credit cards, only the merchant must be authenticated.

In this chapter, the variables 'likelihood', 'impact' and 'average security are defined.

6.1 Impact Factor

Some security violations are much more harmful to the user than others. For example, confidentiality of a single order paid with iDeal – hence no credit card number is at issue – is under most circumstances a nuisance. A bank account which is empty all of a sudden and a user who has to go through miles of bureaucracy to have his name removed from debt registration agencies has a much worse impact.

Impact is also different for each individual user. A user who secretly tries to obtain homosexual adult entertainment videos while his wife is oblivious of his sexual preferences will value confidentiality of past orders much higher than an ordinary shopper at amazon.com. This makes a precise scale for 'impact factor' an impossible task.

6.1.1 Values

Impact factor is measured in an ordinal scale.

{low, medium, high}

Low	Loss of confidential data like order history, but not including credit card numbers, CVV's, expiration date, login codes and passwords. Does not include losing any amount of money. Does not include paperwork to regain money or ordered commodities.
Medium	Includes loss of credit card number[6] and/or a limited amount of money in the order of magnitude of a single transaction. Lost

[6] Loss of credit card number is not counted as 'high impact' as Mallory has to use the number until the customer will notice impact. Not all lost credit card numbers are used for fraud.

	money refunded by a bank or credit card company does *not* count. Paperwork to regain lost money *does* count.
High	Money lost without refund beyond the order of magnitude of one transaction.

6.1.2 Defined impact factors

A successfully carried out attack may have an impact in more than one way. Of course, financial loss is a serious impact, but not all impact is financial. The trouble a victim may have to go through to reclaim stolen money may be considerable and sometimes the confidentiality of past transactions is worth more than a large sum of money. Besides, the simple idea that a system or company money was entrusted to has failed to protect the victim will be unbearable for many.

- *Financial*

The financial impact factor deals with the amount of money a customer loses *in the end*. This does not include losses which are repaid by banks or credit card companies, but only losses for the customer which he will not get refunded in the end.

- *Confidentiality*

The confidentiality impact factor deals with the loss of confidential data.

- *Practical*

The practical factor looks at the amount of hassle a customer needs to go through to get his money refunded, his name removed from credit registration agencies etc.

6.2 Likelihood

An attack with a very high impact but a next-to-zero chance to occur will not render a system unsafe.

Sometimes the likelihood can be determined with a very high amount of precision. For example, if the total number of transactions in the area of research is known and the number of altered transactions, it comes down to basic statistics. Usually it is not very simple to determine likelihood. Many data might be secret or otherwise impossible to obtain. In that case, only an educated guess can be made with different levels of precision.

6.2.1 Values

Because accurate data will more often than not be hard to find, only an ordinal scale can be used.

{theoretical, unlikely, medium, likely, very likely}

Theoretical	Not impossible, but with such great hurdles that becoming a victim has a chance of next to zero.

Unlikely	Technically possible, but hard to carry out on a significant amount of users.
Medium likely	Possible with a reasonable chance of success for Mallory.
Likely	Easy to carry out, hard to defend against.
Very likely	The customer should count on becoming the victim of the attack as soon as he uses the system a couple of times.

6.2.2 Defined likelihood factors

Likelihood factors are all factors which contribute to the likelihood that a certain attack takes place. These include technical factors and non-technical factors. Technical factors deal with the possibilities to bypass security systems and other technical countermeasures as well as the technical skills Mallory must possess to carry out an attack. Non-technical factors – comparison other methods, profit and catch chance – may increase or decrease the likelihood of a certain attack as well. Some attacks may be easy to carry out, for example the malicious merchant attack, but their likelihood may still be low as it is very hard for a malicious merchant to prevent arrest and subsequent conviction.

- *Technical*

The technical factor deals with the technical obstacles which must be overcome to successfully carry out an attack. This includes installing malware, rewiring hardware, installing alien devices, hacking routers et cetera.

- *Expertise*

The expertise factor deals with the required amount of expertise in the field of IT, computer networking – software and hardware level - and skills in programming.

- *Countermeasures*

The countermeasures factor deals with the possible countermeasures against a certain kind of attack, making some attacks unlikely to succeed.

- *Comparison with other methods*

The comparison factor looks at the likelihood that a certain attack will be preferred by Mallory. If a certain attack is unlikely to provide better results than an attack which is even easier to accomplish, the former attack is highly unlikely to be carried out.

- *Profit*

The Revenue factor deals with the expected profit of a successfully carried out attack. Attacks which provide very little profit are unlikely to be made.

- *Catch chance*

The catch chance factor deals with the expected chance for Mallory to be caught by the police.

6.3 Average Security

'Average security' is essentially the average result of all likelihoods multiplied with all the impacts of both systems compared to each other. The ordinal nature of the measured variables makes such a comparison impossible. Therefore, the average security can only be measured by common sense and the results will always be subject to debate unless the differences between both systems are very large.

6.4 Viewpoints

There is more than one way of looking at the research results. An IT specialist will mostly look at the technical likelihood factors and will have less interest in impact factors than a financial advisor. A customer will prefer a system with as little fuss as possible while still staying on the safe side. Therefore, the results will be presented from three different viewpoints.

6.4.1 Technical security viewpoint

The technical security viewpoint only takes the following factors into consideration:

- Technical
- Expertise
- Countermeasures

And no impact factors.

The technical security viewpoint is interesting to an IT security specialist, but much less to customers, merchants or Mallory. By making a security system *technically* secure, the likelihood of an attack must made as low as possible, and preferably impossible to carry out at all. Therefore, the likelihood factors comparison with other methods, profit and catch chance are not included as they have nothing to do with technical security. Impact factors are not taken into consideration since technical security is about lowering the chance of an attack, not limiting its impact.

6.4.2 Financial

The financial viewpoint takes into account the following likelihood factors:

- Technical
- Expertise
- Countermeasures
- Comparison with other methods
- Profit
- Catch chance

And the financial impact factor.

The impact factors ‘confidential impact’ and ‘practical impact’ are not taken into account. Confidential impact is ignored because even if the confidentiality of data is violated, this should not lead to financial loss. Practical impact is ignored because if the customer is able get his money refunded – regardless of the required hassle –, his financial security is not violated.

The financial viewpoint is a useful viewpoint for customers who care only for their money but are not interested in the confidentiality of their data and trouble they might go through to have their money refunded.

6.4.3 Overall

The overall viewpoint includes the following likelihood factors:

- Technical
- Expertise
- Countermeasures
- Comparison with other methods
- Profit
- Catch chance

And all three impact factors: financial impact, confidential impact and practical impact.

The overall viewpoint is the preferred viewpoint for customers, merchants and Mallory, as she wants to reach maximum impact with as little technical trouble as possible. A conceptual IT specialist – as opposed to a technical IT specialist as mentioned in 6.4.1 – might also prefer this viewpoint to the purely technical security viewpoint as a conceptual IT specialist might also take impact factors into consideration.

7 Attacks

There are several attacks possible to threaten the assets as described in chapter 5.

At first, an introduction is provided on the different types of attack Mallory can try. Each attack type has an own section in this chapter. These sections cover iDeal and credit cards each on their own. Detailed scenarios are provided for iDeal and credit cards to determine the likelihood Mallory can carry out an attack successfully. As countermeasures – obviously – decrease Mallory's chance of success, these are taken into consideration as well and are described in their own sections. Since attacks are not *supposed* to be easy to perform, Mallory needs to overcome hurdles which decrease the likelihood of an attack further. These hurdles have an own section for each attack type as well.

When the likelihood and impact of an attack are determined, a conclusion is drawn which summarizes the likelihood and impact of an attack with the effects of countermeasures included. These conclusions are the fundaments of the final conclusion in chapter 9.

7.1 Introduction

Several cryptographic attacks are known in literature. Many of them will be too impractical to carry out in the real world, like breaking the encryption algorithm of a data stream. Others, like the unauthorized use of a credit card number, happen every day.

Some attacks require a reasonable degree of technical knowledge and can only be carried out by experts. An example of this is the man-in-the-browser attack (see 7.6), as writing a browser hack is not an easy job except for trained software programmers. Other attacks, like the Malicious Merchant attack (see 7.5), only require somebody to create a web shop, but such people can be hired.

The most feared attack to date is the man-in-the-browser attack. The man-in-the-browser attack manages to bypass the 2-factor authentication[7] which is used by most banks. According to [20 paragraph 1.4], a number of security systems can be circumvented including tokens, TAN-codes and iTan-codes.

The attacks described in this chapter are grouped under different types. The next paragraph describes the possible types of attack.

7.2 Attack types

This section describes the different types of attack which Mallory can carry out.

[7] 2-factor authentication is an authentication concept which requires two different user-specific factors. For example, a bank card *and* a PIN-code or a fingerprint *and* a physical ID card.

7.2.1 Man-in-the-Middle Attacks

One speaks of a man-in-the-middle attack when Mallory gets between the website of the merchant and the customer. This means that Mallory can read and alter all the data sent from the merchant to the customer and vice versa. There are no data sent from the customer to the bank and vice versa.

If Mallory does not alter any data, neither the customer nor the merchant will notice anything. Mallory will still be able to obtain valuable data, so this would still constitute as an attack.

7.2.2 Key Logger Attacks

To carry out this attack, Mallory must install a key logger of some sort to the customer's computer. This might be performed by malware or, if Mallory has physical access to the customer's computer, a hardware device. Whichever way is used, let us assume that Mallory succeeds and for a certain period of time, she will be able to record and retrieve all keystrokes of the customer.

7.2.3 Malicious Merchant Attacks

Let us assume that Mallory disguises herself perfectly as a merchant, attracting customers who sincerely want to buy products at her web shop. Mallory, however, doesn't intend to grow rich by fair trade. Rather, she wants to rob her customers one way or the other.

There are several ways she might try to accomplish this.

- Trying to trick the customer into paying a much higher amount then he intends.
- Receiving the money but not sending the ordered commodities.
- Combination with man in the middle attack.
- Use obtained data for malicious purposes.

7.2.4 Man in the Browser Attacks

Mallory might try to hack the customer's browser. One way to do this is by sending a Trojan horse to his mail address and hoping the customer is foolish enough to execute it. A second way is to trick the user into installing a malicious browser extension. For a more complete listing, see 7.6.3. According to [20], Firefox, Internet Explorer and Opera have been successfully targeted. According to [20 paragraph 2.1], the time-to-market for this kind of attack is less than one day and everyone with web design expertise can craft a successful attack.

A hacked browser provides countless opportunities for Mallory to wreak havoc on the customer, but only iDeal and credit cards will be explored in detail.

7.2.5 Social Engineering Attacks

Not all attacks require Mallory to have a degree in information technology. Social Engineering requires manipulation of the victim itself, rather than software or hardware. Because no technical knowledge is required, everybody can resort to social engineering. However, at least average psychological skills are required to be successful.

7.3 Man-in-the-Middle Attacks

This section the possible ways Mallory can carry out a man-in-the-middle attack on either credit cards or iDeal. It has several subsections as there are several places where Mallory can get 'in the middle' or when certain countermeasures are used.

7.3.1 Man in the middle when SSL is not used

Though SSL will often be used to protect against man-in-the-middle attacks and eavesdropping attacks, not every merchant might use it. This chapter describes the man in the middle attack if SSL is not used.

7.3.1.1 Man in the Middle between Merchant and Customer (iDeal)

Mallory somehow gets between the merchant and the customer. For ways to accomplish that, see 7.3.4. When the merchant intends to redirect the customer to his bank's website, Mallory alters the redirection link to make it point at a website she has created herself and which looks exactly like the bank website the customer expects. The customer will then visit Mallory's website, still being convinced he is at the bank's website to authorize his payment. Mallory must quickly visit the real bank's website to create a money transfer from the customer's bank account to her own bank account, or write a script to accomplish this without human intervention. Postbank users have an advantage here. Because the total amount of the transaction is displayed in the SMS with the TAN-code, Mallory can rob the customer only for that amount of money. If she wants to get more money at once, the customer will notice the amount in the SMS is too high and this may trigger alarm.

The authorization of transfers takes place by signing a nonce using a device called a 'token' or by entering a TAN-code if the Postbank is used.

To authorize the transfer, Mallory sends the nonce to the website the customer is visiting – the fake bank website created by Mallory –, who will then sign the nonce with his token. The signed nonce is what Mallory needs in order to authorize the transfer from the customer to Mallory.

7.3.1.1.1 Scenario

For a detailed overview of the protocol if no attack takes place, see 4.2.2.

Let us assume that Mallory, in some way or the other, is able to get between the customer and the merchant. Mallory can read and alter data sent from the customer to the merchant and the other way round. If Mallory does not alter data, the customer cannot find out he is actually communicating with Mallory instead of the merchant. The protocol would then be as follows.

	Customer	Mallory	Merchant	Bank
1	iDeal, Bank →			

	The customer, on the website of the merchant, chooses to pay using iDeal and selects the Rabobank. The data, however, are intercepted by Mallory but passed through unaltered.		
2		iDeal, Bank →	
3			OrderDetails, OrderId →
	The merchant fetches the order at the website of the bank.		
4		← Red, OrderId	
	Mallory alters the redirection data. This means the user is not redirected to the website of his bank, but to a fake website Mallory has created before. This website looks like the website of his bank.		
5	←RedMallory		
6	(customer goes to Mallory's website)		
7	(Mallory goes to bank's website)		
8		←NonceLogin	
	Mallory is required to login on the website of the bank to create a money transfer to her account.		
9	←NonceLogin		
	Mallory passes the nonce from step 8 to the customer. He must sign it with his token for Mallory to succeed.		
10	$[NonceLogin]_{key}$ →		
	The customer signs the NonceLogin with his token and intends to send it to the bank. Mallory is the one who will receive it.		
11		$[NonceLogin]_{key}$ →	
	Mallory is now able to login on the website of the bank under the customer's name.		
12	(Mallory quickly prepares a money transfer to her bank account)		
13		← NonceAck	
	To authorize the transaction, Mallory needs a second nonce, the NonceAck (of acknowledge) to be signed by the customer's token.		
14	← NonceAck		
	Mallory passes the NonceAck to the customer.		
15	$[NonceAck]_{key}$ →		
	The customer, willing to authorize what he think is a genuine iDeal transaction, signs the NonceAck with his token.		
16		$[NonceAck]_{key}$ →	
	With the signed NonceAck, Mallory is able to authorize the transaction from the customer to her.		
17	(customer is redirected to error page)		
	Normally the customer would be redirected back to the merchant's website, but Mallory is unable to accomplish that. Therefore, she redirects the user to an error page or some similar page (see 7.3.1.1.2 - Wrong final page).		

