

SYSTEMATIC DESIGN OF A FAMILY OF
ATTACK-RESISTANT AUTHENTICATION PROTOCOLS

April 1992

R. Bird
I. Gopal
A. Herzberg
P. Janson
S. Kuttan
R. Molva
M. Yung

IBM Raleigh, Watson & Zurich Laboratories

IBM

Systematic Design of a Family of Attack-Resistant Authentication Protocols

R. Bird¹
I. Gopal²
A. Herzberg²
P. Janson³
S. Kutten²
R. Molva³
M. Yung²

Abstract

The pervasive use of open networks and distributed systems poses serious threats to the security of end-to-end communications and network components themselves. A necessary foundation for securing a network is the ability to reliably authenticate communication partners and other network entities. One-way, password-based authentication techniques are not sufficient to cope with the issues at hand. Modern designs rely on two-way, cryptographic authentication protocols. However, most existing designs suffer from one or more limitations: They require synchronization of local clocks, they are subject to export restrictions because of the way they use cryptographic functions, they are not amenable to use in lower layers of network protocols because of the size and complexity of messages they use, etc. Designing such cryptographic protocols for large and dynamic network communities presents substantial challenges in terms of ease of use, efficiency, flexibility, and above all security.

This paper discusses the above challenges, shows how a few simple protocols, including one being standardized by ISO, can easily be broken, and derives a series of desirable properties that authentication protocols should exhibit to meet the requirements of future large and dynamic network communities. Then the paper describes a methodology that was developed to systematically build a canonical description of a family of cryptographic two-way authentication protocols that are as simple as possible yet resistant to a wide class of attacks, efficient, easy to implement and use, and amenable to many different networking environments. It also discusses several possible embodiments of the canonical protocol that present various advantages in specific distributed system scenarios.

1. Introduction

The pervasive use of open networks and distributed systems poses serious threats to the security of end-to-end communications and network components themselves. A necessary foundation for securing a network is the ability to reliably authenticate communication partners and other network entities. One-way, password-based authentication techniques are not sufficient to cope with the issues at hand. Modern designs rely on two-way, cryptographic authentication protocols. However, most existing designs suffer from one or more limitations: They require synchronization of local clocks, they are subject to export restrictions because of the way they use cryptographic functions, they are not amenable to use in lower layers of network protocols because of the size and complexity of messages they use, etc. Designing such cryptographic protocols for large and dynamic network communities presents substantial challenges in terms of ease of use, efficiency, flexibility, and above all security.

¹ IBM Corp., Research Triangle Park, NC.

² IBM T. J. Watson Research Center, NY.

³ IBM Zurich Research Laboratory, Switzerland.

This paper elaborates on the design of a family of secure authentication protocols that was originally discussed in [Bird91]. In a first part, starting from the basic principles of cryptographic authentication and looking at existing designs, we show that several simple protocols, including one being standardized by ISO, are easily broken. Through an examination of the problems encountered in such designs, we derive a set of requirements for defining cryptographic authentication protocols that are at the same time simple and yet resistant to a wide class of attacks, while being easy to use and applicable to many networking environments.

Based on the requirements outlined in the first part, the second part of the paper then develops systematically a canonical form of a simple cryptographic two-way authentication protocol. We show that protocols matching this canonical form resist a wide range of attacks, we show a couple of concrete embodiments of the canonical form, and we discuss the properties of such protocols. One of the simple embodiments of the canonical form has formally been proven secure against any attack under reasonable cryptographic assumptions [Bird91]. However this proof extends beyond the scope of the present paper.

2. Basic Principles and Possible Attacks

2.1. Basic Principles of Authentication

Passwords

The authentication method most widely used in network environments today consists of asking users to prove their identity by demonstrating knowledge of a secret they know, typically a password. This widespread but old technique has several weaknesses:

Passwords are transmitted in the clear: In most password systems, the password typed by a user is sent in cleartext over the network to the computer that requested it. This means that an intruder equipped with suitable electro-magnetic tools can tap network lines and spy on passing traffic to collect passwords.

Passwords are easy to guess: A relatively low fraction of potential intruders are so dedicated and affluent that they would actually resort to the above electronic wire-tapping. However simpler attacks are also possible. Since users need to memorize their passwords, they typically select passwords that they can easily remember. Unfortunately, experience has shown that such passwords are selected from within a very small vocabulary, and are thus easily guessed by potential intruders [Morris79, Spafford89].

Authentication is one-way only: Last but not least, password schemes are typically used for one-way authentication only, i.e. computers ask users for their passwords but users never question that they are communicating with the right computer, and thus never challenge a computer to provide any password. This is however a serious exposure: when a user sits at a workstation and requests services from some remote computer, there is no proof that a password prompt appearing on the screen is from the right computer; the prompt could be a faked one displayed by another computer or by a corrupted application designed by an intruder.

Other Techniques

Of course, passwords could be used in both directions, thus barring the way to the latter exposure. However, this has not been done in practice.

Similarly, there exist many alternative techniques to password-based authentication, where users do not have to remember anything so that the risk of an intruder guessing a secret is inexistent. For instance, some systems base authentication on voice, finger-print, or hand signature recognition. However, such authentication techniques have reliability problems and require relatively expensive hardware support, so that they are found only in selected high-security environments, not in general-purpose network environments. Besides, they still suffer from the problem that 'the secret' is often transmitted in cleartext over network lines that can be tapped, thus allowing replay at a later time.

Of all authentication techniques that circumvent the drawbacks of passwords, the most promising ones are those using cryptographic means, whose common use is becoming increasingly feasible thanks to technological progress. With such techniques, users are typically provided with smart cards or chip cards equipped with a processor capable of cryptographic operations. Such cards offer interfaces to communicate either with their owner (through a liquid-crystal display and possibly a numeric keypad) or directly with a computer (through an electronic interface). Whatever the interface details, authentication is based upon using the card to compute or verify cryptographic messages exchanged with the computer.

