What You Enter Is What You Sign: input integrity in an online banking environment

Sven Kiljan, Harald Vranken & Marko van Eekelen

sven@kiljan.org
www.kiljan.org

18 July 2014
Introduction

- Sven Kiljan

- PhD student at Open Universiteit, the Netherlands

- Research: improving technical security in online banking
Introduction to KVDB

- Kennisprogramma Veiligheid Digitaal Betalingsverkeer (KVDB) ('knowledge program safety digital payment traffic')
  - Goal: to improve security of and trust in online banking
  1. Cybercriminal organizations
  2. Self-reliance of bank customers
  3. Technical security
  4. Public-private cooperation
Before we really start: some questions for the room

• Who does NOT conduct online payments?

• Who feels safe and secure when making online payments?

• It makes me uncomfortable from a usable security and convenience perspective. Let me show you by making one single online payment.
Ziet u iets ongewoons? Stop en bel 0900 0905.
Mededelingen

Onderhoud Rabo Internet- en Mobielbankieren en iDeal
Rabobank Internet- en Mobielbankieren en iDeal zijn vanwege onderhoud op zondag 15 juni van 01.00 tot 08.00 uur niet beschikbaar. Vanaf 08.00 uur zijn Rabobank Internet- en Mobielbankieren en iDeal weer beschikbaar.

U kunt deze informatie ook nalezen bij Betalen & Sparen onder Mededelingen.
Conducting an online payment
## Nieuwe opdracht

### Van rekening

<table>
<thead>
<tr>
<th>Selected Account</th>
<th>S.Z. Kiljan</th>
</tr>
</thead>
</table>

### Bedrag

- **EUR**: 10

### Naar IBAN / rekeningnummer

- **NL10 BANK 1234 5678 90**

### Ten name van

- **U. R. Recipient**

### Vestigingsland bank

- **Nederland**

### Omschrijving

- **The description of my payment to you.**

### Betalingskenmerk acceptgiro

- [ ]

### Periode

- **Eenmalig**

### Uitvoerdatum

- **18-06-2014**
## Conducting an online payment

### Random Reader


- Plaats uw **bankpas** in de Random Reader
- Druk op S (signeren)
- Toets uw **pincode** in en druk op **OK**
- Toets het controlegetal **51584 64001** in en druk op **OK**
- Als het totaal van alle bedragen klopt, toets dan de **twee cijfers vóór de komma van het totaal** in, druk op **OK** en nogmaals op **OK**

Vul de signeercode in die op uw Random Reader verschijnt:

### Totaal van alle bedragen

<table>
<thead>
<tr>
<th>Van rekening</th>
<th>Begunstigde</th>
<th>Datum</th>
<th>Bedrag</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NL10 BANK 1234 5678 90</td>
<td>18-06-2014</td>
<td>EUR 10,00</td>
</tr>
</tbody>
</table>

**Totaal van alle bedragen**

| EUR | 10,00 |

---

**Demo**

Waarom en hoe maakt u een digitale handtekening?

› Bekijk de demo

---

Ga alleen verder als de adresregel begint met https://bankieren.rabobank.nl/...

› Hoe controleert u de veiligheid van uw verbinding?

› Lees meer over veiligheid
Before we really start: some questions for the room

• Who does NOT use online banking to conduct online payments?

• Who feels safe or secure when making online payments?

• It makes me uncomfortable from a usable security and convenience perspective. Too many distractions to do MY job!

• Compare:

Slide 10
Different views concerning security actions by users

• Several ways to look at this (Herley, 2009)
  – Psychological: users are hopelessly lazy
  – Social: security tasks are not usable enough and too cumbersome, user education is key
  – Economical: users’ rejection of security advice is equal to the observed economical loss
    • For example, there is less incentive to increase vigilance when banks reimburse damages due to online banking attacks on customers

• I think all views have some truth to them, and new proposals should keep them all in mind.
So that was our warm up. What will this talk be about?