7.3.1.1.2 Hurdles

This attack might seem dangerous, but it has a couple of hurdles.

- *Login required at bank website*

When iDeal is used, the user is *not* required to login at his bank's website. But for Mallory to do her work, she is required to login. When using iDeal, the customer is redirected to the website of the bank, where he sees his order prepared (see Figure 2). When iDeal Advanced is used, the order preparation page has the look-and-feel of the web shop (see 7.3.1.1.2 - iDeal Advanced).

Figure 2: Screenshot of prepared order ([10])

If the customer is targeted by this attack, he is redirected to a login screen which Mallory ensures looks like the ordinary login screen of the bank. An experienced iDeal user might see the difference and notice something is wrong. This, however, does not apply to new users to whom the login screen might seem very normal. It is also possible for an experienced user to think the iDeal system has changed and requires login. After all, login is not unusual for internet banking.

- *iDeal Advanced*

Some web shops which use iDeal Advanced carry out the payment in the look-and-feel of the web shop (see [19 chapter 3.2 first paragraph]). This means that a regular customer might notice a difference when Mallory is doing her work, because instead of an order preparation page in the web shop's look-and-feel, he encounters the standard iDeal form.

- *Wrong address in browser's address bar*

Because the customer is redirected to the website of Mallory and *not* to the website of his bank, the customer might notice the address in the browser window is not correct. However, if Mallory registers an address like www.rabobank-nederland.nl or something similar, the customer might be fooled easily.

- *Wrong final page*

Normally, when iDeal is used, the user is redirected to the website of the merchant, viewing a page which says the order has been paid if payment was actually successful. The redirection link is either specified in the account the merchant has with iDeal or it is provided manually when the merchant fetches the transaction (see [19 chapter 6 paragraph 1]. Because the mentioned UrlSuccess and the other URLs are either part of the account of the merchant or only sent from the merchant to the bank, Mallory is unable to retrieve those. After all, she's between the customer and the merchant and not between the merchant and the bank.

Mallory has to redirect the user to a different page which must fool the customer into thinking the actual order has been carried out. Mallory has several options.

- Error page
  Mallory can redirect the customer to an error page showing that something went wrong during the authorization. A pleasant side-effect of this – for Mallory – is that she might be able to let the customer carry out the order a second time which makes it possible for her to authorize multiple transactions from his bank account to hers. Because it is possible for a user to authorize multiple transactions at once, Mallory is able to rob a lot of money in a single attack.

  Even an experienced user might be fooled. After all it is possible that somewhere, something has gone wrong. An inexperienced user might not notice anything wrong at all.

- General 'order carried out' page
  A second option for Mallory is to create a general 'order carried out' page, preferably with an iDeal look. It needs to contain little more than 'Thank you for shopping using iDeal! We look forward to your next transaction.' This is against the standard iDeal procedure, but most certainly few users will notice. Besides, when the user views the final screen, he has already been robbed.

- Specific 'order carried out' page
  Of course, the best Mallory can do is to create a specific 'order carried out' page which is similar to the real final page. This is nearly impossible, however, because every merchant who uses iDeal has his own final page. With over 6500 [11] merchants supporting iDeal, Mallory needs a sweatshop of cheap website designers. Predicting which merchant a customer will use and creating only the specific final page for that merchant requires either clairvoyance or a detailed shopping profile of the customer.

- *Real order never paid*

Of course, the real order is never paid. When a user checks the status of an order and sees it has not been paid, this may trigger alarm.

- *Getting 'in the middle'*

For a man in the middle attack to succeed, Mallory is required to get in the middle. This is no easy task and is described in 7.3.4. A less obvious way to get in the middle, however, is the malicious merchant attack, which is described in 7.5.

- *Replacing the redirection link*

Mallory has to replace the redirection link so the customer is redirected to her own website, instead of the website of the bank. This must happen quickly so the customer won't notice a delay, although a small delay will remain unnoticed. This means that Mallory has to write a script to replace the redirection link. With over 6500 [11] merchants supporting iDeal, she has to either create a script for the top-selling merchants or very many merchants. The script will only be executed if the customer shops at a merchant which has been specifically scripted. The writing of such scripts is time-consuming which means Mallory has to do a lot of work to have a moderate chance of being successful.

7.3.1.1.3 Countermeasures

A common way to secure entity authentication – which this attack tries to compromise – is the use of a SSL. This makes it harder, though not impossible, to carry out a man-in-the-middle attack (see 7.3.2.1.4 and 7.3.2.2.4).

There are several general countermeasures against man-in-the-middle attack. Those are described in 7.3.5.

The general countermeasures in chapter 8 and especially 8.1.1 also apply to this attack.

7.3.1.1.4 Conclusion

The man-in-the-middle attack on iDeal is hard to carry out. First of all, Mallory must be able to 'get in the middle' in the first place (see 7.3.4). When Mallory has succeeded to get in the middle, the customer must do the following:

- He must not find it unusual to login at the website of the bank, even though that's not the normal procedure with iDeal.
- He must not see or just ignore the fact that the browser has the wrong address in the address bar.
- He must not find it strange he is not redirected back to the merchant, but to a different page.
- He must not check the order status shortly afterwards.
- If iDeal Advanced is used by the merchant, (see 7.3.1.1.2 - iDeal Advanced), the transaction is normally carried out in the look-and-feel of the web shop. Mallory has to use the standard page though. A regular shopper at the web shop might notice the difference.

Few customers might notice the subtle differences. If the attack succeeds after all, the customer might lose a lot of money which the bank may not refund. Therefore, the impact factor is 'high'. Because of the trouble Mallory has to go through to get 'in the middle', the relatively small amount of customers she can target if she succeeds and the trouble of writing the scripts to replace the redirection link, the likelihood of this attack is put on 'theoretical'.

7.3.1.1.5 Summary

Type	Man in the middle
Compromises	Entity Authentication of merchant and customer
Likelihood	Theoretical
Impact	High

7.3.1.2 Man in the Middle between Merchant and Customer on Credit Cards

A man-in-the-middle attack might be an obvious way to get hold of somebody's credit card number. The scenario without the use of a PKI is, however, extremely unlikely as virtually every web shop will require a PKI to at least encrypt the data which are sent to and from the merchant. It might even be required by the credit card company. For the scenario with the PKI, see 7.3.2.2.

Mallory might try, instead of or next to prying into the credit card number, to alter the delivery address so she will receive the ordered commodities instead of the customer.

7.3.1.2.1 Scenario

	Customer	Mallory	Merchant
1	Order details →		
2		Order details →	
3	OptCC→		
	The customer opts to pay using his credit card		
4		OptCC→	
5	Credit card number and order data →		
6		Credit card number and order data →	

Eve, who is in charge now, gets the credit card number – and other data – in step 5. The other data may include the credit card's expiration date and CVV number, which will aid her in her fraudulent attempts.

Altering the data is harder. Mallory either does it by hand or with some script. If she does it by hand, quick fingers are required and she has to be present 'in the middle' in person when a customer places an order. Because a man-in-the-middle attack is an attack on a specific group of users on a network, she might need to wait for days or weeks.

Scripting might be a solution, but she will have to create a script for every merchant to alter exactly the right data fields. If she is willing to spend so much time writing script by script, she can earn a lot more by getting a job as a typist.

7.3.1.2.2 Hurdles

It is hard to 'get in the middle'. Ways to do it are described in 7.3.4. But if Eve or Mallory succeeds, the attack is easy to carry out from that moment and does not have significant hurdles as long as Eve is satisfied with the credit card number. To alter data like the delivery address, she has two more hurdles to overcome:

- Creating a script for every merchant
- Manually alter the form data, which means she has to wait like a spider in its web until a customer actually places an order.

7.3.1.2.3 Countermeasures

The most obvious countermeasure against a man-in-the-middle attack is SSL. The man-in-the-middle attack on credit cards when SSL is used is described in 7.3.2.

There are several general countermeasures against man-in-the-middle attack. Those are described in 7.3.5.

7.3.1.2.4 Conclusion

The man-in-the-middle attack on credit cards is unlikely to succeed. First of all, Mallory has to 'get in the middle'. Because of the trouble of getting 'in the middle', the relatively small amount of customers she can target after succeeding in that and the trouble of writing scripts, the likelihood of this attack is 'theoretical'.

If Mallory succeeds after all, she has obtained valuable data like the customer's credit card number, possibly the CVV which is not required for all transactions and possibly the customer's name, address, telephone number and email address. This depends on the data which the customer must supply to the merchant. Because of the generous refunding policy of credit card companies, the impact is only 'medium'. Paperwork and caution – checking bank statements to notify fraud – are required by the customer, preventing the impact from being 'low'.

7.3.1.2.5 Summary

Type	Man in the middle
Compromises	Confidentiality of credit card number
Likelihood	Unlikely
Impact	Medium

7.3.2 Man in the Middle when SSL is used

A common way to prevent a man-in-the-middle attack is Secure Socket Layer (SSL). When SSL is used, the customer can be certain he is actually talking to the bank or the merchant, not Mallory.

The SSL protocol is taken from [30]. A simplified version can be found on [21].

7.3.2.1 iDeal

This section describes the man-in-the-middle attack if, somewhere in the process, SSL is used for additional security and the customer wants to pay his order using iDeal.

7.3.2.1.1 Scenario

SSL can be used between the customer and the bank and between the merchant and the customer. The scenario when SSL is used between the customer and the bank is as follows.

SSL between Customer and Bank

Let us have a look again at the protocol for an ordinary man-in-the-middle attack on iDeal in 7.3.1.1.1. In step 6, the customer is redirected to a fake bank website of Mallory. From that moment on, the customer is communicating with Mallory's website without realizing it is not the real bank's website[8]. Mallory herself is communicating with the real bank's website. That connection is most certainly secured using SSL, but that will not help the customer in any way. Mallory might use SSL for the communication between the fake bank website and the customer. This will give the customer a mistaken feeling of safety as the address in the browser's address bar starts with https and the tiny padlock will appear in the lower right corner of the browser - or at some other location if not Internet Explorer or Firefox is used.

Therefore, SSL between customer and bank is useless. The customer will never reach the bank.

SSL between Merchant and Customer

The situation, however, is different if SSL is used between the merchant and the customer. Mallory can try to intercept the transition from http to https. Instead of allowing the customer to connect securely to the merchant, she tricks him into connecting to her instead.

The following scenario is a simplified version of the protocol in [21] with only the relevant data.

	Customer	Mallory	Merchant
1	HandshakeData →		
	The customer tries to start an https request with the merchant. Mallory, however, tricks the customer and lets him connect to herself.		
2	← CertificateMallory		
	Mallory sends her own certificate to the customer.		

[8] This requires Mallory to register a credible URL, like http://www.payment-checkout.nl or something different which is not easily recognizable as an address of Mallory.

3	(https between customer and Mallory established)	
4		HandshakeDataMallory →
	Mallory sends her own handshake data to the Merchant with the intention to establish a secure connection to the merchant.	
5		← CertificateMerchant
	The merchant sends his certificate to Mallory.	
6	(https between Mallory and merchant established)	

After step 6, the customer is communicating with Mallory and Mallory with the merchant. The connection between the customer and the Mallory is encrypted using a session key from step 3 and further. The connection between Mallory and the merchant is encrypted with a *different* session key from step 6 and further.

Mallory will receive any response from the merchant and can send it to the customer and vice versa. Therefore, the customer won't notice anything out of the ordinary except for one thing: the address in the browser's address bar points to Mallory and *not* to the merchant.

As soon as the redirection link is sent to the customer in line 4 of the protocol in 7.3.1.1.1, Mallory can alter the redirection link. The customer will be redirected to Mallory's fake bank website and Mallory is in.

7.3.2.1.2 Hurdles

There are several hurdles Mallory must overcome to succeed

- *Getting in the middle*

Getting in the middle in the first place is not easy (see 7.3.1.1.2 - Getting 'in the middle').

- *Writing scripts to intercept transition from http to https*

Mallory has to write a script for each merchant she wants to target. The purpose of this script is to intercept the transition from http to https which can take place when, for example, the customer reaches 'checkout'[9]. Instead of making the customer connect to the merchant, he has to connect to Mallory. Mallory, on her side, has to connect to the merchant. A second purpose of this script is to intercept and alter the redirection link so Mallory redirects the customer to her fake bank website instead of the real website of the bank.

- *Invalid certificate*

In step 2 of the scenario, the customer receives the certificate of Mallory and *not* the certificate of the merchant. Very few users will verify the certificate though. The browser of the customer doesn't know any better than that a secure connection with Mallory is requested.

[9] If Mallory does not intercept the transition, the data will be encrypted using the public key of the merchant which means Mallory cannot read or alter any data.

7.3.2.1.3 Countermeasures

The following countermeasures are possible against a man-in-the-middle attack on iDeal when SSL is used.

- *Checking the address in the browser's address bar*

The customer can find out he's under attack by examining the address in the browser's address bar. It will not point to the merchant's website, but to Mallory. If Mallory is smart enough to register an address like 'https://www.checkoutservice.com' or something, it is easy to fool the customer though.

- *Examining the certificate*

If the customer wants to be certain he's talking to his intended merchant instead of Mallory, he can examine his certificate manually. Then he has to verify if the URL in the certificate matches the merchant. Mallory, however, can register an URL with a similar name or something else believable, like http://www.checkoutservice.com as mentioned in the previous paragraph. To make this countermeasure work, the customer has to reject any connection to anything but the URL of the merchant.

