

Web Security Experience, Indicators and Trust: Scope and Use Cases

W3C Working Draft 1 November 2007

This version:

<http://www.w3.org/TR/2007/WD-wsc-usecases-20071101/>

Latest version:

<http://www.w3.org/TR/wsc-usecases/>

Previous version:

<http://www.w3.org/TR/2007/WD-wsc-usecases-20070525/>

Editor:

Tyler Close, [Hewlett-Packard](#)

[comments in this color by Tim Hahn, 27 November 2007](#)

Copyright © 2007 W3C[®] (MIT, [ERCIM](#), [Keio](#)), All Rights Reserved. W3C [liability](#), [trademark](#) and [document use](#) rules apply.

Abstract

This Note refines the objectives for the Web Security Context Working Group deliverables. It elaborates upon the group's [Charter](#) [[WSC-CHARTER](#)] to explain what the group aims to achieve, what technologies may be used and how technical proposals will be evaluated. This elaboration is limited to the group's technical work and does not cover additional activities the group intends to engage in, such as ongoing outreach and education.

This Note also includes an initial collection of use cases that the group expects will drive its technical work.

Since this Note discusses the assumptions, goals, and processes the group will use to develop its recommendations, the intended audience is similar to that of the charter of the Working Group; group members, the W3C community, developers of web user agents, web content providers (server administrators), and parties interested and engaged in what the Web Security Context Working Group's plans and directions are. It is explicitly not targeted at the presumed beneficiaries of the group's work, the users of the web, and it is not expected that an average user would be able to read this document and understand it.

Status of this Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current W3C publications and the latest revision of this technical report can be found in the [W3C technical reports index](http://www.w3.org/TR/) at <http://www.w3.org/TR/>.

This is a Last Call Working Draft of "Web Security Experience, Indicators and Trust: Scope and Use Cases". The W3C Membership and other interested parties are invited to review the document and send comments to public-usable-authentication@w3.org (with [public archive](#)) through 30 November 2007.

After addressing any issues raised as part of last call feed-back to this document, the Working Group will publish its final version as a [W3C Working Group Note](#).

This document was produced by the [Web Security Context Working Group](#), as part of the [Security Activity](#).

Publication as a Working Draft does not imply endorsement by the W3C Membership. This is a draft document and may be updated, replaced or obsoleted by other documents at any time. It is inappropriate to cite this document as other than work in progress.

This document was produced by a group operating under the [5 February 2004 W3C Patent Policy](#). The group does not expect this document to become a W3C Recommendation. W3C maintains a [public list of any patent disclosures](#) made in connection with the deliverables of the group; that page also includes instructions for disclosing a patent. An individual who has actual knowledge of a patent which the individual believes contains [Essential Claim\(s\)](#) must disclose the information in accordance with [section 6 of the W3C Patent Policy](#).

Table of Contents

- 1 [Overview](#)
- 2 [Goals](#)
 - 2.1 [Document the status quo](#)
 - 2.2 [Relevance of security information](#)
 - 2.3 [Consistent presentation of security information](#)
 - 2.4 [User awareness of security information](#)
 - 2.5 [Reliable presentation of security information](#)
 - 2.6 [Reduce the number of scenarios in which users need to make trust decisions](#)
 - 2.7 [Authoring and deployment techniques](#)
 - 2.8 [Best practices for other media](#)
- 3 [Non-goals](#)
 - 3.1 [Presentation of all security information](#)
 - 3.2 [Non-HTTP Web interactions](#)
- 4 [In scope](#)
 - 4.1 [Web interactions](#)

- 4.2 [User agents](#)
- 4.3 [Entity identification](#)
- 4.4 [Third-party recommendation](#)
- 4.5 [Historical browsing information](#)
- 5 [Out of scope](#)
 - 5.1 [Protocols](#)
 - 5.2 [non-Web interactions](#)
 - 5.3 [Security context information for consumption by automated agents](#)
 - 5.4 [New security information](#)
 - 5.5 [Content based detection](#)
 - 5.6 [Security information about the user's computer](#)
 - 5.7 [User agent exploits](#)
 - 5.8 [User separation](#)
 - 5.9 [Content production exploits](#)
 - 5.10 [Other security challenges](#)
- 6 [Use cases](#)
 - 6.1 [User decisions](#)
 - 6.1.1 [Providing sensitive information to a web site](#)
 - 6.1.2 [Believing information to come from a known author](#)
 - 6.1.3 [Installing software downloaded from a web site](#)
 - 6.2 [Navigation](#)
 - 6.2.1 [Unidentified destination](#)
 - 6.2.2 [Unidentified source](#)
 - 6.3 [User agent type](#)
 - 6.3.1 [Desktop browser](#)
 - 6.3.2 [Smartphone](#)
 - 6.4 [Accessibility](#)
 - 6.5 [Scenarios](#)
 - 6.6 [Threats](#)
 - 6.6.1 [Subverted navigation](#)
 - 6.6.1.1 [URL typo](#)
 - 6.6.1.2 [Misleading bookmark](#)
 - 6.6.1.3 [Misleading introduction](#)
 - 6.6.1.4 [Unprotected navigation](#)
 - 6.6.2 [Web site impersonation](#)
- 7 [Security information available to the user agent](#)
 - 7.1 [Defined by web content specifications](#)
 - 7.2 [Defined by SSL related specifications](#)
 - 7.3 [Defined by HTTP related specifications](#)
 - 7.4 [Defined by IP related specifications](#)
 - 7.5 [Defined by DNS related specifications](#)

- 7.6 [Defined by user agent](#)
- 7.7 [State that may be collected by a user agent](#)
- 7.8 [Defined by a third-party](#)
- 8 [Merits of the status quo](#)
 - 8.1 [Widely deployed, strong cryptography](#)
 - 8.2 [Many deceptive imitation techniques prevented](#)
 - 8.3 [Corrected implementation errors](#)
 - 8.4 [Password management](#)
- 9 [Problems with the status quo](#)
 - 9.1 [Poorly defined area for chrome](#)
 - 9.1.1 [Picture in picture](#)
 - 9.1.2 [Visually extending the chrome](#)
 - 9.1.3 [Removing the chrome](#)
 - 9.2 [Poorly defined role for chrome](#)
 - 9.2.1 [Browser window title](#)
 - 9.2.2 [Back and forward buttons](#)
 - 9.2.3 [URL bar](#)
 - 9.2.4 [Padlock icon](#)
 - 9.2.5 [Favicon](#)
 - 9.2.6 [Status bar](#)
 - 9.2.7 [Information bar \(aka: notification bar\)](#)
 - 9.3 [Poor user understanding of chrome](#)
 - 9.3.1 [Padlock icon](#)
 - 9.3.2 [Hostname](#)
 - 9.3.3 [Chrome versus page](#)
 - 9.3.4 [Explanations versus understanding](#)
 - 9.4 [Poor usability of chrome](#)
 - 9.4.1 [Out of sight, out of mind](#)
 - 9.4.2 [Assumed safety](#)
 - 9.4.3 [Poor usability of dialog boxes](#)
- 10 [Process](#)
 - 10.1 [Expertise and experience](#)
 - 10.2 [Reliance on general usability expertise](#)
 - 10.2.1 [Affordance](#)
 - 10.2.2 [Conceptual model](#)
 - 10.2.3 [Match between system and the real world](#)
 - 10.2.4 [Habit formation](#)
 - 10.2.5 [Single locus of attention](#)
 - 10.2.6 [Aesthetic and minimalist design](#)
 - 10.2.7 [Help users recognize, diagnose, and recover from errors](#)
 - 10.2.8 [Provide explanations, justifying the advice or information given](#)

10.2.9	Understand the user
10.2.10	Create task profiles
10.2.11	Consistency
10.3	Learning from past efforts
10.3.1	No user categories in phishing vulnerability
10.3.2	The user must be aware of the task they are to perform
10.4	Implementation and testing
11	Acknowledgments
12	References

[1 Overview](#)

Web user agents are now used to engage in a great variety and number of commercial and personal activities. Though the medium for these activities has changed, the potential for fraud has not. This Working Group is chartered to recommend user interfaces that help users make trust decisions on the Web.

