Computers & Security, 8 (1989) 55–58

Refereed Article

A Remark on Hash Functions for Message Authentication

Chris Mitchell[1], Dave Rush[2] and Michael Walker[2]

[1]*Hewlett–Packard Ltd., Bristol, U.K.*
[2]*Racal Research Ltd., Reading, Berkshire, U.K.*

This paper considers the use of hash functions for message authentication. It is shown that a proposed method for using hash functions does not provide a secure non-repudiation service.

1. Introduction

An application of a special class of hash functions to cryptographic applications is considered in this paper. These hash functions are used in cryptography to construct manipulation detection codes (MDCs), which are added to messages to give some measure of assurance to the recipient that it has not been altered in transit. The basic idea is that a publicly known hash function is applied to the message to compute a hash value of fixed length. This hash value is then encrypted by the message originator and added to the message as an MDC.

We need to distinguish two types of security service that can be provided through the use of MDCs, namely message integrity and non-repudiation of origin. We are primarily concerned here with the latter service, and we show that a hash mechanism proposed in Davies and Price's book [6] is insecure for this application.

The term "message integrity" is used in this paper to mean that the recipient of a message can rely on the integrity of the message contents given that the message originator is trusted. The term "non-repudiation of origin" is used to describe a much stronger service whereby the recipient of a message is given a guarantee of the message's authenticity, in the sense that the recipient can subsequently prove to a third party that the message is authentic even if its originator subsequently revokes it. The idea of this latter service is to mimic the traditional role of signatures.

Message integrity can be provided by the originator hashing the message and then encrypting the hash value using a symmetric block cipher under control of a secret key shared with the intended message recipient. It should be observed that this type of service can also be provided using conventional "message authentication codes" (MACs) based solely on block ciphers; see, for example, ANSI X9.9 [3]. Nevertheless, in certain applications it is more convenient to use the combined hash function and encryption approach; see, for example, Jueneman [11] and Mitchell and Walker [12].

0167-4048/89/$3.50

Non-repudiation of origin is rather more difficult to provide. Again it is first necessary for the message originator to compute the hash value for the message. A "digital signature" algorithm is then applied to the hash value to obtain a "signature" for the message. This signature is then transmitted with the message. Although a full discussion of digital signatures is beyond the scope of this paper, suffice it to say that they are usually based on an asymmetric cipher system. The signature is computed using the secret key, which is known only to the originator, and can be checked by anyone having access to the public key. Examples of digital signature algorithms are provided by the RSA algorithm [13] and the Fiat–Shamir system [7, 8].

2. Properties Required of Hash Functions

If a hash function is to be used to provide either kind of security service, then it must satisfy certain properties. Perhaps the most important property that it should satisfy is that it must be "collision free", i.e. it must be computationally infeasible to construct two distinct input messages which hash to the same result. This property implies that the hash function must be "one-way", i.e. given any possible hash result, it is computationally infeasible to construct a message which hashes to this result.

The one-way property is clearly vital, since otherwise, given a message with an encrypted hash, it would be possible to construct another message having the same hash and hence the same encrypted hash, regardless of the encryption scheme used. The reason for requiring the stronger, collision-free property is a little more subtle. Suppose h is a hash function which is not collision free. In certain circumstances it may now be possible for a malicious user, B, to construct two messages, one, M_1, which user A will happily sign, and one, M_2, which A would not sign, such that $h(M_1) = h(M_2)$. User B then offers M_1 for A to sign, and then later claims that A signed M_2, by appending to M_2 the signature A generated for M_1.

3. Birthday Attacks and Defences

Suppose h is a hash function which gives 64-bit hash values. If a user constructs two messages, and then computes 2^{32} variations of each message (2^{32} is sufficiently small for this to be feasible), elementary probability theory says that there is a very strong chance that there will be a pair of variants, one for each message, having the same hash value (Davies and Price [6] show how such message variants can be constructed and discuss the probability computations). This is the so-called "birthday attack", and shows that 64-bit hash functions are vulnerable to the attack described above and are certainly not collision free.

In general, if the hash function produces hash values of n bits (i.e. there are 2^n hash values) then it is necessary to generate $2^{n/2}$ variants of each message in order to have a reasonable chance of finding two variants with the same hash value. Thus one defence against the birthday attack is to choose a hash function with a large number of hash values. This approach is indeed widely advocated, and a large number of authors suggest that hash functions should produce at least 128 bits; see for example, Akl [1] and Jueneman [11]. Examples of 128-bit hash functions can be found in CCITT Draft Recommendation X.509 [4], Damgard [5], Girault [10] and Jueneman [11].

An alternative approach, which allows the use of 64-bit hash functions, is proposed by Davies and Price [6]. This is attractive since n-bit hash functions can be constructed from n-bit block ciphers in such a way that the hash function is provably one-way if the block cipher is secure (see Winternitz [14, 15]). Since apparently secure 64-bit block ciphers are well known, e.g. DES [2, 9], 64-bit hash functions are readily constructed. The Davies and Price approach requires the originator of a message to append a random value to it before performing the hash function. This will clearly foil the attack described in the last section, even though the hash function is not collision free. Unfortunately, when the hash value is to be used as part of a non-

repudiation mechanism, this approach is flawed, as we now discuss.

