Global Information Assurance Certification Paper

ADK Exploit to PGP
Steven Gillis
September 13, 2000

On August 24, 2000, Ralf Senderek, a researcher from Germany, announced the discovery of an exploit in Pretty Good Privacy (PGP). While this exploit requires several concurrent conditions to be met in order to work, it none the less presents a potential way for an attacker to decrypt messages sent with PGP security added.

This exploit centers on the use of Additional Decryption Keys (ADKs). PGP uses ADKs to provide a third party (usually an employer) a way to decrypt messages in the event the owner of a PGP key is no longer employed or not available. In order to understand how this exploit works, one must first understand how ADK works with PGP.

As stated, ADK was developed for the corporate customers of PGP to recover from the loss of the owner of a PGP key to their respective employer. Examples of this would be employee termination or in a worst case scenario, the loss of an employee's life. The use of ADKs is an option available only with the commercial versions (not the freeware) 5.5 through 6.5.3. ADKs are add-ons to the unhashed area of the existing private key of a PGP user. In theory, allowing "authorized extra decryption keys to be added to a user's public key certificate does this". [1] The exploitation takes advantage of the way that this extra decryption key is added and detected by PGP key users.

As discovered, "an implementation flaw in PGP allows unsigned ADKs which have been maliciously added to a certificate to be used for encryption.

Data encrypted with PGP 5.5.x through 6.5.3 using a modified certificate will generate ciphertext encrypted with the ADK subject to the conditions list in the impact section. The attacker who modified the certificate can obtain the plaintext from this ciphertext". [1]

In addition, "PGP does not correctly detect this form of certificate modification because it fails to check if the ADK is stored in the signed (hashed) portion of the public certificate. As a result, normal methods for evaluating the legitimacy of a public certificate (fingerprint verification) are not sufficient for users of vulnerable versions of PGP". [1]

Philosophically, these vulnerabilities fly in the face of the original assurances that ADKs could only be added with the consent of the owner of the private key. Additionally, "ADKs were designed for use within a closed group of individuals, i.e. in a company and will not affect the use of user's keys who do not wish to benefit from ADKs". [2] As seen, these assurances were not fully realized.

Specifically, Ralf Senderek's research reached these conclusions:

1. Any DSS/DH-key can be manipulated to comprise new ADKs without the user's consent or knowledge. The manipulated keys perform as well as if the user had included the ADKs for himself originally.
2. RSA-keys which are transformed into the new key-format with a new self-signature can be fortified with ADKs in the same way.
3. If you want to avoid to risk those manipulations being made on your own key or on other users' keys you are well-advised to use PGP-2.6x, or PGP-Classic, which guarantees that only ADK-safe signatures will be made and which rejects to use DH-keys or RSA-keys in the new format reliably. [2]

While the exploit of ADKs certainly exists, there must be a series of conditions present to work. These conditions are:

- the sender must be using a vulnerable version of PGP
- the sender must be encrypting data with a certificate modified by the attacker
- the sender must acknowledge a warning dialog that an ADK is associated with the certificate

- the sender must already have the key for the bogus ADK on their local keyring
- the bogus ADK must be a certificate signed by a CA that the sender trusts
- the attacker must be able to obtain the ciphertext sent from the sender to the victim [1]

In addition the CERT Advisory CA-200-18 points outs that the use of ADKs are clearly visual by "viewing the keys in a GUI interface". [1]

As one can see, such a series of conditions are unlikely to occur. Phil Zimmermann, the creator of PGP, puts it better when he notes that "it would not be an easy scam to pull off, because chances are, the sender does not have the bogus ADK on his keyring, and even if he goes through the extra trouble to get it from a server, the bogus ADK is probably not going to be signed by a Certificate Authority trusted by the sender, so PGP will object to him using that ADK to encrypt the message. This is a daring attack, an attack that has a very high probability of being detected". [3]

Therefore, in order to further reduce the threat of this exploit it is important that all keys are checked for ADKs before being added to ones keyring. Any ADK from unknown keys should be especially scrutinized. Version 6.5 of PGP has corrected this ADK flaw. In addition, CERT CA-2000-18 suggests that one "make a reliable copy of your public certificate publicly available". [1]

References:

[1] Unknown. "CERT Advisory CA-2000-18 PGP May Encrypt Data With Unauthorized ADKs". Last Revised: August 29,2000.
URL: http://www.cert.org/advisories/CA-200-18.html (9/10/2000).

[2] Senderek, Ralf. "Key-Experiments – How PGP Deals With Manipulated Keys".
URL: http://senderek.de/security/key-experiments.html (9/12/2000).

[3] Zimmermann, Phil, "Message from Phil Zimmermann, Creator of PGP".
URL: http://www.pgp.com/other/advisories/phil-message.asp (9/12/00)

Unknown. "PGP ADK Security Advisory". Last Update: September 5, 2000.
URL: http://www.pgp.com/other/advisories/adk.asp (9/10/2000)