Cryptographic Techniques

The basic idea of cryptographic authentication consists of challenging the user or communicating party being authenticated to prove its identity by demonstrating ability to encipher or decipher some item with a secret or private key known to be stored inside its smart card (or other secure storage device if the communicating party is a computer).

Of course, since the secret or private key stored on the card or secure device changes infrequently, the item to be enciphered or deciphered with it must change for every authentication instance, otherwise, even though the secret never flows in cleartext over the network, an intruder could still tap a line, record the cryptic message that flows over it, and play that recording back at a later time without even knowing what it means.

To guarantee that the item that gets enciphered, called the **challenge**, is different for every authentication instance, three techniques are used. The challenge may be derived either from a real-time clock reading, in which case it is called a **time-stamp**, from a counter that is incremented for every authentication operation, or from a random number generator, in which case it is called a **nonce**, that is used for only one authentication operation.

With time-stamps, the user or entity being authenticated, further referred to as A, enciphers the current reading of his clock and sends the result to the computer or party requesting the authentication, further referred to as B. B then decipheres the received message, and verifies that the time-stamp corresponds to the current real-time. The drawback of time-stamps is thus immediately apparent. A and B must have synchronized real-time clocks for the verification to be possible. However, since clocks can never be perfectly synchronized and messages take time to travel across networks anyway, B cannot expect that the deciphered time-stamp received from A will ever be equal to its own real-time clock reading. It can at best (and of course must) be within some limited time window of its own real-time clock. However, as soon as a time window of tolerance is defined, a potential intruder could exploit it to impersonate A by replaying A's recent authentication messages within that time window. Preventing this requires that B store all messages from A within the time window, which requires an amount of storage in direct proportion with the size of the time window. Because of these clock synchronization and window storage problems, time-stamps are not the most convenient way to generate challenges.

With counting challenges, A and B maintain synchronized counters of the number of times they authenticated one another. Every time A wants to sign on to B, it enciphers its counter and sends the result to B, who decipheres it

and verifies that it matches its counter value, whereupon both parties increment their respective counters for the next time. The drawback of such counting challenges is that both parties must maintain synchronized counters, which poses stable storage and counter management issues in the long run. Since counters will unavoidably lose synchronization at times, following loss of stable storage or of network messages and acknowledgements, special procedures are required to re-synchronize them when needed. For these reasons, counting challenges are useful for authenticating messages during an on-going dialog between A and B. However, counters alone are insufficient to support authentication of occasional communications over a long term.

The best technique for this purpose, and also the simplest one to implement, consists of using nonces. The price for this simplicity is an extra network message. While A can authenticate itself to B with a single message if time-stamps or counters are used, two messages are necessary with nonces. Indeed, it is B and not A who needs to be sure that the nonce was never used before. Thus it is B and not A who must generate it. B must encipher it and send it to A, then A must decipher it and send in back in cleartext for B to authenticate it, which costs a total of two messages. The cost of one more message is usually tolerable if it can be amortized over many subsequent messages authenticated with sequence counters. Given these advantages of nonces over time-stamps and counters, the rest of this paper focuses on nonce-based authentication protocols.

2.2. Simple-minded Cryptographic Authentication

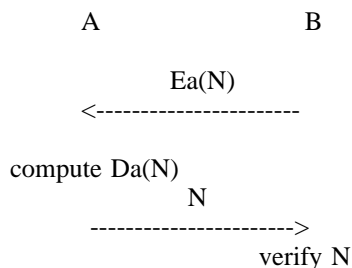


Figure 1. One-way authentication of A

Figure 1 is a simple representation of the nonce-based one-way authentication protocol described in the previous section, where N is a nonce generated by B and $E_a(N)$ is its value enciphered under some key K_a that B knows is associated with A: It may be a secret key shared between A and B or the public key of A. The protocol allows B to authenticate A.

