Too Much, Too Late: What Just-in-Time Notifications Really Indicate

David G. Gordon
Carnegie Mellon University
5000 Forbes Ave.
Pittsburgh, PA
dggordon@cmu.edu

Janice Tsai
Microsoft Research
One Microsoft Way
Redmond, WA 98052
Janice.Tsai@microsoft.com

ABSTRACT
Whether through cleverly designed phishing websites, malicious downloads, or other means, users face numerous ways through which they may unintentionally compromise their privacy or security. Often, these problems are addressed via just-in-time notifications, with the potential risks of the user's decision communicated immediately prior to the action's execution. These notifications can be very valuable, and are able to convey a myriad of information, including the options available and their potential harms, contextually relevant details, resources for additional education, and more. However, we believe that these notifications can be an indicator of another issue: the lack of a comprehensive risk communication process. In this short paper, we discuss two examples and the issues underlying them.

Categories and Subject Descriptors
D.4.6 [**Security & Protection**]: Risk Communication, Verification

General Terms
Design, Security, Human Factors

Keywords
Privacy, security, warning, just-in-time, notification

1. INTRODUCTION
Whether downloading files, checking e-mails, or just browsing the Internet, users are frequently at risk of compromising the privacy or security of valuable information. The consequences of compromised information are substantial: for an individual, this could result in identity theft, reputational damage, a loss of data - and for an organization, exposure of trade secrets, damage to internal systems, or worse. Communicating these risks to the user is of great importance, and has been the focus of a significant body of research [ECH08, HC09]. A common method in which users are warned is through the use of pop-up or just-in-time (JIT) warnings [MSDN].

Warnings are generally defined as safety communications that inform people about hazards so that they may be minimized or avoided altogether [MSW09]. They can serve multiple purposes, including reminding the individual about the hazard, effecting individual's behavior in an effort to reduce harm, and providing relevant details so the individual can make a more informed decision [MSW09]. For the purposes of this paper, we classify just-in-time warnings as warnings that are delivered to the user immediately prior to the context in which it is relevant. In the context of IT security and privacy, two prominent examples of just-in-time warnings include web browser notifications regarding Secure Socket Layer (SSL) certificate errors [SEA09], and operating system dialogs requiring confirmation from the user before opening a file that was downloaded from the internet [APP13, WIN13].

The effectiveness of these and similar warnings has been empirically tested [SEA09], and they continue to see improvement. Despite their value, however, we believe that these warnings and others like them are indicative of another issue: a lack of comprehensive risk communication. As JIT warnings serve as a last resort prior to the decision faced by the user, their composition or mere presence can serve as a warning to educators and developers that existing risk communication prior to the JIT warning is incomplete or otherwise ineffective.

In this short paper, we discuss two JIT warnings - browser SSL Certificate Errors, and "confirmed execution" dialogs for downloaded files - and the issues underlying them.

2. SIGNALING ISN'T EDUCATING
The need to communicate securely online led to development of the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. When implemented correctly, a website uses a special certificate to verify the identity of the website and to encrypt the communication with a user's web browser. A number of problems can arise during this process: a certificate may be revoked (i.e. was fraudulently used or obtained), the website identity may not match that contained in the certificate, the certificate may be out of date, or the certificate may not be from a trusted source [SEA09]. In some cases, this problem is attributable to human error, and in others, it is the result of malicious intent. All modern browsers notify the user of these errors and ask whether they wish to continue onwards to the website.

Research has shown that these warnings should not be issued frivolously, as over inundating the user can cause them to lose their impact and be ignored [WMG06, ECH08, SEA09]. Although early examples of these warnings were confusing and unhelpful for users, examination of current approaches, such as that used in Google Chrome (**Figure 1**), follow many guidelines for effective warnings, such as including the listing consequences of the hazard and avoiding technical terms [MSW09].

Too much information: We agree that progress has been made in this area and that current warnings are both more comprehensible and informative. However, users continue to disregard these warnings. We believe that the problem can

be discerned from the warning itself, which is tasked with educating the user just as much as signaling the user. Notice the volume of text in **Figure 1**; the warning assumes (correctly) that the user has little or no knowledge of certificate errors, the potential harms that may result from them, or the likelihood of these harms [SEA09]. The warning does an admirable job including this information, but in so doing indicates that any prior risk communication on this topic has been largely ineffective or nonexistent.

