Trust & Usability on the Web, a Social/Legal perspective

Rigo Wenning, W3C Legal counsel, Bert Bos, W3C, Style Activity Lead

Version: final
January 21, 2014

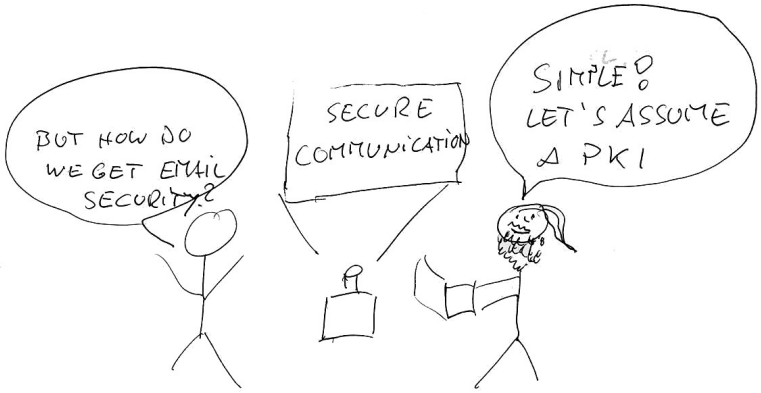

Figure 1: Let's assume a PKI

Abstract

There is no doubt that the user interface of TLS in browsers needs serious improvement. But we also have to challenge the thought model that currently determines how we do transport security and its interface in the browser. The author suggests a user centric approach.

1 Looking at the Workshop page with Chromium

Have you ever tried to understand what the security symbols in your browser actually mean? We started off with padlock symbol. And we have heard a lot of criticism of the padlock symbol. There is a vulnerability indicated in the Web Security Context User Interface Guidelines (2010)[1], that a favicon could be used to mimic a padlock to fool the user into believing the site uses TLS/SSL. So nowadays, some browsers display names of companies. This was a first step. It is time to look again how the market has evolved and whether the security implementations actually address questions that the user may have.

Lets say a user surfs to a web page and wants to know whether the site is securely usable. Going to the STRINT Workshop homepage, my browser indicates with a padlock that the site uses TLS. The progress in Chromium seems to be that the padlock is now green. But Chromium still uses a padlock. The padlock in Opera is yellow. Both Chromium and Opera show no favicon. Konqueror shows some strange green icon with a check-mark on the right side of the location bar and the favicon on the left side.

[1]Web Security Context: User Interface Guidelines, W3C Recommendation 12 August 2010, http://www.w3.org/TR/wsc-ui/

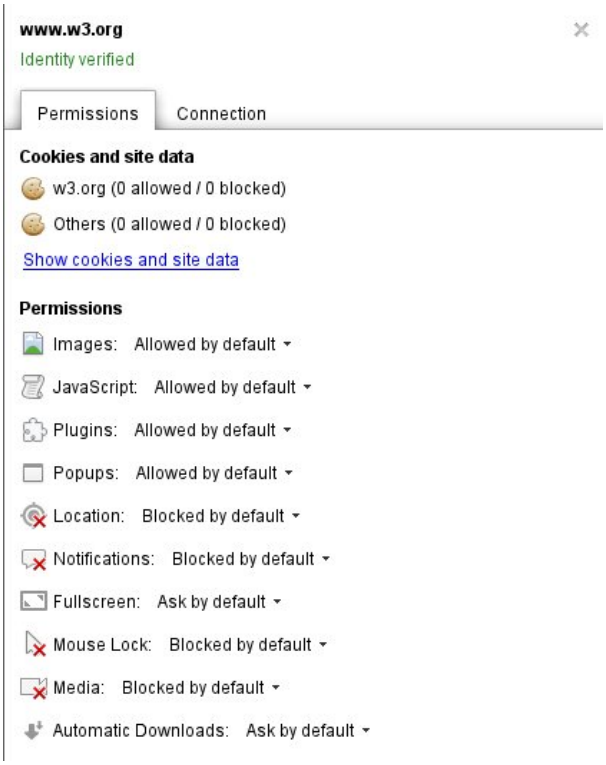

Figure 2: Clicking on the padlock opens an roll-down menu

Chromium gives a range of details concerning the site. The origin only says "www.w3.org, identity verified". Clicking on the connection button tells me, that: "The identity of this website has been verified by Gandi Standard SSL CA". That opens a link to the "certificate information". The certificate information is the well known tech-gibberish with serial numbers and fingerprints.

