HTTP PGP Authentication

Patrick Grasso

Mark Wilson

Jonah Mania

Stevens Institute of Technology

ABSTRACT

We will provide a proof-of-concept for PGP key-based authentication via HTTP as an extension to [RFC 7235]. While this is not the first attempt to create a key-based client authentication protocol, it lends from the benefits of PGP and the Web of Trust. PGP public-key infrastructure already exists for public key sharing and key certification and has been thoroughly peer-reviewed. We present a way to build atop this infrastructure, providing authentication on the web without the need for a password for each site the user authenticates with.

1. Problem Statement

HTTP was initially developed without much concern for security, as the early web consisted mainly of static, public documents. As stateful HTTP [RFC 6265] and user-oriented services began to appear, the need for authentication and security became more imperative. Today, there exists a mechanism for authentication in the HTTP 1.1 protocol [RFC 7235], which can be extended with new methods of authentication. The authentication is not frequently used, but websites will implement their own version of the same thing. This method entails password authentication, which is heavily relied upon but often does not provide sufficient security (1).

2. Importance of the Problem

Password authentication has, for many years, been shunned for a few reasons. One of these is that the security factor is dependent on the user's ability to create a hard-to-guess password, which many users do not do. As a result, if the database containing the hashed passwords and their respective salts is leaked, it can sometimes be fairly trivial to recover the original passwords.

Users will often re-use the same password for multiple services, which is problematic if one of these services has a security breach and users' passwords are able to be recovered by the attacker. Moreover, good passwords are difficult to remember and frequently forgotten by users. To solve this, some services provide the ability to reset one's password by sending an email to the address associated with one's account. This places trust in the mail services that users use to receive e-mail, trust which may be misplaced.

The reason for password authentication's popularity is its flexibility and usability. It does not require techinical knowledge and does not depend on the same machine being used to access the site. While password authentication relies only on what the user **knows** (as opposed to what she **has**, as is the case for public-key authentication), PGP has many

benefits which outweigh the cost of carrying around a private key.

3. Previous Approaches

HOBA (HTTP Origin-Bound Authentication) [RFC 7486] uses signature-based authentication with a key pair attached to the user's agent (browser). This method follows the spirit of our approach, but lacks the benefits of PGP's public key infrastructure and Web of Trust. Users' information associated with keys published in public key servers (e.g. pgp.mit.edu) can be used to supply account information for services utilizing our proposed authentication method (2).

OBCs (Origin-Bound Certificates) were proposed as a solution to client authentication by modifying TLS so that the server would check certificates held by the client in addition to verifying the server's x509 certificate. This solution operates below the application level, which perhaps targets a use case for client authentication different from that which we are trying to address (3).

4. Proposal Description

We proprose to implement the HTTP Authentication type and in a web client. The server will offer the WWW-Authenticate header upon access to restricted resources. Instead of the header will contain relevant <options>. The client, upon seeing this, will ask the user for confirmation before signing the nonce and returning it to the server. From this, the server should be able to query PGP services for information about the key used to sign the nonce and use that to populate account information (e.g. email address, which is typically used as a user ID).

5. Project Evaluation

We will implement a prototype to demonstrate the potential capabilities for such a protocol. The server should be able to verify the signature that a client has provided via HTTP. The client agent should be able to identify the HTTP WWW-Authenticate header with PGP as the authentication type and query the user to determine whether or not to continue the login flow. If the user chooses to proceed, the agent will sign the nonce provided by the server and return it in another HTTP request.

References

1. R. Fielding, and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Authentication," RFC 7235 (Jun 2014).
2. S. Farrell, P. Hoffman, and M. Thomas, "HTTP Origin-Bound Authentication (HOBA)," RFC 7486 (Mar 2015).
3. Michael Dietz, Alexei Czeskis, Dirk Balfanz, and Dan S. Wallach, "Origin-Bound Certificates: A Fresh Approach to Strong Client Authentication for the Web," *Proc. of 21st USENIX conference on Security symposium*, pp. 16-16 (Dec 2012).