This first Working Group document elaborates upon the group's [Charter \[WSC-CHARTER\]](#) to explain what the group aims to achieve, what technologies may be used and how proposals will be evaluated. This elaboration is limited to the group's technical work and does not cover additional activities the group intends to engage in, such as ongoing outreach and education.

The work outlined in this document is expected to take existing standards and best practices into account. Where relevant, such existing work will be leveraged.

[2 Goals](#)

[2.1 Document the status quo](#)

Security information within the Working Group's scope will be catalogued, along with corresponding presentations and user interpretations reported in user studies.

[2.2 Relevance of security information](#)

The Working Group will analyze common use cases to determine what security information the user needs to safely accomplish their current task and recommend security information that should, or should not, be presented in each case.

[2.3 Consistent presentation of security information](#)

The Working Group will recommend a set of terms, indicators and metaphors for consistent presentation of security information to users, across all web user agents. For each of these items, the Working Group

will describe the intended user interpretation, as well as safe actions the user may respond with in common use cases.

2.4 User awareness of security information

The Working Group will recommend presentation techniques that integrate the consumption of security information by the user into the normal browsing workflow. Presenting security information in a way that is typically ignored by the user is of little value.

2.5 Reliable presentation of security information

The Working Group will recommend presentation techniques that mitigate deceptive imitation, or hiding, of the user agent's presentation of security information.

2.6 Reduce the number of scenarios in which users need to make trust decisions

No matter how well security context information is presented, there will always be users who, in some situations, will behave insecurely even in the face of harsh warnings. Thus, the Working Group will also recommend ways to reduce the number of situations in which users need to make trust decisions.

2.7 Authoring and deployment techniques

The Working Group will recommend authoring and deployment techniques that cause appropriate security information (see [7 Security information available to the user agent](#)) to be communicated to users. Techniques already available at authoring and deployment time which reduce the need for communication of security information to the user will be considered in the recommendations.

2.8 Best practices for other media

Users' interpretation of security information on the web will necessarily be affected by experience with other media that are not part of this Working Group's scope; such as email, print, radio or video. The Working Group will provide best practice guidelines for other media to follow so as not to undermine the presentation of security information on the web.

3 Non-goals

This section outlines a range of work items which the group will not focus on, but which may be covered as beneficial side effects of the group's work. Work items listed here won't be a priority, and the group won't expend collective resources on tackling them.

3.1 Presentation of all security information

Web user agents contain a great deal of information relevant to security. This Working Group does not

aim to recommend a presentation for all of this information. Recommendations will be narrowly focused on presentations that satisfy the Working Group's usecases, see [6 Use cases](#).

[3.2 Non-HTTP Web interactions](#)

Recommendations that this group makes may or may not be relevant to Web related interactions that use protocols other than HTTP or HTTPS. While the group will aim for its recommendations to be generically useful -- where appropriate --, it considers recommendations specific to other protocols as a Non-Goal.

[4 In scope](#)

This section enumerates categories of technology and information that are within this Working Group's scope, as initially defined by the group's [Charter \[WSC-CHARTER\]](#). A complete enumeration of in scope artifacts is provided by the section [7 Security information available to the user agent](#).

[4.1 Web interactions](#)

User interactions on the Web (see [Architecture of the World Wide Web \[WEBARCH\]](#)), using the HTTP and HTTPS protocols, are at the core of the Working Group's scope. Where Web interactions involve other application-level protocols (including, e.g., SOAP or FTP), the Working Group considers these in its scope and will aim that its recommendations be applicable; however, applicability to non-HTTP Web interactions (see [3.2 Non-HTTP Web interactions](#)) is a non-goal.

[4.2 User agents](#)

A user agent is software to access Web content, including desktop graphical browsers, text browsers, voice browsers, mobile phones, multimedia players, plug-ins, and some software assistive technologies used in conjunction with browsers such as screen readers, screen magnifiers, and voice recognition software. This definition is in line with [Web Content Accessibility Guidelines 1.0 \[WCAG\]](#).

Use cases considered by this Working Group must involve a web user agent, operated by a human user. In all instances, the use case is only relevant to this Working Group if the presentation of security information should affect the user's interaction with the web resource.

[4.3 Entity identification](#)

A web browsing session is like a conversation, where the user converses with various entities, some known, and others newly encountered. Each resource the user interacts with is identified by a URI. Through specifics of the underlying protocol, including DNS and SSL, other designators are bound to these resources and the entities that provide them. Recommending a presentation for these designators that helps the user recognize which entity they are currently conversing with, and when they are switching to a different entity, is a primary concern of this Working Group.

4.4 Third-party recommendation

A user's perception of an entity is strongly influenced by the opinions of others. The recommendations of certificate authorities, visited web sites or reputation services integrated into the user agent are in scope for this Working Group.

4.5 Historical browsing information

The Working Group may also use information about past interactions between the user and an entity in presentation recommendations. Relevant historical browsing information includes entity designators used in past browsing sessions, as well as information provided by the user to the entity during those sessions.

5 Out of scope

This section enumerates a number of possible work items that the Working Group will not consider.

5.1 Protocols

The Working Group considers recommendations for lower level protocols (such as SS7, ISDN, or NANP) out of scope.

5.2 non-Web interactions

The Working Group considers recommendations specific to interactions that do not involve the Web (e.g., rich text display in an e-mail user agent) out of its scope. However, where such interactions use Web Technologies, recommendations may turn out to be applicable ([e.g. Network-delivered \(HTTP\) content viewed within an e-mail user agent window](#)).

5.3 Security context information for consumption by automated agents

The Working Group will only consider Web interactions in which a human participates in making a trust decision this group is chartered to address. Situations in which all security relevant information is consumed and acted upon only by automated agents are out of scope.

5.4 New security information

The Working Group will neither create nor extend any protocol or data format, nor create recommendations for protocols or data formats that are not yet widely deployed. Recommendations will only be made for the presentation of currently deployed security information.

5.5 Content based detection

Techniques commonly used by intrusion detection systems, virus scanners and spam filters to detect illegitimate requests based on their content are out of scope for this Working Group. These techniques

include recognizing known attacks by analyzing the served URLs, graphics or markup. The heuristics used in these tools are a moving target and so not a suitable subject for standardization. The Working Group will not recommend any checks on the content served by web sites.

5.6 Security information about the user's computer

Security information about the user's computer, such as that provided by virus scanners, or trusted computing infrastructure, is out of scope for this Working Group. No recommendations will rely on such services, or any aspect of trusted computing. As a result, presentation techniques recommended by this Working Group may be undermined by malware that has infected the user's computer.

