# Password Knight

## Protecting Users from Insecure Password Fields

**Sameer Patil**
Helsinki Institute for Information Technology HIIT
Aalto University, 00076 Aalto Finland
sameer.patil@hiit.fi

**Tanvi Vyas**
Mozilla Corporation
Mountain View, CA 94041, USA
tanvi@mozilla.com

**Problem:**
Nowadays, people typically use a great of variety online services. As a result, entering a password to login to these accounts is a routine Web task. However, Web pages do not always make it apparent whether the entered password will be encrypted during transmission. Login forms on unencrypted Web pages (i.e., pages delivered using the HTTP protocol) leave passwords vulnerable to man-in-the-middle attacks. Even if the login form is on a page using an encrypted protocol (i.e., HTTPS), this does not guarantee that the page will transmit the password securely. In fact, indicators for the "secure" status of a login page, such as the familiar lock icon, may lead users to a false sense of security regarding transmission of login information. When the password is transmitted in cleartext, it can be captured by third parties. Moreover, if the HTTP GET protocol is used, the password is included as part of the URL. When the password is included in the URL, it is also captured in various server and system logs, further increasing vulnerability to attacks from malicious intruders.

A compromised password can impact privacy in two important ways. Firstly, it allows access to sensitive and identifiable information held in the compromised account. Secondly, it could enable access to more than a single account owing to password reuse across accounts [2] and/or discovery of other passwords from information stored in the compromised account.

**Current Solutions:**
Browsers typically warn users of these risks by displaying a dialog box informing them when a form will be transmitted without encryption. However, the effectiveness of these warnings may be limited because:

- users may ignore the warning due to habitual "swatting away" of dialog boxes [3], and
- users may not understand the practical meaning of the information, especially if the text uses technical jargon [1].

**Password Knight:**
Password Knight[1] is a Firefox Web browser extension that aims to overcome these shortcomings and increase the effectiveness of mechanisms that protect users from insecure password fields on Web pages. To avoid the limitations of warning dialogs, Password Knight places its warnings right near the context of use: within the password field itself (see Figure 1). In order to prevent security warning fatigue, the warnings appear only when a user shows the intent to login by interacting with the login form. The warnings are displayed as easy-to-interpret visual icons that can be easily understood by lay users. Hovering over the icon displays relevant text information. When Password Knight encounters an insecure login page, it can search for a corresponding secure login page. If a secure alternative exists, Password Knights provides the user an option to switch.

[1] Password Knight: https://addons.mozilla.org/en-US/firefox/addon/password-knight

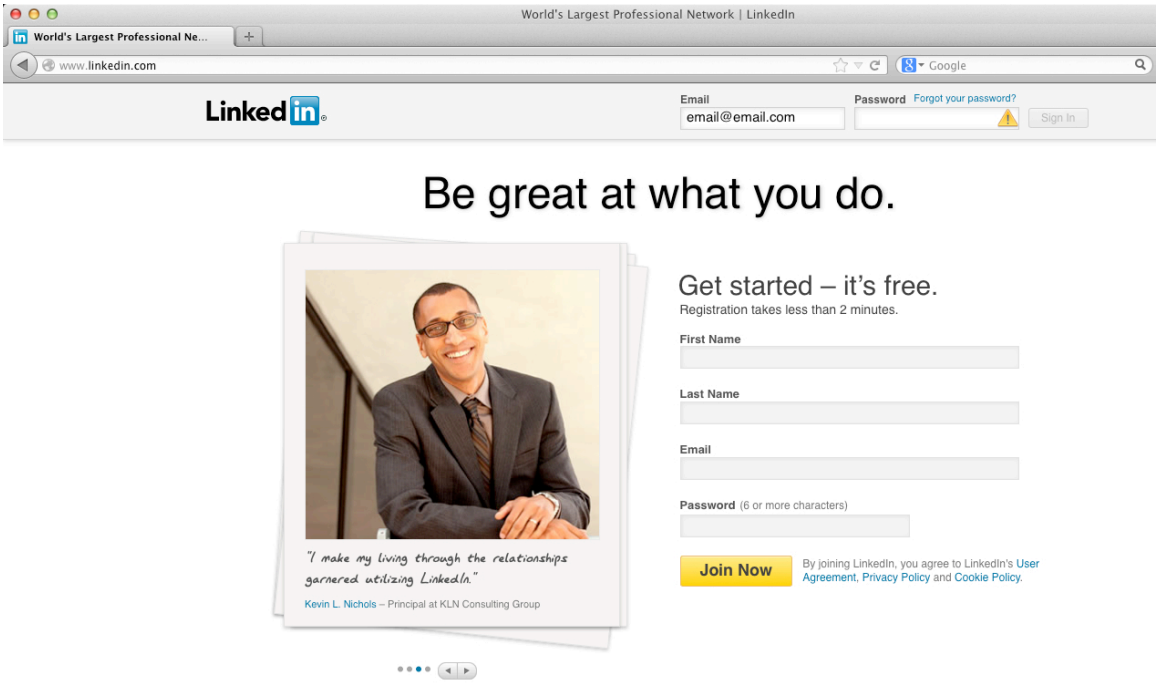


*Figure 1: Password Knight warns of insecure transmission of the password from a Web page.*

**Challenges:**
When designing and building Password Knight, we encountered several challenges. In particular, we found that several special cases – such as flash-based forms, iFrame-based site designs, etc. – can make it difficult and/or impossible to detect insecure password transmission. Password Knight currently ignores such cases and handles only commonly encountered types of login pages. Further work is needed to ensure exhaustive coverage of login mechanisms. A second challenge was trying to determine whether a secure version of a given login page existed. Given the absence of a standard repository that can be queried for such a purpose, Password Knight currently uses techniques such as checking whether the URL can be accessed by switching to the secure (i.e., HTTPS) protocol. However, such an approach does not work if the secure version of a Web site uses a different domain and/or path. Password Knight and similar tools can benefit from a standardized repository of secure URLs for login pages on the Web. It should also be noted that we decided against automatically redirecting users to secure pages; users do not always login when they visit pages and implementing automatic redirect when users do not intend to login can unnecessarily burden the infrastructures of the underlying sites.

**Future Work:**
We are currently developing plans for user evaluation of Password Knight. We anticipate iterative improvement based on feedback from user studies. Although Password Knight is currently a browser extension, we hope that its functionality will eventually be incorporated into the Firefox browser core.

**Acknowledgments:**
We acknowledge Kasper Hirvikoski, Erno Hopearuoho, Juho Kallio, Carolina Lindqvist, Titti Malmivirta, and Paul Sawaya for their help in the coding and development of Password Knight.

## References:


1. Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. Android permissions: User attention, comprehension, and behavior. In Proceedings of SOUPS 2012: The Eighth Symposium on Usable Privacy and Security, SOUPS '12, ACM (New York, NY, USA, 2012), 3:1–3:14.
2. Ives, B., Walsh, K. R., and Schneider, H. The domino effect of password reuse. Communications of the ACM 47, 4 (Apr. 2004), 75–78.
3. Krol, K., Moroz, M., and Sasse, M.-A. Don't work. Can't work? Why it's time to rethink security warnings. In (CRiSIS) 2012: 7th International Conference on Risk and Security of Internet and Systems (2012), 1–8.