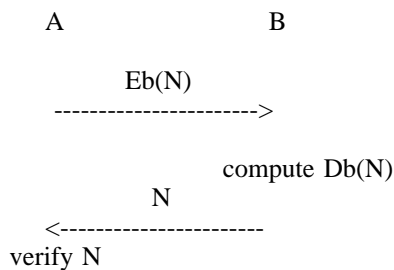


Figure 2. One-way authentication of B

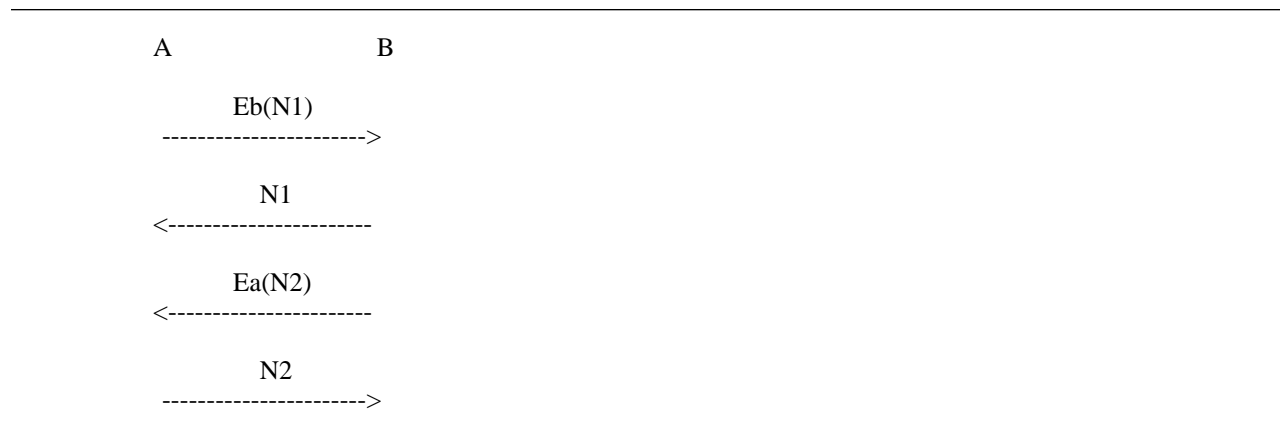


Figure 3. Two-way authentication



Figure 4. Two-way authentication with three messages

As suggested earlier, many scenarios in practice require two-way rather than one-way authentication, i.e. A must also authenticate B. This could of course be achieved simply by inverting the roles of A and B in Figure 1 on page 4, as represented in Figure 2 on page 4, where a $E_b(N)$ stands for the value of N enciphered under a key K_b that is either a secret shared between A and B or the public key private to B. Putting the two protocols together leads to Figure 3 for a complete two-way exchange. One can then immediately observe that the resulting protocol may be simplified by combining the second and third messages to save one network transmission, as represented in Figure 4. With symmetric cryptographic systems, the keys K_a and K_b could be the same, so that E_a and E_b indicate encryption under the same shared secret key.

Unfortunately, this simple and elegant two-way authentication protocol, which was derived most naturally by combining two instances of the simplest possible one-way protocol, is insecure, especially if symmetric cryptography is used. It leaves several doors open for an intruder to attack. We now examine these flaws, especially those affecting symmetric cryptography, since we are looking for protocols that are not restricted to asymmetric cryptography.

2.3. Attacks on Simple Cryptographic Authentication

Specifically, the protocol suffers from a number of defects:

Known plaintext attacks: A first weakness of the protocol, which is not a real exposure but still an undesirable feature, is its openness to known plaintext attacks. Every enciphered message flowing between A and B is the ciphertext of a bit string (the nonce) that flows in plaintext in a subsequent message between A and B. This enables a passive wire-tapping intruder to collect two cleartext-ciphertext pairs every time

the protocol is run, which at the very least helps it accumulate encryption tables in the long run, and may even help it break the scheme and discover the encryption key, depending on the quality of the encryption algorithm used. It is in general desirable that the plaintext of exchanged enciphered messages not be known or derivable by intruders.

Chosen ciphertext attacks The situation is in fact worse in the sense that a potential intruder may even turn known plaintext attacks into selected text attacks by playing an active instead of passive role. Pretending that it is A or B, the intruder may send the other party (B or A) a ciphertext message that it selected itself and wait for the other party to reply with the deciphered value of that text. Of course the intruder, not knowing the right key, may not be able to complete the third protocol flow. However, it can accumulate knowledge about cleartext-ciphertext pairs **of which it selected the ciphertext itself** (or the cleartext, with protocols that challenge parties to show ability to encrypt). So it may try specific ciphertext strings such as all zeros, all ones, or whatever else might help it break the key faster, depending on the cryptographic method used. It is in general desirable that an intruder not be able to trick legitimate parties into generating deciphered versions of selected ciphertext messages [Biham90].

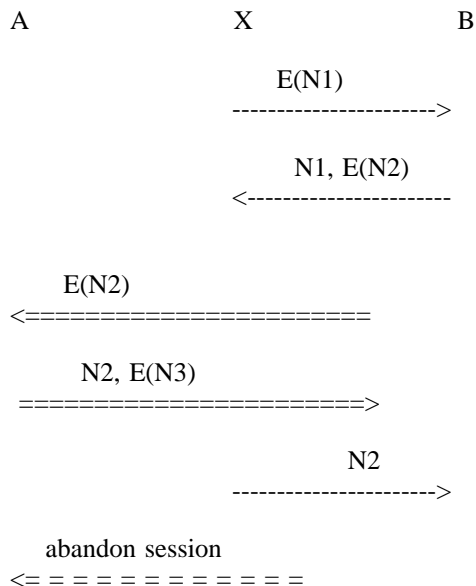


Figure 5. An oracle session attack

Oracle session attacks: In fact, using symmetric cryptography with the simple protocol suggested earlier, the intruder actually **can** break the authentication without even breaking the key. This is illustrated in Figure 5, where the intruder, noted X and posing as A, starts a session with B by sending B some enciphered nonce E(N1). B replies with the decrypted value N1 and its own enciphered challenge E(N2). X cannot decipher N2, but it can take advantage of a selected ciphertext attack on A, using A as an oracle who will provide the necessary deciphered value N2. X accomplishes this by posing now as B to start a separate 'oracle' session with A, sending E(N2) as the initial message on that session. A will reply with the needed value N2 and some own enciphered nonce E(N3). X then drops the oracle session with A since it cannot and does not care about deciphering N3. but it then turns around, and successfully assumes its faked identity A with respect to B by sending E(N2) to B.

This example exposes one fundamental flaw of the protocol: the cryptographic flows used for each direction of the authentication must be different from one another in the sense that it must not be possible for an intruder to use messages appearing in one of the directions to derive, reconstruct or fake messages needed for the other direction.



Figure 6. The ISO two-way authentication protocol

This observation was made independently by the designers of an improved authentication protocols now standardized by the ISO SC27 [ISOSC27] and represented in Figure 6. In this protocol, the challenge of authentication in one direction consists of demonstrating ability to *encipher* a given cleartext nonce, while in the other direction it requires ability to *decipher* a given ciphertext nonce. Thus an intruder can no longer misuse one party as an oracle 'decryption server' against the other. Unfortunately, this slightly improved protocol still suffers from a fourth type of defect, also present in the original protocol, and discussed hereafter.