5.7 User agent exploits

Attacks that exploit a programming error in the user agent are out of scope. This Working Group's recommendations assume a properly functioning user agent.

5.8 User separation

Many computers are shared among multiple users, either in the home, or as a kiosk in a public place. In such scenarios, the activity of one user must not be accessible to another. Providing this functionality may be best done by the operating system, or other software, and is out of scope for this Working Group.

5.9 Content production exploits

Programs that produce HTML, or other web content, commonly suffer from quoting errors that enable Cross-site scripting (XSS) attacks [\[tjh: would be good to have a reference here for further information\]](#). The web user agent is in a poor position to detect these attacks, since it sees only the output. Web content formats are not currently designed such that the receiver can readily distinguish content that was produced on purpose versus content that was produced by accident. Consequently, this kind of attack is out of scope for this Working Group.

5.10 Other security challenges

As stated in the [charter](#), the mission of the Web Security Context Working Group is to specify a baseline set of security context information that should be accessible to Web users, and practices for the secure and usable presentation of this information, to enable users to come to a better understanding of the context that they are operating in when making trust decisions on the Web. While the work this group does may have a positive and beneficial effect on other security challenges on the web, directly addressing such challenges is out of scope. This section lists several specific challenges, but the list may not be exhaustive.

6 Use cases

This Working Group is concerned with: the trust decisions users must make when using the Web; what

information may inform these decisions; and usable ways of communicating needed information to the user. Our use-cases are first structured by the kind of decision facing the user, where each kind of decision brings different risks. The information available to inform a decision is primarily determined by how the user navigated to the web page where the decision arose. Our use-cases are further categorized by the different means of navigating the Web. Finally, the feasible user interactions for communicating relevant information are limited by the I/O features of the web user agent. Our use-cases are finally tailored to the kind of web user agent.

These use cases are categorized by the kind of decision a user is making, how the user navigated to the web site the user is now navigating to, and the kind of user agent being used. These can be considered as three independent directions to define the space of these use cases.

6.1 User decisions

6.1.1 Providing sensitive information to a web site

Many activities on the Web, such as logging into an account or completing a purchase, require providing sensitive information to a web site. If the user is interacting with the intended site, and they are not reassured of this case, they may not complete a desired transaction. If the site is not the intended one, and the user is not warned of this case, a thief may receive sensitive information.

6.1.2 Believing information to come from a known author

The Web is most often used for viewing information produced by others. Sometimes, the user may form an opinion, or make a decision, based on this information. This act may be greatly influenced by who the user believes to be the information's author. If the user is misled about authorship, a thief may convince the user to take an unwarranted action. If the user is unsure about authorship, they may not act on needed advice.

6.1.3 Installing software downloaded from a web site

Not all content available on the Web remains confined to the web browser. Some content can be installed as an executable application on the user's computer, or as an extension to an existing application, or extend the web browser itself. On today's popular operating systems, an installed application has much greater access to the user's computer than does a web page. An application may abuse this additional authority by stealing the user's files, rendering the computer unusable, or using it to attack yet other computers. Choosing to not install an application may also be detrimental, as a needed security patch is not applied, or desired functionality is not acquired.

6.2 Navigation

A hyperlink is navigated from a source to a destination. Information about each may be relevant to a trust decision the user makes on the destination web page, but this information is not always available. Even when available, this information may not be meaningful to the user. The identification provided by either

source or destination may not correspond to any entity known to the user.

6.2.1 Unidentified destination

Information about the destination of a hyperlink may be unavailable because:

- the web page does not support authentication, such as provided by SSL
(In the absence of SSL, communication with the destination host may be intercepted by a compromised DNS lookup, or an illegitimate wifi access point.)
- the provided authentication certificate is unrecognized, or expired

6.2.2 Unidentified source

In addition to the ways destination information may be unavailable, source information may be unavailable because:

- navigation was initiated from another application, such as an email or chat client
- the user typed in the destination URL
- the source web page makes no warranty as to the purpose of the hyperlink, such as is common for a search engine or open discussion forum

[tjh: I suggest a third section here: Unintended Destination – The destination of a hyperlink may not be intended by the user and not noticed by the user as the web site is contacted. An example of this:

- navigation was initiated by a HTTP re-direct and this re-direct was not noticed by the user.

6.3 User agent type

The use-cases address two different kinds of user agent, each distinguished by characteristic I/O features.

6.3.1 Desktop browser

A desktop browser typically has:

- a large, full color viewing area
- a pointing device
- a full-size keyboard
- speakers

6.3.2 Smartphone

The user agent in a mobile browser typically differs from its desktop counterpart in several ways:

- Screen: a small, limited color viewing area
- Navigation input: small keyboard, stylus or pointing device

- Small keyboard pad: on-screen keyboard and predictive text technology, such as T9
- Tactile feedback: vibration
- A/V interfaces

Traffic cost awareness, slow connection speed and trust in the mobile network infrastructure may also affect how users interact with their smartphone's user agent. These factors influence how security indicators are presented by different smartphone user agents.

In mobile browsers, the chrome has fewer options and overlaps with the phone's menus. Obtaining secondary information is cumbersome, requiring several clicks. Due to a lack of screen space, the padlock is shown but the URL is only partially shown, if at all. Password management is not supported in all phones. In some cases, an accessed web page has a modified look and feel, different from simply viewing the page on a small screen. These changes may create suspicion among security-aware users. User agents rarely check for certificate revocation, since doing so generates network traffic. Some certificate authorities commonly found in desktop browsers are not included in smartphone user agents. [Users rarely check the default/pre-packaged set of trusted CA certificates shipped with the user agents they use.](#) Consequently, the user may be presented with warnings that do not appear when the same site is visited using a desktop user agent. Large pages that do not fit in the phone's RAM can cause unexpected behavior in the user agent's security indicators.

[When a user switches between devices, there is nothing which ensures that the configuration is similar between these user agents.](#)

6.4 Accessibility

The use cases in this document make no particular assumptions about the capabilities and cultural background of the user in question. [\[WCAG\]](#)

- They may not be able to see, hear, move, or may not be able to process some types of information easily or at all.
- They may have difficulty reading or comprehending text.
- They may not have or be able to use a keyboard or mouse.
- They may have a text-only screen, a small screen, or a slow Internet connection.
- They may not speak or understand fluently the language in which the document is written.
- They may be in a situation where their eyes, ears, or hands are busy or interfered with (e.g., driving to work, working in a loud environment, etc.)
- They may have an early version of a browser, a different browser entirely, a voice browser, or a different operating system.

6.5 Scenarios

<u>Navigation</u>	<u>User Decision</u>		
	<u>Providing</u>	<u>Believing</u>	<u>Identifying</u>
Identified source, Identified destination	<u>any any</u>	<u>any any</u>	<u>any</u>
Identified source, Unidentified destination	<u>any</u>	<u>any</u>	<u>any</u>
Unidentified source, Identified destination	<u>any any smartphone</u>		<u>any</u>
Unidentified source, Unidentified destination	<u>any</u>	<u>any any any any</u>	<u>any</u>

The cells in the table describe the user agent type being used by the user. “any” refers to either of the user agent types described.