- *Client certification*

SSL allows for client certification – as opposed to only server authentication – as well. It should be noted, though, that client certification is rarely used, especially not for online shopping and this section has been included mostly for completeness. Client certification means the client has to prove that he is who he claims. To accomplish that, the customer has to obtain a certificate with some of his credentials like his name, date of birth and possibly his IP address. Mallory has different IP! Let's have a look at the scenario below:

	Customer	Mallory	Merchant
1		← Nonce	
2	← Nonce		
3	clientCertificate, $[Nonce]_{PrivCustomer}$ →		
	The customer sends his certificate and a nonce signed with his private key to Mallory.		
4		clientCertificate, $[Nonce]_{PrivCustomer}$ →	
	Mallory simply passes the data to the Merchant. The merchant will now be convinced he is talking to the customer.		

The merchant intends to send a nonce to the customer in step 1. Mallory allows this nonce to reach the customer in step 2. The customer now responds by sending his certificate and the nonce encrypted with his private key in step 3. Again, Mallory doesn't intervene and allows the data to slip through and reach the merchant.

The merchant will now be convinced he's talking to the customer. He has provided his certificate and proved the ownership of the private key by encrypting the nonce with it. The authenticity of the certificate of the customer can be validated by a Certification Authority, but that's beyond the scope of this thesis.

7.3.2.1.4 Conclusion

A man-in-the-middle attack on iDeal is even harder to perform when SSL is used. Next to the already present problem of getting in the middle in the first place, new problems arise for Mallory. She has to create scripts for quite an amount of merchants to be successful which is a long and tedious job.

Against this kind of attack, https is powerless. The only advantage it will bring, as long as Mallory does her work well, is that the browser bar will not display the URL of the merchant, but the URL of Mallory. It requires a smart user to notice the difference. The iDeal checkout address is also different, which means Mallory must register a not-too-conspicuous address which does not arouse suspicion of the customer.

Mallory doesn't even need to use https between herself and the customer. In that case, the address in the browser's address bar will not start with https but with http. This should signal the customer he is under attack, but very few will notice.

It will take a lot of effort for Mallory to get 'in the middle'. If she succeeds, she can target only a small amount of potential customers. She has to create scripts for the merchants his intended victims want to shop on. Then she's dependent on the users of the network to actually place orders she can intercept. All in all, there are so many problems for Mallory that the likelihood of this attack is put on 'theoretical'. If she succeeds, she will be able to rob one or more customers and it's questionable the bank will refund the loss. After all, the transaction was signed with the token of the customer. Therefore, the impact factor is 'high'.

7.3.2.1.5 Summary

Type	Man in the middle
Compromises	Entity Authentication of merchant to customer and entity authentication of bank to customer.
Likelihood	Theoretical
Impact	High

7.3.2.2 Credit cards

This paragraph describes the man-in-the-middle attack on credit cards when SSL is used.

7.3.2.2.1 Scenario

As soon as https is used between the merchant and the customer, Mallory is out of the game. She won't be able to alter or even read data, as they are encrypted.

The scenario is similar to the scenario provided in 7.3.2.1.1 section 'SSL between merchant and customer'. Mallory has to intercept the redirection from http to https. She can do that by writing a script for the merchant the customer is dealing with. As soon as the customer is intended to be redirected to https, she must ensure the customer is redirected to her own website. She, on her side, has to connect to the merchant's website, impersonating the customer. The merchant cannot find out he's not dealing anymore with the customer but with Mallory.

Mallory will be able to read everything the customer provides. This includes the credit card number. She doesn't need to do that manually, she can write a script for that.

7.3.2.2.2 Hurdles

- *Getting in the middle*

Getting in the middle in the first place is not easy (see 7.3.1.1.2 - Getting 'in the middle').

- *Writing scripts*

To successfully intercept the transition from http to https, she has to write a script. As the websites of merchants can differ significantly, she has to write a separate script for each merchant. This script must take care of the redirection of the customer to her own website as well as obtaining the credit card number as soon as the customer provides it.

- *Wrong address in address bar*

The address in the browser's address bar of the customer will not display the merchant's website, but Mallory's website. Few customers will notice the difference, as long as Mallory registers a website which has a seemingly normal name like 'http://www.checkoutservice.com'.

7.3.2.2.3 Counter measures

The counter measures are the same as the counter measures provided in 7.3.2.1.3.

7.3.2.2.4 Conclusion

The man-in-the-middle attack on credit cards when SSL is used is very hard to perform. First of all, the problem of 'getting in the middle' is present. That is hard enough in itself. If Mallory succeeds, she has to write scripts for the specific merchants she wants to target. Then she is dependent of the intended victims, the users of the network she gained access to. They have to place orders at the merchants she has targeted. If she's lucky, she can obtain a handful of credit card numbers and other data like the CVVs of the credit cards. She can use the credit card numbers for fraudulent transactions.

Still, SSL adds security as they require Mallory to write scripts for each merchant. If SSL would not be used, she could simply try to eavesdrop all traffic and scan automatically for sequences of 16 numbers which have a high probability of being credit card numbers.

There is so much trouble altogether for Mallory that the likelihood of this attack is put on 'theoretical'. If she manages to obtain a credit card number and manages to use it to rob the customer, the generous refunding policy of the credit card companies will compensate the customer. This requires time and effort on the customer's side. Therefore, the impact factor is put on 'medium'.

7.3.2.2.5 Summary

Type	Man in the middle
Compromises	Confidentiality of credit card number
Likelihood	Theoretical
Impact	Medium

7.3.2.3 Conclusion

A man-in-the-middle attack is hard enough to carry out in itself (see 7.3.4). SSL makes it a little harder. This because Mallory has to intercept the transition from http to https and – if she wants to use https between herself and the customer – she has to obtain a certificate. Those are not hard to get though and may provide the user with a false feeling of security. The browser's address bar will display an URL starting with 'https' and the tiny padlock will appear on the lower right corner of the browser or at a different location if not Internet Explorer is used.

Those are not the hardest problems for Mallory. The hardest problem for her to overcome is creating a script for every merchant she wants to target to ensure redirection to her own website. Technically, this is not a hard problem. It is just a tremendous amount of work.

7.3.3 Man in the Middle on the ISP of the Customer

Another way of Mallory to carry out a man in the middle attack is by somehow being present at the Internet Service Provider (ISP) of the customer. All traffic the customer sends to any other party on the internet will pass the ISP. Let us assume that Mallory is present at the ISP of the customer. She might just be an employee who decides to use the level of access she has to the equipment of the ISP for her own malicious intentions.

She will be able to install certain software which can read and alter traffic between the customer and the merchant. For example, she might be willing to read credit card numbers which the customer sends to the merchant. Another option is to alter the routing tables of the routers at the ISP so traffic intended for a merchant is send to herself instead.

7.3.3.1 Man-in-the-middle on ISP of customer on iDeal

This paragraph describes the possibilities of Mallory carrying out a man in the middle attack on a customer who uses iDeal. Mallory is at the ISP of the customer, not on the ISP of the merchant who is most likely at a different ISP.

7.3.3.1.1 Scenario

Mallory, being present at the ISP, installs a script that can read and alter all data the customer sends to the merchant and the customer sends to the bank. Another option is altering the routing table of the router at the ISP, so all traffic intended for a certain merchant will be redirected to any device Mallory chooses. Then, she will not be required to install scripts on the ISP router, she can install them on her own computer.

If Mallory carries out an attack, the protocol would be exactly as described in 7.3.1.1.1. It is reprinted here for convenience.

Take a look at step 4. The merchant sends the redirection link to the customer. Mallory, using her script, can identify that piece of information and is able to substitute the redirection link with a link to her own fake website. After that, the customer will mistakenly sign the NonceLogin and NonceAck with his token. Mallory is in and the customer has lost quite an amount of money.

	Customer	Mallory	Merchant	Bank
1	iDeal, Bank →			
	The customer, on the website of the merchant, chooses to pay using iDeal and selects the Rabobank. The data, however, are intercepted by Mallory but passed through unaltered.			
2		iDeal, Bank →		
3			OrderDetails, OrderId →	
	The merchant fetches the order at the website of the bank.			
4		← Red, OrderId		
	Mallory alters the redirection data. This means the user is not redirected to the website of his bank, but to a fake website Mallory has created before. This website looks like the website of his bank.			
5	←RedMallory			
6	(customer goes to Mallory's website)			
7	(Mallory goes to bank's website)			
8		←NonceLogin		
	Mallory is required to login on the website of the bank to create a money transfer to her account.			
9	←NonceLogin			
	Mallory passes the nonce from step 8 to the customer. He must sign it with his token for Mallory to succeed.			
10	$[NonceLogin]_{key}$ →			
	The customer signs the NonceLogin with his token and intends to			

	send it to the bank. Mallory is the one who will receive it.			
11		[NonceLogin]$_{key}$ →		
	Mallory is now able to login on the website of the bank under the customer's name.			
12	(Mallory quickly prepares a money transfer to her bank account)			
13		← NonceAck		
	To authorize the transaction, Mallory needs a second nonce, the NonceAck (of acknowledge) to be signed by the customer's token.			
14	← NonceAck			
	Mallory passes the NonceAck to the customer.			
15	[NonceAck]$_{key}$ →			
	The customer, willing to authorize what he think is a genuine iDeal transaction, signs the NonceAck with his token.			
16		[NonceAck]$_{key}$ →		
	With the signed NonceAck, Mallory is able to authorize the transaction from the customer to her.			
17	(customer is redirected to error page)			
	Normally the customer would be redirected back to the merchant's website, but Mallory is unable to accomplish that. Therefore, she redirects the user to an error page or some similar page (see 7.3.1.1.2 - Wrong final page).			

7.3.3.1.2 Hurdles

This attack is not an easy one to carry out. Mallory must overcome severe hurdles.

- *Gaining access to an ISP*

The biggest hurdle, of course, is actually being able to install software on a server on an ISP or alter the routing table. This will require either a great talent in social engineering or – probably much easier – get a job at the ISP. Even as an employee, she must get access to the servers which route the incoming traffic to install scripts or alter the routing table. This requires a high level of access to the servers. It also requires that the routers either have the possibility to have scripts installed, or Mallory must install a router between the router of the ISP itself and the client. She can use a computer and program it to let all packets through except for those she needs to alter, which are altered and then put through. If these evil practices interfere with the daily routine of the ISP, like slowing down the traffic, alarm may be triggered.

- *Writing scripts*

Furthermore, the scripts she has to write can only target one merchant each. She has to write a great many scripts to be successful and she can only target merchants which have customers connected through the particular ISP she targets.

7.3.3.1.3 Conclusion

The likelihood of a man-in-the-middle attack on iDeal at the ISP of the customer is only theoretical. Mallory has to gain access to an ISP and be able to install software on their routers. She must write scripts for each merchant she wants to attack, of course without any security system of the ISP or a co-employee triggering alarm.

Writing the huge amount of scripts to alter the web pages of the merchant on the fly is a tedious job as well. To make it worse, only customers who are connected to the targeted ISP can possibly be victims. The likelihood for a customer to be targeted therefore is very low which will discourage Mallory from trying which decreases the likelihood even further.

The customer may lose a significant amount of money though which the bank may not refund. The impact therefore is 'high'.

7.3.3.1.4 Countermeasures

One way to prevent this kind of attack is by screening new employees on a criminal past. Applicants with previous convictions, especially of similar offenses, should be rejected. Restricting access to the servers only to administrators – which should be the most trusted employees of the ISP – is to be recommended, not only to prevent a man-in-the-middle attack but also similar eavesdropping attacks.

7.3.3.1.5 Summary

Type	Man in the middle
Compromises	Entity authentication of bank
Likelihood	Theoretical
Impact	High

7.3.3.2 Man-in-the-middle on ISP of customer Credit cards

This paragraph describes the possibilities of Mallory carrying out a man in the middle attack on a customer who uses credit cards. Mallory is at the ISP of the customer, not on the ISP of the merchant who is most likely at a different ISP.

7.3.3.2.1 Scenario

The scenario is identical to the scenario in 7.3.1.2.1 and is reprinted for convenience.

	Customer	Mallory	Merchant
1	Order details →		
2		Order details →	
3	OptCC→		
	The customer opts to pay using his credit card		
4		OptCC→	
5	Credit card number and order data →		
6		Credit card number and order data →	

In step 5, Mallory gets hold of the credit card number and other data which is entered in the form like address and telephone number. All Mallory has to do is to create a script which recognizes the form page when it arrives at the ISP, snoop the credit card number and without any further intervention, a nice list of credit card numbers is created.

Furthermore, Mallory might be able to alter the delivery address of the customer to an address she has access to or alter other data.

Of course it isn't as easy as that. Before Mallory can accomplish this, she has to overcome several problems which are described in the next chapter.

7.3.3.2.2 Hurdles

The same hurdles as described in 7.3.3.1.2 are present. Being able to install software on an ISP is the hardest part, if the router allows scripts in the first place.

Surprisingly, SSL doesn't make much of a difference. As can be seen in 7.3.2.2, it is possible for Mallory – if she writes a specific script for the merchant – to bypass SSL.

7.3.3.2.3 Conclusion

Though theoretically possible, the man-in-the-middle attack on the customer's ISP when a credit card is used should not be feared. For a customer to get into trouble, he first must be connected through an ISP which is penetrated by Mallory. Mallory has to write a script for that specific merchant and all merchants she doesn't specifically target are safe to use. In the unlikely case that Mallory succeeds in this, the customer may lose his credit card number or, less likely, his ordered goods may be sent to Mallory's address. Not that much of impact, the credit card company will repay fraud.

7.3.3.2.4 Counter measures

The counter measures are the same as the counter measures when iDeal is used. They can be found in chapter 7.3.3.1.4.

7.3.3.2.5 Summary

Type	Man in the middle
Compromises	Confidentiality of credit card number
Likelihood	Theoretical
Impact	Medium

7.3.3.3 Conclusion

This attack is so hard to carry out that customers using either iDeal or credit cards don't need to fear it. If, against all the odds, Mallory succeeds, a customer is better off with a credit card than with iDeal because of the refunding policy of credit cards.

7.3.4 How to 'get in the middle'

This attack requires Mallory to get between the customer and the merchant, being able to read data from the customer and send them to the merchant and the other way round. This is not an easy task. There are several ways to try to accomplish this.

