Practical Secret Protection

Thomas Martin   Laurence O'Toole

November 6, 2005

Abstract

In [1], the author discusses the pros and cons of a practical automatic key recovery system. We propose a similar solution to the problem of key protection.

1 Introduction

The phrase "Rubber-Hose Cryptography" is used to refer to the direct application of pressure on any individual withholding information so that they might feel the "joy at being given the opportunity to confess their secrets". Strictly speaking, this is an inaccurate term because this method only involves breaking a cipher or recovering a key. The term "Rubber-Hose Cryptanalysis" is more applicable. The purpose of this article is to explore the more literal meaning of "Rubber-Hose Cryptography".

2 Active Secret Protection

Let us consider the standard scenario and our basic method of secure communication: Alice wants to send a secret message to Bob while a third party, Eve, wishes to eavesdrop this message. To implement "Rubber-Hose Cryptography" Alice simply kills Eve and sends the message in clear. Note that this renders the method mentioned by Beynon [1] useless. Even assuming the process is completely automated, and the information is extracted from Alice or Bob, this information will never get back to Eve (assuming some rather definitive properties on the nature of the afterlife). Also, there is no need for a cryptographic key of any kind, or indeed any encryption algorithm at all, which significantly reduces the number of operations required (to 1) and consequently the implementation time. We call our system "Practical Secret Protection", or PSP for short.

This is a rather simplified view of things, as there will most likely be more than one person who will try to find out the secret. The level of protection provided by PSP can be increased to the level necessary for specific cases. It may be necessary for Alice to delete[1] all of Eve's associates, employers and likely replacements. It should be noted that the number of operations this system has to perform only grows linearly with the number of eavesdroppers (i.e. the two values are equal).

Unfortunately, a major problem with this scheme is that Alice can only operate on known eavesdroppers. There is a way around this though, to be demonstrated in following Section.

3 Passive Secret Protection

The above method depends on Alice's ability to identify (and remove[2]) all threats to security. This is obviously a non-trivial task but there is a subtle way of doing this that requires no direct action by either Alice or Bob. As a precursor to sending the actual secret, Alice sends Bob a message intended to be intercepted by Eve. On attempting to obtain, or upon discovering the contents of the message, Eve will then remove him/herself from the scenario as a result of intense emotional or physical trauma. There is the option of either having good physical security around the transport medium (e.g. electric fences, providing the physical trauma), or careful selection of the message itself (providing the emotional trauma). The latter may have to be a message specific to the eavesdropper (e.g. "I know what you did last summer"), but a well-chosen generic message can achieve the same result. A good generic message may be something along the lines of "I won't bother sending you that Ultra-secret message next week, because the world is going to end Thursday afternoon". This will have sufficient credibility if it includes a signed message by a expert in the appropriate field (black-hole formation within the solar system use Stephen Hawking's secret key, Global Nuclear Warfare use George W. Bush's). To obtain the necessary secret keys we refer the reader to the previous article, [1].

4 Provably Secure Secret Protection

It may be argued that neither of the above methods would be sufficient to protect extremely sensitive material. It could also be argued

[1] kill

[2] kill

that with PSP, one would be lucky to neutralise[3] more than the first eavesdropper. Some sceptics might even think there is no message that could cause the reader such physiological harm they cease their eavesdropping immediately (not even spam?), although the work of Cleese et al. [4] is worth mentioning. However, it is possible for a sufficiently paranoid Alice (or Bob) to employ an extended version of PSP that provides guaranteed secrecy.

There are two scenarios for using the system as such:

- It is not feasible or even possible to merely eliminate all potential eavesdroppers.

- The secret is of such high importance that no-one besides Alice and Bob may know it (not even a native of a hereto undiscovered South American rainforest tribe, who has no knowledge of Alice, Bob, the language they are communicating in, or even the most basic knowledge of how to break DES).

The modified system is this: Alice wants to send a secret to Bob. Alice kills everyone on the planet except Bob, and sends the message in clear. It should be noted that although this method could potentially involve $2^{32.5}$=6,000,000,000 operations[4] this is significantly fewer than the 2^{56} that are required to brute-force attack the simplest cipher known to man. Furthermore, these operations only need to be performed once ... ever, after which Alice and Bob can communicate in perfect secrecy as often as is required. For time and resource efficient methods of reducing the world's population to 2, the reader is directed to the various works of Flemming([2],[3]), as well as a myriad of blockbuster films, comics, and Saturday morning cartoons.

5 Conclusions

It must be said that even when used in the most secure mode, the system is only conditionally secure. The condition is that the set of potential eavesdroppers is limited to the current live human population of Earth. Further work is required to see if the following threats can/need also be guarded against:

- Time Travellers

- Telepathic Aliens

- The Dead

[3] kill
[4] killings

- Dimension Hoppers
- Cockroaches

Or any combination of the above. (e.g. Dead, time-travelling, dimension-hopping, telepathic, alien cockroaches.)

We would like to thank the referees, and to assure them that we have no reason to suspect that they would ever try to eavesdrop our communications.

References

[1] David Beynon, *Practical Key Recovery*, Journal of Craptology 1 (1999).

[2] Ian Flemming, *You only live twice*, (1967).

[3] Ian Flemming, *Moonraker*, (1979).

[4] Monty Python's Flying Circus, Episode 1, *The Funniest Joke in the World*, (1969).