Withholding of Information

Philipp Gühring <p.guehring@poboxes.com>
Futureware 2001, Hebenstreitstr. 16, A-2602 Neurißhof, AUSTRIA
http://futureware.at/artikel/paper1.ps

2nd January 2000

Abstract

This paper describes a man-in-the-middle attack against the Chaffing&Winnowing method, and possible countermeasures.

1 Introduction

If you haven´t read the original paper about Chaffing and Winnowing yet, I suggest that you do it now.

In this paper, I define a package as the triple consisting of the Serial number, the Message and the MAC.

Let´s design a implementation of the Chaffing and Winnowing system. We assume to use it as a realtime communication link between two hosts over the Internet. For example, Alice wants to transmit the data from the original paper to Bob:

Hi Bob Meet me at 7PM Love-Alice

I added the last package to have more packages with the same serial number:

Package	Grain	Serial	Message	MAC
1		1	Hi Larry	523105
2	*	1	Hi Bob	465231
3	*	2	Meet me at	782290
4		2	I'll call you at	793122
5		3	6PM	891231
6	*	3	7PM	344287
7		4	Yours-Susan	553419
8	*	4	Love-Alice	312265
9		4	Love-Philipp	823949

This would lead to the idea to implement the decoding for the receiver the following way:

1. Read an incoming package .
2. Calculate the MAC, if it is ok, then add the message to the plaintext.
3. Do the upper loop with the next package, until all packages were processed.

2 Problem

But there is a problem. What shall Bob do, if he does not receive enough packages to restore the whole message? What if packages get lost? What if there is no package for a serial number, which is recognized as grain? If only one of the packages 2,3,6 or 8 get lost, the message will be incomplete. This could happen by errors on the communication link. So we create a new design:

1. Read an incoming package.
2. Calculate the MAC, if it is ok, then add the message to the plaintext.
3. Do the upper loop with the next package, until all packages were processed.
4. Are there serial numbers left? Rerequest all missing serial numbers, where no correct package was found.

3 Attack

Now let´s assume that there is Mallory (the man in the middle), who receives the message from Alice, and forwards only the following sequence (he only sends the first package of every serial number) to Bob:

1	1	Hi Larry	523105
3	2	Meet me at	782290
5	3	6PM	891231
7	4	Yours-Susan	553419

Then Mallory waits, which serial numbers are rerequested. Bob will be able to identify package 3 as authentic, so he rerequests the serial numbers 1, 3 and 4. Mallory catches the rerequests, and gains the knowledge, that the serial numbers, which were not rerequested are authentic. In this case only the number 2 was not rerequested, so package 3 has to be correct.

Now there are 2 possibilities: With the serial number 1 and 3, Mallory can assume that the packages left (2 and 6) are grain. But that isn´t necessarily the case. They could be wrong as well. Think a moment about the case when there are two mallory´s, who withhold the information each other. Then the remaining packages do not necessarily need to be authentic. Let´s assume that Mallory believes that they are authentic. So Mallory decides to send the next package from the serial number, where he doesn´t know the answer yet:

8	4	Love-Alice	312265

Bob "acknowledges" this packet by rerequesting serial numbers 1 and 3, which tells Mallory that the package 8 is correct. So Mallory knows the following: Packages 3 and 8 are authentic; Packages 2 and 6 can be guessed to be authentic. Mallory can terminate the connection to Bob now! But look at the knowledge of Bob: Bob has acknowledged the Packages 3 and 8. Bob has no authenticated information about the serial numbers 1 and 3!

4 Thinking

Mallory uses the following method: "If I can not distinguish between wheat and chaff, I have to "ask" the one, who can"

Bob spreads the information that he did not receive a valid package for a serial number.

So, the problem is the following: Mallory gains knowledge by the withholding of information. Rivest had the idea that it is an advantage that Mallory can insert new packages without disturbing the communication. But the problem is that the feature always/often (?) leads to the possibility to withhold information. And that is a weakness of the concept.

So we should find a solution, which makes the withholding of information nearly impossible.

5 Countermeasure

My idea is to reuse the MAC over all the packages, after the packages have been built:

Package	Serial	Message	MAC
1	1	Hi Larry	523105
2	1	Hi Bob	465231
3	2	Meet me at	782290
4	2	I'll call you at	793122
5	3	6PM	891231
6	3	7PM	344287
7	4	Yours-Susan	553419
8	4	Love-Alice	312265
9	4	Love-Philipp	823949
MAC	682343		

The last MAC has to be calculated from the secret and all the packages together. Let´s have a look at the new algorithm:

1. Read all the packages and the MAC.
2. Calculate the MAC over all packages.

3. If the MAC is not correct, then Rerequest all packages, start again, until the MAC is correct.

4. For each package:

5. Calculate the MAC, if it is ok, then add the message to the plaintext.

Another method could be to create a MAC for every serial number. This could be more efficient for huge amounts of data (You do not need all packages in memory to create the MAC):

Package	Serial	Message	MAC
1	1	Hi Larry	523105
2	1	Hi Bob	465231
MAC	345725		
3	2	Meet me at	782290
4	2	I'll call you at	793122
MAC	434634		
5	3	6PM	891231
6	3	7PM	344287
MAC	825236		
7	4	Yours-Susan	553419
8	4	Love-Alice	312265
9	4	Love-Philipp	823949
MAC	380313		

There is one open question: What could have happened when there are still no authentic packages for a serial number, although the MAC over all the packages is correct? We could make a feature out of that, by "inventing" fake serial numbers, and say "When there are no valid packages for a serial number, then just leave it out".

6 Implementation

The weakness in Chaffing and Winnowing, I found, is possible as soon as there is a protocol mechanism to react on missing packets. If you are developing an implementation of Chaffing and Winnowing, you should ask yourself the question: How is the system reacting, if there are missing packets? If it´s just ignoring the missing packets, then there might be data missing, but you are not directly vulnerable to the attack. (But please think about the protocol, the "user" is "running". What will the user do, when he recognizes that the message is not complete? Will he rerequest it?) If you just rerequest the missing packets, then you are vulnerable. And if you are rerequesting the packets, but preventing the attack, then you don´t miss anything, and the system is secure (against this man-in-the-middle attack).

7 Conclusion

Although there is a weakness in the concept of chaffing and winnowing, it is forseeable, and can be compensated with a minimal effort. I personally hope that there are no more weaknesses in Chaffing and Winnowing.

8 Acknowledgements

I would like to thank Markus Bauer, Markus B Fleck and Peter Broadwell for helpful comments and conversations.

References

[Riv95] Ronald L. Rivest. Chaffing and Winnowing. http://theory.lcs.mit.edu/˜rivest/chaffing.txt
The original paper.

[Fit98] http://www.fitug.de/debate/9804/msg00001.html
http://www.fitug.de/debate/9804/msg00004.html
http://www.fitug.de/debate/9804/msg00005.html
http://www.fitug.de/debate/9804/msg00006.html
http://www.fitug.de/debate/9804/msg00007.html
http://www.fitug.de/debate/9804/msg00010.html
A discussion about Chaffing and Winnowing

[Pla98] http://www.plasm.com/not.a.crime/
An implementation of Chaffing and Winnowing on Video-Streams, only for demonstration.

[Wil98] http://www.medsch.wisc.edu/˜annis/creations/Chaffe.html
An bitwise implementation of Chaffing and Winnowing in Perl.