7.3.4.1 Mallory deploys a hub

A hub is a device similar to a switch in an Ethernet network. It makes it possible to expand the number of connection ports of a router. There is, however, one important difference between a hub and a switch. A switch is smart, a hub is dumb. A switch will target traffic from the source computer only to the intended target, as determined by the IP addresses. A hub, however, simply sends all incoming traffic to every IP address connected to the hub. This, of course, is the eavesdropper's paradise.[10]

Hubs are rarely used nowadays, commonly replaced by switches. It is, however, still easy to obtain a hub. By replacing a switch in an Ethernet network with a hub, there are several opportunities for Mallory. In [6] can be found:

[10] Technically speaking, an eavesdropping attack is not the same as a man-in-the-middle attack. They are dealt with together for the sake of clarity.

"Eavesdropping attacks are enabled by the use of shared media in networks such as Ethernet (with hubs) and Wi-Fi. In an eavesdropping attack, the attacker configures the respective network interface in random mode. In this mode, the attacker's computer receives any packets sent on the network, including packets destined to other nodes. If packets are unencrypted, the attacker can read packets' data, possibly including passwords and other credentials. Many easily available applications can be used for eavesdropping, including tcpdump [3] and ethereal [4]."

Of course, carrying out a man-in-the-middle attack using a hub requires Mallory to be on the same network. This is hard to carry out in a home environment, but far from impossible in an office environment.

7.3.4.2 Mallory abuses a switch

If a switch is used instead of a hub, saving Mallory the trouble of replacing the switch with a hub, a man-in-the-middle attack can still be carried out. [2] Says:

"In networks that do not use shared media (e.g., switched Ethernet) or where packets are encrypted, an attacker may be able to use a MITM attack to intercept communication between a client and a server. By impersonating the server, the attacker may be able to fool the client into connecting with the attacker rather than the server. The attacker can then capture the client's credentials (e.g., id and password), and use those credentials to connect to the server as the client."

In [2], various ways are explained to carry out the man-in-the-middle attack.

As with a hub, it requires Mallory to be on the same network, which might be a treat in office environments.

7.3.4.3 Mallory uses Wi-Fi

In [2] it is also mentioned that a man-in-the-middle attack can be carried out if the customer uses wireless Internet (Wi-Fi), by using a rogue access point with a stronger signal. The user will then not connect to his regular access point, but to the rogue access point, giving Mallory the opportunity to read and/or alter the data.

Using a rogue access point is not an easy task. It requires Mallory to either place the rogue access point much closer than the original access point or amplifying the signal. Besides, many users use some kind of security like WPA, which encrypts the traffic between the connected computer and the access point. Even if a weaker safety system is in use like WEP, Mallory is required to hack it which makes her task even much harder.

7.3.4.4 Mallory penetrates an ISP

The man-in-the-middle attack when Mallory penetrates an ISP is described in chapter 7.3.3.

7.3.5 Countermeasures against man in the middle

There are several countermeasures against man-in-the-middle attacks.

7.3.5.1 Checking the switches

Mallory can carry out a man-in-the-middle attack by replacing a switch on a network with a hub (see 7.3.4.1). Regularly checking the network to ensure all the switches are still switches and not replaced by hubs will make this specific kind of man-in-the-middle attack highly unlikely.

7.3.5.2 Scanning for rogue access points

A man-in-the-middle attack when Wi-Fi is used is possible, as described in 7.3.4.3. This requires Mallory to install a rogue access point. Installation of rogue access points can be prevented by a Wireless Intrusion Prevention System (WIPS). A WIPS can automatically detect rogue access points and trigger alarm.

7.3.5.3 Checking the address in the internet browser's address bar

When Mallory carries out a man-in-the-middle attack, the customer communicates with Mallory, rather than his intended web site. Contrary to a man-in-the-browser attack (see 7.6), Mallory cannot alter the address in the browser's address bar. The browser actually displays the address the customer is visiting and by altering the address, Mallory will force the customer to visit a different web site. This means that, if the customer checks the address the browser displays while being the victim of a man-in-the-middle attack, he might see that he's at Mallory's website, not the bank's website or the merchant's web shop.

It requires an aware and smart customer, though, to distinguish the good from the bad addresses. An address may start with an IP number instead of a domain name. This should trigger alarm, but how many customers will notice if everything else seems normal?

7.3.5.4 Against ISP penetration

The countermeasures against penetration of an ISP by Mallory are described in 7.3.3.1.4.

7.3.6 Conclusion

Man-in-the-middle attacks are hard to carry out. It requires a great deal of expertise to actually 'get in the middle'. If that succeeds, Mallory is dependent on the people on the same network to actually place orders on web shops. When iDeal is used by the customer, there are also some subtle differences which may alarm the customer. This is not the case with credit cards.

The question remains if it's rewarding enough for Mallory to go through all the trouble of installing a rogue access point, replace a switch with a hub and writing the scripts required to automate either retrieving data from forms (credit cards) or initiate a transaction from the customer to herself and authorize it with the signed nonces (iDeal).

7.4 Key logger Attacks

This chapter provides detailed attack scenarios for key logger attacks and a conclusion, separately for iDeal and credit cards. Because the hurdles and countermeasures against key loggers are the same for iDeal and credit cards, they are not described separately.

7.4.1 Key logger attack on iDeal

Because of the technical differences between iDeal payments and online credit card payments, the key logger attack on iDeal differs significantly from the key logger attack on credit cards.

Let us first assume that Mallory has succeeded in installing the key logger and succeeds in reading the keystrokes afterwards. This is a challenge in itself and is described in 7.4.3.

7.4.1.1 Scenario

Let us have a look at the protocol in 4.2.2. The only step where the customer has to type something on his keyboard is step 6. That is the step where he types the signed nonce on his keyboard. This means that Mallory may intercept the signed nonce.

But that doesn't bring Mallory any further. If it is assumed that the nonce is really used only once, as its name implies, Mallory cannot use the signed nonce to authorize a transaction to her bank account. Besides, if only a key logger is used, she will have no clue what the nonce is which is signed by the number the customer enters.

The nonce signing system of the Postbank is quite different from that of the other banks, but this makes no difference in case of the key logger attack. The number which is sent by SMS to the customer can still be used only once, so it does not matter if Mallory can retrieve it somehow. Even if the much less secure system of TAN-lists (see 4.2.2) is used, Mallory will achieve nothing. A key logger will not be able to retrieve the index number of the desired TAN-code so Mallory will end up with a list of TAN-codes but no clue when to use which TAN-code.

7.4.1.2 Conclusion

iDeal is perfectly safe against key logger attacks.

7.4.1.3 Summary

Type	Key logger
Compromises	<nothing>
Likelihood	impossible
Impact	<none>

7.4.2 Key logger Attack on Credit Card

This attack might be used against iDeal and credit card transactions but they differ in the way they are used and the technical background, as well as the assets which might be compromised.

7.4.2.1 Scenario

Let us examine the protocol from 4.1.1 in more detail.

	Customer	Merchant	Credit card company
1	order details →		
2	credit card →		
	The customer opts for paying with a credit card.		
3	payment details →		
	The customer must enter his payment details. This step is described in greater detail below.		
4		AckReq →	
5		← Ack	

Manual entry of the credit card number and data like address details are not required upon every order. There are three ways for the merchant to acquire the relevant data.

Manual entry
If none of the two methods below are used, the user is required to type his credit card number for each and every transaction. When he does, the credit card number – and all other keystrokes – are recorded by the key logger. When Mallory reads the data from the key logger, she takes possession of the credit card number of the customer.

Cookie
Cookies should only be used to store an account number [13], where any valuable data are stored on the merchant's server. The merchant will be able to recognize the customer when he enters the site.

Because the account number is never typed in directly, it is safe from key logger attacks. Therefore, cookies provide additional safety from key loggers. The amount of gained safety is quite small as a cookie has to exist for each separate website which requires manual entry of the credit card number upon each first order on a merchant's website.

User login required

First the user has to register at the website to get a username and password. During the registration process, he has to provide his credit card number and other details. Upon checkout of any following order, he is required to login and provide his username and password to authenticate. After the authentication process, the merchant can retrieve the credit card number. This means the customer is not required to type his credit card number, bypassing possible keyboard loggers.

This might provide additional security against key loggers, but *only* if the customer is not able to view his credit card number in his personal details. Otherwise, Mallory can simply retrieve the username and password from the key logger, login herself and read the credit card number. It is possible, however, that the merchant only shows the last four digits of the credit card number. In that case, a user login provides a little additional security against key loggers.

This method has a major drawback though when it concerns key loggers. The key logger will be able to record the username and password when it is typed in. Mallory can then log in on the customer's account and will be able to carry out orders in the customer's name, unless an additional security measure is in place.

The same goes for cookies. The user must create a user account at every website he wants to shop at. This means typing in the credit card number, which the key logger can record. Therefore, the additional safety of a required login is relatively small.

7.4.2.2 Conclusion

It is hard to carry out a key logger attack on credit cards on a specific user. For a software key logger, the problems are:

- The customer must install programs he receives by spam, or programs from an unknown source. Both are heavily discouraged! OR
- Mallory must be able to install software on the customer's computer.

For a hardware key logger, the problems are as follows:

- Mallory must have physical access to the keyboard to install the key logger.
- Mallory must have physical access to the key logger to read the recorded keystrokes.

7.4.2.3 Summary

Type	Key logger
Compromises	Confidentiality of credit card number
Likelihood	medium
Impact	medium

According to [22], 6% of consumers PCs were infected with system monitors in the second quarter of 2006, the most common of them being Perfect Keylogger. Because key loggers are hard to detect, the true infection rate may not be reliably estimated which makes it hard to determine the likelihood of this attack. [23] Says: "Spyware is just as prevalent; anti-spyware vendor Webroot Software Inc. previously detected an average of 28 pieces of the software on each PC, and recently noted that one in three of the 1.5 million PCs it surveyed contained some sort of key logger." The big difference between these numbers – 6% of consumer PCs has system monitors of which a common kind is Perfect Keylogger according to one source, and one in three is infected with a key logger according to a different source – makes it hard to determine the likelihood of this attack. Other statistics on key loggers have not been found despite searching over a hundred of pages in Google and Google scholar.

As an educated guess – even the lower estimate is still a substantial part of 6% of consumers PCs – the likelihood is put on 'medium'.

The generous refunding policy of the credit card issuers limits the impact. This requires paperwork on the side of the customer, blocking his credit card and awaiting a new one and keeping track of bank statements and money transfers. Therefore, the impact factor is still 'medium'.

7.4.3 Hurdles

There are a number of difficulties in carrying out a key logger attack. These are described in this paragraph.

7.4.3.1 Installing a software key logger

There are several ways to install a software key logger on the computer system of a customer. One way is by the use of a Trojan horse. Surprisingly, key loggers are hard to detect. As indicated in [2], many key loggers can hide themselves in such a way that they are very hard to detect.

The user is required to execute a Trojan horse to install the key logger first.

Another way of installing a key logger is simply installing one on somebody else's computer. This is particularly dangerous in office environments where computers might be shared among different workers or where it is not uncommon to 'borrow' somebody else's computer. This requires a high level of user privileges for the logged in user (see [2]).

7.4.3.2 Reading data from a software key logger

Recording the keystrokes is useless unless Mallory can read the recorded keystrokes once in a while. A smart key logger will email or use ftp to send the recorded keystrokes to Mallory (see [2]). This means that Mallory is not required to log in at the infected computer, which would have been a very hard job.

7.4.3.3 Installing a hardware key logger

The installation of a hardware key logger requires physical access to the customer's keyboard. It goes without saying that this is a difficult task. It requires breaking into the customer's home or office and installing a hardware device. Even if that succeeds, the customer might easily see that there is a strange device between his computer and his keyboard. To circumvent this, Mallory might install the key logger directly into the keyboard where it will hardly be noticed. This requires a higher level of technical abilities.

Even if a hardware key logger is present, reading the recorded keystrokes is not easy. It might require access to the key logger again. If Mallory is trusted by the customer, she might be able to accomplish installation of a hardware key logger with ease.

7.4.4 Countermeasures

As indicated in [2], there are several countermeasures against key loggers.

- Most Windows users should have restricted privileges by making them part of the User group.
- The Administrator group should have very few entities, and they should have a strong password policy.
- No one should ever connect to Internet or even the internal network while logged in to the computer as an administrator. This gives network eavesdroppers *carte blanche* access to the machine and the opportunity to remotely install software.

The countermeasures against hardware key loggers are quite straightforward. They are the same as the countermeasures against burglary when computers at home are concerned. However, it may be different in offices where unknown people may be regular guests. Even then, Mallory or one of her henchmen must enter in person to install an alien device on a keyboard. Regular checking of the keyboard for a hardware key logger is recommended in office environments.

To be on the safe side, online shopping and especially typing in the credit card number are definitely advised against on any computer which is not exclusively your own. For paranoid customers, using a laptop might be a good idea as installation of a hardware key logger on a laptop is much harder than on an ordinary keyboard.

7.4.5 Conclusion

iDeal is perfectly safe against keylogger attacks, but credit cards are not. The risk to become a victim of a key logger attack is 'medium'. The 2-factor authentication with numbers used only once are a definite security advantage of iDeal over credit cards when it comes to key logger attacks.

7.5 Malicious Merchant Attacks

This section provides detailed attack scenarios for malicious merchant attacks. Since the malicious merchant attack can be used in for different purposes – authorizing a to high amount, data gathering or malicious merchant in the middle – this section is subdivided accordingly.

7.5.1 Authorizing a too high amount

Mallory might try to increase the sum of the transaction, which the user authorizes.

7.5.1.1 Malicious merchant on iDeal – Authorizing a too high amount

Take a look at step 4 of the protocol in 4.2.2. Mallory redirects the customer to the website of the bank. In the background and invisible to the customer, the order is prepared at the bank's website in step 2.

7.5.1.1.1 Scenario

Mallory can try to increase the payment, but this will easily be noticed by the customer. Take a look at the screenshot below:

Figure 3: Screenshot of iDeal ([10])

The amount the user has to pay – €22,95 – is clearly visible. Only a very clumsy customer will authorize far too high an amount. Mallory would also lose her cover very quickly and it is unlikely her web shop will exist for more than a couple of days.

