

3679

20-80-002

~~SECRET~~

C742
G0
1
Q422

Reference: HM/INF NOTE/22

Issued by: HM

Date: 21 December 1977

Copy No: 20

THE AUTHENTICATION PROBLEM

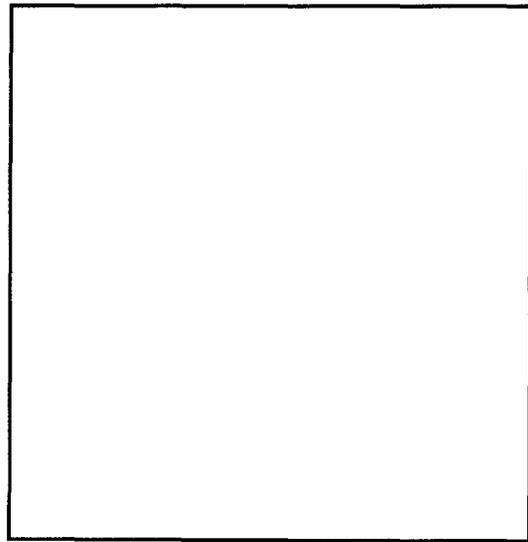
By J H Ellis

KEYWORD

NON-SECRET ENCRYPTION

Summary

This note discusses the authentication problem and gives the arguments scattered over previous papers in a compact form. It shows that the need for authentication does not invalidate Non-Secret Encryption.



(b) (1)

HM/INF NOTE/22
[7 pages]
AGD

FILE COPY
DO NOT REMOVE FROM LIBRARY

~~SECRET~~

~~SECRET~~

2

HM/INF NOTE/22

1. Non-Secret Encryption has now reached the phase where it is being considered for possible applications, and I find that many people are worried that the danger of spoofing may make its use untenable. This note therefore discusses this problem; it contains little that is new, but deals with the subject on its own, not as part of general NSE, and so may provide a more convincing demonstration than the arguments mixed with other matters.
2. The argument against NSE runs as follows:- if an enemy impersonates the legitimate user (spoofs) he can obtain secret information. In order to authenticate the other end of the link some secret information is needed, and if we need to supply this we could just as well supply key.
3. These are two implications here. One is that pure NSE is impossible because some secure or special situation is needed to give authentication; and the other is that the problems of authentication make NSE impractical.
4. This note is concerned with the second of these. The theoretical problem of pure NSE is interesting and important but of little relevance to a question of whether it is profitable to use NSE in a given practical situation. The theoretical answer must depend also on the precise definition of pure NSE adopted, and, while cases which I regard as pure NSE do exist, using the definitions which I find sensible, they are necessarily limited and perhaps it is possible to choose a sensible definition which can be proved impossible to realise. Therefore we consider the practical aspects here.
5. The final demonstration that NSE can be useful is of course to find a practical use for it, and various suggestions are made in the references. However I should like to give a straight general answer to the argument of para 2, both, hopefully, to avoid suspicion of evading the issue and also to try to reveal the real nature of the problem.
6. Let me first rephrase the argument. Secret encryption provides a key which acts as an authentication code, a non-secret encryption does not and must therefore make separate provision for authentication. NSE therefore only has advantage if this provision is easier than key distribution. I think this is a fair statement and one which is basically true, apart from the possibility of some other advantage from NSE. The point of this way of looking at it is that it compares the ease with which spoofing can be prevented in the two cases and does not worry about secure paths or prior secret information in principle.

~~SECRET~~

~~SECRET~~

3

HE/INF NOTE/22

7. Let us also assume that the NSE means available are as cheap and simple and secure as is necessary. Thus we can look at the authentication problem in isolation without considering other practical difficulties. Of course the sum of these difficulties is the deciding feature in practice and the component for authentication may well tip the balance against NSE, but we are here concerned mainly to refute the idea that it makes NSE fundamentally untenable.

8. Now let us turn the argument of para 6 upside down. Secret key will provide authentication (except in very special circumstances) but information adequate for authentication is hardly likely to be suitable for key. Thus we can always authenticate by distributing key and therefore the easiest means of authentication can never be less easy than key distribution. Or, using 'cost' in a general sense, the cost of authentication with NSE is always less than, or equal to, that of authentication with secret key. The key distribution is regarded as part of the secret key authentication for the purpose of this comparison. This is clearly also true even if the key is not adequate for authentication as we can still do the same as for secret key in the worst case.

9. If our assumption of zero-cost NSE were true this would mean that NSE should always be used, as it would never cost more than secret encryption, could cost less, and would at least have some fringe advantages. Indeed it is obvious that if secure key just dropped out of the sky as required at both ends of a link it would be foolish not to take advantage of it.

10. If however NSE is expensive and authentication costs as much as key distribution then we would not normally use NSE. A possible exception is in key updating but let us ignore this for the moment.

11. We see then that conditions favour the use of NSE when the cost of authentication is substantially less than that of key distribution. An obvious result which can be obscured by insistence on a total absence of secret information.

12. The first conclusion from this is that where secret key is freely, easily and securely available there is little point in NSE. Again obvious; the prime objective of NSE is to help when the provision of secret key is expensive or difficult.

