Technical Disclosure Commons

Defensive Publications Series

December 04, 2017

Secure web proxy resistant to probing attacks

Benjamin Schwartz

Secure web proxy resistant to probing attacks

ABSTRACT

Secure web proxies are popular for sending internet traffic via alternative paths. Access to a secure web proxy is typically password protected. A malicious third party that does not know a username or password can detect a secure web proxy server by attempting a connection and observing a distinctive response from the proxy server, e.g., an HTTP 407 Proxy Authentication Required response. Traffic from clients that utilize web proxy servers that are detected in this manner can then be blacklisted.

The techniques of this disclosure enable secure web proxies that are resistant to probing attacks. The output of distinctive signals by the proxy servers is limited to authorized clients by making use of a secret key known only to such authorized clients.

KEYWORDS

- Secure proxy
- Probing attack
- HTTP 407
- Proxy probing
- Web server
- Shared secret

BACKGROUND

Secure web proxies (e.g., HTTPS proxy servers) allows for transmittal of confidential information over the internet. Secure web proxies transmit client traffic via alternative and anonymized paths. Access to a secure web proxy is controlled typically by a username and password arrangement.

A malicious third party that does not know a username or password can identify a secure web proxy server by attempting a connection and observing the distinctive response from the proxy server, e.g., a HTTP 407 Proxy Authentication Required response. This is known as a probing attack. Attackers use proxy probing to discover proxy servers. Once the proxy servers are discovered, attackers can use various techniques to block such servers or users that are detected as using the servers.

There are some non-standard proxy server technologies that can resist probing attacks. However, servers that implement such technologies are not compatible with large installed base of browsers and other client software that can communicate with a secure web proxy.

DESCRIPTION

A typical password-protected connection between a client and a secure web proxy server proceeds in the following manner. The client is configured to be aware of the proxy server. To fetch a resource over the network, the client attempts to connect to the proxy server, and requests the resource. If the proxy server is password-protected, it responds with an HTTP 407 Proxy Authentication Required response. The client then retries the request, and transmits a username and password to the proxy server.

Once the authentication is successful, the client software stores information indicative of having received the 407 response from the proxy server. In subsequent requests, the client software includes the username and password. Thus, during each client session, all requests from the client software other than the initial request include the username and password, and the proxy server transmits only a single HTTP 407 response.

As explained previously, the HTTP 407 response potentially reveals existence of the secure web proxy server to malicious third parties. To achieve probing resistance, techniques of

this disclosure limit HTTP 407 responses by the proxy server to queries from authorized clients. If a request is received from a client (or party) that is not authorized, the proxy server does not emit HTTP 407 response. However, per current standards, clients do not include the username and password in the request until after the 407 response is received from the server. Thus, the server cannot use the username and password to determine whether the client is authorized or not. Also, to maintain compatibility with existing clients, it is important that no changes be imposed on the protocol.

To allow existing clients to prove their authorization, techniques of this disclosure introduce a concept referred to as the Secret Destination. A specific destination, or set of destinations, is identified as the Secret Destination, and the first valid request from the client to a proxy server includes the Secret Destination as a domain name or URL. The value of the Secret Destination is known to authorized clients and unknown to a malicious client. The proxy server is implemented such that it responds with an HTTP 407 response only when the incoming client request includes the Secret Destination. Proxy requests to other destinations are either rejected in the manner of a normal (non-proxy) web server or, if they include a correct username and password, served as a proxy request.

