October 06, 2017

Hash comparisons to provide warnings of phishing attacks

Pedro Gonnet Anders

Hash comparisons to provide warnings of phishing attacks

ABSTRACT

This disclosure describes techniques to warn users when a password for a particular online domain is being submitted by a user device to a domain different than the one for which it was originally registered. The warning alerts the user of possible phishing attacks. Cryptographic hashes of user passwords along with corresponding domains are stored. When a user attempts to send data to a website, e.g., via form submission, hashes of the data are calculated and compared with the stored hashes of password. In the case of a match, a warning is presented to the user. The techniques can be implemented as a feature of a web browser, a browser plugin, as standalone software, as part of an operating system, etc.

KEYWORDS

- phishing
- password manager
- password hash
- security

BACKGROUND

Phishing is a type of online attack where a hacker poses as a trustworthy entity, such as a bank, a social networking site, etc., in an attempt to obtain sensitive information such as usernames, passwords, financial information, etc. from a user. Phishing attacks also include attackers pretending to be someone else, e.g., by setting up fake websites that imitate websites that users access commonly, e.g., social networking, e-mail websites, bank websites, ecommerce websites, etc. Users may not realize when accessing such fake websites that they are providing sensitive information to hackers. Once user information is obtained, hackers can use such

information to represent themselves as the user to obtain more information or to engage in harmful activities such as identity theft, bank fraud, etc.

Software, including web browsers, plugins for web browsers, password management tools, etc. can store usernames and/or user passwords, when permitted by a user. Users find such features convenient, e.g., since it saves users the effort to remember such information. Some tools also include features to automatically generate secure passwords for the user. A user can use such software for automatic generation and entry of passwords, e.g., for various websites. While such software offers ease of use, it does not mitigate phishing attack that tricks users into revealing information.

DESCRIPTION

This disclosure describes techniques that automatically detect form submissions that include user password information to unverified or fake websites. When such submissions are detected, the user is warned of a potential phishing attack and asked to provide confirmation to submit the form data.

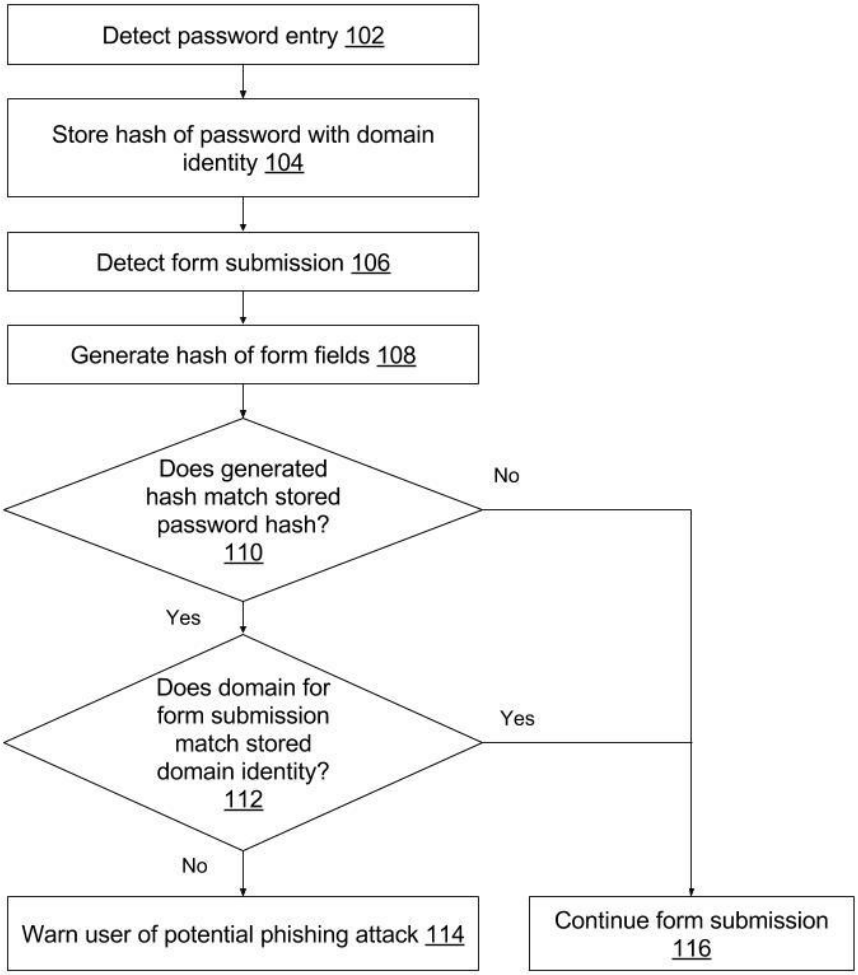

Fig. 1: Generating warning of potential phishing attack

Fig. 1 illustrates the technique to prevent phishing attacks using password management features. The techniques can be implemented as a feature of a web browser, a browser plugin, as standalone software, as part of an operating system, etc. The techniques are implemented upon specific user permissions, e.g., to store user data such as domain names, password hashes, etc. If the user does not provide permission, the techniques are not implemented.

