Display Security for Online Transactions: SMS-Based Authentication Scheme *

[1]Mohammed Alzomai, [1]Bander Alfayyadh, [2]Audun Jøsang
[1]*Queensland University of Technology, Australia*
[2]*University of Oslo, Norway*
m.alzomai, b.alfayyadh {@isi.qut.edu.au}
josang@unik.no

Abstract

Secure online transactions with human users normally require visual display for verifying the correctness of central elements of the transaction before it is submitted. When commodity computer platforms get exposed to the Internet, even for a short period, there is a real and substantial risk that they become infected with malware that can modify anything on the computer, including what is displayed to the user and what is being sent over the Internet. This threat makes visual verification of transaction data unreliable and undermines other security mechanisms used to protect online transactions. This paper proposes a method for display security to make the verification of displayed data in the SMS-based authentication scheme more robust against the threat of compromised platforms.

1. Introduction

Users generally rely on what they see on a computer display to read the output of transactions, to verify that they type correctly, and to ensure that the data being sent through online transactions is according to their intentions. In general, all this depends on the integrity of the computing platform to which the VDU (Visual Display Unit) is connected. In practice it is extremely difficult to assess the integrity of a general purpose computing platform, and thereby to ensure that what the VDU displays is correct [2, 10, 11, 15, 16, 17].

The prospect that the computer display can lie to us is both frightening and real. This problem is amplified by the fact that we often read data from platforms that are not under our control, and that there are financial incentives for trying to manipulate the systems and the way data is displayed.

This paper describes a method for assuring the correctness of displayed data in online transactions, i.e. to ensure that what is displayed on the VDU correspond to what is being transmitted to other parties in online transactions. It assumes that the user has a PDA (Personal Digital Assistant) with integrated camera, OCR (Optical Character Recognition) and communication functions. The method is based on using a portable PDA/camera (e.g. mobile phone) to capture the data from the VDU, recovering the data from the image through OCR, and using an out-of-band channel for matching this data with the data received by the transaction partner. In order to successfully falsify data by attacking the platform integrity, the attacker has to compromise both the client platform and the PDA simultaneously, which is clearly more difficult than to only compromise one of them. Our proposal therefore provides a robust method for verifying displayed data because it is considered hard to simultaneously compromise both platforms.

2. Related Work

A system with display security assurance concept developed by Cronto Limited [12] already exists in the marketplace. However, these systems require that both parties involved in authentication process (i.e. the costumer and bank server) be equipped with proprietary cryptographic tools in order for the system to work, and is based on displaying encrypted data rather than clear text data.

The Cronto system, which is based on a research undertaken at the University of Cambridge, provides a transaction authentication solution for online banking that takes advantage of the camera in the customer's mobile phones. The Cronto solution is based on capturing a visual cryptogram sent by the online bank server and extracting the transaction details from it.

The scheme starts when the customer initiates a new transaction with the online bank. Upon receiving the transaction request, a Cronto server-based software module in the online bank side takes the requested transaction details from the banking application and generates a unique visual cryptogram challenge which hides the transaction details and then passes the cryptogram to the customer for authentication.

The server then validates the client's response and determines whether the transaction should be authorized or not.

(*)International Conference on Internet Technology and Secured Transactions (ICITST2010), London 8-11 November 2010.

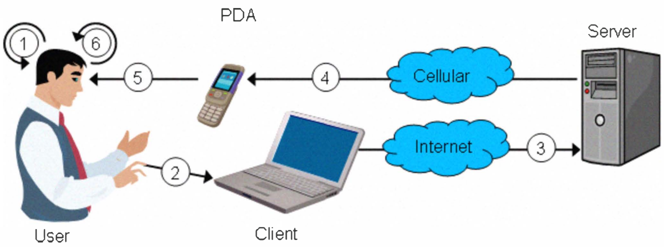


Figure 1. SMS-based transaction integrity check

Table 1. Messages in the SMS-based transaction integrity check scenario

#	Message/Action description
1.	The user types and inspects the transaction data displayed on the client VDU
2.	The user initiates the transaction from the client platform
3.	The transaction data are sent by the client to the server
4.	The assumed transaction data with authorization code are sent as SMS to the user's mobile
5.	The assumed transaction data and authorization code from the SMS are displayed
6.	The user reads the assumed transaction data which enables him to make a conclusion about the integrity of the transaction. In the positive case the user copies and submits the authorization code to confirm the transaction. In the negative case the user aborts the transaction.

