Software Update Security Framework: Client Library Replay and Freeze Attack Protection

Justin Cappos, University of Washington
Justin Samuel, University of Washington

1. Overview

Replay and freeze attacks pose a great risk to software update systems. Most software update systems are vulnerable to these attacks, putting their users in jeopardy. The software update security framework's client library will be used by software update systems to check for and obtain updates from a repository while remaining secure against these attacks. Developers integrate the client library into their own software update systems, thus they include it with the software they distribute.

This document covers the client library, how it is used, and how it protects against replay and freeze attacks. The details of the metadata file formats and definitions of some terms used in this document are provided in the repository library design document.

Modern software update systems are also insecure in other ways. These issues include the lack of selective trust delegation as well as the lack of a secure means of key revocation. These issues are outside the scope of this document and will be addressed in the client library after replay and freeze attack protection has been implemented.

2. Design Goals

The client library will handle all aspects of metadata verification, determination of available software updates, and download and verification of updates.

The client library will provide a simple interface through which software update systems can check for and obtain updates made available by developers. The client library will not perform the actual update of software on client systems. Once the updates are downloaded and verified, the client library has performed its duties and the installation of the updates is left to the software update system.

In the case of inability to check for updates, including in the event of a replay or freeze attack, the client library notifies the software update system of the problem. The client library will not have the responsibility of deciding on the correct course of action in all error situations. This is because the correct course of action will vary for different applications and users. Instead, the client library will provide the software update system with relevant information about the situation.

3. Update Process

The following steps outline the process of checking for and obtaining updates. Only some of these steps are visible to the software update system using the client library.

1. Query. The software update system asks the client library to check the repository for the latest software updates.

2. Retrieve Metadata. The client library securely retrieves signed metadata that describes the available software updates. After verifying the signatures on the metadata, the client library checks the timestamp in the metadata to

ensure that the file is not older than the last metadata the client has seen. The client library also checks the expiration time listed in the signed metadata to ensure that it has not expired.

3. Interpret Metadata. The client library uses the downloaded and verified security metadata to decide which software updates are available.

4. Inform. The client library informs the software update system whether software updates are available and provides the details of any available updates.

5. Request Updates. The software update system uses the information about available updates to determine which software update files it wants to download. It then tells the client library to download these files. The software update system does not download any files directly.

6. Retrieve Updates. The client library retrieves the requested software update files from the repository mirrors.

7. Verify Updates. The client library verifies the integrity and authenticity of the downloaded software update files. It does this by comparing the cryptographic hash and the length of each downloaded file with the same information listed in the signed metadata.

8. Provide Updates. The client library provides the verified files to the software update system.

9. Install Updates. The software update system installs the updates. This step is performed without any involvement from the client library.

4. Threat Model and Analysis

When the client library prevents replay and freeze attacks from being successful, it does not mean that a client will always be able to obtain updates during the attack. Fundamentally, an attacker positioned to intercept and manipulate a client's communication will always be able to prevent the client from obtaining updates. The aspects the client library has control over are the prevention of incorrect updates and the detection of a failure to obtain updates.

Replay attacks. In a replay attack, the adversary answers client requests with old versions of files that previously existed on the repository. Even if the metadata files are properly signed and unexpired, if the client were to accept files that were older than those which the client had previously seen, the client could be tricked into "updating" to old versions of software with known vulnerabilities. An attacker could then compromise the client by exploiting these vulnerabilities.

The client library protects against replay attacks by checking timestamps in the signed metadata to ensure that metadata files retrieved from the repository are never older than previously accepted metadata. By ensuring that new metadata files are always more recent than the last, replay attacks are prevented from being successful.

Freeze attacks. A freeze attack is similar to a replay attack in that the adversary is responding to client requests with old but properly signed metadata. However, with a freeze attack, the adversary is not trying to trick the client into installing previous and exploitable versions of software. Instead, the goal of the attack is to prevent the client from being aware of available updates. If successful, the attack allows the adversary more time to exploit vulnerabilities in the current version of software the client has installed.

The client library protects against freeze attacks by watching the expiration dates of cached and downloaded metadata to identify whether unexpired metadata cannot be obtained. As with replay attacks, freeze attacks may not always indicate an attack. Outdated repository mirrors may also provide old metadata. Also similar to replay attacks, an adversary who can prevent a client from obtaining current metadata can always prevent a client from obtaining updates. The client library's role in such a situation is to detect the problem and notify the software update system

which can then take appropriate measures. In many cases, this will simply involve the software update system notifying the user of the inability to obtain updates and providing information about how the user can proceed if the problem persists. Importantly, the client library ensures that the user will not remain unaware that their software is outdated and potentially vulnerable.