If I'm an X.509 expert, the information may be useful. If I'm a user, the information is mostly noise. Chromium mixes SSL information with other information, namely cookies, permissions and whether the browser loads graphics. Drilling down for information by further clicking ends in the raw certificate information. The Opera browser shows "securely connected" and "Details". Clicking on details gives the raw view on the certificate.

From a legal communications point of view, I can summarise the entire system to the following assertions:

- Some entity Gandi asserts that www.w3.org is the www.w3.org that has their certificate
- the connection is using TLS 1.2, encrypted with AES 256 CBC, using SHA1 for message authentication and ECDHE RSA for the key exchange

But the legal or social questions of interest are:

- Who is Gandi, where are they and what do they do?
- Are they asserting the identity of an entity and which identity are they asserting corresponds to what?
- Who is www.w3.org, what legal entity is behind www.w3.org and how can I reach them in case of problems
- How secure is TLS 1.2, encrypted with AES 256 CBC, using SHA1 for message authentication and ECDHE_RSA for the key exchange, compared to the state of art?

The trick is that for statements in the first list, it is very hard to assert liability. If the statements are meaningless, nobody will rely on those statements to make a decision, thus there is less deception possible as there are no expectations in the first place. Consequently the risk of problems for those making assertions is proportionally low to the degree those statements are socially or legally useful to the user.

The second list of statements is meaningful for end users that are not complete newbies. The information contained is so valuable that there are commercial databases providing that information for a fee. Gandi is a legal entity that is registered with a lot of information at the commercial register in Paris. www.w3.org points to W3C. W3C is a complex entity, but gives you pointers in case of questions and also all legal information. It has 4 registered legal entities as hosts. A user can contact the nearest one in case of problems. Finally, a

metrics of security may be used. We know that SHA1 has some distant weaknesses, so the security may not be 100%. But to look at a Workshop site, even 40% is good enough. For client-attorney communications that may be of interest for the government, this may not be good enough. All this information is very valuable for users and they will base decisions on the fact that they think they are dealing with a certain legal entity that has some asserted properties. All those assertions, if wrong, can lead to wrong decisions. Wrong decisions often lead to damages. And the risk of liability for the CA and the site increases.

1.1 Conclusions on messages conveyed

That means the lack of usability in the security interface is not a bug, it is a feature. It is most probably and at the very basis the expression of unwillingness of the entire TLS system to stand in for their assertions. Which is understandable. Because given a high liability risk, TLS certificates will probably be 10 times more expensive. certification authorities will carefully check the information before issuing a certificate to avoid liability. The social process of securing the social side of a secure communication channel will establish itself.

2 Security configuration with Chromium

Looking into the general security configuration menu confirms a low attention to the issue in current browsers. Most browsers have an implementation of TLS/SSL. TLS/SSL itself relies on X.509 and other existing technology for the trust relationship. Now try to find things. In Chromium, it is all about Usability, but in the interest of whom? The answer is obvious. The first point in the Chromium settings dialog is:

> **Sign in**
>
> Sign in to Chromium with your Google Account to save your personalised browser features to the web and access them from Chromium on any computer. You'll also be automatically signed in to your favourite Google services.

No security on the first page of settings, not even the word. "On startup", "Appearance (Themes)", "Search", "Users" and "Default browser" give us an indication what the browsermaker thinks the user will find important. Or what the browsermaker thinks the user should find important.

The click on advanced settings expands the listing. After "Privacy", "Passwords and forms", "Web content", "Network", "Languages" and "Downloads" I finally find a point "HTTPS/SSL". Still no "Security". But I had heard that "HTTPS/SSL" has something to do with security. There is a button "Manage certificates". This results in a pop up window with caption "Certificate manager" defaulting on "Your Certificates". The listing is empty. Clicking on the "Servers" tab results in a curious listing.