Mallory might try to make iDeal display an amount which is different from the one that is actually authorized, but she will not be able to succeed in realizing this. When the order is prepared at the bank, there is only one amount. Figure 3 shows a screenshot of a prepared order. Unless a man-in-the-middle attack takes place (see 7.3.1.1), this is a genuine page created by the bank showing the total amount of the prepared order.

As can be seen in the screenshot below, the amount is shown not only in the SMS but also on screen. The user must be twice as foolish if he uses the Postbank to be fooled.

Figure 4: Screenshot of iDeal using Postbank ([10])

7.5.1.1.2 Hurdles

The only hurdle Mallory has to overcome is the sanity of the customer. Virtually every customer will notice if he's authorizing a too high amount. Mallory can try, but she will lose her cover quickly.

7.5.1.1.3 Countermeasures

Despite the attack being only theoretically possible, there are still possible countermeasures which decrease the likelihood of this attack even further.

- *Only shop at trustworthy merchants*

One way to avoid any malicious merchant attack is by only shopping at reliable companies. It is quite much out of the question a reputable company like Amazon or BOL will try to trick the customer this way. A new, not well-known company should not be trusted that easily and the customer must check the amount he ultimately authorizes. This, however, naturally applies to reputable companies as well.

- *Distrust offers which are too good to be true*

To try this trick, Mallory has to lure genuine customers to a web shop. One way to do that is of course by offering commodities below the market price. A general rule to this is: 'if something is too good to be true, it most certainly isn't.'

7.5.1.1.4 Conclusion

Only the most foolish of customers will authorize a too high amount when iDeal is used by a malicious merchant. Next to that, Mallory will lose her cover quickly as soon as robbed customers go to the police and spread the name of the shop on the internet on sites like www.opgelichtopinternet.nl. Still, Mallory might give it a try. Therefore, the likelihood is 'theoretical' as opposed to 'impossible'.

The impact is 'high'. The customer authorizes a transaction with his token, so the bank might claim he was willing to pay that amount to Mallory which may make them decide not to refund it.

7.5.1.1.5 Summary

Type	Malicious Merchant
Compromises	Money
Likelihood	Theoretical

Impact	High

7.5.1.2 Malicious merchant on Credit cards – authorizing a too high amount

It is possible a customer intends to sincerely order commodities at a web shop and wants to authorize a genuine payment of the amount of the transaction. What stops Mallory, disguised as a legitimate merchant, from claiming a much higher amount?

7.5.1.2.1 Scenario

The customer is shopping around for certain commodities and, one way or the other, arrives at Mallory's web shop. He orders the commodities for let's say €40.00 and proceeds to 'checkout'. Then, he provides data like his address and – most importantly – his credit card number and possibly the expiration date and CVV.

Mallory, instead of withdrawing €40.00, withdraws €400.00. Later, she may claim it is a mistake or she can try to get a significant amount of profit and go into hiding.

7.5.1.2.2 Hurdles

Mallory can try this trick a couple of times and maybe she'll be lucky. It will not be that easy for her to overcome the hurdles though.

- *Sane customers and bank statements*

A sane customer who carefully checks his bank statements will find out within weeks he has been robbed. He will inform his credit card company and get his money refunded. Mallory will keep nothing in the end.

- *Revocation of Mallory's credit card account*

Mallory can claim having made a mistake a couple of times, much to the chagrin of the credit card companies. Besides, as the transaction is supposedly automated, Mallory will generally not have to enter the total amount of the transaction herself anywhere in the process. Her claim that a mistake has been made will not be believed easily.

A credit card company willing to ensure the security its customers will revoke Mallory's credit card account and Mallory will not be able to continue.

7.5.1.2.3 Countermeasures

Several countermeasures can be taken against this attack.

- *Preferring reputable merchants*

A customer is much safer if he prefers a reputable merchant over a new merchant or especially an ill-reputed merchant. As mentioned in hurdle7.5.1.1.2 - Revocation of Mallory's credit card account, a credit card company will quickly revoke the credit card account of a malicious merchant.

- *Checking bank statements*

The real amount Mallory deduces from the customer's bank account is visible on his bank statement. The customer should take the time to examine those bank statements to ensure all transactions are legitimate and have the right amount.

Any detected fraudulent transaction should be reported to the credit card company immediately so Mallory can be stopped and the customer will have his money refunded.

- *Taking transaction out of merchant's environment*

When using iDeal, the transaction takes place between the customer and the bank. Most importantly, the customer has to provide his authorization details to the bank, rather than to the merchant, though a man-in-the-middle attack might circumvent this. The man-in-the-middle attack is hard to carry out though (see 7.3.6).

One possible countermeasure against this kind of attack is by lifting the whole transactions procedure out of the environment of the merchant in a way similar to iDeal. This means that the transaction must be set up at a website of the credit card company. Let's call this website the 'Checkout Service'. This makes it much harder for Mallory to tamper with the transaction details. If she intends to withdraw more money from the customer than the customer intends to pay, she has to include the higher amount in the transaction she fetches at the Checkout Service. The customer, upon providing his credit card details, will see the higher amount – at least if he checks the form before submitting as everyone should – and should refuse providing his credit card details.

7.5.1.2.4 Conclusion

It is hard to estimate the likelihood of the malicious merchant attack on credit cards when the merchant wants to trick the customer into authorizing a too high amount reliably. Since Mallory will be out of service quickly as soon as a handful of customer has complained at the credit card company, the likelihood seems to be low, rather than medium.

Customers have to check their bank accounts and contact their credit card company for a refund. The impact factor, therefore, is medium.

7.5.1.2.5 Summary

Type	Malicious Merchant
Compromises	Money
Likelihood	Low
Impact	Medium

7.5.1.3 Conclusion

iDeal is better protected against the malicious merchant attack when Mallory wants to have a too high amount authorized, since Mallory won't be able to prevent the final iDeal checkout screen from showing the right amount. This is not the case with credit cards. Therefore, the likelihood of this attack occurring with iDeal is only 'theoretical' while on iDeal, it is 'low'.

7.5.2 Data gathering

A malicious merchant is dealing directly with the customer and can capture all data the customer provides. It will be impossible for a web shop to be operational if they cannot retrieve data like the customer's address or credit card number. A malicious merchant will try to abuse these data.

7.5.2.1 Malicious merchant on iDeal – data gathering

When it comes to iDeal, there are virtually no data the merchant can obtain and use for malicious purposes. The actual payment is carried out within the iDeal environment and takes place between the bank and the customer, which means the merchant will not even be able to retrieve signed nonces. The only useful information a malicious merchant can obtain is information he can use to blackmail a customer. This might be the case if a customer orders explicit pornographic material or Nazi paraphernalia, for example. As this has nothing to do with the payment method, this is beyond the scope of this thesis.

There are no data in the payment process which are useful to Mallory. As long as the nonces which must be signed by the customer are used only once, neither the nonce nor the signed nonce is useful to Mallory. Next to that, Mallory will not be able to retrieve data sent from the customer to the bank and vice versa.

A malicious merchant might use the data on *when* orders have been carried out for a social engineering attack though. This is described in 7.7.2.

7.5.2.1.1 Conclusion

There are no data sent from the customer to the merchant which are useful to Mallory when iDeal is used. Therefore, the likelihood of the malicious merchant attack with the purpose of gathering data is put on 'impossible'. This, obviously, leaves the impact on 'none'.

7.5.2.1.2 Summary

Type	Malicious Merchant
Compromises	<nothing>
Likelihood	<impossible>
Impact	<none>

7.5.2.2 Malicious merchant on Credit cards – data gathering

Contrary to iDeal, data gathering might be much more of a problem for credit cards. A customer provides the malicious merchant with useful data like his credit card number, CVV, address, email address and phone number.

7.5.2.2.1 Scenario

Mallory intends to obtain credit card number to use them herself or to sell them to the highest bidder. To accomplish that, she starts a web shop. If she actually delivers ordered commodities, it will take a long time until customers realize their credit card numbers are sold out. She simply has to store all the credit card numbers of the customer and she can even verify if they are valid. She has to check the credit limit of the credit cards to cash the money the customers pay for her commodities.

Mallory will be able to keep her cover for quite an extended period of time. It will be hard to prove she sells credit card numbers or abuses them, especially if she sells only a small percentage of them and destroys the rest.

7.5.2.2.2 Hurdles

There are few hurdles to this attack. All Mallory needs to do is start a web shop. She might actually be able to make profit by honest, hard work and zeal and consider the profit on the credit card numbers as tip.

7.5.2.2.3 Countermeasures

There is little a customer can do to prevent a merchant from selling his credit card number.

- *Dealing only with reputable companies*

One way to prevent this attack from taking place is by only shopping at reputable companies. A large, well-known company has much more to lose than to gain by selling out credit card numbers. Smaller and less well-known companies should be avoided.

- *Data mining on fraud occurrence*

Customers should report any case of fraud immediately so their credit cards can be blocked. When many customers with blocked cards turn out to have shopped at the same merchant, it's reasonable to assume that particular merchant is either the victim of an intruder in the system or a malicious merchant. Still, it will be hard to prove and it might be very inconvenient to block all the credit cards used at his web shop just in case.

If credit cards which have hardly been used are compromised and it turns out there is a single merchant where they have been used, that particular merchant should be supervised closely.

This counter measure can be countered itself by selling only a small percentage of the credit card numbers. If

7.5.2.2.4 Conclusion

A customer using a credit card has to live with this risk. There is little he can do to prevent a malicious merchant gathering data, except for only dealing with reputable companies. Even then, he might not be safe. According to [29], 94 million (!) accounts of TJX customers were compromised, not by a malicious merchant but by an intruder.

This is definitely a case where the refunding policy of credit card companies is essential to ensure security of the system from a customer's point of view. The 'likelihood' of this attack is put on 'likely' as there are very few countermeasures, no ways to prevent Mallory from doing this and hardly ways to find out if she carried out this attack. The 'impact' is decided on 'medium'. The customer is only an actual victim if his credit card number is used for unauthorized transactions. Even then, his money will be refunded. The customer has to keep track of bank statements and go through paperwork to have his money refunded, which means the impact is above 'low'.

7.5.2.2.5 Summary

Type	Malicious Merchant
Compromises	Credit card number and other data
Likelihood	Likely
Impact	Medium

7.5.3 Malicious merchant in the middle

The 'Malicious merchant in the middle' attack is a combination of a malicious merchant attack and a man-in-the-middle attack. A customer might shop at a malicious merchant who can redirect him to a fake bank website instead of the standard iDeal checkout page.

7.5.3.1 Malicious merchant in the middle – iDeal

As described in 7.3.4, it is very hard for Mallory to carry out an ordinary man in the middle attack. But by disguising herself as a merchant, the man in the middle attack becomes much less hard to carry out technically.

7.5.3.1.1 Scenario

Take a look at the protocol in 4.2.2. In step 4, the user is redirected to the bank's website. Mallory, however, can redirect the user to any website she wants. This means she can also redirect him to a fake iDeal checkout page and use the provided credentials to impersonate the user. This is very similar to the man in the middle attack this attack will alleviate the problems described in 7.3.4, but the first five hurdles in 7.3.1.1.2 will remain in place.

7.5.3.1.2 Hurdles

The hurdles are mostly the same as with the ordinary man-in-the-middle attack. The first five hurdles of 7.3.1.1.2 are still in place.

7.5.3.1.3 Countermeasures

This attack is harder to prevent than the ordinary man-in-the-middle attack. This because Mallory doesn't need to alter a network to get in the middle. All that she is required to do is start a web shop, attract customers and abuse their credentials.

The customer can check the address in the address bar of the browser to ensure he is actually at the website of the bank.

7.5.3.1.4 Conclusion

Technically, the malicious merchant in the middle attack is easy to carry out on iDeal. Mallory does not even need an iDeal account. All she needs is a web shop and a fake iDeal checkout page. This does not mean the likelihood is 'high'. Mallory's cover will be blown quickly as soon as customers find out they do not receive ordered commodities and when they check their bank statements and see Mallory has obtained way too much money.

Customers who order commodities on her web shop can be targeted. After a relatively very small amount of customers, her cover will be blown. The chance a customer is so unlucky he is among that small amount of customers is very, very low. Besides, a customer might notice he is not following the standard iDeal procedure as all of a sudden user login is required. Therefore, the likelihood is put on 'theoretical' rather than 'low'.

With the credentials provided by the customer, Mallory can transfer a great deal of money to her bank account unless the Postbank with the SMS-system is used, as the total amount of the transaction will be in the SMS. The impact, therefore, is 'high'.

7.5.3.2 Malicious merchant in the middle – Credit cards

The system behind online credit card transactions and iDeal transactions is fully different. Therefore, a 'malicious merchant in the middle' attack turns out to be a 'data gathering' attack which is described in 7.5.2.2.

7.5.3.3 Conclusion

The malicious merchant in the middle attack is specific for iDeal and is not possible on credit cards. The likelihood that the attack takes place on iDeal is only theoretical, though.

7.5.3.3.1 Summary

Type	Malicious Merchant
Compromises	Money
Likelihood	Unlikely
Impact	High

7.6 Man in the browser attack

The most feared one of all…

This section describes the man in the browser attack on iDeal and credit cards, each with their own countermeasures, hurdles and conclusion.

7.6.1 Man in the browser attack on iDeal

It might be possible to write a browser hack for iDeal which somehow makes Mallory rich. It has worked in the past with ordinary Internet banking (see [25 page 1]), but will it work on iDeal as well?

7.6.1.1 Scenario

The customer places an order and opts to pay using iDeal. The merchant fetches the order at the bank and redirects the customer to his bank's website. The customer, however, will never reach that site. Instead, he will see a fake checkout page which is created by the browser hack. Secretly, the web browser starts a second session with the bank. A login is required and the fake page asks the browser to login. The browser hack takes the nonce from the second – invisible – session and displays it on the fake page. The user will then sign the nonce, and the second browser session is logged in at the bank under the user's name. The hacked browser will automatically create a transaction – or series of transactions – to Mallory's bank account with a high amount of money. To authorize the transaction, a new nonce must be signed. That nonce is sent to the fake page which the user sees. If he signs the nonce, the transaction of the second session will be carried out. As more than one transaction can be authorized by signing a single nonce, the potential loss of the victim and gain of Mallory is substantial.