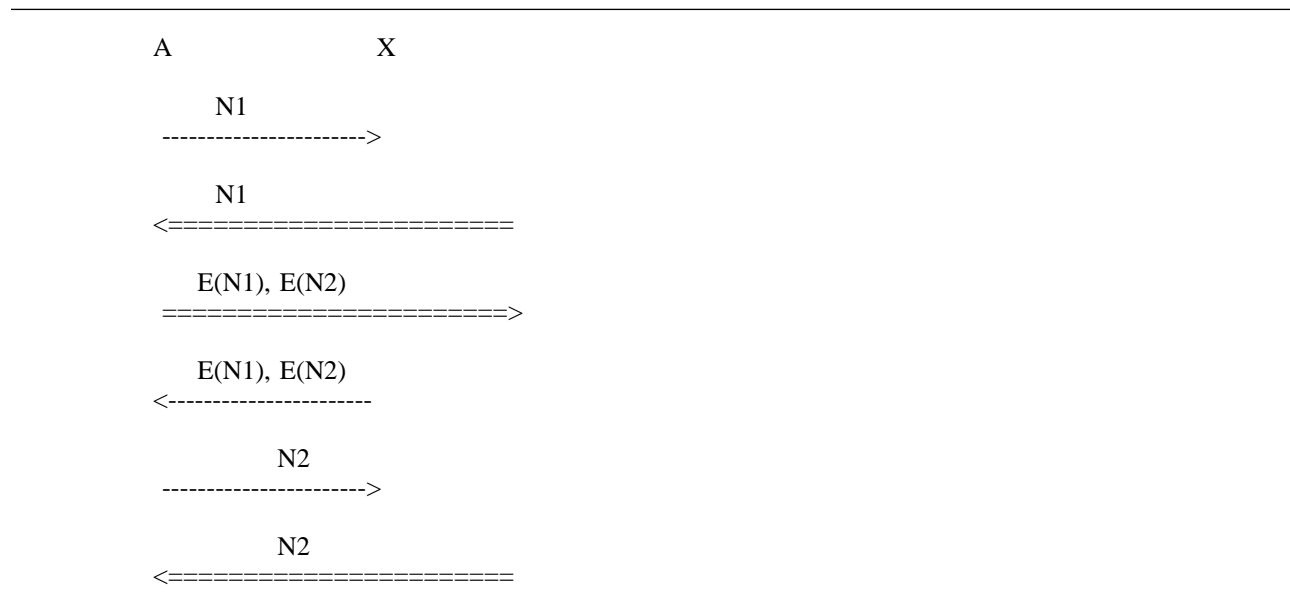


Figure 7. A parallel session attack

Parallel session attacks: Another defect commonly found in simple protocols such as those seen above is depicted in Figure 7, where the intruder assumes a passive role instead of an active one. It intercepts a call from A to B with challenge $N1$, and, leaving B completely out of the picture, turns A into an oracle against itself. Since X cannot answer the challenge $N1$ by replying $E(N1)$, it simply pretends that it is B trying to start a parallel session with A. Of course it selects to use just the same $N1$ as the first challenge on that session, thus causing A to provide it with precisely the answer $E(N1)$ needed to complete the first authentication. A also sends its own enciphered challenge $E(N2)$ on the parallel session. X then replies to the original challenge $N1$ by sending $E(N1)$ back. With that reply, X may even send the same enciphered challenge $E(N2)$ it just got from A. A will then complete the first

authentication exchange by replying with $N2$, which is again exactly what X needs to complete the second authentication. Thus X has succeeded doubly in posing as B on both the original and the parallel sessions! (He could also have dropped one of these, of course.)

Many connection set-up protocols at different layers of different network architectures do not allow the simultaneous establishment of multiple sessions. However, there also exist many networking environments where such parallel sessions are legal by design. Where they are allowed, it would be feasible to warn implementers to check that the first challenge received on one session is not a replay of a challenge outstanding on another session. This is indeed the implementation advice given with the ISO protocol. However leaving session security up to implementers rather than guaranteeing it by design is bad practice. Furthermore, in typical implementations, session parameters are instantiated independently for each session so that it is not possible for one session to check on parameters of other sessions.

Parallel session attacks illustrate another fundamental flaw of many simple authentication protocols: the cryptographic expression used in the second message must be asymmetric (i.e. direction-dependent) so that its value in a protocol instance initiated by A cannot be used in a protocol instance initiated by B .

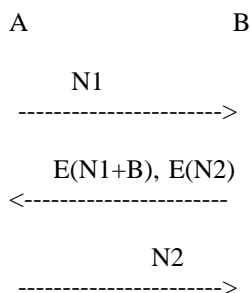


Figure 8. A more complex and asymmetric two-way authentication

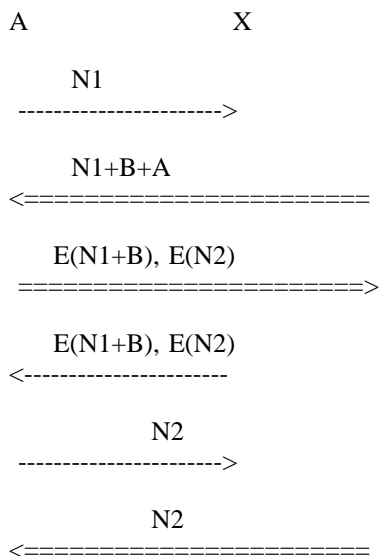


Figure 9. An offset attack (through a parallel session)

Based on the above observations that the cryptographic message in the second flow must be asymmetric (direction-dependent) and different from the one in the third flow, one may be tempted to declare that a protocol such as the one in Figure 8 should be secure. Here, enciphering $N1$ has been replaced by enciphering a simple function of $N1$ ('+' stands for exclusive-or in this example). Beyond the fact that known- and selected-text attacks are still possible, the problem now is that the simple function has not fixed anything: an intruder can still resort to a parallel session attack; it merely needs to use proper offsetting in addition, as illustrated in Figure 9 on page 8. The simple and apparently sound protocol of Figure 4 on page 5 is thus broken in many ways.