- Identified source, Identified destination, Providing

Once a week, Alice pays her bills. She opens her web browser, follows the habitual bookmark to her bank's site, logs in by entering her credentials, and follows the routine course through the online banking system.

- Identified source, Identified destination, Providing

Betty's home wireless router has a web interface for making configuration changes. When the router is installed, it generates a self-signed SSL server certificate. Sometime later, Betty attempts to make a configuration change. How does Betty know she's connected to the router she setup earlier, and not her neighbor's?

- Identified source, Unidentified destination, Providing

Once a week, Alice pays her bills. She opens her web browser, follows the habitual bookmark to her bank's site, and is directed to an unfamiliar site at a new domain, announcing that her bank has recently acquired another one and changed names a bit. She is asked to enter her usual credentials, succeeds, and quickly adapts to the new online banking system.

- Unidentified source, Identified destination, Providing

In the advertising leading up to a re-run of the 1970s movie classic "The Sting," Doyle sees an offer for a new-fashioned investment that he can't refuse, offered by a brand that he has heard of before. He memorizes the URL that is given toward the end of the advertising. Coming back home, he mis-types the URI at first, corrects a spelling error, and then reaches a web site that matches the investment firm's branding and name. He's asked for identifying information that he provides.

- Unidentified source, Identified destination, Providing

Example Inc. has use of example.com, example.net and example.org. Each is used to manage a different part of the company's online operations. Betty initially found Example at example.com

and created her online account through a page hosted at that domain. She has yet to interact with any of Example's other hosts. Sometime later, Betty receives an email claiming to be from Example and alerting her to a pending task that she must attend to. The email provides a hyperlink to a page that will help Betty complete the task. After clicking on the hyperlink, Betty's user agent displays a page from the example.nethost. The page asks Betty to enter her username and passphrase before being allowed to access her account. How is Betty to know that her Example credentials can be safely entered into the page?

- [Unidentified source, Identified destination, Providing, smartphone](#)

While on the move, Alice suddenly remembers she has to make an urgent banking transaction. She has used her mobile browser previously for retrieving information from the web, but this time she decides to use her phone due to the urgency. She starts her mobile phone browser and enters a URL that she recalls having seen on her home desktop browser. After some delay, longer than usual, the phone starts showing a page. Due to screen size, Alice notices that the layout is somewhat familiar, but still not the same as the one in her desktop. She can't see the full URL either. Alice scrolls and spots the link that takes her to the transaction page and clicks on it. After some delay, the phone displays a page asking her to enter her usual bank credentials. How is Alice to know that her bank credentials can be safely entered into the page?

- [Unidentified source, Unidentified destination, Providing](#)

Example Inc. has a popular online service that processes many credit card transactions a day. Betty occasionally uses the service and trusts it with her credit card information. Malcolm is a thief with an idea. He creates an imitation of the Example web site and begins directing users to it. Malcolm contacts victims through email, or even the phone, and links to his imposter site from popular blogs and chat forums. He's also given his imposter site a domain name that is just a typo away from Example's authentic web site, so some victims will arrive by accident. Betty is about to enter her credit card information into a site that looks just like Example's. How is she to know if it's the authentic site, or the imposter?

- [Identified source, Identified destination, Believing](#)

Betty occasionally visits the example.com web site. On each connection, Betty's user agent receives an SSL server certificate issued by the same certificate authority. On the current connection, the received certificate was issued by a different certificate authority. What should the user agent display? Can Example Inc. affect this display through the content of the new certificate?

- [Identified source, Identified destination, Believing](#)

Betty clicks on a hyperlink to the web page at `<https://www.example.com/>`. The received HTML page includes content received from `<https://www.example.net/>`. Betty's user agent is unaware of any relationship between the `www.example.com` and `www.example.net` web sites.

- [Identified source, Unidentified destination, Believing](#)

Betty visits the web page at `<https://www.example.com/>`. The received HTML page includes content received from `<http://www.example.com/>`, i.e., content received using a different security context.

- [Unidentified source, Unidentified destination, Believing](#)

Betty tries to connect to a web site at `<https://www.example.com/>`. Her user agent's SSL implementation detects that the domain name specified in the certificate differs from `www.example.com`. What should the user agent display?

- [Unidentified source, Unidentified destination, Believing](#)

Betty is planning a trip to a foreign country. Searching the web, she finds a widely recommended local travel agency. When she connects to their web site, her user agent does not recognize the certificate authority that issued the travel agency's SSL server certificate. What should the user agent display?

- [Unidentified source, Unidentified destination, Believing](#)

Like many users, Betty has grown accustomed to quickly clicking through any warning dialogs presented by her user agent. Out of habit, Betty dismisses another one, then quickly becomes suspicious about some of the web page's content.

- [Unidentified source, Unidentified destination, Believing](#)

Betty has travelled to a foreign country. In a coffee shop, she is reading a political web site from her home country. She wonders whether the information that is displayed to her is authentic, and whether there will be eavesdropping on her interactions.

- [Identified source, Identified destination, Installing](#)

Once a week, Alice pays her bills. She opens her web browser, follows the habitual bookmark to her bank's site. Her bank's web site informs her that, as a countermeasure to recent attacks against online banking customers, she needs to install a piece of proprietary software on her computer that will be the conduit for her future interactions with the bank.

- [Identified source, Unidentified destination, Installing](#)

Frank regularly reads a frequent flyer forum while sipping his first cup of coffee in the morning. He clicks on a link and walks off to the coffee-maker for a refill. Returning, he notes that his computer screen now includes pop-up advertising for a new cheque-management program which is purportedly offered by his bank. A free demonstration version is available for download. The advertising is served from an advertising agency's web site, not from the bank's.

- [Identified source, Unidentified destination, Installing](#)

Vicki is interested in finding out more about art auctions in the greater Boston area. She engages a search engine and tries to follow a link there. Her web browser consults a reputation service

which has recorded that the link target will attempt to subvert the browser and install malicious software.

- [Unidentified source, Identified destination, Installing](#)

Watching more cinema advertising, Doyle sees a somewhat irritating, but intriguing movie teaser that ends with a dark screen that has a URL fading away quickly. He mis-memorizes the URL. Coming back home, he types in what he remembers, and gets directed to a web site that immediately causes a software download. A pop-up window informs him (in graphical layout that matches the teaser's last screen) that software will be installed on his system in order to enable him to fully benefit from the web site's ~~multimedial~~[multi-media](#) offerings.

- [Unidentified source, Identified destination, Installing](#)

Steve runs a suite of security software on his machine that regularly upgrades certain components. The typical workflow is that a specific browser window is opened automatically. Steve will then control the selection of software upgrades, will download them from the web, and they will then be installed.

- [Unidentified source, Unidentified destination, Installing](#)

Once a week, Alice pays her bills. She opens her web browser, follows the habitual bookmark to her bank's site. A download process starts, and a pop-up window informs Alice that she needs to install a piece of software locally that will henceforth be her conduit for her future online interactions with her bank.

- Identified source, Identified destination, No interaction

Betty tries to connect to a web site at `<http://www.example.com/>`. She visits this site frequently to read various news and articles. Since her last visit, the site example.com has been compromised by some method, and visitors are now being infected with malware. At the time of the current request, Betty's user agent now has information saying that example.com is a known bad site. What interaction, if any, should occur?