The protocol with a hacked browser is as below. Data between '<>' are invisible to the user because they are requested by the second session.

	Customer	Mallory	Merchant	Bank
1	iDeal, Bank →			
	The customer opts to pay using iDeal and indicates which bank he uses.			
2			Fetch order →	
	The merchant fetches the order at the bank.			
3	← redirect			
	The merchant intends to redirect the customer to the iDeal checkout page			
4	(Start second session)			
5	<← NonceLogin>			
	In order for the second session to login, a nonce must be signed with the token of the customer. In this step, the nonce is sent to the customer and intercepted by the hacked browser. This leads to step 6.			
6	(Browser creates fake page with NonceLogin)			
	The hacked browser receives the NonceLogin from step 5.			

	Then, a checkout page is created by the hacked browser and the NonceLogin is displayed in order for the customer to sign it with his token.
7	$[NonceLogin]_{key}$ →
	The customer signs the NonceLogin with his token. The hacked browser can use it to login under the customer's name with the second session which remains invisible to the customer.
8	The browserhack quickly creates a series of transactions from the customer to Mallory. In order to authorize these transactions, a new nonce must be signed with the token of the customer. This nonce is called 'NonceAck'.
9	<← NonceAck>
	The NonceAck is sent to the customer. The browserhack intercepts this NonceAck and displays it to the user using the general iDeal layout.
10	(Brower creates fake page with NonceAck)
	The customer, convinced he's paying a genuine order, signs the NonceAck with his token.
11	$[NonceAck]_{key}$ →
	The NonceAck, signed with the customer's token, is used by the browserhack to authorize the series of transactions created in step 8.
12	(Customer is redirected to final page)

Note: step 2 and 3 do not play a part in the protocol. The fetched order in step 2 will never be paid and the redirection in step 3 will be ignored by the hacked browser.

As can be seen, the attack is very similar to a man in the middle attack as described in 7.3.1.1. There is, however, one big difference: Physically Mallory doesn't need to be on the same network or in the range of a wireless access point. As this is the hardest to achieve in a man in the middle attack, the man-in-the-browser attack is much more dangerous. Besides, this kind of attack can be carried out fully automatically without requiring any interaction of Mallory personally. This means that Mallory can try to hack as many browsers as she can in a short time, wait a while until the money pours in and then go into hiding.

7.6.1.2 Hurdles

Hacking the browser itself is the hardest part for Mallory. Even after this is accomplished, most of the hurdles of the normal man in the middle attack are still present. They are described in 7.3.1.1.2. No part of the hurdles are 7.3.1.1.2 - Wrong address in browser's address bar', 7.3.1.1.2 - Getting 'in the middle' and 7.3.1.1.2 - Replacing the redirection link. This because it is assumed that the browser hack will display a genuine address in the browser's address bar**.**

7.6.1.3 Countermeasures

There are several possible countermeasures. Chapter 3 of [20] provides a number of security measures against man-in-the-browser attacks as well.

7.6.1.3.1 Captcha required to authorize transactions.

This might be an easy yet very effective way to completely eliminate this possible attack. The second, invisible session is created solely by the browser and invisible to the user. Therefore, a captcha might be useful to prevent the browserhack from authorizing a transaction. An example of a captcha is shown below.

Figure 5: Example of a 'captcha'

The captcha above is taken from an attempt to reset a hotmail password for purely scientific reasons. It is assumed that it is impossible for a computer to recognize the characters in a captcha which means a human is required to accomplish that. By requiring the user to enter the characters in the captcha to authorize the transaction, the browserhack – which will be unable to recognize the characters – is stuck.

Of course, this measure requires the character in the captcha to be unrecognizable by a computer. The validity of captchas is beyond the scope of this thesis.

7.6.1.3.2 Custom client for online banking

A custom client instead of a web browser for online banking will make the man-in-the-browser attack unfeasible. A specific custom client can be written with security measures to prevent hacking.

In the specific case of iDeal, this is very impractical. iDeal was written on top of an already present online banking system. A custom client will require a major overhaul of the system to the point it won't even resemble iDeal anymore. Besides, a lot of the advantages of using a web browser for online banking will disappear, such as portability across operating systems and the ability to use any computer with a web browser and an internet connection without the need to install additional software.

7.6.1.3.3 Amount of transaction required as challenge

Currently, to authorize transactions it is only required to enter the amount of the transaction on the token for high amounts. The hacked browser is able to intercept the redirection to the iDeal site in step 3. This means that the hacked browser can look up the order details including the total amount of the transaction.

If the total amount of the transaction is not required as a challenge, Mallory can create a series of transactions with a very high amount in step 8. By adding the amount of the transaction as a challenge for every transaction, the loss for the customer will at least be limited to the amount he actually wanted to authorize.

This countermeasure is already present for Postbank users which use the system of TAN-codes by SMS as the total amount is shown in the SMS.

7.6.1.4 Conclusion

The man in the browser attack is not easy to carry out on iDeal. First of all, Mallory must find a way to infect the web browsers of potential customers (see 7.6.3). Second, the customer must do the following as in the normal man-in-the-middle attack:

- He must not find it unusual to login at the website of the bank, even though that's not the normal procedure with iDeal.
- He must not find it strange he is not redirected back to the merchant, but to a different page.
- He must not check the order status shortly afterwards.
- If iDeal Advanced is used by the merchant, (see 7.3.1.1.2 - iDeal Advanced), the transaction is normally carried out in the look-and-feel of the web shop. Mallory has to use the standard page though. A regular shopper at the web shop might notice the difference.

Contrary to the ordinary man-in-the-middle attack, Mallory is not required to create a script for every merchant she intends to attack (see 7.3.1.1.2 - Replacing the redirection link) which means she can target all merchants at once. Secondly, she can save herself the effort of getting in the middle (see 7.3.4). This means the attack is more dangerous than the ordinary man-in-the-middle attack.

If Mallory decides to infect browsers, she doesn't need to target iDeal specifically. If she targets regular online banking instead of iDeal, she has a much higher chance of success. According to [26], 20% of the online transactions annually are carried out by iDeal. Of course, Mallory can write a browserhack to target iDeal as well as regular banking to get her share of the 20% of iDeal transactions.

It is hard to estimate the likelihood of this attack. It is possible to carry out this attack, which means the customers are at Mallory's mercy. The visible signs to the customer which indicate he is under attack are relatively minor.

Because the advantages to Mallory if she targets regular banking instead of ideal are substantial, the likelihood of this attack is put on 'low'. Because of the risk that Mallory will decide to take her share of the 20% iDeal transactions is also substantial and because the amount of iDeal transactions is increasing (according to [26]), a likelihood of 'medium' would be justifiable as well.

The customer may lose quite an amount of money which the bank may not refund as the transaction to Mallory is authorized with the token of the customer. The impact factor, therefore, is 'high'.

7.6.1.5 Summary

Type	Man in the browser
Compromises	Money

Likelihood	Low
Impact	High

7.6.2 Man in the browser attack on Credit cards

A man-in-the-browser attack can easily be used to gather data when credit cards are used as well. The data might be encrypted when they are sent to the merchant's website, but a hacked browser can gather the data before, when they are typed in the form. Mallory can receive all data like the credit card number, CVV, expiration date, name and address of the customer and nobody will notice anything (according to [20 first paragraph], there is no difference to be seen) until she actually starts using the data.

There are some problems, though. The browser hack must be designed to gather useful data, which means it has to be preprogrammed with a list of merchants, so it can detect a user visiting a merchant's website. Then, the browser hack must read the right data fields and send the values to Mallory.

7.6.2.1 Scenario

The scenario of a man-in-the-browser attack on credit cards is very simple and is shown below.

	Customer	Merchant	Mallory	Credit card company
1	Checkout Details →			
	The customer, at the final stage of ordering, provides details like his credit card number, name, address etc.			
2	(hacked browser intercepts predefined data fields like credit card number and CVV)			
3	Checkout Details →			
	The hacked browser sends the obtained data to Mallory.			

The customer can't possibly notice anything. The browser hack will not alter any data or interfere with the data sent from the customer to the merchant. It simply reads a preprogrammed list of data fields and sends it to Mallory.

7.6.2.2 Hurdles

In order for Mallory to be effective, she must overcome the following hurdles.

7.6.2.2.1 Writing the browser hack

Though according to [20] writing a browser hack is not difficult, this does not mean Mallory only has to spend a couple of hours to write the hack. The browser hack would be ineffective if it can target only a handful of merchants. This means that Mallory, when creating such a browser hack must spend a lot of time analysing many web shops to make the browser hack work against them. She can, however, be quite successful if she targets only the best-selling merchants.

7.6.2.2.2 Installing the browser hack

The worst problem is infecting the customer's browser with the browser hack. This problem is described in chapter 7.6.3.

7.6.2.3 Countermeasures

Chapter 3 of [20] provides a number of security measures against man-in-the-browser attacks.

Defending against this attack is not easy. Quoted from [20 paragraph 1]: "Distinct from Phishing attacks which rely upon similar but fraudulent websites, these new attacks cannot be detected by the user at all, as they are using real services, the user is correctly logged-in as normal, and there is no difference to be seen." According to [25], "Part of the frustration with a man in the browser attack is that the bug is very hard to detect and even harder to remove from the system."

7.6.2.4 Conclusion

It is hard to protect against the man in the browser attack when a credit card is used. According to [20], detecting a browser hack is very hard and, contrary to iDeal (see 7.6.1.4), the user won't see any difference between using a non-hacked browser or a hacked browser.

The customer must go through his bank statements carefully to detect unauthorized transactions so he can block his credit card and start the procedure to regain his money. Of course, he must also adhere to the general man-in-the-browser countermeasures as provided in 7.6.4.

According to [22 chapter 'Global Trojan Horses'], the worldwide infection rate of Trojan horses is 504 per 1000 PCs. Quoted from [22 chapter 'System Monitors']: "Webroot Internet spyware scans revealed that system monitors are present on 6 percent of infected machines during Q2 2006, the same percentage as last quarter." These numbers are high enough to put the likelihood of this kind of attack on 'high'. The customer has to take action to regain his money, which means the impact is put on 'medium'.

7.6.2.5 Summary

Type	Man in the browser
Compromises	Credit card number
Likelihood	Medium
Impact	Medium

7.6.3 How to Hack a Browser

Of course, to accomplish this attack, Mallory has to hack the customer's browser. There are several ways to accomplish this.

7.6.3.1 Trojan horse

A Trojan horse is one of the easiest ways to hack a browser. There are many ways to send Trojan horses to a customer. A customary way is sending them to the customer's mail address. An advantage of this is that many addresses can be spammed at once to increase the chance the Trojan will actually be run by a significant amount of potential victims.

Putting the Trojan on a website where it can be downloaded and hopefully executed is another option.

7.6.3.2 Browser Extension

A browser like Firefox and Internet Explorer allows installation of browser extensions which add some functionality to the browser. Those extensions can be created by anybody, including Mallory. Next to the malicious features of the extension, the extension must actually provide desired functionality or it will be uninstalled or not downloaded at all.

Browser extensions in Firefox are generally not signed [15] and even if signed, it does not mean they are not browser hacks [15].

7.6.3.3 Road apple

A third way is a 'road apple'. Mallory can put a memory stick or some other data carrier which is labeled like 'Confidential diary of <some known person>' in any place where her intended victim might find it. The victim, eager to read the confidential diary, unwittingly and unintentionally installs malware. A drawback of this method is that it is hard to apply to a large amount of victims.

7.6.4 Countermeasures

Countermeasures against browser hacks are possible, most of them based on common sense.

7.6.4.1 Distrust executables from unreliable sources

Not executing any executable sent by mail unless one is really really really sure it comes from a reliable source is one of the most effective ways to prevent browser hacks. Attachments sent by mail should never be executed. Even better, the mail client or even the mail server should be programmed not to let executables of any kind through. Executables downloaded from file sharing networks should not be executed as well.

7.6.4.2 Use of anti-spyware programs

Running anti-spyware software regularly or preferably permanently in the background will also provide additional security though according to [25], this amount of security is very low.

7.6.4.3 Use of non-standard web browsers

Running a different web browser than MS Internet Explorer reduces the risks, as most browser hacks will be targeted at the most widely used browser. According to [20], at 12-9-2006 it was not known if Konqueror, Lynx, Safari and other browsers had already been targeted but Firefox, Internet Explorer and Opera were.

7.6.5 Conclusion

The man-in-the-browser attack is currently the most feared attack of all. There are several reasons for this. First of all, the man-in-the-browser attack is easy to use on a massive amount of targets. Contrary to a man-in-the-middle attack, the attack doesn't take place on a specific network of users, but can target every user on the internet. This, naturally, makes the potential profit for Mallory very high. Second, it is hard to protect against man-in-the-browser attacks.

7.7 Social Engineering Attacks

This section describes social engineering attacks on credit cards and iDeal, each with their own countermeasures, hurdles and a conclusion.

7.7.1 Social engineering attack on credit cards

There are many ways in which Mallory can try to obtain the customer's credit card number and preferably CVV and expiration date using social engineering, too many to mention them all. Because the scope of this thesis is limited to online orders in The Netherlands, the social engineering attack can only be researched within this context.

7.7.1.1 Scenario

A customer places a genuine order with a genuine merchant and opts to pay using his credit card. He submits the necessary information and the transaction is authorized. The customer happily waits until the ordered commodities are delivered and the merchant is counting his money. So far, so good…

Mallory, one way or the other, knows about this transaction as well. She contacts the customer by phone or email and informs him deceitfully that something went wrong during this transaction. She requests the customer to carry out the transaction again and guides him to a fake checkout page. In the best possible case, this fake website has the look and feel of the company the customer actually placed the genuine order with. If the customer is convinced he is actually correcting an error, he will provide the necessary details like a credit card number, his home address and perhaps a delivery address etc.