- Authentication in online banking
- How malware attacks work around existing authentication schemes
- What You See Is What You Sign: a new authentication scheme introduced by banks
- What You Enter Is What You Sign: our proposal for an alternative authentication scheme
Authentication in online banking

- **Authentication, what is it? To proof by...**
  - Something you know (passwords, PINs...)
  - Something you possess (card, mobile device...)
  - Something you are (biological and behavioral characteristics)

- **Entity authentication**
  - Authenticates entities, such as people: proof who you are
  - Do when starting an online secure session with a bank

- **Transaction authentication**
  - Authenticates information: proof what you (want to) do
  - Do when making online payments
Authentication in online banking

• Transaction authentication
  – What is a transaction (or rather, a transaction request)?
    • Critical data: destination account number, amount, currency...
    • Less-critical data: name of recipient, description...
  – What makes a transaction authentic?
    • A transaction is authentic if a legitimate party (such as the account holder) deliberately created it
    • To be able to proof that a transaction is authentic, the creation process and the integrity of transactions must be protected between the legitimate party and the bank
Authentication in online banking

• Popular examples of traditional authentication methods from the last decade (Claessens et al., 2002, Kiljan, et al., 2014)
  – One-time passwords, also called transaction authentication numbers (TAN)
  – Mobile TAN (by text message)
  – Challenge-response

• These are all adequate for entity authentication, but not transaction authentication
  – There is quite a high level of certainty that a legitimate user is involved
  – There is no certainty that the legitimate user deliberately created transactions when these authentication methods are applied
Using traditional transaction authentication

Alice

Alice's computer

Internet

Bank computer

Bob

123456789

Charlie

987654321

Token

D1: 123456789, S1: € 500
D2: 987654321, S2: € 100

D1: 123456789, S1: € 500
D2: 987654321, S2: € 100
Malware attack on traditional transaction authentication

- Alice
  - Computer
  - Transaction 1: D1: 123456789, S1: €500
  - Transaction 2: D2: 987654321, S2: €100

- Bob
  - Transaction: D1: 123456789, S1: €500

- Charlie
  - Transaction 1': D1': 321654987, S1: €500
  - Transaction 2: D2: 987654321, S2: €100

- Mallory
  - Token: 321654987
  - Malicious activity detected

- Internet
  - Bank computer

- Open Universiteit
  - www.ou.nl
An overview of the malware threat

- The bank knows the user is involved due to entity authentication, but the information flow between user and bank is vulnerable due to a lack of transaction authentication.
So traditional authentication methods are vulnerable to malware attacks. Now what?

- Banks apply back-end pattern-based recognition of fraudulent transactions in different ways, so not all hope is lost.
- Still, knowing whether incoming information was deliberately created by the user and not a man-in-the-middle aids in recognizing fraudulent transactions.

Transaction information attack surface

- Confidentiality protection
- Integrity protection

Legend
- Alice
- Alice's computer
- Internet
- Bank computer
- Bank employees
- Transaction information
- Token
What You See Is What You Sign: a new authentication scheme by banks

- Banks: let the user verify the information we receive on correctness to secure the information flow’s integrity

Transaction information attack surface

Confidentiality protection

Integrity protection

Alice’s computer

Internet

Bank employees

Transaction verification device

Alice’s computer

Internet

Bank employees

Transaction verification device
Transaction information (for a set of transactions)
1. Entered by customer
2. Possibly modified by customer's computer
3. As received by the bank (secure channel)
4. Shown to customer for verification
5. Customer's decision: accept or reject (secure channel)
What You See Is What You Sign: a new authentication scheme by banks

Alice

Alice's computer

Bank computer

Legend of information flows

Regular information flow

Optionally use one or more traversed devices to forward messages

Transaction verification device

From original source of information (as sent in step 1)

Result (step 5)

From transaction verification device (as received in step 4)

D1: 213243546, S1: € 500
D2: 123456789, S2: € 100

D1: 213243546, S1: € 500
D2: 123456789, S2: € 100

Slide 22
What You See Is What You Sign: a new authentication scheme by banks

Legend of information flows

- Regular information flow
- Optionally use one or more traversed devices to forward messages

Transaction verification device

From original source of information (as sent in step 1)

Result (step 5)

From transaction verification device (as received in step 4)

<table>
<thead>
<tr>
<th>D1</th>
<th>S1</th>
<th>S2</th>
</tr>
</thead>
<tbody>
<tr>
<td>213243546</td>
<td>€500</td>
<td></td>
</tr>
<tr>
<td>123456789</td>
<td></td>
<td>€100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D1</th>
<th>S1</th>
<th>S2</th>
</tr>
</thead>
<tbody>
<tr>
<td>292685316</td>
<td>€500</td>
<td></td>
</tr>
<tr>
<td>123456789</td>
<td></td>
<td>€100</td>
</tr>
</tbody>
</table>
What You See Is What You Sign: comparing numbers is quite similar to...

