

Optimising authentication features in the web browser

Dieter R. Bartl and Matthias Stoffel

{ Dieter.Bartl, Matthias.Stoffel } (at) SIZ.de

SIZ - Informatikzentrum der Sparkassenorganisation GmbH

Simrockstraße 4 - 53113 Bonn – Germany

Over the last two years, phishing has become a permanent threat, with bank customers particularly at risk. Phishing criminals use emails to lure customers to expertly faked bank web servers. Any personal details entered on these fake web sites are forwarded to the frauds who are then able to use the information for unauthorised transactions.

Phishing targets the weakest link in the chain, the customer. Despite increased awareness, we have to assume that customers will keep following phishing mail instructions and ultimately visit fake web servers. What is critical here is whether the customer is able to distinguish the original from the fake and actually checks for the differences. These two issues are reflected by the questions web browser vendors are asked:

- Do users actually use these features to verify the identity of a web server?
- How fake-proof are browser authentication features used to identify a web server?

Keeping these two issues in mind, we will outline aspects and requirements for improving web browser authentication features and user acceptance of these features.

1. Web browser authentication features

The first question is how a user can verify whether he has displayed the web page he wanted to display in his browser. Browsers offer a variety of possibilities for this purpose (see Figure 1)¹:

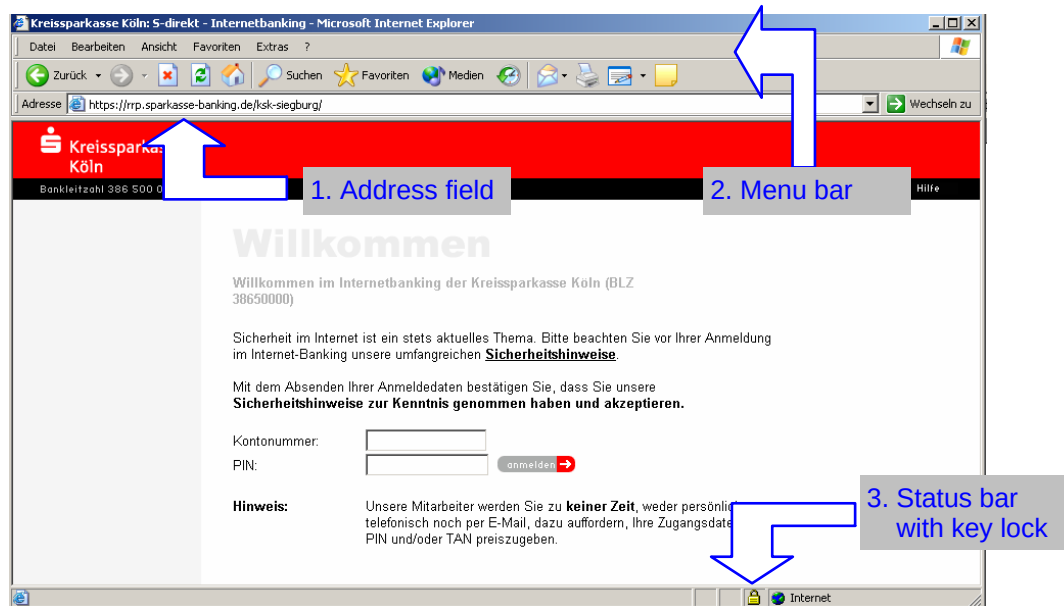


Figure 1: Web browser authentication features

1. Address field: Displays the URL of the web page
2. Menu bar: Displays properties/information of a web page
3. Status bar with key lock: Displays a secure HTTPS connection
4. Key lock properties: Displays certificate properties (see Figure 2)

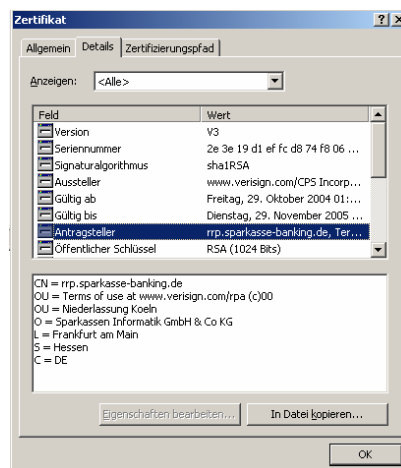


Figure 2: Displaying certificate properties by clicking on the key lock

¹ The screenshots were created using Microsoft Internet Explorer. Other browsers provide similar views.

