A System for Point-of-Sale or Access, User Authentication and Identification

Gustavus J. Simmons

Sandia National Laboratories
Albuquerque, New Mexico 87185

Abstract

The most important function in the control of assets and resources is the verification of an applicant's identity and authority to use or have access to those assets. Elaborate, and legally accepted, protocols to accomplish this function are central to all commercial and private transactions. When the resources are remotely accessible, as in the case of computer/data files, electronic fund transfers (EFT), automated bank tellers, and even in many manned point-of-sale systems or when access is controlled by automated unmanned portals, no satisfactory counterpart to the established protocols for verifying individual identity and/or authority to use a resource have been found. Almost all proposals -- and systems -- for achieving this function "identify" the applicant through his being able to exhibit a private pass: personal identification number (PIN), password, etc. The problem is that this pass is not uniquely associated with the individual, and hence does not necessarily identify him. In this paper we describe a means of solving this problem, i.e., of identifying an individual and of verifying his authority to use a resource that makes use of an authentication channel in a novel application of a two key cryptographic algorithm.

+ This work performed at Sandia National Laboratories supported by the U. S. Department of Energy under contract number DE-AC04-76DP00789.

An Abbreviation of the Paper

The first application of an asymmetric (read also public key or two key) cryptosystem reported in the open literature was to an unmanned access portal designed by the Sandia National Laboratories which was first fielded at the Zero Power Plutonium Reactor (ZPPR) in Idaho in 1979 [1,4,5]. This system is a paradigm of a way in which the authentication channel -- in which the decrypt key is publically exposed while the encrypt key is kept secret -- may be applied in an automated (unmanned) system to verify the identity -- and delegated authority -- of an individual. In the paper presented at Crypto'81, three such applications with quite different requirements that had been made by the Sandia National Laboratories were discussed. In this abbreviated version, only the ZPPR access portal application will be covered since it remains the most novel of the several individual identity verification systems developed thus far.

Remote or automated access to valuable information, assets or facilities is usually controlled by a private password or user identification number activated portal -- in other words, the requestor's identity and authority are verified through his being able to produce a piece (or more) of information (pass) that was once known to be in the authorized user's private possession. Clearly, the system is identifying the pass, not the individual, hence the system will validate anyone presenting the pass. The problem is that the pass may be in the possession of someone other than the authorized user -- either through inadvertent disclosure or surrender under duress. In addition, there are reasonable scenarios in which the authorized holder of the pass may be the party wishing to defraud the system in which circumstance he cannot be trusted to keep the pass secret. Although some element(s) in the system must be trusted, it is possible to transfer this trust from a party that could profit from its violation to either mechanisms that could only betray the trust through failure or else to multiple persons in the expectation that collusion to defraud the system becomes less probable as the number of persons that must collude is increased.

In an asymmetric cryptosystem it is possible to expose (either deliberately by design or else because exposure denies secrecy) one or the other of the keys -- while the other key is kept secret of course -- and to still retain some secure communications capability [3]. If the transmitter key is the one exposed and the receiver key is the one protected, we have the well known privacy or public key channel. If on the other hand, it is the receiver key that is exposed and the transmitter key that is kept secret, we have the authentication or signature channel. It is this authentication channel (using the RSA algorithm [2]) that the Sandia National Laboratories have applied in several personnel identification systems. Roughly speaking, an authentication channel will be used to transfer the ability to authenticate a delayed message -- just as in the dual system a privacy channel can be used to establish a secondary privacy channel between subscribers.

The function of the authentication system to be described here is to identify an individual by his unique attributes using only reference materials that he has in his possession and which he supplies to the automated access portal at the time he requests access to the protected resource. There is the additional restriction that very little advance communication to other sites be required. Finally, there is the practical constraint -- arising from multi-site dispersal of the receivers or access controllers, as well as both the number of persons and the turn-over in staff having access to the access control at the sites -- that while information at a site can be protected from alteration or substitution, it is generally not possible to guarantee its secrecy.

The solution is simple. A central facility, the trusted element in the system, is entrusted by all of the parties (sites) that will need to verify individual identities with the task of first establishing the identity of individuals to whatever degree of certainty that is deemed necessary and of then generating ID records that are given to the individuals they identify. This record will consist