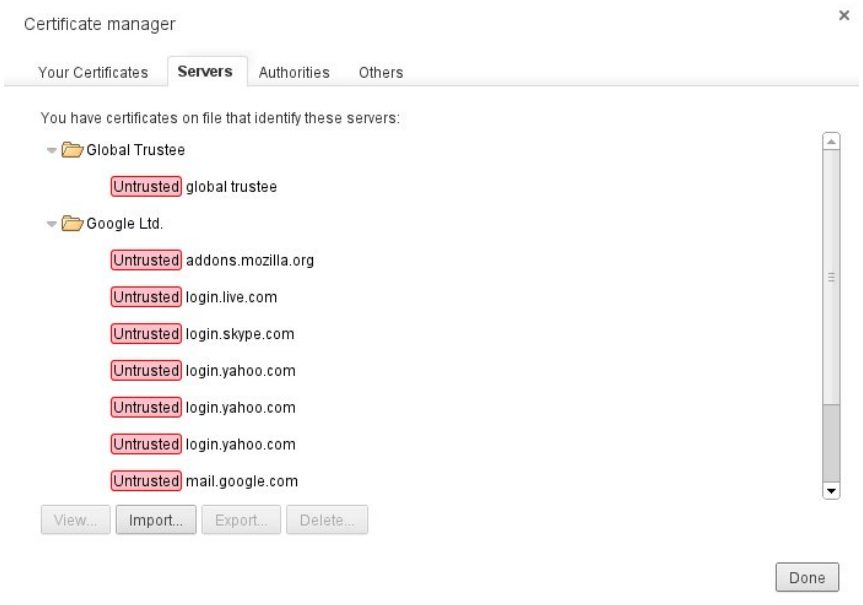

Figure 3: An incomprehensible list of trust statements

From the listing you can see that Google Ltd does not trust addons.mozilla.org and other services like login.yahoo.com. Global Trustee does not even trust itsef as the global trustee server is marked as untrusted in

the Global Trustee tree. What would a user derive from this. Even the author of this paper, with some record in looking security issues despite being non-technician, can not deduct any useful information from the listing.

Remains the "Authorities" tab and "Others". The "Authorities" tab contains the list that says *You have certificates on file that identify these certificate authorities* It is intriguing that *You* have those *certificate authorities on file*. But in fact, the *browsermaker* has them on file. "Edit" does not edit the certificate but the trust attached to it. The trust for *A-Trust Ges. f. Sicherheitssyteme im elektr. Datenverkehr GmbH* is ticked by default. But how would the user know? The user can select to trust this certificate to also `identifying email users` and `software makers` but those are not pre-ticked. As the Chromium tested has no email client, it is unclear whether this will influence the trust level of email within other email clients on a system.

2.1 Conclusion

The current certificate manager in Chromium is not well designed for a user to manage her trust relations to sites. Interfaces of other browsers are not really better or much worse.

3 Who has to trust whom?

The Web Security Context: User Interface Guidelines[2] have dealt with some of the issues. But they were written with a certain idea in mind. This idea transpires from the concepts used. And the idea is to trust the commercial structure of the Web more than the actual end user. The Guidelines define a certificate as:

> A trust anchor represents an authoritative entity represented by a public key and associated data.

From a user's perspective, this is actually true for root Certificates as well as for certificates indicating a certain website. The Guidelines subsequently distinguish between a *trust anchor or certificate is interactively accepted* and a new category called *Augmented Assurance Certificate*. The latter are defined as

> a public key certificate where the issuer asserts that the subject entity has been authenticated by means of some process that adheres to the requirements of an augmented assurance specification supported by the user agent.

The underlying model of thinking is revealed in this statement:

> Trust anchor installation is typically handled by user agent vendors, systems administrators and device manufacturers, based on out-of-band information. Note that updating trust anchors is therefore often handled as part of user agent or operating system software updates.

Interalia, the Web Security Context: User Interface Guidelines distrust user interaction and user control in favor of the classic CA schemes. We have seen in section 1.1 that the user has not enough useful information to assess his own trust anyway. We also have seen that the information contained in the certificates is not useful for a user to assess trust. It is only useful for the current CA system to assess whether the commercially organised trust had a loophole or was compromised in some way.

In fact, the browser trusts a commercial system more than the user. This does not come as a surprise as the current interfaces within the browser do not provide sufficient comprehensible information. The user just has to trust the god in the machine which is in those certificate authorities that have verified everything. The user can not even see what they have verified, let alone whether they have done so diligently or whether their root certificate was compromised by governmental influence.

