Practical Data Protection

Sanjay Rawat [*]and Amitabh Saxena
<rawat, amitabh>@dit.unitn.it
Dept. of Information and Communication Technology
University of Trento
38050 Trento, Italy

April 23, 2008

Abstract

We present a very easy and practical method to send the information in a secure manner such that its disclosure to unintended recipient is not possible. Our method does not require the distribution of shared key at all. Our idea is inspired by the popularity of a very recent phenomenon of "Disclaimer Statement" in corporate emails.

1 Motivation

It has been seen that very recently, almost all of the corporate mails append a "Disclaimer" which states (often forcefully) that if the mail/information is not for you, you must notify the sender of the mail, without keeping a copy of the mail. One example of such a disclaimer is:

> "*This message is being sent from University of Trento (Italy) and may contain information which is confidential. If you prefer to receive these kind of messages at another e-mail address, please advise the sender by replying this e-mail. If, due to a technical error, you receive this message but you are not the intended recipient, please advise the sender immediately by replying this e-mail and delete this message and any attachments without retaining a copy.*"

We are inspired and motivated by the popularity of this type of disclaimers. As it is being used by almost all the corporates, we assume it is working and serving its purpose, otherwise why should all the big companies append a large disclaimer with every mail leaving the mail server? In many cases, in fact, the main message is much smaller than the disclaimer itself.

Please note that the above paragraph also serves as the proof of concept for the solid underlying idea of our approach. Hence, we also have provided a empirical proof of our method. In the following section, we present the method.

[*] Currently, the author is associated with Infosys Technologies Ltd, Hyderabad, India and can be reached at tosanjayr@gmail.com

2 Our Method

As mentioned above, our method is based on the a popular phenomenon of putting a "disclaimer" (a similar method was used for creating a very deadly virus [1]). This disclaimer is appended at the end of the mail. We propose that instead of putting the disclaimer at the end of the mail/message, it should be inserted at the very beginning of the mail. In this way, the receiver will first read the disclaimer and if he is not the intended recipient, he must not read that message and must delete that. These "MUST" properties are the characteristics of the disclaimer method and are well accepted in practice [5]. Following is an example of such a disclaimer:

> "*This message is being sent from University of Trento (Italy) and may contain information which is confidential. If you receive this message but you are not the intended recipient, stop reading a single line after this disclaimer onwards, advise the sender immediately by replying this e-mail and delete this message and any attachments without retaining a copy (don't forget to delete the mail from your "Sent Mails" folder). We appreciate your cooperation, otherwise you will be in big trouble.*"

We can see that the above disclaimer provides very tight confidentiality. Our method is well protected by the law [7, 8] and is highly flexible in the sense that you can design very creative disclaimers based on your security requirements and level. Few disclaimers are available online [6][1]. Furthermore, the disclaimers can be inserted via the outgoing mail server so that individuals don't have to worry about that.

As a fine tuning parameter, we advise you not to mention the subject of the message in the "Subject" field as it may give an adversary some information leakage to do further cryptanalysis. Instead, write the Subject after the disclaimer, as a part of message body.

Finally, to counter the powerful cryptanalysis method of Knudsen and Mirza [3], we recommend that the very first line of the disclaimer must be "*Do not remove this disclaimer.*" This makes our method resistant to "deletion cryptanalysis."

Proof of security: One of the anonymous referees emailed us a solid security proof of our method. However, for security reasons his outgoing mail server appended a disclaimer to that mail. Unfortunatley, due to that very secure disclaimer, we could not mention the proof in this paper. In fact this proves the effectiveness of our method.

Related Work: We compare our method with the distinguished work proposed by Martin and O'Toole [4]. Firstly our method require far less operations[2] than that of [4] (i.e., the time required to type a disclaimer). Secondly, their method is only useful when Alice wants to communicate with Bob forever. However, it is natural that Alice will eventually get bored with Bob and would like to meet other guys too. Our method would allow Alice to broadcast a message so that only pre-determined recipients (eg., with blue eyes, blonde hair, etc) will be able to read it, without even knowing the recipients names.

Also note that since our method does not involve the use of any keys, it is secure from the key recovery attack of Beynon [2].

[1] If you are not able to find/compose a good disclaimer, please contact us. We also do consultancy at a nominal charge.

[2] kills

Efficienty Issues: We have observed that longer disclaimers seem to provide better security. Typically a disclaimer must consist of 500 to 1000 words. Although that may appear to be a lot of precious bandwidth, this is acceptable considering the amount of time wasted in expensive cryptographic operations and studying mathematics.

3 Conclusion

In this research, we have exploited a popular phenomenon to propose a very easy-to-implement method to satisfy confidentiality requirements. Our method is very light in the sense that it does not require further computing resources than the ones require to read text. Our new method makes all current encryption methods obsolete.

Open Question: Can this method be extended to provide authentication and non-repudiation?

In conclusion, this disclaimer technique has been around for a while and it is quite surprising that its applications in craptography had not been noticed till now.

Acknowledgment

We are thankful to all the corporations/organizations that use such disclaimers as this has given us lot of confidence that our method WILL work. We are also thankful to the anonymous referees, Nigel Smart and Tom Bersen, for useful suggestions and an elegant proof of security (which unfortunately we cannot mention due to a discalimer).

References

[1] *Hi, I'm a deadly Blonde Virus. Please forward this email to all the contacts in your address book. Then delete all the files on your hard disk. Thank you very much. -Blonde Virus.* Cyber Space Journal of Advanced Virology, vol X (Y). 2005

[2] David Beynon, “Practical Key Recovery.” Journal of Craptology, Vol 0. No. 1, April 1999

[3] Lars R. Knudsen and Fauzan Mirza, “Deletion Cryptanalysis.” Journal of Craptology, Volume 0. No 0. 1998.

[4] Thomas Martin and Laurence O'Toole,“Practical Secret Protection.” Journal of Craptology, Vol. 2. July 2006

[5] See the email, coming from (specially) any IT company. It has a disclaimer.

[6] Some free disclaimers can be found at:
http://www.goldmark.org/jeff/stupid-disclaimers/fun.html

[7] http://www.email-policy.com/

[8] http://www.emaildisclaimers.com/