At the user side, the costumer uses the camera of his/her mobile equipped with the Cronto client software to capture the visual cryptogram provided by the bank, extract the transaction details from it, verify the transaction details and confirm the transaction by entering a generated code into the client browser.

3. Prior Art: SMS-Based Authentication

A method often used for verifying the correctness of online bank transaction data consists of sending the data with an authorization code by SMS to the user's mobile phone. This enables the user to verify that the transaction data assumed by the bank are according to the user's intentions and to confirm the transaction. For this to work the user must manually copy the authorization code from the mobile phone display to the client platform and submit it to the online bank server as a confirmation of the transaction. The scenario is illustrated in Figure 1, where the numbered circles indicate the sequential order of the actions/messages described in Table 1.

The main advantage of the SMS-based integrity check and authorization is that SMS messages sent from the bank to the user's mobile phone pass through the cellular network, which is separate and independent from the Internet. By verifying the authorization code received from the client platform, the bank can conclude that the user received the SMS message through the cellular network, read it and submitted it through the Internet. This is then interpreted as a genuine intent to confirm the transaction. The security of this scheme is based on the assumption that it is difficult for an attacker to steal the user's personal mobile phone and to attack the cellular network [9].

Assuming a so-called man-in-the browser attack, i.e. that an attacker changes the amount and/or the destination account number by a Trojan program on the client platform, the modified amount and account number will appear in the SMS message. The scheme relies on user awareness, and it is assumed that the correctness of the amount and of the destination account number is verified by the user before copying the authorization code from the SMS message. Assuming that the user verifies the correctness of the amount and of the bank account number in the SMS message, this scheme is secure against attacks on the client platform, and is in fact independent of the security of the client platform. This represents a considerable security improvement. However, if a user victim fails to notice that the bank account number in the SMS message is not the same as the intended account number, the attack will succeed.

While the mental load of verifying the correct amount and destination account specified by the SMS message is probably acceptable for a single transaction, the repeated process of verifying the same for each transaction can be quite tedious and therefore lead to user apathy. It has been noted that when faced with a frustrating security task, users may usually bypass or ignore that task [1, 5, 14].

In an experiment [3] we studied the usability of the SMS-based authorization scheme by observing whether users are able to perform the extra tasks of verifying the correctness of transaction detail. This is important because banks would normally assume that users are responsible for transactions authenticated with the authorization code. However, if a significant proportion of users are unable to use the method correctly, this assumption would be unreasonable and should be reassessed by the banks.

According to the study [3] about 21% of realistic attacks were successful, meaning that 21% of the users failed to notice that half the digits in the destination account number had changed. This in our opinion represents an inadequate level of security for the SMS based authorization system. The study also found that a *stealthy attack*, where only one out of eight digits of the destination account number is altered, was successful in 61% of the attacked transactions. This shows that as the number of altered digits decreases the success rate of attacks increases. In general this reflects a fundamental limitation in the user's ability to reliably verify long strings of data. The validation process will even be more difficult with the trends to use the International Bank Account Number (IBAN). The IBAN is an international standard for identifying bank accounts aiming at minimizing the risk of propagating transcription errors and can consist of up to 30 digits.

To enhance the SMS-based authentication scheme without compromising the strong authentication process of validating every transaction, the validation process has to be automated. The burden caused by the extra task of validating every transaction in a sufficient manner can be shifted to the mobile phone. The user will never need to manually revalidate the correctness of the transaction details after they have been typed on the client terminal; instead the verification process can be executed by the mobile phone. The next section describes the system outline of the proposed scheme.

4. The Display Security Architecture

The main idea of the new enhanced scheme is to use a personal portable platform that is able to convert the analogue visual representation of a transaction data from the VDU into its original digital representation using OCR (Optical Character Recognition) software. The conversion from analogue to digital form first requires the analogue optical image emitted from the VDU to be captured by a digital camera. The bitmap representation of the analogue image produced by the digital camera is then translated to a digital data representation by an OCR.

