The Flamel-DaVinci Clairvoyancy Algorithm

Vedaal Nistar[φ]

Abstract. This paper describes a devastating new cryptanalytic Clairvoyancy attack vector, for which there is, as yet, no known defense. We describe a new Clairvoyancy algorithm, verifiable by the non-Clairvoyant cryptographic community.

1 Introduction

It has long been known, that those who can See with the Inner Eye, can easily discern the plaintext within its ciphertext covering. There has been a recurring problem, however, that Intelligence agencies that have relied upon Seer cryptanalytic techniques, have been presented with the plaintexts of intercepted ciphertexts, but without a means to verify that the plaintext indeed corresponds to the ciphertext in question. In fact, there have been some who have gone as far as to suggest, (not without reason), that the plaintexts were *fabricated*[1]. This has further been complicated by the lack of a verifiable testing mechanism, as the Seer community has repeatedly taken the position that the Inner Eye cannot be taxed with trifles such as decrypting test ciphertexts of known plaintexts, and must instead be reserved for gazing upon only those intercepted ciphertexts of great moment and significance. [2]

This paper will now describe a verification mechanism agreeable to both the Seer and non-Clairvoyant cryptographic communities.

2 The Flamel – DaVinci Algorithm

The Flamel-DaVinci Algorithm™ `(copyleft, GPL)` is so named as a mark of respect for the brilliant scholars, Nicholas Flamel and Leonardo DaVinci, who were known for their interest in cryptographic treatises and applications. The algorithm describes a Seer cryptanalytic technique that can be used by the non-Clairvoyant cryptographic community to verify that the plaintext rendered by a Seer, does indeed correspond to the ciphertext presented to the Seer for analysis.

Methods

The ciphertexts to be studied are intercepted PGP encrypted e-mail messages and/or attachments. Instead of having the Seers just reveal the plaintext, they have graciously consented to provide the session key as well.

φ Address reprint requests directly to the Publisher (the author is currently 'between affiliations')

The session key for an OpenPGP message is randomly obtained from a keyspace of 2**256 for newer algorithms such as Rijndael or Twofish. [3]

In order to forestall demands for escrow of private keys, GnuPG has made it possible to release the session key for any particular message. This can be done by using the option of '—show-session-key' during ordinary decryption. Once the session key is obtained, the message can be decrypted without the use of the keypair, by using the option of '—override-session-key string'. As the session key must be in a simple enough form to release to the authorities without involving any computers or data storage media, GnuPG shows the session key as a string of 2**6 hexadecimal characters.[4]

It is this point in the decryption process that is Clairvoyantly attacked :

The Seer would first summon a Random Oracle.

Recent improvements in Laptop Orb manufacture have made Oracle consultation a quick and portable process.[5] Once communication with the Random Oracle has been established, the Inner Eye would be trained upon the ciphertext, and the Seer would ask in Truth:

"Is the first character of the session key string that corresponds to this ciphertext a '0' ?"

If yes,

then the first character of the session key is recorded, and the Seer proceeds to examine the second character of the string.

If no,

then the Seer would again ask in Truth:

"Is the first character of the session key string that corresponds to this ciphertext a '1' ?"

The Seer would continue his/her Knowing Gaze for each of the hexadecimal characters 0, 1, 2, …, 9, A, B, …, F of a particular position of the session key string, until a True value is returned by the Random Oracle.

This algorithm would then be tried in turn for each of the 2**6 positions of the string until the complete session key would be obtained.

As this algorithm uses the Seer Oracle technique for each character independently, it allows for a Brute Force Clairvoyant Attack involving only 2**4 possibilities for each individual character of the session key string, for each of the 2**6 characters, i.e. 2 ** 10 possibilities; instead of the classical 2 ** 256 possibilities, [(2**4)**64], of a conventional non-Clairvoyant Brute Force cryptanalysis of the keyspace. This represents a quite feasible attack in real-time, by even the slowest of Seers[6].

Upon receipt of the session key, the non-Clairvoyant cryptanalyst can proceed to decrypt the ciphertext and verify that it produces the plaintext provided by the Seer.