4. A Weakness in the Davies and Price Scheme

To describe the weakness, we start by re-examining the non-repudiation service. One of the main aims of this service is to protect the recipient of a message from a fraudulent originator who wishes to later revoke a "signed" message. The whole principle of digital signatures relies on the fact that a signature is effectively unique to a message. If there is a way for any party to construct a second message with the same signature then the validity of the non-repudiation service is destroyed.

In the Davies and Price scheme, the malicious user B described above cannot compute the hash values for messages which A will be prepared to sign. In particular B is unable to launch a birthday attack against the 64-bit hash function. However there is nothing in the scheme to prevent a malicious user A from exploiting the birthday attack to generate two messages, M_1 and M_2, having the same signature. If A signs M_1 and sends it to B, B will believe that A cannot later revoke the message. However, at a later date A can claim to have sent M_2. The existence of two messages with the same signature will destroy the validity of the signature, and B will have been defrauded.

5. Concluding Remarks

The weakness we have just described has important ramifications for designers of systems incorporating measures to provide for authentication and non-repudiation of data. The most important conclusion we can draw is that 64-bit hash functions should never be used where non-repudiation services are required. For such applications, in order to preserve the essential collision-free property, all hash functions should output hash values of at least 128 bits.

A number of possible candidate functions do exist, and examples can be found in CCITT Draft Recommendation X.509 [4], Damgard [5], Girault [10] and Jueneman [11]. However, all these examples are of relatively recent design, and require further study before they can be regarded as accepted practice. In general, there is a shortage of sound proposals for hash functions, and further research is needed.

Finally note that it is not the case that 64-bit hash functions are unsuitable for all applications. Indeed, the Davies and Price scheme remains a possible candidate for use when other types of authentication service are required, i.e. if the recipient of a message trusts the originator.

Acknowledgment

This paper has been prepared under the auspices of the LOCATOR project, a part of the Alvey Mobile Information Systems Large Demonstrator Project.

References

[1] S.G. Akl, On the security of compressed encodings, *Advances in Cryptology: Proceedings of Crypto '83*, Plenum, New York, 1984, pp. 209–230.

[2] ANSI X3.92-1981, *Data Encryption Algorithm*, American National Standards Institute, New York, 1981.

[3] ANSI X9.9-1986, *Financial Institution Message Authentication (Retail)*, American Bankers Association, Washington, DC, August 1986.

[4] CCITT Draft Recommendation X.509 (Version 6), *The Directory – Authentication Framework*, CCITT, Geneva, June 1987.

[5] I.B. Damgard, Collision free hash functions and public key signature schemes, paper given at the *Eurocrypt '87 Conf.*

[6] D.W. Davies and W.L. Price, *Security for Computer Networks*, Wiley, Chichester, 1984.

[7] A. Fiat and A. Shamir, How to prove yourself: practical solutions to identification and signature problems, *Advances in Crytology: Proceedings of Crypto '86*, Springer, Berlin, 1987, pp. 186–194.

[8] A. Fiat and A. Shamir, Unforgeable proofs of identity, *Proceedings of Securicom 87*, Paris, March 1987, pp. 147–153.

[9] FIPS 46, *Data Encryption Standard*, National Bureau of Standards, Washington, DC, 1977.

[10] M. Girault, Hash-functions using modulo-n operations, paper given at the *Eurocrypt '87 Conf.*

[11] R.R. Jueneman, Electronic document authentication, *IEEE Network Mag.*, 1 (1987) 17–23.

[12] C.J. Mitchell and M. Walker, Solutions to the multi-destination secure electronic mail problem, *Comput. Secur.*, 7 (1988) 483.

[13] R.L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, 21 (1978) 120–126.

[14] R.S. Winternitz, Producing a one-way hash function from DES, *Advances in Cryptology: Proceedings of Crypto '83*, Plenum, New York, 1984, pp. 203–207.

[15] R.S. Winternitz, A secure one-way hash function built from DES, *Proceedings of the 1984 IEEE Symposium on Security and Privacy, Oakland, April–May 1984*, pp. 88–90.

Chris Mitchell is Project Manager for System Security at the Information Systems Centre of Hewlett-Packard Laboratories, where he has worked since 1985. He received his B.Sc. (1975) and Ph.D. (1979) degrees from Westfield College, London University. He has worked on various aspects of information security since 1979, and his research interests include cryptology and combinatorial mathematics. He is a member of the British Computer Society, the Institution of Electrical Engineers and the London Mathematical Society and a fellow of the Institute of Mathematics and its Applications.

David Rush received the B.A. degree in physics from Oxford University in 1979, and the M.A. degree in 1987. After graduation he joined Racal Research, where he has been involved with many areas of data communications. He is currently a principal engineer, working on protocols for message handling and data security.

Michael Walker is Head of Mathematics at Racal Research Ltd., where he is responsible for much of the company's work in cryptography, data security and coding for error control. Before joining Racal in 1983, he was a lecturer in mathematics at the University of Tübingen, where he undertook research in finite geometries, groups and combinatorics. He was educated at Royal Holloway College, University of London, where he received a B.Sc. in 1969 and a Ph.D. degree in 1973, both degrees in mathematics. He is a member of the London Mathematical Society and a Fellow of the Institute of Mathematics and its Applications.