Mallory has all she wants now. This method can work by email or by phone. The customer will not notice anything out of the ordinary afterwards unless Mallory abuses his data immediately. If email is used by Mallory, she can target many customers at once but the amount is limited by the actual amount of transactions which has recently been carried out.

7.7.1.2 Hurdles

Before Mallory has a chance to succeed, she has to overcome certain hurdles.

7.7.1.2.1 Getting hold of transaction

Mallory can only carry out this method if she acts within at most a couple of days after the genuine transaction was carried out. Furthermore, she has to get hold of the total amount of the transaction – she'll make a fool of herself if she asks the customer if he remembers what the amount was.

The only serious way to accomplish this is by working at the merchant. She might be able to get access to these details.

7.7.1.2.2 Acquiring the customer's contact details

Mallory must be able to get hold of a mail address or phone number of the customer so she can contact him. Again, this might be possible if she's an employee of the merchant.

7.7.1.2.3 Distrust of the customer

A customer might realize it is actually Mallory, not the genuine merchant, who is trying to make him authorize the transaction a second time. It is after all possible something actually *did* go wrong but it is conspicuous the customer gets informed only later.

The amount of customers which will fall for this trick is hard to estimate.

7.7.1.3 Countermeasures

This attack is only possible if an employee is abusing his position to rob his employer's customers.

7.7.1.3.1 Screening potential employees

Employees of online merchants should be screened to ensure they are trustworthy. Of course this doesn't make it impossible for Mallory to get a job at a merchant, but it surely makes it harder.

7.7.1.3.2 Distrust of the customer

A security-aware customer is careful with his credit card details and personal details. Just in case, he can contact the merchant to verify Mallory's email or phone call.

7.7.1.4 Conclusion

A social engineering attack on credit cards appears to be possible. It seems certainly possible either an employee of a merchant abuses his position and data access or Mallory successfully acquires a job at a merchant. According to [28 page 98], the total amount of credit transfers in 2005 in The Netherlands was 1,224.78 million, of which 996.18 million were not paper-based. As Mallory is unable to target a great many customers at once (see 7.7.1.1), the chance a customer is targeted by this attack is very low. A little distrust on the customer's side will make the chance even lower. Therefore, the likelihood of this attack is put on 'low'. If Mallory succeeds, she will have obtained valuable data like the credit card number and CSV number. The generous refunding policy of credit card companies limits the impact to 'medium'.

7.7.1.5 Summary

Type	Social engineering
Compromises	Credit card number and other information
Likelihood	Low
Impact	Medium

7.7.2 Social engineering attack on iDeal

It is possible to carry out a social engineering attack after the customer has used iDeal to pay an order. There are two possible scenarios, described in 7.7.2.1.

7.7.2.1 Scenario

There is a possible scenario. If Mallory is able to keep track of iDeal transactions of a certain merchant and gets hold of the email address or phone number of a customer, she can try a social engineering attack.

The scenario is as follows: The customer orders certain commodities at a certain merchant. He intends to pay using iDeal and goes through the regular procedure to authorize the transaction. So far, nothing out of the ordinary has happened. At this moment, Mallory comes in. She phones or mails the victim, impersonating either a bank employee or an employee of the merchant. She will try to convince the customer his transaction was refused or some error occurred, or whatever is necessary to make the customer attempt a new transaction. Now, there are two things Mallory can do.

7.7.2.1.1 Login with customer's credentials

Mallory can lure the customer to a website with an iDeal look or merchant's look and ask the customer to login. This will provide Mallory with a signed login nonce, which means she can login under the customer's name at his bank. If she doesn't yet know the customer's bank account number, she can ask the customer to enter that as well.

Mallory has to quickly prepare a transaction from the customer to her own bank account. She can use a script for that. Authorizing this transaction requires a signed authorization nonce from the customer as well. Mallory must redirect the customer to a second page, in which she displays the authorization nonce. The customer must then use his token again to sign that nonce. Mallory has all she needs.

This method can be carried out by phone or by mail. The potential profit for Mallory is very high, as she has a signed nonce to authorize a transaction to herself. Besides, this scenario can be scripted which doesn't require Mallory to do anything but sending a mail to a customer after he has carried out an iDeal transaction.

7.7.2.1.2 New transaction with Mallory's bank account

This is an easier method than the one described in 7.7.2.1.1. Mallory has to convince the customer to pay the order again as – as mentioned in 7.7.2.1 – the customer thinks the previous transaction was rejected. All Mallory has to do now is providing her own bank account number and, hopefully for Mallory, the customer wires the amount of the order to Mallory. *Note: the transaction to Mallory is not carried out using iDeal!*

This method can be carried out by phone or by email. The potential profit for Mallory is as high as the amount of the genuine order the customer previously placed.

7.7.2.2 Hurdles

There are several hurdles Mallory has to overcome to succeed.

7.7.2.2.1 Keeping track of iDeal transactions.

Mallory has to be triggered somehow when the customer performs an iDeal transaction. This is possible if she is an employee of the merchant and can keep track of transaction records. Of course, this severely limits the potential amount of victims.

7.7.2.2.2 Acquiring the customer's contact details

Mallory must be able to get hold of a mail address or phone number of the customer so she can contact him. Again, this might be possible if she's an employee of the merchant.

7.7.2.2.3 Staying under cover

The customer may realize he has been robbed when he checks his bank statements. At that moment, the bank account of Mallory is known and Mallory won't be hard to track down.

Contacting the real merchant to check if everything is all right will trigger alarm. This does not mean Mallory's identity is revealed directly. Both mentioned scenarios require Mallory to either call or mail the customer. By using a phone booth or stolen portable phone she can remain into obscurity. Sending mails from a hotmail, gmail or other free account will not reveal her identity as well.

7.7.2.2.4 Customer distrust

A customer might realize the received mail or incoming phone call are not from the genuine merchant, but from Mallory. This doesn't apply to all customers, after all it *is* possible something went wrong with the previous transaction. A customer might contact the real merchant to check if everything is all right and this will trigger alarm.

7.7.2.3 Countermeasures

There are several possible countermeasures against this attack, either on the side of the merchant or on the customer's side.

7.7.2.3.1 Screening potential employees

As mentioned in 7.7.2.2.1 and 7.7.2.2.2, one requirement for this attack is keeping track of iDeal transactions. This might be possible for an employee of the merchant who has access to the relevant data. Employees of online merchants should be screened to ensure they are trustworthy. Of course this doesn't make it impossible for Mallory to get a job at a merchant, but it surely makes it harder.

7.7.2.3.2 Distrust on the customer's side

It is the customer who must provide Mallory with the information she needs. Incoming mails or phone calls should either not be trusted or verified. The customer can contact the merchant to check if everything is all right. He can also check his bank statement online to see if money has been transferred from his bank account. If that is the case, he can be sure the mail or phone call is from an untrustworthy source.

7.7.2.4 Conclusion

A social engineering attack on iDeal is a genuine possibility. It is possible that Mallory gets a job at a merchant, or one of the regular employees decides to abuse his position. The scenario in 7.7.2.1.2 is easy to carry out. It doesn't require Mallory to create a website, all she has to do is contacting the customer until she finds one who is willing to transfer money to her. The scenario in 7.7.2.1.1 is harder. Mallory has to create a website with an iDeal look and she has to create a script which prepares transactions. The potential profit is very high in that case. Besides, the attack can be automated to a high level.

The attack is certainly feasible. Still, the likelihood is put on 'low'. Mallory's cover will be blown quickly so she won't be able to operate for an extended period of time. Second, the customer has to do what Mallory intends and not every customer will fall for her tricks. Third, it requires Mallory to be an employee of a merchant. Of the millions iDeal transactions (see [26]), few will lead to this social engineering attack.

The impact, on the other hand, is high. Especially if the scenario in 7.7.2.1.1 is used, Mallory can rob the full bank account of the victim at once! The impact, therefore, is definitely 'high'.

7.7.2.5 Summary

Type	Social engineering
Compromises	Money
Likelihood	Low
Impact	High

7.7.3 Conclusion

Social engineering attacks on credit cards as well as iDeal are possible, in a very similar way. The risk is not that high though, as both have a likelihood of 'low'. Customers with a credit card might benefit from the refunding policy of the credit card companies in case something actually goes wrong. Credulous customers who fear their own naivety should use a credit card.

8 General Countermeasures

Some of the described attacks are actually feasible, making Mallory rich. The actual fraud with credit cards is very high, up to £400 million in the UK in 2006 which translates to approximately €600 million [1]. I have not been able to find a single successfully carried out iDeal fraud attempt. Either the security or cover-up methods must be excellent.

Of course there's always one barrier between Mallory and success: the law.

8.1 Hiding Mallory's Identity

Ideally - for Mallory -, Mallory keeps her identity hidden for the customer, any merchant and any bank. But that is not always easy to accomplish and might be a harder task than carrying out the fraud itself.

8.1.1 iDeal

Where iDeal is concerned, it will be very hard for Mallory to keep her identity secret. Because iDeal only works within The Netherlands, she must have a bank account to transfer stolen money to. To create a bank account, a proof of ID is required. Mallory's identity will be known to the police as soon as the first victim lodges a complaint. An option is to use a straw man, for example a homeless person or drug addict to create a bank account, but it is not easy for a homeless without an address or a junk to create bank accounts.

Even then, the question is if it is worth all the trouble. The attacks on iDeal require a real customer placing a real order and it will be hard for Mallory to rob a lot of money before the police knock at her door. She will be caught sooner or later and even if she should have managed to hide the money somewhere, she can be glad if the amount is more than a couple of thousands of Euros. This might be a reason why iDeal fraud is a rare or non-existent incident.

The same is also true for the malicious merchant attack. Mallory might be able to get some money, but within weeks the police will receive the first complaints. One of the possible reasons iDeal fraud is so rare is that the financial world has provided her with a much better platform to commit fraud on, namely credit cards.

8.1.2 Credit cards

It is much easier for Mallory to keep her identity secret if she performs fraud with credit cards rather than with iDeal. She can use any stolen credit card number to order goods and send them to any address she has access to. A different way is to create a fake web shop and use the stolen credit card information to place orders. A disadvantage of this is that she must have a bank account and therefore it will be very hard to hide her identity. The former method is much more convenient. There are algorithms to produce lists of valid credit card numbers but they are less useful nowadays because the expiration date or CVV must also be provided.

Because of the effort it requires to hunt and prosecute credit card criminals they are often not prosecuted. The credit card companies simply refund the stolen money to the robbed customer and only actively work on cases with higher fraudulent amounts. Of course there are security measures in place, like the CVV and the fact that shipments to other addresses than the card holder's registered address are not allowed, but still fraud is widespread. The fraud could be reduced with firmer security measures but that would decrease the use of credit cards and consequently the profit of the credit card company. Therefore, the goal is not to stop fraud altogether but to reduce it to manageable levels.

8.2 General Distrust

A customer must realize he's authorizing money transfers. One wouldn't trust a salesman on the market selling the Elixir of Life, nor would anybody buy a Van Gogh without a serious appraisal by one or more experts. Any customer should only deal with a merchant whose reputation is absolutely impeccable. Large, well-known companies are to be preferred to small, new companies as their intention might be just to gather credit card numbers. If something is too good to be true, it most certainly is not.

Some users get careless because credit card companies very often refund stolen money. This is a pity because it helps Mallory and makes credit card transactions more expensive, also for less careless users.

Sadly, because of the number of people – however small – who agree to offers in spam, spam still exists. It also proves that there are still plenty of very naive customers.

Any computer user linked to a network – especially the Internet – must be careful with all software he installs. Trojans can be spread by mail or downloaded from websites or peer-to-peer networks. A nice screen saver might just as well be a key logger. Key loggers are very hard to detect [2]. The man-in-the-browser attack (see 7.6) is the most dangerous attack and requires installing a Trojan or some browser extension. Incidentally, the man-in-the-browser attack is more dangerous when not iDeal but general Internet banking is used. This is because a man-in-the-browser attack on general Internet banking is completely invisible to the user but the iDeal protocol must be altered to provide a login (see 7.3.1.1.2 - Login required at bank website□).

Most browser extensions are unsigned – unapproved by the authors – and the user never knows what he installs.

Regular checking of bank statements to make sure no money is transferred to unknown bank accounts is highly recommended. If one is faced with a suspicious transaction, the police must be informed immediately. In the case of credit cards, the credit card must be blocked as soon as possible. In the case of iDeal, the bank must be informed.

8.3 Anti-virus software, anti-spyware software and firewalls

Anti-virus software will do little to protect the user against the specific attacks described in chapter 7. Most anti-spyware software will not detect key loggers or malicious browser extensions. Firewalls will not provide protection against hacked browsers because they cannot prevent web browsers from accessing the Internet. Such a firewall would be far too strict and therefore rarely used.

Of course the use of anti-virus software, anti-spyware software and firewalls is greatly recommended, but this in itself is not sufficient.

8.4 Additional challenges for authorizing transactions

Currently, authentication and authorization of the user happens by signing a nonce or providing username and password to login, and a second nonce to authorize the transaction. The Postbank system has some additional safety. The user who uses the SMS system – as opposed to the TAN-list system – will see the amount he is authorizing in the SMS. Users of any of the various banks will not see the amount of the transaction he is actually authorizing, making it possible for Mallory to alter the amount and still fooling the user into signing it. Adding the total amount to the challenge will provide additional safety.

9 Conclusion

The final conclusion is presented from three different *viewpoints*: the technical security viewpoint, the financial viewpoint and the overall viewpoint. Each viewpoint takes into account different *likelihood factors* and *impact factors*.

The viewpoints correlate with three different ways to look at a security system. The likelihood factors are used to determine how high the chance is one falls victim to a certain attack. The impact factors are used to determine how large the impact is *if* an attack is successful.

In **Error! Reference source not found.** the likelihood factors and impact factors are summarized. In 6.4 the different viewpoints are explained in more detail. In 9.1 the actual conclusion is provided for each viewpoint. Finally, the overall conclusion is in 9.2.

9.1 Viewpoints conclusion

In this paragraph, the conclusions of the different viewpoints are described.