To be more precise, the idea is to check the transaction data received through e.g. an SMS message against the trusted transaction data extracted from the analogue visual representation of a transaction data. So, when the user starts a transaction involving a bank account and receives a confirmation SMS from the bank, a validation application on the PDA will be activated to validate the transaction details. The validation application will compare the received transaction data in the SMS against the data extracted from the analogue photo. As a result of the comparison, the PDA will either display a message confirming validity or display a message warning the user about invalid transaction data.

4.1. Scenario

The proposed scenario is a modified version of the SMS-based authorization scheme illustrated in Figure 1 and Table 1. In the new scenario, we have substituted steps 5 and 6 with the new steps 5, 6, 7, 8, 9, and 10 to allow the auto validation process of the transaction data. In the new steps, the PDA checks the transaction data received in the SMS against the transaction data extracted from the analogue visual representation of the transaction data in the display of the client platform. Also, the PDA will signal the success or failure of the comparison to the user who can then make a conclusion about the integrity of the transaction data.

The scenario is initiated by the user, and the result enables him to make a conclusion about the security of the displayed data. The scenario is illustrated in Figure 2 where the numbered circles indicate the sequence of messages and actions described in Table 2.

4.2. Practical Aspects

Mobile phones commonly have integrated digital cameras, so that they already have the necessary functional basis for the proposed method. The inclusion of software for the OCR and for comparing transaction data is all that is needed.

Commercial and open source OCR software packages are available. In its simplest form, OCR software takes scanned documents and converts them into text files. More advanced graphical layout of digital documents will require a standard for geometrically formatting documents so that the translation from analogue bitmap format to digital document format is unambiguous.

With current technology, many mobile phones are equipped with OCR capabilities. As an example, Figure 3 shows a screen shot of a sample transaction taken from a simulated Web page of a real bank (The commonwealth bank, Australia). It displays the transaction details of a funds transfer to be transmitted to the online bank.

Figure 4 shows a snapshot photo of a simulated portion of the bank Web page that shows the transaction details to be verified. The photo is taken by an iPhone 3GS mobile with OS version 3.1.2 and is equipped with an auto focus 3 mega pixels camera [6]. Figure 5 shows the transaction text data resulting from applying an OCR function on the photo of Figure 4 executed by one of the iPhone's OCR applications called *ocrNow!* that converts images

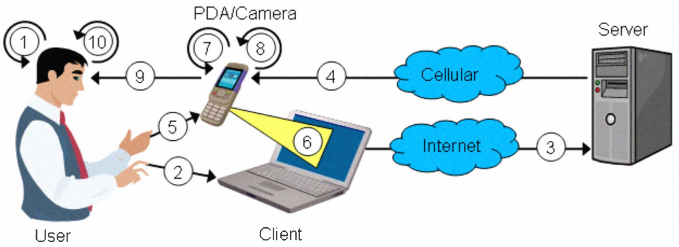
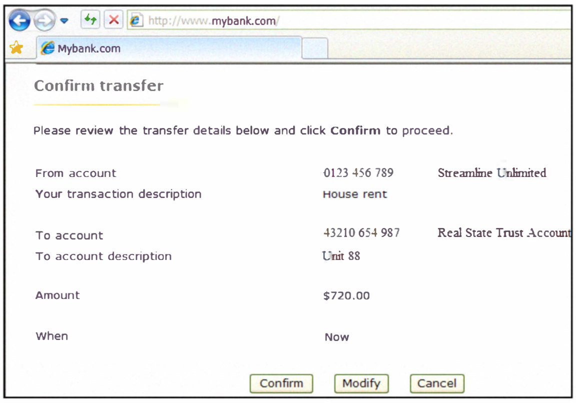


Figure 2. Scenario for the display security architecture

Table 2. Messages and actions in the display security architecture

#	Message/Action description
1.	The user types and inspects the transaction data displayed on the client VDU
2.	The user initiates the transaction from the client platform
3.	The transaction data are sent by the client to the server
4.	The assumed transaction data with authorization code are sent as SMS to the user's mobile
5.	The user activates the camera function on the PDA
6.	A photo is taken of the ASCII text displayed on the VDU
7.	The OCR function in the PDA recovers the ASCII text from the photo
8.	The PDA compares the transaction data from photo and from server
9.	The PDA signals the success/failure of the comparison to the user
10.	The user receives the signal from the PDA and can make a conclusion about the integrity of the displayed/transmitted transaction data.