We have come across and designed many simple and apparently secure two-way authentication protocols which, upon careful examination, proved to be subject to oracle-session attacks, parallel-session attacks, offset attacks, and/or many other types of attacks or combinations thereof that involved replaying messages and functions of challenges observed in other runs of the protocol. We further refer to all such attacks collectively as **interleaving** attacks. We came to the conclusion that the design of simple protocols that resist such interleaving attacks is hard and requires a careful and systematic approach, as explained in the remainder of this paper.

2.4. Existing Designs

This does not mean that there exists no secure two-way authentication protocol. Many such protocols have been designed. However most use time-stamps or counters, thus avoiding the known- and selected-text attacks at the cost of clock and counter management issues. Many make abundant, in fact redundant, use of cryptographic operations, which seem to enhance security but at the cost of efficiency. Many use large cryptographic messages (tens to hundreds of bytes), which is no problem for application-layer protocols but such messages are hard or impossible to carry within lower-layer networking protocols where limited packet sizes are an important consideration. Last but not least, many are so complex that, while they appear to resist interleaving attacks, there is no formal proof that they actually do by definition [see for instance Stubblebine92]. Much promising work has recently been done on proving formal statements about authentication protocols [Burrows89, Gong90, Cheng90, Abadi91]. However many existing protocols have not yet been subjected to such scrutiny and none has been shown to resist the sort of attacks described earlier.

Academic designs including one- and two-way authentication protocols (usually coupled with key distribution functions) have been discussed, for instance, in [Needham78, Bauer83, Denning81, Otway87, Burrows89]. Examples of practical designs in actual use can be found, among others, in Kerberos [Steiner88] and ANSI X9.17 [ISO8732] implementations. While not yet available commercially, implementations of the CCITT X.509 [ISO9594] standards will most likely appear soon. As suggested above, all these designs either use time-stamps or counters, or/and many cryptographic operations, or/and long cryptographic messages. None of them comes with any assurance of security while some (e.g. the ISO SC27 protocol) are known to contain design security defects [Bellare90, Janson90].

2.5. Design Requirements

The objective of the work discussed here is thus to understand what it takes to design two-way authentication protocols that are complex enough to resist interleaving attacks, yet remain economical and simple enough to be usable in low layers of network architectures. To understand the boundary conditions on our design space, we summarize here requirements that such protocols must meet, most of which are derived from the discussion so far:

Nonce-based: Because of an explicit intention to avoid clock synchronization and stable counter storage issues, the protocols should preferably use nonces.

Resistant to common attacks: It must be possible to show that the resulting protocols are intrinsically secure against known- and selected-text attacks, as well as interleaving attacks, i.e. that a potential intruder can never derive a 'good-looking' cryptographic message from any reply to or manipulation of past messages it may have observed or triggered itself. (A more formal definition of interleaving attacks is given in [Bird91].)

Usable at any layer of any network architecture (small messages): The protocols must be suitable for low-level networking mechanisms as well as for application-layer authentication, meaning they must be based on cryptographic authentication messages that are as short as possible, hopefully the length of a single block of ciphertext with the given encryption algorithm.

Usable on any processing base (few computations): The protocols must be easily executable on smart cards as well as on low-end, entry-level networking components and workstations (e.g. PC's) with little processing power and no specialized cryptographic processing chip, i.e. they must involve as few cryptographic operations as possible.

Together, the latter two requirements, short and simple messages are aimed at securing communication in primitive environments, such as for instance a link-layer protocol or a secure boot service, where minimal complexity and minimal message size are required.

Using any cryptographic algorithm: The protocols must be able to use any of the known and typical cryptographic algorithms, either symmetric ones, such as DES [DES77], or asymmetric ones such as RSA [RSA83] for instance.

Exportable: Keeping in mind that import/export of cryptographic technology is tightly controlled in many countries, authentication protocols designed to be used without geographical restrictions should conform to applicable regulations. Most regulations restrict the export of technology allowing bulk data encryption/decryption. However, export of technology aimed solely at data integrity and authentication is generally possible with proper licensing. Thus the chance to receive proper licensing for a technology is larger if it relies only on data integrity and authentication techniques and not on data confidentiality functions, i.e. if it provides only Message Authentication Code (MAC) computation and verification and does not require encryption and decryption of large messages. This constitutes an additional requirement for us, which is also not fulfilled by designs such as Kerberos or X9.17 that rely on encryption and decryption of time-stamps or counters.

Designing protocols with the above properties is hard and is the subject of the rest of this paper.

3. Systematic Derivation of a Minimal Protocol

Our objective in the rest of this paper is to construct systematically two-way authentication protocols meeting the security and other design requirements discussed above. To this end we first derive a canonical form for such protocols through a set of intuitive steps. Then we show how its security can be tested against interleaving attacks. Finally, we give examples of some of the simplest possible protocols matching the canonical form and we discuss their relative merits. One of the simple embodiments of the canonical form has formally been proven secure against any attack, under reasonable cryptographic assumptions [Bird91]. However, this proof extends beyond the scope of the present paper.

3.1. Canonical Protocol

To produce a canonical form for all protocols fulfilling the security and design requirements seen above, we examine one-by-one each requirement and derive immediate implications on the possible canonical form.