- Unidentified source, Unidentified destination, No interaction

Frank regularly reads his email in the morning. This morning he receives an email that purports to be from his bank and asks him to verify a recent transaction by clicking on the link embedded in the email. The link does not display the usual URL that he types to get to his bank's website, but it does have his bank's name in it. He clicks on the link and is directed to a phishing site. The phishing site has been shut down as a known fraudulent site, so when Frank clicks on the link he receives the generic Error 404: File Not Found page. Frank is not sure what has occurred.

- [\[tjh: What about AJAX-type requests?\]](#)

[6.6 Threats](#)

The scenarios provided above are vulnerable to a wide range of threats. Threats which are in scope for

this Working Group are further discussed in [4 In scope](#). Section [5 Out of scope](#) covers threats which, though dangerous and important, will not be directly addressed by this Working Group. A comprehensive threat tree, for both in scope and out of scope threats, is work in progress; see [Web User Interaction: Threat Trees \[WSC-THREATS\]](#).

6.6.1 Subverted navigation

When following a hyperlink, the user may have an expectation, based on how they found the hyperlink, for what the destination page should be. These expectations will be misplaced if an attacker can replace the expected hyperlink with one that leads to a different destination page.

6.6.1.1 URL typo

In scenarios where the user types a URL into their browser, there is a risk of mistyping. An attacker can acquire the rights to common typo variants of a hostname and so cause the navigation to lead to an attack page, instead of the expected page.

6.6.1.2 Misleading bookmark

In scenarios where the user navigates to a page via a bookmark, there is a risk of selecting the wrong bookmark. Browsers commonly identify bookmarks by the corresponding page title, the value of which is chosen by the page author. If an attacker can convince the user to bookmark a page, using another pretense, the user will have a bookmark identified by a name of the attacker's choosing and leading to a page of the attacker's choosing.

6.6.1.3 Misleading introduction

Discussion forums and search engines serve content produced by others, or derived from content produced by others. A user may apply the trust they have for these sites to the hyperlinks they serve. Most often, this trust is well placed, since the sites aim to serve useful hyperlinks. An attacker, posing as a normal site contributor, may cause the site to serve a hyperlink to an attack page. In this case, a user may follow the hyperlink, and apply their trust for the site to the attacker's page.

6.6.1.4 Unprotected navigation

Most of the URLs currently in use do not use SSL, or similar protection. An attacker with access to the network layer can replace a requested URL with one of their own choosing. Consequently, even a hyperlink that refers to the expected destination page can be made to refer to a page of the attacker's choosing.

6.6.2 Web site impersonation

If an attacker is unable to subvert the navigation step, it still may be possible to convince the user that the attack page is the expected page. Techniques for doing this are described in [9 Problems with the status quo](#). That section discusses deficiencies in the browser user interface.

[\[tjh: Is the concept of mashups covered here? Portal and mashup environments are useful, but wind up blurring the source of the content being displayed. How does this impact our use cases and the definition of “web site”?\]](#)

7 Security information available to the user agent

This section provides an enumeration of the security information this Working Group has determined to be in scope and so available for use in recommendations. The Working Group's scope is detailed in sections [4 In scope](#) and [5 Out of scope](#). Information is grouped into sub-sections according to the references that should be consulted to determine its semantics.

7.1 Defined by web content specifications

- MIME type

The reported MIME type, along with other information the user agent may collect, such as filename extension, affect what user agent features are triggered by the receipt of web content.

- target URI

The target URI for an HTTP request is constructed according to the instructions provided by the web content from which the request was produced. The target URI determines the recipient of the request.

- presence of client-side dynamic content

The rendering of a web page composed of only static content has a completion point, after which the rendered view remains constant until the user chooses to navigate to another web page.

Dynamic content is anything that changes this interaction or is given additional access to user agent functions. Java and Javascript are two current examples, as is an HTML META tag specifying a page refresh.

- [Is the rendered view composed from multiple resources, such as referenced images or stylesheets? composition from multiple items on the same host](#)

The message communicated by a web page may be significantly affected by partial rendering. The web content specifies what resource the web page's author considered part of the rendered view.

- [Is the rendered view composed from resources from distinct hosts? composition of multiple items from distinct hosts](#)

When a web page includes by reference a resource from another host, the rendered view may be significantly different than the page author expected. For example, the HTML IMG tag can lead to such surprises. [There are also cases of using data:// and jar:// URI formats to consider.](#)

7.2 Defined by SSL related specifications

- SSL server certificate chain [\[PKIX\]](#)
 - certificate authority
 - distinguished name
 - public key
 - validity timeframe
 - extended validation [\[EV Cert\]](#)
- Ciphersuite
 - public key algorithm and key length
 - symmetric key algorithm and key length
 - message digest algorithm
- revocation status

Both CRLs [\[PKIX\]](#) and OCSP [\[OCSP\]](#) provide information about the revocation status of a certificate.

7.3 Defined by HTTP related specifications

- HTTP redirect [\[HTTP\]](#)
- HTTP-Auth handshake [\[HTTP Auth\]](#)
- cookie handling [\[HTTP Cookie\]](#)
- Must requests be transmitted using SSL? [\[HTTPS\]](#)
- [HTTP header information \(additional attributes\)](#)

7.4 Defined by IP related specifications

- server IP address
- localhost versus intranet versus internet
- network diagnostic information, such as provided by ping or traceroute

7.5 Defined by DNS related specifications

- server hostname
- DNSSEC protection of hostname lookup [\[DNSSEC\]](#)
- [DNS lookup results \(where the IP address came from – local hosts file, which DNS server\)](#)

7.6 Defined by user agent

- installed certificate authorities
- installed search engines
- [installed extensions](#)
- default window layout
- default bookmarks
- default configuration

7.7 State that may be collected by a user agent

- Has rendering of a page completed?
- referring page
- SSL session [\[TLS\]](#), if any, that protected content transmission
- submitted passwords
- submitted form values
- bookmarks
- browsing history
- [\[tjh: additional notes about a page as collected from the user at some point in the past?\]](#)
- installed client certificates
- installed server certificates
- How was the URL entered?
 - typed into address bar
 - pasted into address bar
 - clicked hyperlink
 - command from another application
- user agent customization
- user response to prompts

7.8 Defined by a third-party

- reputation service
- other visited web pages that link to the current page
- search engine results

8 Merits of the status quo

Successive generations of web user agents have improved upon past implementations and achieved greater deployment of security relevant infrastructure. This work provides a base upon which this Working Group will build its recommendations. This section calls out the aspects of the currently deployed web infrastructure that have already narrowed the problem space we need to address, or that we intend to learn from or build on.

8.1 Widely deployed, strong cryptography

Since its first deployment, the SSL protocol has undergone multiple revisions, culminating in the current TLS/1.1 protocol. Both client and server implementations are widely deployed, enabling applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

8.2 Many deceptive imitation techniques prevented

The most current generation of desktop web browsers contain several changes aimed at protecting users from the types of spoofing attacks seen in the past. Some of these changes are invisible to users, such as preventing a web site from opening a window which is larger than the visible desktop. Other changes are more noticeable, such as warning dialogs which alert users when they arrive at a website that matches an entry on a list of suspected phishing sites.

8.3 Corrected implementation errors

Recent web browsers correct many of the security relevant implementation errors in past browsers. Many errors in the implementation and application of the SSL protocol are now corrected.