2. User acceptance of authentication features

One of the most important aspects for assessing the effectiveness of the authentication features is user acceptance. Feedback from “Sparkassen-Finanzgruppe” (German Savings Banks Organisation) customers has shown that not all authentication features are equally accepted. Some of these features are unknown, some are too inconvenient to use. So, the effectiveness of these features can be derived from their familiarity and acceptance. Features can be roughly classified as follows:

	Familiarity	Use	Effectiveness
Address field	High	Frequent	High
Menu Bar	Low	Rare	Low
Key lock	Medium	Frequent	Medium
Key lock properties	Low	Rare	Low

3. Ways to falsify authentication features

Phishing attacks try to deceive customers by creating web sites which resemble the originals as closely as possible. This approach is also referred to as visual spoofing. Over time, the approach has evolved: In the past, frauds only imitated the web page contents of the original servers. For example, page layout, logos and text were copied from the originals. As customers have been made aware of these methods, frauds have begun to falsify the authentication features of the web sites as well.

The address bar is frequently used to deceive users. Various techniques are employed to produce the fakes:

- domains with similar names
 - o other top-level domains (e.g. savingsbank.info)
 - o transposed letters (e.g. savnigsbank.com)
 - o letters which look similar (e.g. savlngsbank.com)
 - o internationalised domain names (e.g. cyrillic "a")
- Java script is used to obscure the address field

But the other features, specifically the key lock, are also falsified more and more often. For this purpose, the capability offered by many browsers to open an empty window which does not include the features above is exploited. For example, such a window may be opened using JavaScript². To fake this window, the authentication features are displayed as graphics in the HTML page.

The display of the certificate's properties produced by clicking on the key lock may also be falsified. A fake can also be created using JavaScript, with a copy of the certificate properties displayed in the original page inserted as a graphic.

As a result, it must be said that fakes are hard to recognise even for customers who are aware of the problem.

² <Script language=JavaScript> window.open(“Empty_Window.html”,”, “toolbar=no, location=no, directories=no, status=no, menubar=no, scrollbars=yes, resizable=yes, copyhistory=yes”); </script>

Fake techniques can be classified as follows:

	Complexity of the fake	Effect of the fake	Risk
Address field	Low	High	High
Menu Bar	High	Medium	Medium
Key lock	Low	High	High
Key lock properties	High	Medium	Medium

In the past, malware has also been used to create fakes. The malware modifies HTML content of bank pages on infected customer PCs to deceive customers. Authentication features remain unchanged in this case.

4. Optimisation approaches

To work against the threat of faked web-sites, two main demands are necessary:

- Technical possibilities for creating fakes must be reduced.
- Users should be offered authentication features they can accept.

The following areas offer potential for optimisation:

- Standardising authentication features (address field, status bar with key lock) by all web browser vendors as a non-alterable component of each browser window.
- Optimising the display of the certificate properties with respect to the finger print (e.g. words instead of hexadecimal figures)
- Incorporating new standardised authentication features for e-business pages controlled by a central or custom whitelist (e.g. traffic lights)
- Incorporating specific authentication features stored for and displayed to users by the web site operator for certain web pages (shared secret)
- Including an option for starting the browser with a higher security level with fewer technical features.

5. Conclusion

With the advent of massive phishing attacks, it is increasingly important for users to recognise whether a web page they open in their browser is authentic or faked. While web browsers are capable of verifying web page authenticity, these capabilities do not work for two reasons:

1. Authentication features implemented in web browsers to date are not known to all users, require technical expertise and sometimes complex procedures. This is why acceptance is low.
2. Authentication features can be faked and fakes are also difficult to recognise.

For these reasons, dangerous phishing attacks causing financial damage will continue. This will damage the reputation of e-business and the internet as a whole.

To counteract this problem, browser vendors need to create new, optimised and standardised authentication features which will be difficult to fake and will be accepted by users. In addition, users must be made aware of these issues and helped to feel confident about using authentication features.