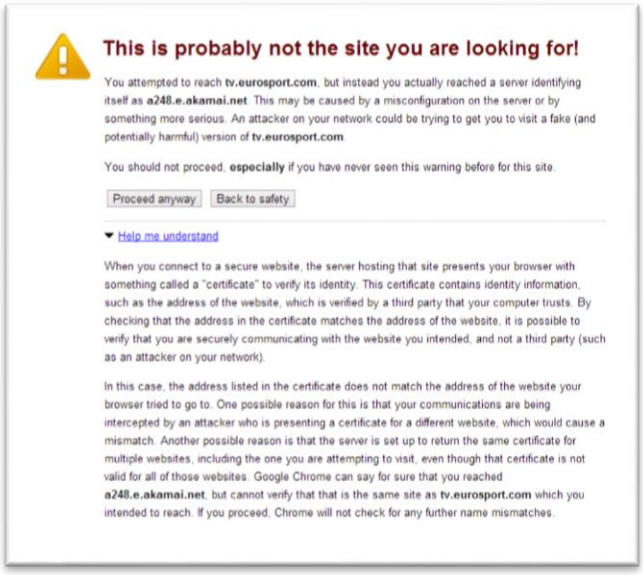

Figure 1. SSL Certificate Error in Chrome v. 26

3. ADDRESSING BIGGER PROBLEMS

As downloaded files are a common source of malware and viruses, many modern operating systems have mechanisms in place that make use of JIT warnings, notifying the user the first time they try to open the file [APP13, WIN13]. An example can be seen in **Figure 2**, which comes from OS X 10.7; note that the warning includes the name of the file, as well as the time and location it was downloaded.

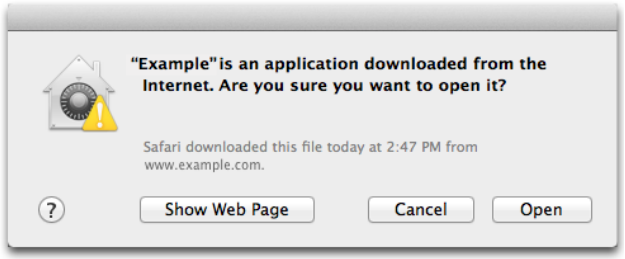

Figure 2. Downloaded File Warning from OS X 10.7 [APP13]

Too late: In most cases, we can assume that the user would have reasonable expectations of the name, source, and time a file was downloaded before opening it, as well as the results of opening it. In this way JIT warnings may be beneficial in that they allow users to recognize when their expectations to not match reality, though such cases are rare. More importantly, though, is the timing of the warning: *after* the user has already attempted to open the file. The user is already focused on their task and more likely to ignore any interruptions. If the user is in the habit of opening files without knowing their origin, they clearly do not have an understanding of the risks of doing so. This lack of understanding cannot be fixed with a JIT warning.

4. CONCLUSION

We do not advocate for the removal or alteration of JIT warnings; when used correctly, they can be an effective component of a larger risk communication effort. However, JIT warnings lack the development and thoroughness of other forms of risk communication [MF01]. Providing this support is a complex and nontrivial challenge, and there are already efforts to ensure users have the right knowledge before encountering these decisions. JIT warnings are indeed a solution, but if tasked with user education, or misdelivered, they are indeed too much, too late.

5. REFERENCES

[APP13] Apple. About file quarantine in OS X. Online. Available: http://support.apple.com/kb/ht3662. 2013.

[ECH08] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In CHI '08: Proc. of the SIGCHI conf. on Human factors in Computing Systems, pages 1065–1074, New York, NY, USA, 2008. ACM.

[HC09] Herley, C.: So long, and no thanks for the externalities: the rational rejection of security advice by users. In: Proceedings of the 2009 Workshop on New Security Paradigms Workshop, NSPW 2009, pp. 133–144. ACM, New York. 2009.

[MF01] Morgan, Granger M., Fischoff, B. et al. Risk Communication: A Mental Models Approach. Cambridge University Press, USA. 2001.

[MSDN] Microsoft Developers' Network. Warning Messages. Online Available: http://msdn.microsoft.com/en-us/library/windows/desktop/aa511263.aspx. 2013

[MSW09] Wogalter, M.S.: Purposes and scope of warnings. In: Wogalter, M.S. (ed.) Handbook of Warnings. Human Factors and Ergonomics, 1st ed., pp. 3–9. Lawrence Erlbaum Associates, Mahwah. 2006.

[SEA09] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying Wolf: An empirical study of SSL warning effectiveness. In Proceedings of 18th USENIX Security Symposium, pages 399–432, 2009.

[WIN13] Microsoft. Downloading files from the internet: frequently asked questions. Online. Available: http://windows.microsoft.com/en-us/windows7/downloading-files-from-the-internet-frequently-asked-questions. 2013.

[WMG09] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI '06), pages 601–610, New York, NY, USA, 2006.