13. Now we come to the vital question of why authentication should cost less than key distribution. First consider authentication codes (ACs), which are some form of secret knowledge sufficient to identify the user. They have these properties:-

~~SECRET~~

~~SECRET~~

4

HM/INF NOTE/22

- a. ACs can be very simple with few alternatives, requiring only enough variety to make a first-time guess very unlikely to be correct. Thus they are easier to distribute in the first place, easily stored (perhaps remembered) and easy to change; for example a current serial-number could be used.
- b. ACs can be of a vague form such as names, personal details or bits of background information, and so could be improvised if necessary. In doing this it would be highly desirable if authentication took the form of replies to questions or as to avoid the possibility of a few facts having been learned and used by a spoofer.
- c. There is no loss of security if an AC is revealed after it has been used, providing this is known or suspected. It does, of course prevent it being used again, but it means that much less security is needed for ACs than for key.
14. Authentication can be achieved in other ways. For instance:-
- a. Dialling back to a telephone caller if the switching network is reliable.
- b. Regular use of specified times would reveal an impostor, as both he and the legitimate user would come up together, stopping communication but not losing security.
- c. If the station being impersonated could hear the spoofer it could come up and denounce him.
15. Intangibles such as mannerisms and voice can be used as a kind of AC, the ability to produce them being a kind of secret knowledge. A familiar person can be identified on a telephone with considerable reliability.
16. A different means of authentication is provided by the idea of Public Key suggested by Hellman. In our terms this means storing the first leg of an MSE transmission in an accessible public place or openly distributed to other users. Only the originator knows the number from which the transmission was generated. Specifically, in the Williamson method P would have a secret number p, Q would have a secret number q and they would make a^p and a^q respectively public. This could either be kept for authentication or used to form a^{PQ} for encipherment key. Thus only one piece of authentication key is needed per user and he can change it easily.

~~SECRET~~

~~SECRET~~

5

HM/INF NOTE/22

17. This list is unlikely to be exhaustive but it shows that there are a wide variety of means of authentication other than the use of secret key. In [] an extreme example is given of authentication of a patrol with no uncompromised key, no suitable mutual private knowledge, may have been captured with all data by an enemy who can impersonate any of the patrol and that no member of the patrol can be expected to resist interrogation. This is an unrealistic situation but it does indicate what can be done.

(b) (1)

18. Another feature is the inherent difficulties of spoofing.

a. It requires active participation by the spoofer and may require considerable skill and knowledge, also it may require a more advantageous position in terms of transmission quality than is needed for interception.

b. It must be timely: A spoof must take place while the AC is still current, as delays while a bust is exploited or special equipment made could easily prevent it.

c. There is a high risk of detection, and even if successful the spoof is only likely to remain undiscovered until the genuine user communicates or some similar event takes place. So the available exploitation time is likely to be short.

These features reduce the risk and so the cost of authentication.

19. This should demonstrate that there is considerable opportunity to obtain low-cost authentication and so there is good reason to suppose that there are useful fields of application, particularly where there is special difficulty in providing secret key in the normal way.

20. A possible exception to this rule we have mentioned is key updating. Here the provision of key would follow its same pattern but the use of NSE as part of, or instead of, the normal updating would provide an extra element of security by breaking any chain of compromise which might be started. Once a normal updating system has been broken completely it remains open from then on, if the loss is not suspected. This is the fringe advantage referred to in para 9. Spoofing following the break of a current key could be prevented by making the NSE transmission for the next key the first use of each new key.

~~SECRET~~

~~SECRET~~

6

HM/INF NOTE/22

21. A form of spoofing particularly relevant to line communication needs to be mentioned. This is the case where the interceptor breaks the link and inserts two NSEs back-to-back, so that clear signal is between them. Authentication would pass between the two ends as though nothing had happened for the break should be transparent. No impersonation or knowledge of ACs is needed, and, if successful, there is no reason why it should be discovered later.
22. There are a number of ways of preventing this. One set depends on the fact that the key at each end is different. This can be detected by sending a number derived from key over the enciphered link. In principle the interceptor could change this particular piece of signal to correspond with the key at the other end, but in practice detecting the difference from the other traffic, before it had been sent, would be impossibly difficult. For instance the number would be simply spoken over a telephone or included early in teleprinter link. Foolishness like sending the information automatically after an alerting signal would, of course, have to be avoided.
23. Another way of detecting the difference would be for a change to be made to the key at both ends, using the change as an AC. In this way the intercept would need to know the AC. This is rather like secret encryption, but the AC can be extremely simple as there is no time to do even simple cryptanalysis.
24. A quite different safeguard is to use the increased time delay necessarily introduced by the interception. Some sort of automatic echo device could be used, switched on at random to prevent cancellation, and the return of a signal at double delay would detect the intruder.
25. Of course any use of the Public Key idea of para 16 would prevent this kind of spoofing completely.
26. Enough has been said, I think, to illustrate ways in which authentication can be substantially easier than key-distribution. Perhaps two final comments may be relevant. One is that secret key authenticates an equipment (generally speaking) and gives no safeguard against an unauthorised user, who must therefore be prevented from having access, while separate authentication can equally apply to a person. The other is that authentication is always needed for secret traffic, if only to satisfy ourselves in the first place that a particular user is a suitable person to have access. This involves secret encryption with the vague authentication process which we have associated with NSE. Forgetting this fact is a source of much of the confusion. Following this process some form of AC could easily be given and retained, but not so key, which is complex and needs frequent changes.

~~SECRET~~

~~SECRET~~

7

HM/INF NOTE/22

REFERENCES



(b) (1)

~~SECRET~~