- You will have to do this frequently
- We will not tell you about how many differences there are (if any at all)
- There are actually 15 differences in this figure

Figure by Jan Pieńkowski (2000)
Traditional and WYSIWYS compared

Transaction information attack surface

Confidentiality protection

Integrity protection

Traditional transaction authentication

What You See Is
What You Sign-based transaction authentication
What You See Is What You Sign
How secure is it?

- Assuming a correct implementation, everything can be quite secure from a technical perspective.

- However, security is more than technology, especially if you place an extra burden on the user.

- Remember the earlier discussed views:
  - Psychological: users are hopelessly lazy.
  - Social: security tasks are not usable enough and too cumbersome, user education is key.
  - Economical: users’ rejection of security advice is equal to the observed economical loss.
What You See Is What You Sign
How secure usable is it?

- From a usability perspective, this is not a usable and therefore not a secure solution at all!

- 21% of attacks against the user’s ability to recognize significantly changed account numbers succeed (AlZomai, et al., 2008)
  - This was surveyed in a controlled environment over a limited time span
  - We think that this rate will be higher when users work with the system for a longer period of time
What You See Is What You Sign
How secure usable is it?

Transaction information

Transaction information and verification code

Verification code

Decision 1

Decision 2
Not deliberate!
What You See Is What You Sign
How secure usable is it?

- The main flaw of using What You See Is What You Sign is that it merely moves the problem to the user, thereby presenting a critical moment where users can slip-up easily.

- We should not accept ‘user errors’ as a source of security problems if a system makes insecure behavior easy and attractive (Zurko, 2005).
Our proposal for an alternative authentication scheme

- The natural way to use a system should be the secure way (Yee, 2002), so this is not secure:

  What You See Is What You Sign

  Decision 1

  What You Enter Is What You Sign

  Decision 2

- A user expresses his or her desire to create a transaction by entering information in a system (the natural way)
Our proposal for an alternative authentication scheme

What You Enter Is What You Sign

Transaction information (for each critical value)
1. Entered by customer (deliberate decision)
2. Forwarded by customer's computer (secure channel)
3. Received by the bank (secure channel)
4. Result
5. Result
What You Enter Is What You Sign: our proposal for an alternative authentication scheme

Transaction information attack surface

Confidentiality protection

Integrity protection

Alice

Alice’s Internet computer

Bank computer

Bank employees

Critical transaction information

Critical transaction information

Digital signature
Possible implementations

- As a keyboard-like peripheral (for PC’s)
  - Concept device is known as ‘Trusted Entry Pad’

- As a separate, disconnected device (for mobile devices)
  - The base of a prototype for such an authentication device can be a smartphone

- Embedded in a Trusted Execution Environment (TEE)
Further research

• A sophisticated comparison (for security and usability) of possible implementations has not yet been made
  – Also important for any implementation is affordability. If an implementation is not affordable now, when will it be?

• A formally tested security protocol has not yet been made

• We have not done any usability tests
  – In some possible implementations a separate input device is suggested. IBAN account numbers can use alphanumerical characters, which present a usability challenge.

  FR14 2004 1010 0505 0001 3M02 606
  MT84 MALT 0110 0001 2345 MTLC AST0 01S
  QA58 DOHB 0000 1234 5678 90AB CDEF G
Limitations

- An implementation of our proposal by itself does not protect against social engineering attacks (such as ‘phishing’), which might still be assisted by malware
  - Determining the influence of unambiguous labels, functions and warnings on short and long term user behavior might provide valuable information on whether this can aid against social engineering
Related work

- **hPIN/hTAN, by Li, et al. (2012)**
  - Offers a secure display to verify critical data as it is entered using an insecure input method by the user.
  - Forwards the data to the bank using a secure channel after secure (one button) confirmation by the user.

  - Can be adjusted to prototype What You Enter Is What You Sign.
Conclusion

• Transaction authentication methods potentially offer more security when they are suited to a user’s needs and capabilities. We have to keep in mind that:
  – Users are lazy, so we have to deal with it by making security tasks usable and not too cumbersome.
  – What You See Is What You Sign can be secure from a technical perspective, but is not usable and therefore not secure from a usability perspective. It puts users in a cumbersome position which makes it easy and attractive to reject security advice. This makes it impossible to authenticate transactions which the user deliberately makes.
  – What You Enter Is What You Sign is a first step in introducing added security to transaction authentication without placing an additional burden on the user. It does this by relying on actions which the user has to do deliberately.

• Thank you for your attention. Are there any questions?


