J4 The Authenticity of Questioned Pretty Good Privacy (PGP) -Signed Digital Documents

Martin S. Olivier, PhD, University of Pretoria, Pretoria, GP 0028, SOUTH AFRICA*

Learning Overview: The goal of this presentation is to question the authentication of digitally signed documents and whether they will stand the test of time based on a case study involving 55 PGP-signed documents.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by highlighting the many problems encountered (primarily obtaining a public key or finding grounds for trusting a public key). This presentation also points toward basing trust in keys on known good exchanges where the key was used.

In principle, authentication of digitally signed documents is a simple computational process. PGP was created in 1991 as a cryptographic tool that enabled users to communicate privately, but also to achieve a range of other functions, including the ability to sign documents.[1] For over three decades, PGP (or PGP-compatible software) was a standard tool for users who wanted to encrypt and/or sign documents. The open source implementation (the GNU Privacy Guard [GnuPG]) is based on the OpenPGP standard.[2] This presentation uses the term PGP to refer to any implementation PGP of functionality.

While other (better) solutions than PGP have been developed, none have achieved the widespread acceptance and name recognition PGP has. The shortcomings of PGP are well known, but when used correctly, PGP remains useful.[3]

One question about authentication of digitally signed documents is whether they will stand the test of time. This presentation presents a case study in which 65 documents signed with PGP have been examined to determine whether their authenticity can (still) be established. The dates of these documents range from July 22, 1998, to May 15, 2018. The primary tool used for signature examination was Gpg4win—an implementation of GnuPG for Microsoft® Windows®. Gpg4win version 3.1.10 released on July 14, 2019, was used.

The 65 documents were not selected randomly; thus results cannot be generalized. Moreover, problems encountered can be seen as predictable, based on PGP critiques. However, an empirical case study provides insight into the relative prevalence of such expected problems.

The selection of older documents was intentional: The forensic document examiner is often confronted by authenticity of older documents, such as a last will or an old contract. The first problem (predictably) stemmed from the age: the signatures were associated with defunct email addresses.

Consider a specific example: one of the files examined was signed by the signator on October 19, 1998. The key remains available on public key servers, even though the associated address has not been used for well over 15 years. The key is not signed by a third party; the signator removed the key long ago from his keyrings. Backups were found, but were corrupted. Two options existed (claim ownership or sign the key). However, both rely on the signator's recollection of key authenticity. Both lead to "successful" verification of the document.

Some general remarks can be made about observations in this case study. About half of the keys used to sign documents were available from key servers. However, none of the keys were signed by third parties. Hence, key servers were not useful to find a chain of certificates between any key used and the a signator's key. Availability of about half of the public keys made it possible to proceed with verification if grounds existed to trust the public key.

As noted, many keys are linked to obsolete email addresses, which complicates signer identification. Users arguably do not have much information available. In any case, relying on the user's cooperation enables repudiation. Web searches were performed for key fingerprints but yielded no useful information for any search.

Another problem: about half the keys found on key servers had expired. Gpg4win in such a case reports "The signature is invalid: Signing certificate is expired." GnuPG 1.4.20 and GnuPG 2.1.11 on Lunix® produced potentially more useful results (with the caveat about trusting the key). It reports "Good signature", but warns the user (twice) that the key had expired.

The problem of key authenticity is pervasive. One promising possibility remains: where the key has been used in other exchanges known to be valid, such knowledge may be used as grounds to trust the key. An email interchange between two users who know one another is one possible example.

Reference(s):

1. Garfinkel, Simson. 1994. *PGP: Pretty Good Privacy*. O'Reilly.
2. Callas, J., L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer. 2007, November. *OpenPGP Message Format.* Request for comments 4880, IETF.
3. Whitten, Alma, and J.D. Tygar. 1999, August. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*. Washington, DC, 169–184.

Digital Signatures, Questioned Digital Documents, PGP

*Presenting Author