M.I.T. LABORATORY FOR COMPUTER SCIENCE August 30, 1977
Computer Systems Research Division Request for Comments No. 148

ON DIGITAL SIGNATURES

by Jerome H. Saltzer

Recently, Diffie and Hellman [1] have suggested a novel application for cryptographic techniques: authentication of received messages without prior explicit and private agreement between sender and receiver. They have used the term "digital signatures" to name the application, because the problem being solved is analogous to that for which a handwritten signature is used. However, the scheme is less general, in some important ways, than traditional handwritten signatures. The limitations are sufficiently important that this short note outlines them in detail.

Briefly, Diffie and Hellman's technique is as follows. Every message originator who wishes to send messages that can be authenticated by any receiver devises a unique encipherment and decipherment function pair, E_i and D_i, where the subscript i identifies the message originator. These two functions are chosen to have two properties:

1) for any message M, $D_i(E_i(M)) = M$. This property simply states the usual effect of enciphering and deciphering algorithms that an enciphered message can be deciphered.
2) Complete knowledge of the function D_i, together with matching samples of cipher and clear text, are not sufficient to allow deduction of the function E_i*.

The message originator places on public record the function D_i, for any potential recipient to inspect and use, and keeps secret the function E_i. To send an authenticated message, the originator enciphers it with E_i, which no one else knows. The recipient of a message that is alleged to have come

---

* This requirement is non-trivial; Rivest et al., have recently suggested a family of such function pairs based on the relative ease of verifying primeness of a number compared with the difficulty of actually factoring a number found not to be prime [2].

---

from originator i goes to the public record, obtains D_i, and attempts to decipher the message with it. If the message deciphers, it must have been sent by i, since no one else knows how to perform function E_i.

There are two limitations of this scheme related to recognition of the message and to secrecy of the function E_i. Let us consider first the recognition consideration, since it is easily dealt with. Suppose that the message from i consists of a just-computed, totally random string of bits. In that case, the recipient, upon applying the function D_i, finds exactly this random bit string. Suppose some interloper has delivered a fake message. The fake message will decipher to a different random string of bits, not particularly distinguished from the legitimate message. In order for the recipient to authenticate the message, there must be some part of its deciphered content that is predictable. This predictability could be in any of several forms -- the first hundred bits could be a standard pattern, or the bits of the message could be encoded in an error-correcting code.

From an information-theoretic point of view, the (presumably) unpredictable message bits must be accompanied by some number of predictable authentication bits. Further, the number of authentication bits must be large enough that the probability that the predicted bit pattern occurs accidentally is satisfactorily small.

From a legal point of view, the authentication bits represent the way that the receiver establishes fulfillment of a contract that must have been negotiated in advance (perhaps indirectly) between the originating and receiving parties. Thus an arbitrator attempting to resolve a dispute would insist on seeing not only the authenticating bit pattern, but also the contract that specified that the bit pattern is the one expected.

We conclude that an essential requirement of the digital signature system is advance agreement on the pattern of the authenticating information, and inclusion of this information with message being transmitted.

The second area of concern with digital signatures concerns secrecy, and is not so easily dealt with. The system depends on each user i maintaining perfect secrecy of his own enciphering function E_i. Unfortunately, human beings are not terribly good at maintaining absolute secrecy. The user of a digital signature system will inevitably make a mistake that potentially exposes his E_i. Several plausible secrecy compromising scenarios can easily be imagined:

the new user who doesn't appreciate the importance of secrecy for his E_i, the computer room left unlocked for a moment, the computer turned over to a repairman without first clearing the value of E_i, the user under pressure who finds it expedient to "loan" his E_i to a co-worker, and so on.* Whatever the scenario, from the moment of possible compromise onward, messages encoded with E_i are of uncertain origin. Unfortunately, it is not apparent how to provide for accidental exposure of E_i without completely destroying the utility of digital signatures. For example, consider the following strategy: one might store publicly not a single D_i, but a set of $(D,T)_i$ pairs with T being a validity date for the function D. Whenever user i discovers that his E_i may have been compromised, he chooses a new (E_i, D_i) pair, and reports the new D_i and the estimated time of compromise of the previous D_i to the public key storer. The public key storer associates the time of compromise with the old D_i and establishes the new D_i as current. Finally, the contract for authentication must be extended to include putting a date in each message. Now, the recipient of a message obtains from the public key storer the D_i that is thought to be valid for the message in question, deciphers the message, and verifies that the contained data is indeed within the range of validity of the D_i that was used.

There are several problems with this system. The principal one is that any message originator who decides to repudiate a previously signed message need merely report to the public key storer that his D_i was compromised, indicating a date before that stored in the message. If signed messages can be so easily repudiated, the digital signature completely loses its value.

The trouble here is the need for maintaining long-term secrecy of the function E_i. The signature is valid only as long as E_i is secret; the responsibility for maintaining that secrecy lies exclusively with a person who may have an interest in invalidating the signature. That observation suggests that there is a fundamental flaw in the conception of the digital signature system.

A possible repair, though not completely satisfactory, might be attempted if it is quite easy to generate (E_i,D_i) pairs. Suppose one asks the public key storer to generate a different (E_i,D_i) pair for every signed message. The function E_i is used once, by the public key storer, and then discarded; the

---

* Partly because of human fallibility, a standard part of most cryptographic systems is a frequent change of key. As we shall see in a moment, frequent key change is awkward in the digital signature system.

function D_i is remembered by the Public Key Storer along with the timestamp of the unique message that was enciphered with E_i. The Public Key Storer would retain these pairs indefinitely, for future arbitration. This approach retains the cryptographic strategy, but it entails a more active central repository, that is trusted to generate (E_i,D_i) pairs, do correct transformations, and then forget the E_i without fail. This approach resembles the operation of a notary public more than a simple signature.

Perhaps one conclusion to be drawn from this discussion is that, as usual, sound cryptographic and authentication strategies developed in isolation maybe defective when embedded in a computer system, involving people and legal considerations. In any case, it would appear that some more work is necessary to develop a complete, usable system.

[1] Diffie, W. and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, November, 1976.

[2] Rivest, R., et al., "On Digital Signatures and Public-Key Cryptosystems", M.I.T. Laboratory for Computer Science Technical Memo TM-82, April, 1977.