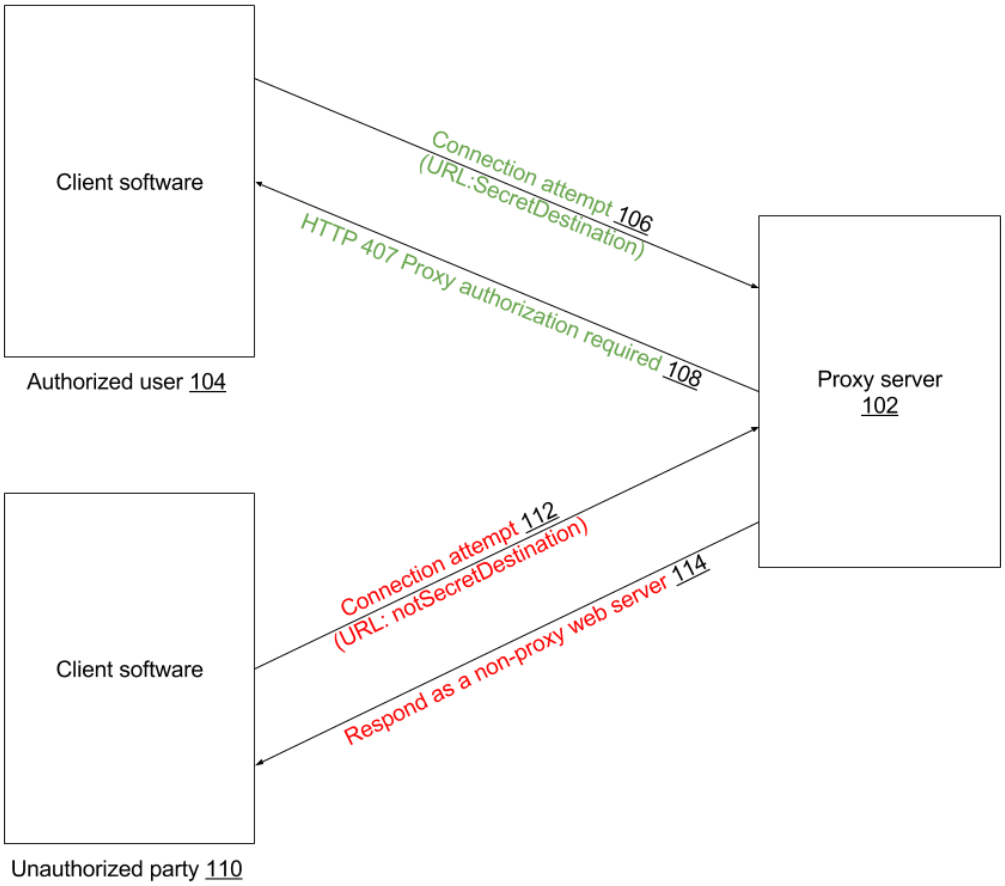

Fig. 1: Limiting proxy authorization required responses to authorized users

The communications interchange between two clients and a proxy server is illustrated in Fig. 1. Client software of an authorized user (104) attempts to connect with proxy server (102). The connection attempt (106) from the client software includes the Secret Destination. The proxy server responds with an HTTP 407 proxy authorization required message (108).

In contrast, a connection attempt (112) by an unauthorized party (110) does not include the Secret Destination (or can include an incorrect Secret Destination). The proxy server responds (114) as would a normal (non-proxy) web server, e.g., with no emission of an HTTP 407 response. In this manner, the probing attack is thwarted.

Per techniques of this disclosure, to use a web proxy server, the client software is configured to use the proxy server, which includes, e.g., sending connections requests that include the Secret Destination. For example, users may enter the Secret Destination as an address in the address bar of a client browser. The user can also provide a username and password to be included in the request. For the remainder of the session between the client software and the proxy server, all queries are directed through the proxy, with appropriate credentials. In this manner, techniques of this disclosure achieve probing resistance without a need to install additional software or to make changes to existing client software.

The techniques do not rely on preemptive client authentication. For example, the techniques do not require that the client include username and password in the initial request. In this manner, the techniques are compatible with most existing client software, e.g., popular web browsers that do not implement preemptive authentication.

CONCLUSION

Techniques of this disclosure harden the resistance of secure web proxy servers to probing attacks. A web proxy server limits distinctively emitted signals, such as an HTTP 407 response only to requests from authorized clients. Authorized clients are configured to include a secret destination in the connection request to the web proxy server.