Resistance to Replay Attacks through Use of Nonces



Figure 10. Canonical protocol 1: Resistance to replay attacks through use of nonces

Given that we focus on authentication protocols using nonces, the most general canonical form for all such protocols is depicted in Figure 10. Here, the initiator A sends some nonce $N1$ to the intended partner B. B authenticates itself by sending back a function $u()$ of several parameters including at least its secret $K1$ and the challenge $N1$ it received from A. In turn it sends a challenge $N2$ to A. A finally completes the protocol by authenticating itself with a function $v()$ of several parameters including at least its secret $K2$ and the challenge $N2$ from B.

Resistance to Oracle Session Attacks

As indicated in the earlier section on attacks, in order for this protocol to resist oracle attacks, the functions $u()$ and $v()$ must be different from one another, meaning that a cryptographic message from flow (2) can never be used to derive the necessary message for flow (3).

No Restriction on Cryptographic System

The protocols being developed must be workable with either symmetric or asymmetric cryptographic systems. With the latter, the secrets $K1$ and $K2$ will be the private keys of B and A respectively. With symmetric systems, $K1$ and $K2$ must be shared secret keys. In fact, in many practical scenarios, they are typically the same shared secret key. We will pursue our step-wise protocol construction under that assumption because it opens the door to attacks that would not be possible otherwise yet must be prevented in any case. Any protocol that resists interleaving attacks using equal symmetric keys is also safe with asymmetric ones while the opposite is not true.



Figure 11. Canonical protocol 2: Use of symmetric cryptography

Under the assumption of possible use of a symmetric cryptographic system with a single shared secret key K , our initial canonical form becomes as depicted in Figure 11, where the functions $u(K1, ..)$ and $v(K2, ..)$ become symmetric encryption (or decryption) operations under (possibly) the same key K of two different functions $p()$ and $q()$ of the remaining parameters.

Resistance to Parallel Session Attacks



Figure 12. Canonical protocol 3: Resistance to parallel session attacks

As indicated in the earlier section on attacks, the prevention of parallel session attacks suggests that function $p()$ must be asymmetric, i.e. direction-dependent. In other words, the arguments to $p()$ must be different depending on whether A or B starts the communication session. This is depicted in Figure 12 by the addition of a parameter D in $p()$, which stands for anything indicating or tied to the direction of the flow (e.g. the name or address of one of the parties).

Small Cryptographic Messages

As shown in Figure 12, the complete protocol requires three messages. In any networking environment, these messages need not travel in packets of their own. In practice, they can and typically would be piggy-backed onto other network packets, such as, for instance, connection requests and confirmations at whatever layer entities are being authenticated (e.g. link, network, transport, application, etc.).

Within packets at any such layer, the authentication fields should take as little space as possible. As it stands presently, the canonical protocol requires carrying a nonce on the first flow, a nonce and a cryptographic expression on the second one, and a cryptographic expression on the third one. (The cleartext of the involved party names or addresses are assumed to be already present in the enclosing packet header.) The required size of nonces is given by the amount of security desired: the larger they are, the lower the probability will be that a given nonce gets

reused. The size of the cryptographic expressions depends on the encryption algorithm used and on the amount of information being encrypted.

To take a concrete example, if the DES is used, the smallest cryptographic expression will be 64-bit long. Since the security of the whole authentication protocol rests on the unforgeability of the cryptographic expressions, if expressions of 64 bits are used, the statistical security of the expressions is 2^{64} , the inverse of the probability that an intruder can successfully guess a cryptographic expression. For many environments such a degree of security is already quite satisfactory.

Without at all precluding that there exist environments where longer cryptographic expressions may be desired, we pursue our step-by-step derivation of a canonical form under the assumption that a degree of security of 2^{64} is sufficient in most scenarios. This suggests that using 64-bit nonces is sufficient. Furthermore it suggests that $p()$ and $q()$ may be restricted to 64-bit functions of their parameters without compromising the degree of security. We further make this simplifying assumption. Using longer cryptographic expressions with standard DES encryption would add nothing since the probability of guessing a DES key remains anyway $1/2^{64}$ (or more accurately $1/2^{56}$).

Resistance to Offset and Selected-Text Attacks

The observation that it is desirable to restrict $p()$ and $q()$ to 64-bit functions to limit message size has severe implications. Indeed, many simple and attractive 64-bit functions of only $N1$ and D (e.g. XOR, rotations, conditional permutations, etc.) could be subjected to selected-plaintext and offset attacks by an intruder playing number games on its nonces to get what it wants enciphered by a legitimate party. As observed in the discussion on possible attacks, it is important that the protocol resist such offset and selected-text attacks. Thus, there must be further conditions on the nature of $p()$.

