# CWE Detail – CWE-451

## Description

The user interface (UI) does not properly represent critical information to the user, allowing the information - or its source - to be obscured or spoofed. This is often a component in phishing attacks.

## Extended Description

If an attacker can cause the UI to display erroneous data, or to otherwise convince the user to display information that appears to come from a trusted source, then the attacker could trick the user into performing the wrong action. This is often a component in phishing attacks, but other kinds of problems exist. For example, if the UI is used to monitor the security state of a system or network, then omitting or obscuring an important indicator could prevent the user from detecting and reacting to a security-critical event. UI misrepresentation can take many forms: Incorrect indicator: incorrect information is displayed, which prevents the user from understanding the true state of the product or the environment the product is monitoring, especially of potentially-dangerous conditions or operations. This can be broken down into several different subtypes. Overlay: an area of the display is intended to give critical information, but another process can modify the display by overlaying another element on top of it. The user is not interacting with the expected portion of the user interface. This is the problem that enables clickjacking attacks, although many other types of attacks exist that involve overlay. Icon manipulation: the wrong icon, or the wrong color indicator, can be influenced (such as making a dangerous .EXE executable look like a harmless .GIF) Timing: the product is performing a state transition or context switch that is presented to the user with an indicator, but a race condition can cause the wrong indicator to be used before the product has fully switched context. The race window could be extended indefinitely if the attacker can trigger an error. Visual truncation: important information could be truncated from the display, such as a long filename with a dangerous extension that is not displayed in the GUI because the malicious portion is truncated. The use of excessive whitespace can also cause truncation, or place the potentially-dangerous indicator outside of the user's field of view (e.g. "filename.txt .exe"). A different type of truncation can occur when a portion of the information is removed due to reasons other than length, such as the accidental insertion of an end-of-input marker in the middle of an input, such as a NUL byte in a C-style string. Visual distinction: visual information might be presented in a way that makes it difficult for the user to quickly and correctly distinguish between critical and unimportant segments of the display. Homographs: letters from different character sets, fonts, or languages can appear very similar (i.e. may be visually equivalent) in a way that causes the human user to misread the text (for example, to conduct phishing attacks to trick a user into visiting a malicious web site with a visually-similar name as a trusted site). This can be regarded as a type of visual distinction issue.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2004-2227: Web browser's filename selection dialog only shows the beginning portion of long filenames, which can trick users into launching executables with dangerous extensions.

**•** CVE-2001-0398: Attachment with many spaces in filename bypasses "dangerous content" warning and uses different icon. Likely resultant.

**•** CVE-2001-0643: Misrepresentation and equivalence issue.

**•** CVE-2005-0593: Lock spoofing from several different weaknesses.

**•** CVE-2004-1104: Incorrect indicator: web browser can be tricked into presenting the wrong URL

**•** CVE-2005-0143: Incorrect indicator: Lock icon displayed when an insecure page loads a binary file loaded from a trusted site.

**•** CVE-2005-0144: Incorrect indicator: Secure "lock" icon is presented for one channel, while an insecure page is being simultaneously loaded in another channel.

**•** CVE-2004-0761: Incorrect indicator: Certain redirect sequences cause security lock icon to appear in web browser, even when page is not encrypted.

**•** CVE-2004-2219: Incorrect indicator: Spoofing via multi-step attack that causes incorrect information to be displayed in browser address bar.

**•** CVE-2004-0537: Overlay: Wide "favorites" icon can overlay and obscure address bar

**•** CVE-2005-2271: Visual distinction: Web browsers do not clearly associate a Javascript dialog box with the web page that generated it, allowing spoof of the source of the dialog. "origin validation error" of a sort?

**•** CVE-2005-2272: Visual distinction: Web browsers do not clearly associate a Javascript dialog box with the web page that generated it, allowing spoof of the source of the dialog. "origin validation error" of a sort?

**•** CVE-2005-2273: Visual distinction: Web browsers do not clearly associate a Javascript dialog box with the web page that generated it, allowing spoof of the source of the dialog. "origin validation error" of a sort?

**•** CVE-2005-2274: Visual distinction: Web browsers do not clearly associate a Javascript dialog box with the web page that generated it, allowing spoof of the source of the dialog. "origin validation error" of a sort?

**•** CVE-2001-1410: Visual distinction: Browser allows attackers to create chromeless windows and spoof victim's display using unprotected Javascript method.

**•** CVE-2002-0197: Visual distinction: Chat client allows remote attackers to spoof encrypted, trusted messages with lines that begin with a special sequence, which makes the message appear legitimate.

**•** CVE-2005-0831: Visual distinction: Product allows spoofing names of other users by registering with a username containing hex-encoded characters.

**•** CVE-2003-1025: Visual truncation: Special character in URL causes web browser to truncate the user portion of the "user@domain" URL, hiding real domain in the address bar.

**•** CVE-2005-0243: Visual truncation: Chat client does not display long filenames in file dialog boxes, allowing dangerous extensions via manipulations including (1) many spaces and (2) multiple file extensions.

**•** CVE-2005-1575: Visual truncation: Web browser file download type can be hidden using whitespace.

**•** CVE-2004-2530: Visual truncation: Visual truncation in chat client using whitespace to hide dangerous file extension.

**•** CVE-2005-0590: Visual truncation: Dialog box in web browser allows user to spoof the hostname via a long "user:pass" sequence in the URL, which appears before the real hostname.

**•** CVE-2004-1451: Visual truncation: Null character in URL prevents entire URL from being displayed in web browser.

**•** CVE-2004-2258: Miscellaneous -- [step-based attack, GUI] -- Password-protected tab can be bypassed by switching to another tab, then back to original tab.

**•** CVE-2005-1678: Miscellaneous -- Dangerous file extensions not displayed.

**•** CVE-2002-0722: Miscellaneous -- Web browser allows remote attackers to misrepresent the source of a file in the File Download dialog box.

## Related Attack Patterns (CAPEC)

* CAPEC-154
* CAPEC-163
* CAPEC-164
* CAPEC-173
* CAPEC-98

## Attack TTPs

**•** T1566.002: Spearphishing Link (Tactics: initial-access)

**•** T1598.003: Spearphishing Link (Tactics: reconnaissance)

**•** T1566.001: Spearphishing Attachment (Tactics: initial-access)

**•** T1598.002: Spearphishing Attachment (Tactics: reconnaissance)

**•** T1534: Internal Spearphishing (Tactics: lateral-movement)

**•** T1566: Phishing (Tactics: initial-access)

**•** T1598: Phishing for Information (Tactics: reconnaissance)

**•** T1566.003: Spearphishing via Service (Tactics: initial-access)

**•** T1598.001: Spearphishing Service (Tactics: reconnaissance)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Hide Activities, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Implementation: Perform data validation (e.g. syntax, length, etc.) before interpreting the data. (Effectiveness: N/A)

**•** Architecture and Design: Create a strategy for presenting information, and plan for how to display unusual characters. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Notes

**•** Maintenance: This entry should be broken down into more precise entries. See extended description.

**•** Research Gap: Misrepresentation problems are frequently studied in web browsers, but there are no known efforts for classifying these kinds of problems in terms of the shortcomings of the interface. In addition, many misrepresentation issues are resultant.