The key role of the CA is re-enforced by the following statement in the User Interface Guidelines:

> Implementations MUST NOT enable users to designate trust roots as augmented assurance qualified as part of a unrelated interaction. In particular, the notions of an augmented assurance qualified trust root and an interactively accepted trust root are mutually exclusive.

This means a user can not achieve the ultimate trust level in his own piece of software without the collaboration of the software makers. Our own systemic thinking is such that we do not trust the user because of *phishing*. Of course there is always a good argument that the user does not understand things and should be protected from herself. There are apparent parallels to the trusted computing here as the user of the browser is the object of policy and operations outside of the user's control. The physical control over a browser via a UI is only apparent while the deeper control of the entities that are trust is with the manufacturers. And this is hurting a feeling of many people as we have a thousand years old tradition to believe that we can control things we can touch.

[2] see previous footnote

In fact, the ultimate goal is still that the user should just look at my shiny website and not worry at all about what is going on behind the scene. Nothing to see, please walk on. The state of the web, the many worries we have and the growing feeling of ambient tailspin show us that user empowerment and user comprehension are of growing importance. Because it is not only important to give control back to the user, but also to make that control visible. Justice has to be seen to be done.

And we have a new piece in the puzzle. Browsers are produced by a few software makers and thus make an easy target for large and powerful entities like governments. The central services of the Web are in the same, or even in a worse situation. While we did not trust the user in the past because he would click on everything that moves, we are now in a situation where we lose trust in the commercial trust system that has incapacitated the users for so long and optimised the solutions for the commercial use, which made sense at the time it was made.

4 Can we imagine solutions?

W3C has worked on the above issues in the past. There is some probability that W3C will work on them in the future. The Web Security Context: User Interface Guidelines were a first timid step in making the social relation that we name *trust* more explicit. We need to continue and give the user more handles to influence the way the trust network is built.

If there are incentives to invest into better UI for users and their understanding of our social and commercial trust relations, we will see highly innovative solutions, security dashboards and new services.

We want to strengthen the Internet because the pervasive monitoring of communications gives unprecedented power to a few. They are mostly looking into *metadata* and what it reveals. An innovative security dashboard that has a user centric view need not limit itself to the pure certificate information. It may as well give a comprehensive access to the wealth of information that can help us to assess our situation. This ranges from exploiting the user's view on protocol data generated by the http interactions over time to information out there on the web. This can be already existing solutions like the inclusion of external services of fraud protection, but also a digested view on an online forum with relevant contributions.

And there is the challenge to make PKI work and to complement it by a network of trust. What should the content of PKI trees be and how do we integrate them into our view on social relations. Because technically, the issue seems to be rather well understood. But do those who understand social hierarchies actually talk to those who understand hierarchies technically? And if the outcome is complex, can we find a way to reduce the complexity to make it understandable and accessible in a comprehensible dashboard? This remains a challenge. The past 30 years have shown that relying on hierarchies only has failed. Relying on a web of trust has failed the same way. But we have not yet explored the middle way: How to easily connect my personal trust network into the hierarchy and how to manage my social relations in a trust dashboard.

But the entire plan to have more control and visibility has a big enemy. It is clear that the less a consumer is disturbed by anything that may raise suspicion, the more the consumer is able to concentrate on buying things and the better the click-through rate will be. This will dictate a browser that gives the feeling that nothing is wrong while the news are flooded with security incidents. Additionally, making meaningful assertions will expose companies to liability for those assertions, so they will try to avoid making meaningful statements.

The only way to work against this is to provide a means that furthers the commercial interest. And this may be done by statistics. What if the dashboard would contain a button that would allow a user to anonymously share whether she trusts a certain site? This could feed back into the dashboard. While security and social networking are quite different, they share some trust building dynamics. So as done in the User Interface Guidelines and implemented in browsers, the brand name in the location bar was a good start, but we need more of that.

Finally, the interface can only convey information and messages and assertions that are in the system. Our initial exploration of the Chromium system has shown that the information we need is not in the certificates. Do we have to re-think the functions and contents of certificates, PKI and the elements of trust relations? I think so. PKI in times of social networking may look differently. But it will only work if there are rings and the possibility to federate rings of trust. And connecting two rings becomes like connecting those networks that ended up being called the Internet[3].

[3]Note that Intertrust was the name of a rights protection company and would not be a good name for such a web of relations