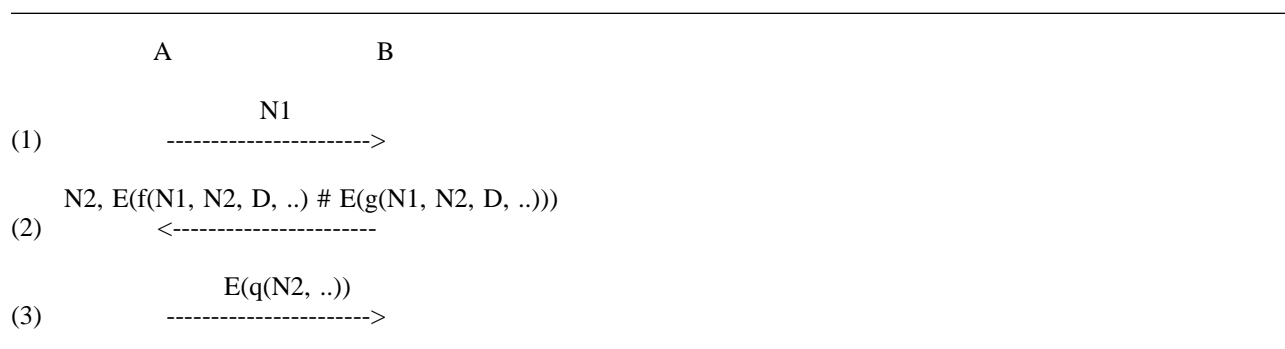


Figure 13. Canonical protocol 4: Resistance to selected-text and offset attacks

By including inside function $p()$ an additional internal encryption function of the same parameters $N1$ and D , one can separate them cryptographically and thus bar the way to offset attacks. Further, by including $N2$ inside function $p()$, one bars the way to a potential intruder using B as an oracle to get some select plaintext enciphered in flow (2). Indeed the cleartext of that flow then depends on nonce $N2$ which is not under the control of the intruder. These further conditions on $p()$ are represented in the new canonical form of Figure 13. In its most general form, $p()$ would thus be a 64-bit function (noted #) of two operands, which themselves include functions $f()$ and $g()$ of $N1$, $N2$, and D .

Few Cryptographic Operations

When we started deriving a canonical form for our protocols, it became immediately evident that any form requires at least two cryptographic expressions (one in each direction), i.e. two cryptographic block operations if we assume the 64-bit size limitation as desirable and satisfactory for most scenarios. Figure 13 suggests using a third cryptographic operation to protect against offset attacks. Yet minimizing the number of required cryptographic operations so the protocols remain efficient even on low-end processors is one of our requirements.

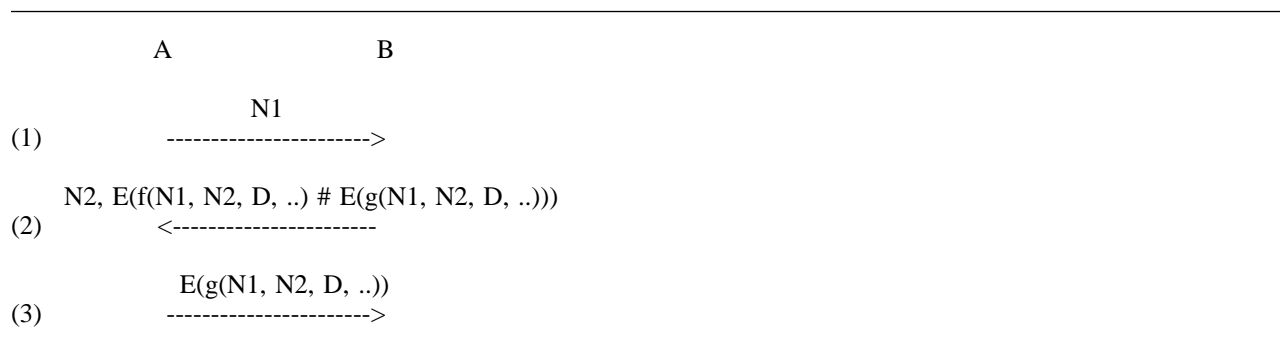


Figure 14. Canonical protocol 5: Minimal no. of encryptions

Fortunately, by putting additional conditions on $q()$, we can return to a protocol requiring only two cryptographic block operations. This can be achieved if desired by imposing that the functions $g()$ and $q()$ actually be the same, as represented in Figure 14. Indeed, in this case, the innermost cryptographic expression required to produce or verify flow (2) is the same as the cryptographic expression of flow (3), and can thus be computed only once and saved to minimize computation.

Resistance to Known Plaintext Attacks

As it now stands, the canonical form for our protocol resists interleaving attacks, as will be tested later. However, it is still open to known-plaintext attacks and can be refined and improved in that direction. Indeed, since all arguments of $g()$ can be obtained (through wire-tapping) by a potential intruder and $g()$ is not a secret function, that intruder can compute the cleartext and observe the ciphertext for flow (3). Similarly, since $f()$ and all its parameters are no secrets, the intruder can compute $f()$. By combining it (with the $\#$ operation) to the ciphertext it observed for flow (3), it can derive the cleartext for flow (2), for which it can also observe the corresponding ciphertext on the network. Thus every run of the protocol still provides an intruder with two cleartext-ciphertext pairs, which is undesirable.

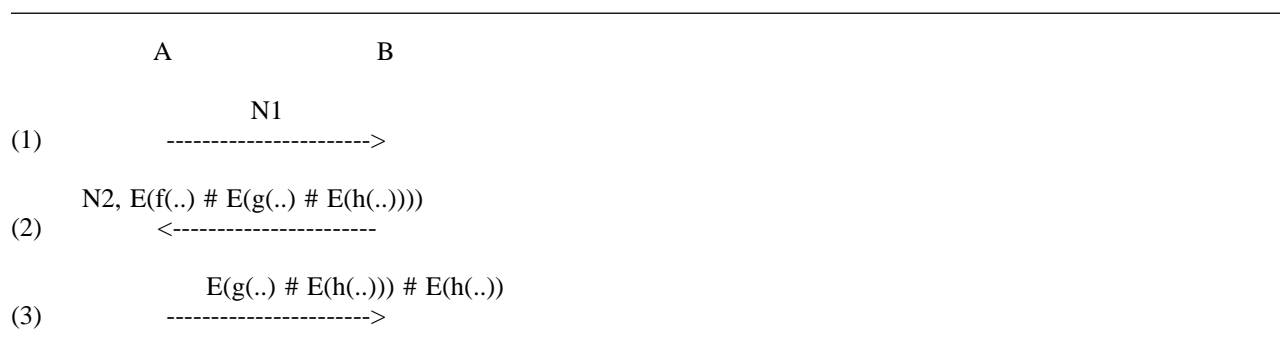


Figure 15. Canonical protocol 6: Resistance to known-plaintext attacks

Closing the door to such known-plaintext attacks does however require an additional encryption operation within $g()$ so that the cleartext value for flow (3) becomes hidden from potential intruders: $g()$ is replaced by $g() \# E(h())$, where $\#$ is again a suitable 64-bit operator. In addition, since the original ciphertext of flow (3) is part of the cleartext for flow (2), it too must be hidden, hopefully without requiring yet another encryption. This can be accomplished, as suggested in Figure 15 on page 14, by using the third encryption not only inside $g()$ but also outside, where it is combined to the original expression for flow (3) using some suitable 64-bit operator again noted by $\#$. ($f()$, $g()$, and $h()$ in the latest canonical form all take the same parameters as $f()$ and $g()$ did in the previous form.)