With user permission, it is detected when a user enters a password, e.g., for a website (102). When the user provides consent, a cryptographic hash of the password is stored along with the identity of the web domain to which the password is submitted (104). The cryptographic hash

is a one-way hash from which the original password cannot be extracted. This is implemented for every password that the user enters. For example, the password entry is recognized when the user signs up at a website, logs in to a website, etc.

At each future instance when a user attempts to submit information to a website, e.g., via form submission, such submission is detected (106) if user has provided consent. The values of different fields of the form are hashed using the same techniques used to generate the cryptographic hash of the password (108). The generated hashes of the form fields are compared with the stored password hashes (110).

If none of the generated hashes match a stored password hash, it is determined that no password data is being sent and thus, form submission is completed (116). If one or more of the generated hashes match a particular stored password hash, it is determined whether the domain for the form submission matches a stored domain identity associated with the particular stored password hash (112). When the domain identities match, it is determined that the password information is being sent to the domain that is associated with the password, and therefore, form submission is continued.

If the domain identities do not match, it is determined that the password information is being sent to a domain that is not associated with the stored password, which is indicative of a potential phishing attack. In this instance, a warning is provided to the user indicating that the website for form submissions does not match that associated with the password (114). The user can then abort the form submission, thus preventing user information from being sent to potentially malicious website. Form submission is continued if the user provides confirmation, e.g., when the same password is used for different domains. The techniques of this disclosure do

not store passwords directly, and are thus suitable for users who do not permit storage of passwords.

Further, the stored hash used for matching can be only a portion of the cryptographic hash of the password. This provides a benefit in that the user password is not recoverable from the stored partial hash, e.g., in case of a dictionary attack. However, this can result in multiple passwords matching to the same stored hash and cause false positives during detection; however, the cost is relatively small, since the user can dismiss warnings generated due to such a match. Further, a password obtained by a dictionary attack on the partial hash will not let an attacker successfully log in as a user, and the user can rely on features by which most online services block or suspend user accounts due to too many failed login attempts.

The techniques described herein are implemented upon specific user permission. The techniques can be implemented in such a manner that a user can skip checking of form submissions for certain web pages, domains, types of domains, etc. Further, the user can designate certain domains for which matching of password hashes is not performed. The techniques can be used in combination with other security mechanisms to enhance security. Password hashes and domain identities are stored only upon specific user permission, and only as permitted by the user. The use of stored hashes is restricted to determine potential attacks and the stored hashes are not used otherwise.

In situations in which certain implementations discussed herein may collect or use personal information about users (e.g., user data, information about a user’s social network, user's location and time at the location, user's biometric information, user's activities and demographic information), users are provided with one or more opportunities to control whether information is collected, whether the personal information is stored, whether the personal

information is used, and how the information is collected about the user, stored and used. That is, the systems and methods discussed herein collect, store and/or use user personal information specifically upon receiving explicit authorization from the relevant users to do so. For example, a user is provided with control over whether programs or features collect user information about that particular user or other users relevant to the program or feature. Each user for which personal information is to be collected is presented with one or more options to allow control over the information collection relevant to that user, to provide permission or authorization as to whether the information is collected and as to which portions of the information are to be collected. For example, users can be provided with one or more such control options over a communication network. In addition, certain data may be treated in one or more ways before it is stored or used so that personally identifiable information is removed. As one example, a user's identity may be treated so that no personally identifiable information can be determined. As another example, a user's geographic location may be generalized to a larger region so that the user's particular location cannot be determined.

CONCLUSION

This disclosure describes techniques to warn users when password for a particular online domain is being submitted by a user device to a different domain. The warning alerts the user of possible phishing attacks. A cryptographic hash of user passwords along with corresponding domains are stored. When a user attempts to send data to a website, e.g., via form submission, hashes of the data are calculated and compared with the stored hashes of password. In the case of a match, a warning is presented to the user.