9.1.1 Technical security viewpoint

Let us have a look at the table below, which is comprised of the summaries provided in the first paragraph of every attack in chapter 7.

		iDeal	**credit card**
Kind of attack		*likelihood*	*likelihood*
Man in the Middle	7.3		
Without SSL	7.3.1	Theoretical	Unlikely
With SSL	7.3.2	Theoretical	Theoretical
On ISP of customer	7.3.3	Theoretical	Theoretical
Key logger			
		Impossible	Medium
Malicious Merchant	7.5		
Authorizing a too high amount	7.5.1	Theoretical	Low
Data gathering	7.5.2	Impossible	Likely
Malicious merchant in the middle	7.5.3	Unlikely	Impossible
Man in the browser	7.6		
		Low	Medium
Social Engineering	7.7		
		Low	Low

Most attacks on iDeal are either theoretical or impossible. The only attacks Mallory has a remote chance in to succeed are the malicious merchant attack on data gathering and the malicious merchant in the middle attack. Credit cards, however, are susceptible to key loggers, man in the browser attack and especially the malicious merchant attack when a malicious merchant intends to gather data.

From a technical point of view, iDeal is more secure than credit cards. The difference in security is substantial.

9.1.2 Financial viewpoint

Let us have a look at the table below.

		iDeal		credit card	
Kind of attack		*likelihood*	*Financial impact*	*likelihood*	*Financial impact*
Man in the Middle	7.3				
Without SSL	7.3.1	Theoretical	High	Unlikely	Low
With SSL	7.3.2	Theoretical	High	Theoretical	Low
On ISP of customer	7.3.3	Theoretical	High	Theoretical	Low
Key logger					
		Impossible	None	Medium	Low
Malicious Merchant	7.5				
Authorizing a too high amount	7.5.1	Theoretical	Medium	Low	Low
Data gathering	7.5.2	Impossible	None	Likely	Low
Malicious merchant in the middle	7.5.3	Unlikely	High	Impossible	Low
Man in the browser	7.6				
		Low	High	Medium	Low
Social Engineering	7.7				
		Low	High	Low	low

There are obvious differences. The financial impact of any attack on credit cards remains low, because credit card companies refund fraud.

What is striking about the financial impact of iDeal attacks is that, though their likelihood is never beyond 'unlikely', the financial impact is 'high' in many cases. Because Mallory can trick the customer into providing authorization information for a regular online transaction, her maximum gain is not limited to the amount the customer actually wanted to authorize. Next to that, regular banks might not be as generous when it comes to refunding fraud as credit card companies.

Despite being technically less secure than iDeal, credit cards are safer when looked upon from a financial viewpoint. It is often convenient to have a large credit card company as a backup when dealing with unknown merchants. When trading with iDeal, the responsibility rests solely with the customer. Besides, an iDeal payment is a payment in advance, before any ordered commodities are delivered.

9.1.3 Overall viewpoint

The overall viewpoint is similar to the financial viewpoint, but also includes the impact factors 'confidential impact' and 'practical impact'. The financial security of credit cards is superior to the financial security of iDeal, not because the system is harder to attack but because of the generous refunding policy of credit cards. This, however, means that customers have to check their regular credit card statements for malicious transactions. As soon as such a transaction is encountered, the customer must request his credit card company to refund the money. An iDeal user has fewer problems to solve and the chance he is the victim of an attack is much lower. This has a price, however. If an attack is successfully carried out, the impact is larger.

A customer must measure the risks. Either gamble on the low chance of a successful iDeal attack but with a higher impact if an attack succeeds, or play safe, use a credit card and accept the possible fuss as a price.

From the overall viewpoint, a credit card is still safer, but that safety has a price: it is perhaps less user-friendly. The choice is the customer's.

9.2 Overall conclusion

iDeal is more secure from a technical viewpoint than credit cards. This is not surprising. iDeal is based on an already existing online transaction system which was created especially for online banking. The 2-factor authentication which uses nonces ensures security against key logger attacks, which for credit cards is still a risk (see 7.4.2.2). The security of credit cards relies mostly on the confidentiality of the credit card number, which is hard to keep confidential when it is actually used for online transactions. This makes credit cards susceptible for malicious merchant attacks and man in the browser attacks.

It might be equally surprising that credit cards provide more *financial* security despite their *lower* technical security. The refunding policy of credit card companies provides this security.

Because iDeal provides more 'technical security' and is much harder to attack, a customer can choose to use iDeal and accept the small risk. He can also choose to be backed up by a credit card company for the financial security which means he has to check his bank statements thoroughly and, in the case of fraud, inform his credit card company. This might lead to a blocked credit card which might be very inconvenient on for example a holiday in a country where credit cards are very common like the USA. All in all, it is simply more fuss. Increased financial security simply has a price.

10 Reflection and future research

In this chapter, a reflection on research and proposals for new research are presented.

10.1 Reflection

Looking back at the final thesis and the trajectory followed to create it...

10.1.1 Scope creep

'Scope creep' was the worst among the problems I have encountered while writing this thesis. The original idea was to measure the likelihood and impact of the possible attacks as taken from literature. The more the research progressed, the more ways were found to attack. As excluding certain attacks would crumble the foundations of the research, ignoring these attacks would render the final conclusion invalid.

An example of this is the man in the middle attack on the ISP of the customer. I was certain the likelihood of this attack would be either 'theoretical' or 'impossible'. Before I can blatantly claim that, however, I must either find credible references or analyze the possible scenarios, including possible countermeasures.

10.1.2 Financial secrecy

Banks and credit cards are not advertising with their fraud rates which meant it was hard to find credible data on actual fraud occurrence. [1] Is a commonly found reference, which is a document published by APACS. APACS introduces itself on its website as 'APACS is the UK trade association for payments and for those institutions that deliver payment services to customers'. This same document has been referenced to by the 'credit card fraud' article on Wikipedia, actually already in the first paragraph.

10.2 Future research

Suggestions for future research…

10.2.1 Lack of measurement standards

One problem I have encountered is the lack of standards to be able to measure 'likelihood' and 'impact'. Despite extensively searching the Internet – mainly but not limited to Google scholar – and databases of scientific papers, no such standards have been found. Some papers have hinted at the lack of standards as well. This makes it difficult to compare security systems to each other, such a comparison is a research in itself.

The scientific community in the field of IT security should eventually create such standards. When a new system is invented, it can be measured against existing systems in a short period of time with repeatable and credible results.

10.2.2 Including other systems

There are alternatives to credit cards and iDeal, for example the giro card which is still often used in The Netherlands. By extending the current research with such systems, the security issues of all systems available to a customer can be evaluated. Because likelihood and impact factors have been created, the comparison of the researched systems will have a sound scientific basis. A side-effect of this will be that Mallory can easily find the possible vulnerability of any system which will aid her in her work but as is generally assumed in the field of IT security, 'security by obscurity' does not work and must at all cost be prevented.

10.2.3 Other viewpoints

The current conclusion is presented from three different viewpoints: technical, financial and overall. Other viewpoints might be possible as well. A possible viewpoint might be the viewpoint of a customer who does not have access to the internet at his living place and has to rely on office networks or internet terminals in public places like libraries. A second viewpoint might be that of customers who use cell phones or other mobile equipment to gain access to the internet. Such a device may easily be lost or stolen.

10.2.4 Comparison iDeal and regular online banking

One surprising conclusion which is beyond the scope of this thesis is that iDeal is actually better protected against man-in-the-browser attacks than regular online banking is. This is because iDeal does not provide Mallory with the required login credentials.

As the man-in-the-browser attack is a dangerous attack, it might be interesting to research iDeal within the same context to create a man-in-the-browser proof online banking system. Currently, this would require a third party to set up the transaction at the bank – the merchant – which is impractical.

11 References

[1]	Fraud, the facts (2007). The definitive overview of payment industry fraud and measures to prevent it. Retrieved 5-11-2009 on http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2007.pdf
[2]	Key loggers: The Overlooked Threat to Computer Security. Kishore Subramanyam, Charles E. Frank, Donald F. Galli. Retrieved 12-19-2007 on http://keylogger.org/articles.cgi?in=Keyloggers_The_Overlooked_Threat_to_Computer_Security&id=7
[3]	tcpdump. [Online] http://www.tcpdump.org/
[4]	ethereal. [Online] http://www.ethereal.com/
[5]	3x kloppen – Veilig blijven Internetbankieren. Retrieved 3-15-2008 on http://www.3xkloppen.nl/html/veelgestelde-vragen.aspx
[6]	Haidong Xia and José Carlos Brustolini, Hardening Web Browsers Against Man-in-the-Middle and Eavesdropping Attacks, Department of Computer Science, University of Pittsburgh, 210 S. Bouquet St. #6135, Pittsburgh, PA 15260 - USA
[7]	Credit Card Statistics. Retrieved 15-3-2008 on http://www.cardratings.com/creditcardstatistics.html
[8]	BBA – British Banker's Association – December 2007. Retrieved 15-3-2008 on http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=470&a=12135
[9]	Waarschuwing ABNRO aan iDeal gebruikers. Retrieved 3-15-2008 on http://forums.oscommerce.nl/index.php?showtopic=16446&st=20&p=94993&#entry94993
[10]	iDeal. Retrieved 3-15-2008 on http://www.ideal.nl/consument/demo/index.html
[11]	iDeal – WAT. Retrieved 3-15-2008 on http://www.ideal.nl/acceptant/?s=wat
[12]	Andrew Tanenbaum, Computer Networks (fourth edition), Prentice Hall, Upper Saddle River, NJ, 2003, ISBN 0-13-038488-7
[13]	Credit card cookie theft 'unlikely'. Retrieved 3-15-2008 on http://news.zdnet.co.uk/Internet/0,1000000097,2075644,00.htm
[16]	Mollie - iDEAL betaalsysteem integreren in uw site. Retrieved 3-15-2008 on http://www.mollie.nl/geavanceerd/ideal/
[17]	40 million credit cards exposed - Security- msnbc.com.Retrieved 3-15-2008 on http://www.msnbc.msn.com/id/8260050/
[18]	Credit Card Fraud Keeps Growing on the Net – International Herald Tribune. Retrieved 1-15-2008 on http://www.iht.com/articles/2007/05/11/news/mcredit.php
[19]	Integratie handleiding iDeal Basic, version 1.3, april 2006. Retrieved 14-2-2009 on http://webdezign.goedbegin.com/clicklink.php?linkid=28
[20]	Concepts against Man-in-the-Browser Attacks (27-1-2007). Philipp Gühring. Retrieved 3-9-2009 on http://www2.futureware.at/svn/sourcerer/CAcert/SecureClient.pdf
[21]	Introduction to SSL. Retrieved 3-14-2009 on http://docs.sun.com/source/816-6156-10/contents.htm

[22]	Webroot: Software | Internet Spyware and statistics about infection rates. Retrieved 3-14-2009 on http://www.webroot.com/resources/stateofspyware/excerpt.html
[23]	Checking account frauds average $1200 per victim | IT Facts. Retrieved 3-15-2009 on http://www.itfacts.biz/checking-account-frauds-average-1200-per-victim/1170
[25]	Mitigating Man-in-the-middle and Trojan Attacks – Best Practices for Combating Emerging Threats with Layered Security. White paper, RSA.inc
[26]	Uw winkel_online – 50 miljoen iDeal transacties in 2012. Retrieved 3-29-2009 on http://www.uwwinkel-online.nl/blog_pakketten_projecten/nieuws_updates/50_miljoen_ideal_transacties_in_2012.html
[27]	Infofilter. Retrieved 4-11-2009 at https://secure.infofilter.nl/InfosecureWWW_tel/php/mijninfofilter.php
[28]	Statistics on payment and settlement systems in selected countries - Figures for 2005 – Netherlands, March 2007. Retrieved 4-12-2009 on http://www.bis.org/cpss/paysys/Netherlands.pdf
[29]	Court filings double estimate of TJX breach. Retrieved 4-25-2009 on http://www.securityfocus.com/news/11493
[30]	RFC 4346 – The Transport Layer Security (TLS) Protocol Version 1

Appendix I. Glossary

Mallory	Mallory is the name given to a fictitious person who wants to hack a security system with the intention to gather personal gain. Mallory is comparable to Eve, except that Eve's only intention is to eavesdrop. The name Mallory is commonly used in literature about computer security, and is derived from the word 'malicious'.
Eve	Eve is the name given to a fictitious person who wants to eavesdrop or rather, wants to read data which is supposed to be secure. She will not modify, substitute or replay old messages.
CVV	Card Verification Value. A CVV is an additional number on a credit card next to the ordinary 16 digit credit card number. This number is used as an additional safety measure against fraud as Mallory now has to obtain the credit card number and CVV to commit fraud.
token	A token is a device used by the client of online banking to sign a nonce. The token makes use of a challenge-response protocol. A token is not uniquely linked to a certain person, it is possible to use somebody else's token. To sign a nonce, the client must insert his personal bank card into the token. The token will then ask the client for his personal identification number (PIN). When the right PIN is provided, the customer must type the nonce (challenge) on the reader. The reader will then show the signed nonce (reponse), a certain number. Because the token only works with the bank card and PIN of the client, It is a strong way to authenticate a person.

Appendix II. List of Figures

Appendix III. iDeal links

The following links are genuine links to an iDeal checkout page.

```
https://betalen.rabobank.nl/ide/qslo.htm?Abs-
Pad=ide/ide.cgi&X009=TOONOFF&X010=0020&X015=&WinVrs=1

https://www.abnamro.nl/nl/ideal/identification.do?randomizedstring=0619843339&trxi
d=50000647713775

https://ideal.fortisbank.nl/UCRSelection.aspx?srp=KsqxLXAK3u&trid=0050000647713827

https://ideal.ing.nl/internetbankieren/SesamLoginServlet?sessie=ideal&trxid=005000
0647715316&random=c74be18c2f2d5770

https://ideal.snsreaal.nl/secure/srb/Pages/Payment.aspx

https://ideal.triodos-onlinebanking.nl/ideal-online/authorise.seam?cid=8283
```

All of these links are the result of checking out the same order at an online shop. These are genuine links, but it is reasonable to assume that Mallory will be able to register a deceptive address like *www.ideal-checkout.com* or something similar.