8.4 Password management

Modern browsers include a password manager that can autofill the corresponding user login credentials for a web site. This feature provides several usability benefits that can help users notice and avoid web based attempts to steal their passwords. Autofilling provides a presentation cue indicating the credentials have been previously submitted to the web site. The user may then infer that the current operation is simply a repeat of a past trust decision, rather than a new trust decision: the decision to give the web site the corresponding password has already been made. A password manager can also eliminate the step of typing a password into a web page, a step highly vulnerable to phishing.

9 Problems with the status quo

Though much implementation progress has been made, there remain problems with the basic design for communicating security information to the user, which is the core of the mission of this Working Group. In current user agents, security information is primarily presented through modal dialog boxes and indicators in the browser's chrome. Chrome is the representation through which the user interacts with

the user agent itself, as distinct from the web content accessed. In graphical layout terms, chrome is the part of the user agent window outside of the area displaying the current web page. This user interface has a number of inherent problems, as well as problems created by the current realization.

9.1 Poorly defined area for chrome

The above definition of chrome reveals a major shortcoming in the concept. Chrome is primarily defined by where it is not, rather than where it is. As a result, there are a number of tricks for confusing the user about which parts of their screen contain browser chrome.

9.1.1 Picture in picture

Modern desktop operating systems support overlapping windows of varying sizes. A smaller browser window overlaying a larger browser window can be visually indistinguishable from a larger browser window displaying a picture of a smaller browser window in the web page area. Using dynamic content technology, this picture of a window can be given functionality that closely mimicks that of a real browser window. In this case, the user may treat the web page content as a real browser window and believe the imitation chrome is real chrome.

This level of visual deception may be unnecessary to fool many users. Studies have demonstrated that many users still do not fully grasp the flexibility of the desktop metaphor and wrongly believe the security indicators of one browser window also pertain to another located on top of, or next to it. [\[Why Phishing Works\]](#)

9.1.2 Visually extending the chrome

The strongest visual cue the user is given for the boundary between the chrome area and the web page area is a change in background color. The chrome uses the background color for application menus, typically a light grey, and the web page area uses whatever background color it wishes, but typically white. There is nothing preventing the webpage from using the same background color as the chrome area for part of the web page area near the chrome. In this case, the chrome area may appear to be extended with additional security indicators specified by the web page. In addition, color only cues often do not work for users who are color blind.

Curiously, recent releases of prominent browsers now use a similar technique to present security information to the user from the web page [content](#) area. Typically the chrome extension uses a light yellow background [and appears near the top of the area](#). A web page could provide an identical presentation with a message like: "This web page is guaranteed by Example Inc. to be safe for e-commerce."; where the name Example Inc. would instead be a brand name widely trusted by users. Since users have been conditioned by the browser to expect relevant security information to be presented in this way, they may trust the message.

9.1.3 Removing the chrome

Employing the above visual tricks may be unnecessary for a successful attack, since the browser may support removing the chrome from a browser window, at the discretion of the visited web site. In this event, the vacated area of the browser window becomes additional web page area. Simply depriving the user of the chrome's security indicators may be sufficient, or the attacker could display imitation chrome in the same area the user expects to find real chrome.

9.2 Poorly defined role for chrome

Replacing the real chrome with imitation chrome may be unnecessary for a successful attack, since currently all of the indicators in the chrome display information chosen by the attacker. By choosing values for these indicators which are likely to deceive the user, the attacker can produce an imitation of the victim web site using the real chrome, rather than imitation chrome. It is unclear in what way the user should rely on the chrome, when the chrome displays only information chosen by the attacker. Following is an exhaustive list of the indicators found in the chrome of common web browsers, and the corresponding source of the displayed information.

9.2.1 Browser window title

The browser's window title is constructed using the content of the HTML TITLE element from the displayed web page. The attacker has full control over the content of the displayed web page.

In a browser with multiple tabs for viewing multiple web pages, the tab title also uses the content of the TITLE element.

9.2.2 Back and forward buttons

Both the back and forward navigation buttons provide a drop down list of previously viewed pages. Each page is identified by the content of the corresponding HTML TITLE element.

9.2.3 URL bar

The current web page's URL is chosen in tandem by the creator of the referring hyperlink and the web site operator. When an attacker is directing victims to an imposter web site, the attacker is both the creator of the referring hyperlink and the web site operator.

Some browsers provide an additional display of the hostname of the visited web site. The displayed hostname is taken from the current web page's URL. An attacker can choose any hostname that is not already in use, including ones that may deceive users. See section [**9.3.2 Hostname**](#) for additional discussion.

9.2.4 Padlock icon

The padlock icon indicates the use of SSL. The decision to use SSL, or not, is again at the discretion of the creator of the referring hyperlink and the web site operator. In a phishing scenario, the attacker still

plays both these roles. When the web site operator is an independent party it may redirect a URL chosen by the attacker to an SSL protected URL; however, this redirect is delivered over the original unprotected connection.

9.2.5 Favicon

Websites can specify a small graphic to act as an icon that appears in the URL bar in most desktop web browsers and on the tabs in some browsers [\[Favicon\]](#). While the desktop web browsers control this chrome, none place any restrictions on the type of websites or the content of the images that will be displayed. Consequently, an imposter web site can display the icon of an impersonated web site in the web browser's chrome.

A website may also choose to display a favicon that looks exactly like the padlock icon that is displayed in the URL bar by many browsers to indicate an SSL connection. In this case, the user may believe that SSL is being used, when it is not.

9.2.6 Status bar

By default, the status bar displays messages from the browser, such as the target of the hyperlink under the mouse cursor. The displayed web page can also display any message of its choosing in this area.

9.2.7 Information bar (aka: notification bar)

Some desktop web browsers use a colored bar called an information bar (or notification bar) across the top of the web content window to communicate with users. These messages are specific to the content of the web content window, and usually alert the user to the fact that a potentially undesirable action has been suspended, such as the automatic installation of software or the opening of a new web content window.

While the content of the information bar is controlled by the web browser, a convincing replica of this interface can easily be created by a malicious web site and placed at the top of their content.

9.3 Poor user understanding of chrome

Employing a great deal of deception might also be unnecessary for a successful attack, since studies have shown many users have a poor understanding of the chrome. The current chrome indicators provide a thin summary of raw technical artifacts drawn from the network protocol's current exchange. The full meaning of these protocol artifacts is not necessarily understood by users.

9.3.1 Padlock icon

The presence of the padlock icon in the chrome only indicates the current web page was transmitted using the SSL protocol. The icon does not denote a guarantee of trustworthiness, nor is it an indication of legitimacy; an imposter site can be accessed using the SSL protocol. On its own, the fact that SSL was used is not actionable. The fact must first be paired with many others before a warranted decision can be

made. Nevertheless, some studies have shown the presence of a padlock icon, when it is noticed, contributes to a user's vague sense of security [\[Users' conceptions\]](#). Relying on the padlock icon in this way is not supported by the mere use of SSL by a web page.

9.3.2 Hostname

DNS is a hierarchical name space. Name assignments on upper layers of this name space are controlled by various policy and business processes and often thought of as identifiers for real-world entities; name assignments on the lower layers are typically chosen freely and often thought of as identifiers for individual hosts or services. However, these intricacies are not widely understood. Studies show that users will interpret brand names that occur on any level of a domain name as a signal that allows them to assume some kind of reliable association between the brand and the domain name [\[Security Toolbars\]](#).