Hitherto, conventional cryptanalysis has reported occasional successful use of a Random Oracle, but has been limited to logical analysis of program execution. Upon examination of the program output, cryptanalysts were able to deduce some few paltry details, (and none to date involving successful PGP/GnuPG decryption). Using the term 'Oracle' to refer to such acquisition of data, is certainly a far cry from the Clairvoyant Oracle techniques where information can be discerned without any apparent logical connection to the ciphertext. [7]

3 Discussion

This paper describes a clear algorithm by which any PGP encrypted message or file can be successfully Clairvoyantly attacked.

While there does not appear to be any defense against this attack vector, the Clairvoyant cryptanalytic community wishes to assure us, that their professional code of ethics respects individual privacy, and they would not train the Inner Eye where its penetrating Sight is unwelcome, *save at dire need.*

In support of their high standard of ethics, they point to the fact, that in Britain, intelligence agencies have had to resort to legislation to obtain private PGP keys; a drastic measure which would *surely be unnecessary if they were able to coerce the Clairvoyant cryptanalysts to decrypt any message at the Government's whim*.[8]

The same may probably also be said of the Guild's American colleagues, whose authorities needed to stoop to the use of *hardware* keyloggers to decrypt PGP messages. Even more so, in China, where cryptography is strictly regulated, the Venerable Wise Ones of the East have maintained their traditional impeccable integrity.

It may be prudent, however, in those countries that permit free use of cryptography, to consider their Clairvoyant cryptographic communities with more careful observation.

4 Conclusion

Both the Clairvoyant and non-Clairvoyant cryptanalytic communities eagerly await a demonstration of the Flamel – DaVinci algorithm in practice. All that remains is the interception of appropriately significant ciphertext messages, worthy of the Scrutiny of the Inner Eye, rather than the abundance of mundane correspondence that is usually encrypted nowadays.

We would like to encourage any and all cryptography users to make every attempt to encrypt and mail their most important secrets, so that there will be an adequate supply of intercepted ciphertexts, fully ripened with profound meaning, to be presented for a widely publicized demonstration of verifiable Clairvoyant decryption.

n. b.

In order to protect the identity and privacy of the encryptors, we ask that they do not PGP-sign their messages. The Flamel-DaVinci Algorithm cannot be used to authenticate unsigned messages, and the Seers have assured us that they will not divulge the identity of the encryptors, and are directing their Sight only upon the content of the ciphertexts, in keeping with their ancient guidelines of professional conduct.[9]

5 Disclaimers:

The author has not received any financial support from either the Clairvoyant or non-Clairvoyant cryptographic community, nor have any gifts been given or offered by any vendors in either community.

The author declares that, to the best of his knowledge, all research in the paper was done without any government intervention, and without bias or preference toward any individual or group.

An armored signed verifiable PGP message to this effect has been submitted to the Journal Editors and Publishers, and is available for public review upon request.

References

1 Intelligence Analysis of Intercepted e-mail Ciphertexts
(Classified available for review only by those with appropriate security clearances)

2 621st Annual Proceedings of the Clairvoyant Cryptanalytic Guild Stonehenge, England, 1997 (unpublished data, personal communication)

3 Encrypted Session Key Packets Sections 5.1, 5.3 Open PGP Message Format draft-ietf-openpgp-rfc2440bis-18.txt May 2006
http://www.ietf.org/internet-drafts/draft-ietf-openpgp-rfc2440bis-18.txt

4 GnuPG Documentation, Man Page http://www.gnupg.org/(en)/documentation/manpage.en.html

5 Throckmurton, B.V., et al, Benchmark Testing and Comparison of Laptop and Desktop Orbs June 2005 Advances in Digital Divination Vol. 17 p.227 – 242

6 Kenilworth Q., Barnes, J.W. Efficiency of Oracle Consultation by the Aging Clairvoyant August 2003 Wizard's Health Vol. 93 p.185 – 203

7 op Cit. 621st Annual Proceedings of the Clairvoyant Cryptanalytic Guild p. 121

8 629th Annual Proceedings of the Clairvoyant Cryptanalytic Guild Loch Ness, Scotland April, 2005, p.87 (italics added)

9 Merlin the Great Code of Honourable Conduct Expected of Witches, Wizards, and Warlocks Camelot, England (some controversy exists as to the exact date)