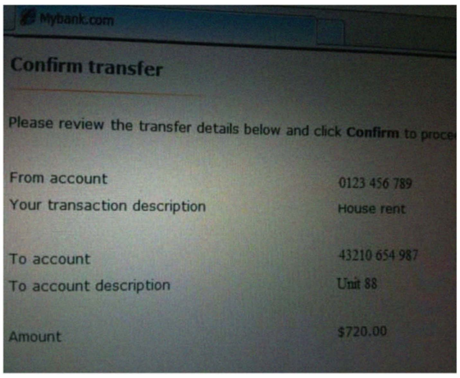


Confirm transfer

Please review the transfer details below and click Confirm to proceed.

From account	0123 456 789	Streamline Unlimited
Your transaction description	House rent	
To account	43210 654 987	Real State Trust Account
To account description	Unit 88	
Amount	$720.00	
When	Now	

Figure 3. Ascreenshotofatransactiondata



Confirm transfer

Please review the transfer details below and click Confirm to proce

From account	0123 456 789
Your transaction description	House rent
To account	43210 654 987
To account description	Unit 88
Amount	$720.00

Figure 4. Aphotoofatransactiondata

photographed on the iPhone camera into text [8]. Many other mobile application with built in OCR capabilities are available.

4.3. Security Analysis

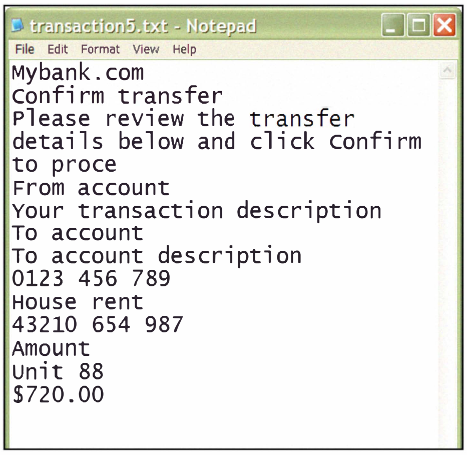
The security of the proposed system requires that the client platform and the PDA are not both compromised simultaneously. However, assuming that the client platform and the PDA have not both been compromised simultaneously, it is possible to verify that the PDA indeed provides the necessary elements for a robust transaction data verification process.

Assuming that the client platform has been compromised, so that the wrong transaction data is sent in message (3), the comparison between the received transaction data in the SMS and the digital data converted from the analogue image by the PDA in step (8) will fail, so that the PDA will signal that the transaction data have been altered.

If the PDA is compromised alone, this will not affect the system security since the client platform will transmit the correct transaction data. However, it is possible that the PDA generates a false alarm.

Let us now consider the possible consequence of a double compromise, i.e. that the client platform has been compromised so that it sends the wrong transaction data to the server in (3), and that the PDA has been compromised so that it wrongfully validates the transaction data in step (9). In this case, the user will instruct the client platform to confirm the altered transaction, so that the attack will succeed.

It thus requires simultaneous compromise of the client platform and the PDA in order to break the security of our system.



```
Mybank.com
Confirm transfer
Please review the transfer
details below and click Confirm
to proce
From account
Your transaction description
To account
To account description
0123 456 789
House rent
43210 654 987
Amount
Unit 88
$720.00
```

Figure 5. Text data resulting from converting a transaction image

The strength of the proposed system is based on minimizing attack possibilities and managing the risk. Attacks are reduced by separating the transaction validation process (executed in the PDA) from the transaction execution process which is performed in the client platform.

4.4. Advantages and Disadvantages

The advantage of the proposed method is that the visual comparison of transaction data intended by the user and assumed by the server is automated, and that this validation process is separated from the client platform where the transaction is managed. Commodity client platforms are typically designed with priority on flexibility and functionality, which unavoidably results in security vulnerabilities.

The security property is based on using a digital camera which ”sees” the digital transaction data to be transmitted exactly as the user sees it. The bitmap image is then converted to the original digital data using OCR techniques. This bridges the semantic distance between the digital data in its binary form and the analogue visualisation of the data. It basically guarantees that what you see is what you intend to transfer.

The security of the proposed method only depends on either the client platform or the PDA being secure. In fact, one of them can be compromised without causing a risk of tricking the user into confirming online transactions to the fake accounts, so the security of our method is independent of the security of the client platform. The PDA can be designed with priority on security, and with limited functionality and flexibility. The PDA is controlled by the user, so he does not have to rely on systems outside his control when confirming financial transactions. This feature will allow mobility where users can apply the new method to any system anywhere as long as the system is able to connect to the online bank and execute financial transactions.