9.3.3 Chrome versus page

Perhaps the most surprising result of user studies is that the distinction between chrome and page area does not exist in the minds of many users. Professional looking content is deemed a more reliable indicator of legitimacy. A padlock icon appearing in the page area has the same significance as one in the chrome [\[Security Toolbars\]](#). Whether an indicator in the chrome is a security indicator, or a decoration set by the web page is unclear [\[Why Phishing Works\]](#). Given the reality of the current functionality of the chrome, these user perceptions are quite reasonable. Current chrome is just a decoration whose content is largely, or entirely, determined by the visited web site.

9.3.4 Explanations versus understanding

Users come to an understanding of security indicators predominantly through use and direct experience, and somewhat through general awareness (discussions with others, news and other information they might receive). Users knowing about the padlock icon at all, for example, shows that user education does happen over time. Experience and history with education on using computer software indicates that users do not learn and act exactly on what is explicitly taught them (for an example of that in user security, see [\[Make Up Your Mind\]](#)). Explicit user education does not override other problems and [does not](#) consistently alter user behavior.

9.4 Poor usability of chrome

Even if the chrome was perfectly implemented and fully understood by users, it still might not, as currently designed, provide effective protection.

9.4.1 Out of sight, out of mind

Browsing the web involves reading text, clicking hyperlinks and filling out forms; all activities which take place entirely within the web page area of the browser window. Consequently, studies have shown that users rarely consult the chrome, instead focusing on the task at hand. Even when the chrome has not been tampered with and is providing the intended presentation, it goes unnoticed by users [\[Security](#)

[Toolbars](#)], [\[Why Phishing Works\]](#).

9.4.2 Assumed safety

Current chrome decorates web pages that provide security information, and remains silent about those that provide none. This design creates multiple problems.

It is difficult for humans to react to the absence of something. Studies have shown that users do not reliably notice the absence of security indicators [\[Why Phishing Works\]](#).

Users, and even experts, commonly attribute more security than is warranted to a web page that is not protected by SSL. A login form on such a page can be readily modified in transit such that it will send the user's login credentials to an attacker before logging the user into the authentic web site.

9.4.3 Poor usability of dialog boxes

Desktop software commonly reports problems through modal pop-up dialog boxes. Such dialog boxes frequently appear during normal software use. Also, the user is frequently given no reasonable course of action other than clicking the OK button. Consequently, users have been conditioned to automatically dismiss such dialog boxes, often without even glancing at their content. User studies confirm this phenomena also holds for security warnings from web browsers [\[Why Phishing Works\]](#).

10 Process

Though research incorporating usable security goes back to the principle of "psychological acceptability" from *Saltzer and Schroeder* [\[Saltzer and Schroeder\]](#), making security usable is still a nascent area for research [\[Security and Usability\]](#). There are no worked examples of formal standards from standards making bodies on usable security to emulate. There are a limited number of worked examples in deployed products to learn from. There are a larger number of attempts with unclear results to learn from. We have yet to get widely-applicable, satisfactory answers to basic questions on usable security. Consequently, this Working Group's recommendations will necessarily contain more innovation than might a traditional standards effort. This section details the process the Working Group will employ to mitigate the significant perils of innovation in a standards effort.

10.1 Expertise and experience

By its very nature, the public reviews of the deliverables of this Working Group via the W3C standards process will provide pertinent and timely input from researchers and practitioners in a variety of disciplines, including usability and design, security, and accessibility. That feedback may be based on experience with other standards efforts, experience prototyping or developing software or devices, experience with deployment or use of software or devices, or other forms of anecdotal evidence. This data represents experience and knowledge that has not been or cannot be captured via document principles, previous studies, or the working group's testing. The Working Group will use such feedback to inform our recommendations.

10.2 Reliance on general usability expertise

Though principles and examples of usable security are scarce, expertise on the general usability of software is more plentiful. Principles of usability aim to help the user understand presented information, discover the actions that can be taken, predict the implications of those actions and so learn how the tool can be made to serve the user's needs. These aims are also a prerequisite for usable security. Listed below are design principles, drawn from the research literature, recognized by the Working Group as relevant to usable security.

10.2.1 Affordance

An element of a user interface should include cues that help the user discover its features [\[Design of Everyday Things\]](#).

10.2.2 Conceptual model

A user will develop a personal model of what something does and how it works. The user interface should present cues that assist the formation of this model and ensure that the actual and perceived state of the system are consistent [\[Design of Everyday Things\]](#).

10.2.3 Match between system and the real world

The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order [\[Ten Usability Heuristics\]](#).

10.2.4 Habit formation

Persistent use of any interface will cause the user to develop habits. A user interface should leverage habit formation to shape the user's workflow [\[Humane Interface\]](#).

10.2.5 Single locus of attention

A user has only a single locus of attention, a feature or an object in the physical world, or an idea, about which they are intently and actively thinking. Humans ignore things that aren't their current locus of attention. The user's locus of attention is only held in short term memory and so will be quickly forgotten once their attention shifts. [\[Humane Interface\]](#).

10.2.6 Aesthetic and minimalist design

Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility [\[Ten Usability Heuristics\]](#).

10.2.7 Help users recognize, diagnose, and recover from errors

Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution [\[Ten Usability Heuristics\]](#).

10.2.8 Provide explanations, justifying the advice or information given

If the user is expected to carry out a task or an action to achieve the desired level of security, they should have access to an explanation that justifies why it is necessary.

10.2.9 Understand the user

Design should begin with an understanding of the intended users. This includes population profiles that reflect training, motivation, and goals [\[Designing the User Interface\]](#).

10.2.10 Create task profiles

With the intended user in mind, designers should formally write down user tasks [\[Designing the User Interface\]](#).

10.2.11 Consistency

The cues should be displayed consistently in location and across sites and web user agents in an attempt to prevent spoofing and user confusion. [\[Designing the User Interface\]](#).

10.3 Learning from past efforts

A growing body of research documents presentation techniques that have not proved effective in providing usable security. The results of these studies will be used to judge the expected effectiveness of presentation techniques. The Working Group will keep abreast of ongoing studies and subject potential recommendations to review by usability experts from both inside the Working Group, and from outside.

Section [9 Problems with the status quo](#) contains a summary of much of what has been learned about phishing. Additional results are listed below.

10.3.1 No user categories in phishing vulnerability

In Why Phishing Works [\[Why Phishing Works\]](#), neither education, age, sex, previous experience, nor hours of computer use showed a statistically significant correlation with vulnerability to phishing.

10.3.2 The user must be aware of the task they are to perform

The user must be aware that a decision is to be made, what information should be used to make the decision, and where to look for the information [\[Johnny\]](#).

10.4 Implementation and testing

Part of a Working Group's activities is developing code and test suites [\[W3C Process\]](#).

The Working Group aims to demonstrate and test the WG's recommendations on usable and robust communication of security context information through implementations within the framework of one or more web user agents. The most likely web user agents to serve as platforms for such implementations are web browsers. To demonstrate that recommendations are sufficiently general and interoperable, we expect implementation in the context of at least two web user agents.

We are targetting three types of testing of our recommendations: functional testing, robustness testing, and usability testing [\[W3C Testing\]](#).

