March 23, 1974

A NOTE ON PRIVACY TRANSFORMATION AS A PROTECTION MECHANISM IN COMPUTER SYSTEMS AND COMPUTER NETWORKS

by J. H. Saltzer

This note is intended to point out three information-protecting techniques which, though previously published[B,S], are not widely known in the computer protection field. These are 1) two-way authentication by transformation synchronization, 2) transformation key leverage, and 3) key distribution for network end-to-end privacy transformation.

Two-way authentication by transformation synchronization

The usual method of authentication of a remote user in time-sharing systems, namely demanding that the user type a secret password, has two defects from a protection point of view:

1) The password is transmitted over the communication network from the user to the computer. Unless the entire network is protected, transmission of the password exposes it to eavesdroppers. (The one-time password[A] is sometimes proposed to help counter this defect.)

2) The authentication is one-way. That is, the password authenticates the user to the computer system, but not vice-versa. An intruder can actively penetrate a password system by intercepting all messages to and from the terminal and directing them to another computer which is under the interceptor's control. This computer can be programmed to "masquerade", that is, to act just like the system the caller intended to use, up to the point of requesting

> him to type his password. After receiving the password, the masquerader gracefully terminates the communication with some unsurprising error message, and the caller may be unaware that his password has been stolen.

A more powerful authentication technique can be used to protect against both these defects. Suppose that the computer and the remote terminal are equipped with enciphering circuitry, such as the LUCIFER system[S], that scrambles all signals to and from the terminal. Such devices normally are designed so that the exact encipherment is determined by the value of a key -- for example, the transformation key may consist of a sequence of 1000 binary digits read from a magentically striped plastic card. In order for a recipient of such an enciphered signal to comprehend it he must either have a deciphering circuit which is primed with an exact copy of the transformation key, or else he must analyze the scrambled stream to try to discover the key. The strategy of encipherment/decipherment is usually invoked for the purpose of providing protection when using an otherwise unprotected communications network. However, it can simultaneously be used for authentication, as follows: the user, at a terminal, begins by bypassing the enciphering equipment. He then types his name. This name passes, unenciphered, through the communication network to the computer he plans to use. The computer looks up the name, just as with the password system. Associated with each name, instead of a secret password, is a secret transformation key. The computer loads this transformation key into its enciphering mechanism and attempts to communicate with the user. Meanwhile, the user has loaded his copy of the transformation key into his enciphering mechanism, and turned it on. Now, if the keys are identical, exchange of some standard handshaking sequence will succeed. If they are not identical, the exchange will fail, and both the user and the computer system will encounter unintelligible streams of bits. If the exchange succeeds, the computer system is certain of the identity of the user, and the user is certain of the identity of the computer.* The secret authenticator--the transformation key--has not been transmitted over the communication network. If communication fails because either the user is unauthorized or the system has been replaced by a masquerader, the legitimate party to the transaction has immediate warning of the apparent illegitimacy of the other party.

Transformation key leverage

A significant problem with the simple encipherment technique mentioned above is that the secret transformation key must be changed relatively frequently, since the probability of the success of cryptanalysis increases with the amount of data enciphered under the key. To help reduce this effect, key leverage may be used. Suppose that the computer system has available a transformation key generator which may be called upon at any time to produce a new, random set of bits for use as a transformation key. The authentication protocol can then be extended by one more step: the first (and only) message sent to the user and enciphered using his private transformation key is a newly generated temporary key. The user receives the new, enciphered, temporary key, deciphers it, and then places it in his enciphering apparatus for all further exchanges with the computer. The computer also uses the new temporary key for all messages after the first one.

---

* Actually, there is still one uncovered possibility: a masquerader could exactly record the enciphered bits in one communication, and then intercept a later communication and play them back verbatim. Although the masquerader learns nothing by this technique, he might succeed in thoroughly confusing the user. A simple protection technique is for the computer to immediately use the enciphered connection to transmit the current date and time, and request the user to echo it back. Each successive message can then include as a cross-check a short piece of the previous message. This technique is described in detail in [S].

With this approach, the original, personal transformation key of the user may be returned to a secure place both at his end and in the computer: only the temporary key need be exposed even as far as placing it inside the enciphering program or hardware. The original key has been used only to transmit a single message (the temporary key) consisting of a random bit string. Even if the temporary key should be compromised through cryptanalysis, only this exchange is compromised; and a very small sample of data transformed under the original key has been obtained.

Key distribution for networks

A small extension of the idea of key leverage can be used to solve a troublesome problem of distributing transformation keys in large networks of computers and terminals. If one wishes to use end-to-end privacy transformation for messages flowing through a packet switching network such as the ARPANET[R], it would seem that each network destination (whether terminal or computer system) might need a list of keys, one for every other destination with which exchange might take place. Then, the two-way authentication scheme described above could be used to initiate a secure individual exchange over the network.

One solution to this problem is to provide one network node (called an *agency* in [B]) which is a protected computer system that is prepared to initiate authenticated exchanges with every destination in the network. A user G_1, wishing to communicate with user G_2 via the network, first initiates a connection to the agency, using the two-way authentication protocol, and further specifies that he wants to communicate with G_2. The agency initiates communication with G_2, using the two-way authentication protocol. Now the agency node generates a new, temporary key for this conversation and sends a copy of the temporary key to G_1, enciphering it with G_1's personal key, and to G_2, enciphering it with G_2's personal key, just as in the key leverage scheme. G_1 and G_2, upon receiving and deciphering the temporary key drop their connections to the agency and begin exchanging messages with each other, using the temporary transformation key for encipherment. Now, if G_1 and G_2 can understand each other's messages, each is certain of the identity of the other party.

References

[B] Branstad, D. K., "Security Aspects of Computer Networks," AIAA Paper No. 73-427, AIAA Computer Network Systems Conference, Huntsville, Alabama, April 16-18, 1973.

[S] Smith, J.L., Notz, W.A., and Osseck, P.R., "An Experimental Application of Cryptography to a Remotely Accessed Data System," Proc. ACM 25th Nat. Conf., August, 1972, pp. 282-297.

[A] Weissman, C., "Security controls in the ADEPT-50 time-sharing system," AFIPS Conf. Proc. 35, (FJCC 1969), pp. 119-133.

[R] Roberts, L.G., and Wessler, B.D., "Computer network development to achieve resource sharing," AFIPS Conf. Proc. 36, (SJCC 1970), pp. 543-549.