4.5. Usability Analysis

The usability of the proposed system is tested against a set of security usability principles defined in [4]. These principles describe user interaction with security systems in terms of usability.

The security usability principles are divided into principles for security action and security conclusion which can be described as follows:

- A *security action* is when users are required to produce information and security tokens, or to trigger some security relevant mechanism. For example, typing and submitting a password is a security action.
- A *security conclusion* is when users observe and assess some security relevant evidence in order to derive the security state of systems.

The eight security usability principles are:

1. Security Action Usability Principles
   a. The users must understand which security actions are required of them.
   b. The users must have sufficient knowledge and the practical ability to make the correct security action.
   c. The mental and physical load of a security action must be tolerable.
   d. The mental and physical load of making repeated security actions for any practical number of transactions must be tolerable.

2. Security Conclusion Usability Principles
   a. The user must understand the security conclusion that is required for making an informed decision. This means that users must understand what is required of them to support a secure transaction.
   b. The system must provide the user with sufficient information for deriving the security conclusion. This means that it must be logically possible to derive the security conclusion from the information provided.
   c. The mental load of deriving the security conclusion must be tolerable.
   d. The mental load of deriving security conclusions for any practical number of service access instances must be tolerable

In the SMS-based authentication scheme described in Section 3, the mental load of repeatedly verifying several account numbers may violate principle 1d and represent a usability concern. As the experiment conducted in [3] showed, users were vulnerable to attacks due to this usability problem.

In the proposed system, usability is improved by delegating the account-number verification task to the PDA, the user only has to interpret the result of the comparison between the OCR generated file and the SMS received from the server. Clearly, this is an easier task to perform than comparing lengthy alpha-numeric numbers.

If the user performs repeated transactions which will require taking many snapshots of the VDU, this may become a usability issue but to a lesser extent than the issue associated with the SMS-based transaction authorization scheme. Taking several snapshots is less of a mental load than several comparisons of lengthy alpha-numeric numbers.

A possible way to improve the usability of this scheme even further is discussed in Section 7.

5. Discussion

In contrast to the Cronto system described in section 2, our proposed solution enhances the SMS-based authentication without the use of additional cryptography and can be applied directly at the costumer side without making any changes at the server side.

The practicality of our proposed solution depends extensively on the capability of the mobile phone scale camera to take good images of the transaction data displayed in the client VDU as well as the integrity of the OCR system that converts these images into text format.

Because taking a good photo of the visual display could easily become a non-trivial task, we examined the integrity of the proposed solution. The example illustrated in Section 4.2 was undertaken repeatedly (60 times) by different people (12 participants) and the successful rate of converting the transaction data from the graphical format to a valid text format was around 82% (49 out of 60). This indicates that one out of five attempts to take a snapshot of the transaction details displayed in the client VDU will result in an image that will not convert to a valid transaction data text. However, with advancing technology, we expect that the successful conversion rate will continue to increase. As an example, the camera used in the practical experiment was an iPhone 3GS camera with limited specs as compared to the lately announced new generation of iPhone 4 auto focus 5-megapixel still cameras which can take more quality photos [7].

The separation of the functionality in the PDA from that on client platform gives the SMS-based authorization scheme its security strength but with current technology it would also be possible for attackers to control the PDA and gain access to its data. In fact, a perfectly secure system will never exist and there will always be weaknesses. For example, attackers can get access to the PDA if it is connected to the Internet or if its Bluetooth is enabled i.e. making it available for a connection. The relatively new attack known as *blue snarfing*, for example, allows intruders to gain access to Bluetooth enabled phones by exploiting a security flaw in the wireless protocol [13].

6. Conclusion

In this paper a new solution aimed at improving the overall security of online transactions by providing display security has been proposed. This removes the cognitive burden of e.g. manually validating every transaction by visual comparison of transaction data in SMS-based authorization schemes.

Current display security technologies are not able to provide high assurance of the integrity of displayed data. We have shown that it is possible to make the security of displayed data independent of the security of the client platform. This is achieved by using a mobile phone equipped with a camera in parallel with the client platform when executing online transactions. The display security is based on using a digital camera which "sees" the displayed transaction data exactly as the user sees it. The bitmap image of the transaction data is then converted back to the original digital form using OCR techniques, so that the displayed transaction data can be automatically compared with those received through SMS from the bank.