All test development and testing is iterative. The recommendations may need to be modified on the basis of all three types of testing. Test development starts when work on the specification starts. Test planning will include guidelines for developing tests. Test suites are typically developed when the specifications are in a reasonably stable state, such as the first full public working draft. Test development will include test execution instructions. Automation of the tests will be considered but is unlikely, as the tests will require human visual confirmation. Clear descriptions of what to expect and how to judge outcome will be part of each test.

Functional testing against the sample code and appropriate deployment configurations will verify that the recommendations can be translated to web user agent code, with no functional ill effects on the rest of the web user agent. It will show that implementations can conform to the recommendations, and that the specifications clearly define behaviors. This is also called conformance testing.

Robustness testing will verify that the recommendations are robust against spoofing attacks. Existing spoofing attacks will be documented, and new spoofing attacks aimed directly at the recommendations (both required and recommended) will be developed. All of these attacks will take the form of web site content returned to the user agent (most typically DHTML or XML that a web browser GETs).

Usability testing will verify that the recommendations provide usable display of security context information. The type of usability testing we do will depend on both the direction of our recommendations and the resources the Working Group is able to tap into. The Working Group aims to perform low fidelity prototyping and testing with a modest number of test subjects (10 - 20) for each proposed practice that involves user feedback [\[Tiny Fingers\]](#). This will be reflected in Candidate Recommendation exit criteria. Prototyping at this level will provide feedback in early design phases at a point where needed changes can be made easily. It will also create a more user-centered design process and will help in the realization of our goals that address usability.

More extensive user testing will be desirable, and is expected to contribute to higher-quality outcomes. More extensive tests may include:

- Incremental testing incorporating feedback from previous iterations
- Recruiting participants from broader groups which better represent target user groups, either in size or relevant characteristics

- Lab testing of sample code, for example [\[Johnny 2\]](#)
- Contextual or "in the wild" testing of sample code [\[Social Phishing\]](#)
- More iterative combinations of the above, throughout the specification lifecycle

11 Acknowledgments

This note is based on input from Tyler Close, Thomas Roessler, Mary Ellen Zurko, Bill Doyle, Maritza Johnson, Phill Hallam-Baker, Hal Lockhart, Brad Porter, Dan Schutzer, Stephen Farrell, Stuart Schechter, Tim Hahn, Luis Barriga, Mike Beltzner, Al Gilman, Rich Salz, Ian Fette, and the members of the Web Security Context Working Group. It has also benefitted from general public and working group commentary on earlier drafts.

12 References

DNSSEC

[DNS Security Introduction and Requirements](#); R. Arends, R. Austein, M. Larson, D. Massey, S. Rose; IETF RFC 4033; 2005.

Design of Everyday Things

The Design of Everyday Things; Donald Norman; Doubleday; 1988.

Designing Trust

[Designing Systems That People Will Trust](#); Andrew S. Patrick, Pamela Briggs, and Stephen Marsh; Security and Usability: Designing Secure Systems that People Can Use, ed. Lorrie Faith Cranor and Simson Garfinkel; 2005.

Designing the User Interface

[Designing the User Interface](#); Ben Shneiderman; Addison Wesley; 2005.

EV Cert

[Extended Validation SSL Certificates - A New, Higher Standard for Internet Security](#); CA/Browser Forum; 2006.

Favicon

[How to Add a Favicon to your Site](#); Karl Dubost; W3C Quality Assurance; 2006.

HTTP

[Hypertext Transfer Protocol -- HTTP/1.1](#); R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee; IETF RFC 2616; June 1999.

HTTP Auth

[HTTP Authentication: Basic and Digest Access Authentication](#); J. Franks, P. Hallam-Backer, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart; IETF RFC 2617; 1999.

HTTP Cookie

[HTTP State Management Mechanism](#); D. Kristol, L. Montulli; IETF RFC 2965; 2000.

HTTPS

[HTTP Over TLS](#); E. Rescorla; IETF RFC 2818; 2000.

Humane Interface

[The Humane Interface: New Directions for Designing Interactive Systems](#); Jef Raskin; 2000.

Johnny

[Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0](#); Alma Whitten and John D Tygar; Usenix; 1999.

Johnny 2

[Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express](#); Simson L. Garfinkel, Robert C. Miller; Symposium On Usable Privacy and Security; 2005.

Make Up Your Mind

[Did You Ever Have To Make Up Your Mind? What Notes Users Do When Faced With A Security Decision](#); Mary Ellen Zurko, Charlie Kaufman, Katherine Spanbauer, Chuck Bassett; Proceedings of the 18th Annual Computer Security Applications Conference; 2002.

OCSF

[X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSF](#); M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams; IETF RFC 2560; 1999.

PKIX

[Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile](#); R. Housley, W. Polk, W. Ford, D. Solo; IETF RFC 3280; 2002.

Saltzer and Schroeder

[The Protection of Information in Computer Systems](#); Jerome Saltzer and Michael Schroeder; Proceedings of the 4th Symposium on Operating System Principles; ACM Press; 1973.

Security Toolbars

[Do Security Toolbars Actually Prevent Phishing Attacks?](#); Min Wu, Robert C. Miller and Simson L. Garfinkel; Conference on Human Factors in Computing Systems (CHI 2006); 2006.

Security and Usability

[Security and Usability: Designing Secure Systems that People Can Use](#); Lorrie Faith Cranor, Simson Garfinkel; O'Reilly; 2005.

Social Phishing

[Social Phishing](#); Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer; School of Informatics Indiana University, Bloomington; 2005.

TLS

[The TLS Protocol Version 1.0](#); T. Dierks, C. Allen; IETF RFC 2246; 1999.

Ten Usability Heuristics

[Ten Usability Heuristics](#); Jakob Nielsen; [useit.com](#); 1994.

Tiny Fingers

Prototyping for tiny fingers; M. Rettig; Communications of the ACM, April, Vol.37, No.4.; 1994.

Users' conceptions

[Users' Conceptions of Web Security: A Comparative Study](#); B. Friedman, D. Hurley, D.C. Howe, E.

Felten, H. Nissenbaum; Conference on Human Factors in Computing Systems (CHI 2002); 2002.

W3C Process

[World Wide Web Consortium Process Document](#); Ian Jacobs; W3C; 2005.

W3C Testing

[Test Development FAQ](#); W3C Quality Assurance; 2005.

WCAG

[Web Content Accessibility Guidelines 1.0](#); Wendy Chisholm, Gregg Vanderheiden, Ian Jacobs; W3C Recommendation; 1999.

WEBAARCH

[Architecture of the World Wide Web, Volume One](#); Ian Jacobs, Norman Walsh; W3C Recommendation; 2004.

WSC-CHARTER

[Web Security Context Working Group Charter](#). World Wide Web Consortium, last modified 17 October 2007. This version is <http://www.w3.org/2005/Security/wsc-charter>.

WSC-THREATS

[Web User Interaction: Threat Trees](#), T. Roessler, Editor, W3C Working Group Note (work in progress), 1 November 2007. This version is <http://www.w3.org/TR/2007/NOTE-wsc-threats-20071101/>. The [latest version](#) is available at <http://www.w3.org/TR/wsc-threats/>.

Why Phishing Works

[Why Phishing Works](#); Rachna Dhamija, J.D. Tygar and Marti Hearst; Conference on Human Factors in Computing Systems (CHI 2006); 2006.