of some collection of personal attributes (photograph, fingerprints, hand geometry, voiceprint, retinal prints, passive signature or dynamic signature, etc.) encrypted along with descriptive identifiers such as name, social security number, etc., using the encrypt key of a two key cryptosystem. Needless to say, the functioning of the system is totally dependent on the central site keeping the encrypt key secret, i.e., on the secure element in the system actually being secure. The decrypt key would be delivered as an authenticated, but not necessarity secret, message to all of the sites who would have to protect the integrity but not the privacy of the key. When, at some later time, an individual appears at a remote site with a claimed identity, he would present the cipher record in his possession and permit his individual attributes to be reread by equipment at the site. Using the decrypt key, the site would first decrypt the ID cipher and verify the authenticity of the cipher by the presence of the expected redundant (authenticating) information. The system would next check for a suitable agreement with the individual attributes as just measured by equipment located at the site. If a match is achieved, the identity of the individual has been confirmed since the cipher could only have been generated using the secret encrypt key held by the enrollment station which was responsible for establishing the identity of the individual before issuing the ID cipher. The only advance communication required between the site and the central facility is the authenticated (but not necessarily secret) exchange of the decrypt key. The other channel of communication is the public one of the user bringing his own ID cipher to the site. Since an authentication channel has been set up between the enrollment station and the site, the system (access portal) can be certain (to the same level as the two key cryptosystem is cryptosecure) that the ID records it has received are authentic, i.e., that they were issued by the central authority. Then, to the degree that the personal attributes encrypted in the ID records can identify an individual, they can also be confident of the transfer of the identification of the applicant from the

central facility to the remote site. No communication with the central facility is required at the time that individual identification is made and more importantly, no files of identifying information for possible users need be transmitted to nor stored at the site! The crucial point is that the separation of the encryption and the decryption capabilities in two key cryptosystems has been exploited to devolve the authentication capability from the sender to the receiver -- and hence has transferred the ability to determine the veracity of the ID records supplied by the applicant to the receiver (site). The fact about two key cryptosystems on which this concept depends is that it is possible to transfer the ability to authenticate (messages) over an authentication channel.

As was mentioned at the beginning of this paper, the first application of the principles described here and indeed the first application of a two key cryptographic system in the open literature is in an access control system designed and successfully installed by the Safeguards Development Department of the Sandia National Laboratories at the Idaho National Engineering Laboratory, Idaho [1]. This system, designated as a Positive Personnel Identity Verification (PPIV) device is an optional supplementary subsystem to the international nuclear material containment portal used by the International Atomic Energy Agency (IAEA) to prevent the unauthorized removal of nuclear materials from a facility.

The international portal is automated so that a human operator is not required to be in attendance during normal operation and is a stand-alone unit so far as its data processing is concerned; i.e., it is not linked to a central computer or data bank. For direct compatibility, the PPIV was designed to operate in the same manner. The individual attribute chosen for corroboration of identity was hand geometry. The measurements are made using a commercially available equipment, the IDentimat 2000T manufactured by the Identimat Corp. of New York. To make it difficult for more than one subject to be certified and authorized entry with a single identity and authority verification, the individual's weight is part of

the ID record, and the weight of the occupant(s) of the booth is read by sensors in the access portal. For added security, a user is required to enter a five-digit, random but private, memorized ID number. All of this information, along with data defining the areas of authorized access, time of day in which access is authorized, period of authorization, etc., is encrypted using the Rivest-Shamir-Adleman algorithm and the resulting ID cipher recorded on a magnetic stripe on the individual's ID badge at the time he is enrolled in the system. The access control station at the site must be initialized with the RSA decryption key, date, time, list of blocked IDs that are to be refused entry and a designation of the area it controls, so that it can correctly respond to the area authorization in the ID ciphers.

The first system has been operational for over two years. A second, expanded, system will be installed in late 1982 at the Savannah River facility. The reliability of the identification is precisely that claimed for hand geometry verification by Identimat (in the 90% region), but the underlying principle is independent of the particular choice of the attribute to be measured. Several other commercially available automatic identity verification devices are available and have been extensively tested in the Air Force Base and Installation Security System (BISS) program: an automatic fingerprint verification (AFV) system by Calspan Corp., Buffalo, New York, an automatic speaker verification (ASV) system by Texas Instruments, Dallas, Texas, and an Automatic Handwriting Verification (AHV) system by Veripen, Inc., of New York. In addition, the Sandia National Laboratory has developed a dynamic signature verification system which is compatible with many identity verification applications.

The bottom line to this discussion is that equipment is available to measure various individual attributes to implement the identification technique described in the preceding sections. The first reduction to practice by the Sandia National Laboratories in the PPIV, using hand geometry measurements, illustrates the

general principle of a method for user identification and remote authentication of messages that should suffice in even the most sensitive commercial applications.

An expanded version of this paper will appear in mid-1983 in Cryptologia.

References

1. P. D. Merillat, "Secure stand-alone positive personnel identity verification system (SSA-PPIV)," Sandia National Laboratories Tech. Rpt. SAND79-0070 (March 1979).
2. R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Comm. ACM, 21, 2 (Feb. 1978), 120-126.
3. G. J. Simmons, "Symmetric and asymmetric encryption," Computing Surveys, 11, 4 (Dec. 1979), 305-330.
4. G. J. Simmons, "Half a loaf is better than none: Some novel message integrity problems," Proceedings of the 1981 Symposium on Security and Privacy (April 1981), pp. 65-69.
5. G. J. Simmons, "Message authentication without secrecy," in Secure Communications and Asymmetric Cryptosystems, edited by G. J. Simmons, AAAS Selected Symposia Series, Westview Press, Boulder, CO, to be published August, 1982.