7. Future Work

A usability concern arises when users need to perform several transactions and repeatedly photograph the VDU and validate each transaction. Usability can be enhanced by minimizing the number of transactions the user needs to validate. As an example, a combined system of our proposed solution and the scheme proposed in [4] can enhance the scheme usability. The scheme works by maintaining several lists of accounts in the PDA generated from previous transaction. Examples of these lists are "Trusted Accounts list", "Malicious Accounts list", etc. The PDA would look into these lists first for comparison with the server's SMS before looking for a new OCR file. As the user continue to use the system, this can significantly reduce the number of snapshots a user needs to take and will not undermine the concept of verifying transaction data on an individual basis as every transaction data is checked by the PDA either against the trusted accounts list (which is separate and independent from the client terminal) or by a new OCR.

8. References

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] A. Alsaid and C. Mitchell. Dynamic Content attacks on Digital Signatures. *Information Management & Computer Security*, 13(4):328–336, 2005.

[3] M. Alzomai, B. Alfayyadh, A. Josang, and A. McCullagh. An experimental investigation of the usability of transaction authorization in online bank security systems. In Ljiljana Brankovic and Mirka Miller, editors, *Sixth Australasian Information Security Conference (AISC 2008)*, volume 81 of *CRPIT*, pages 65–73, Wollongong, Australia, 2008. ACS.

[4] M. Alzomai, Audun Josang, Adrian McCullagh, and Ernest Foo. Strengthening sms-based authentication through usability. In *ISPA '08: Proceedings of the 2008 IEEE International Symposium on Parallel and Distributed Processing with Applications*, pages 683–688, Washington, DC, USA, 2008. IEEE Computer Society.

[5] D. Balfanz, G. Durfee, D. K. Smetters, and R. E. Grinter. In search of usable security: five lessons from the field. *Security and Privacy Magazine, IEEE*, 2(5):19– 24, 2004.

[6] Apple Inc. iPhone-3gs specs. http://www.apple. com/iphone/iphone-3gs/specs.html, August, 2010.

[7] Apple Inc. iPhone4 specs. http://www.apple. com/iphone/specs.html, August, 2010.

[8] Wordcraft international limited. *ocrNow!*, an OCR iPhone's application. http://www.wordcraft. com, August, 2010.

[9] A. Jøsang, M. Alzomai, and S. Suriadi. Usability and Privacy in Identity Management Architectures. In *The Proceedings of the Australasian Information Security Workshop (AISW), CRPIT Volume 68*, Ballarat, Australia, January 2007.

[10] A. Jøsang, D. Povey, and A. Ho. What You See is Not Always What You Sign. In *Proceedings of the Australian UNIX and Open Systems Users Group Conference (AUUG2002)*, Melbourne, September 2002.

[11] K. Kain, S.W. Smith, and R. Asokanm. Digital Signatures and Electronic Documents: A Cautionary Tale. In *Proceedings of IFIP Conference on Communications and Multimedia Security.*

[12] Cronto Limited. The Cronto system. http://www. cronto.com, August, 2010.

[13] S. Pradhan, E. Lawrence, and A. Zmijewska. Bluetooth as an enabling technology in mobile transactions. In *ITCC '05: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) -Volume II*, pages 53–58, Washington, DC, USA, 2005. IEEE Computer Society.

[14] M.A. Sasse. Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI2003), (Workshop on Human-Computer Interaction and Security Systems)*, 2003.

[15] K. Scheibelhoferm. Signing XML Documents and the Concept of What You See Is What You Sign. Masters thesis, Graz University of Technology, Austria, 2001.

[16] Adrian Spalka, Armin B. Cremers, and Hanno Langweg. The fairy tale of 'What You See Is What You Sign - Trojan Horse Attacks on Software for Digital Signatures. In *IFIP Working Conference on Security and Control of IT in Society-II (SCITS-II)*, Bratislava, Slovakia, June 2001.

[17] Arnd Weber. See What You Sign: Secure Implementations of Digital Signatures. In *Proceedings of the International Conference on Intelligence and Services in Networks*, pages 509–520, 1998.