Exportability

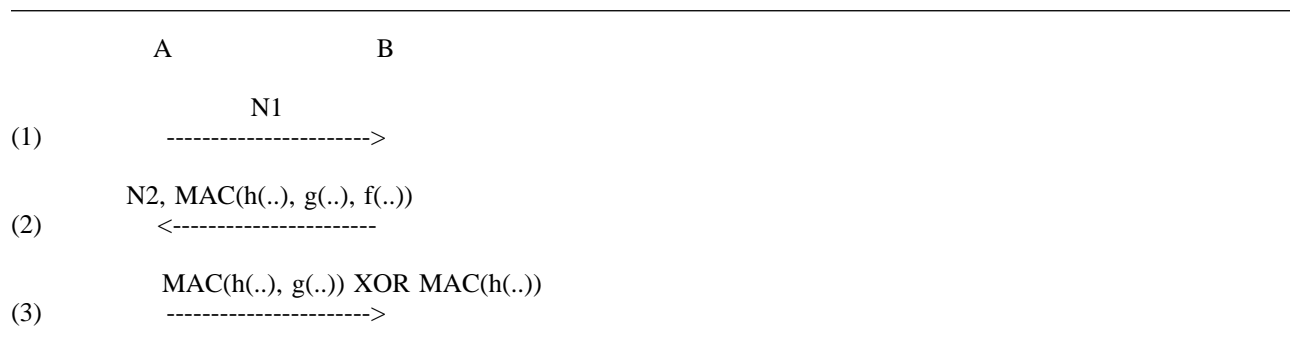


Figure 16. Canonical protocol 7: Exportability

With an eye towards exportability of authentication protocols, the best design is one that can be shown to use only one-way data integrity (MAC) operations instead of requiring encryption operations that would leave a door open to decryption.

In the specific case where the cryptographic algorithm used is DES, and all $\#$ operators in the latest canonical form of the protocols denote XOR operations, one observes that the resulting cryptographic expressions for flows (2) and (3) indeed boil down to combinations of plain 64-bit MAC integrity checks computed using the Cipher Block Chaining (CBC) mode of operation of DES, as represented in the canonical form of Figure 16. While this latest canonical form was derived assuming DES MAC functions, the very same canonical form still works with any other MAC function and cryptographic algorithm.

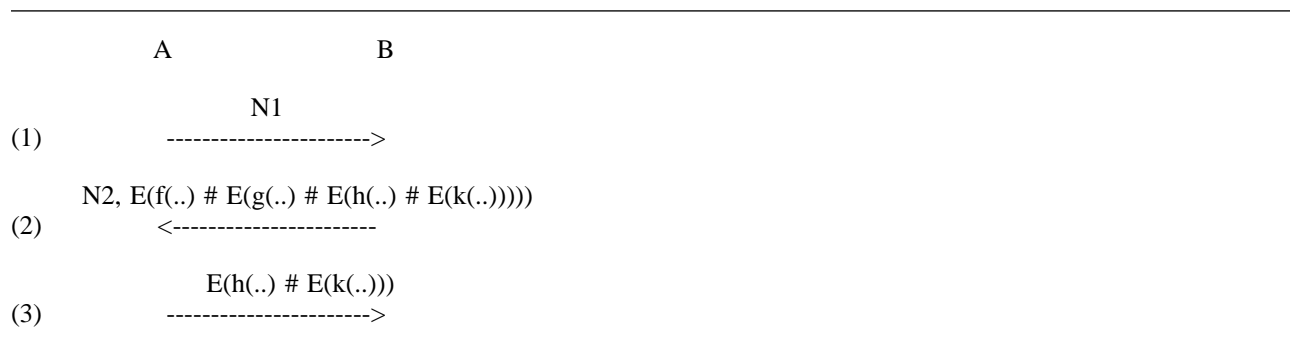


Figure 17. Canonical protocol 8: Cryptographic Hardware support



Figure 18. Canonical protocol 9: Exportability with hardware support

Each of the required three MAC computations is a subset of the previous one, so that an efficient implementation should compute them starting from $\text{MAC}(h(\cdot))$ (i.e. the last one) and save intermediate results for later re-use. If a hardware implementation of a MAC algorithm is available, the cost of a driver invocation for that hardware may actually be more substantial than the cost of an extra cryptographic block operation. In that case, a canonical protocol using just two MAC operations is preferable. However then a fourth block encryption is desirable to protect flow (2) against known plaintext attacks that would otherwise be possible. This is represented in Figure 17 on page 15. In a DES context with all # operators designating XOR operations, this amounts to the MAC-based protocol represented in Figure 18. Again an efficient implementation could compute the second MAC expression as part of the first one and save it for reuse in flow (3). The export of any protocol based on canonical forms 7 or 9 should pose no problem.

Resistance to Interleaving Attacks

The step-wise derivation and refinement of more and more specific canonical protocols has lead us through a series of canonical forms where each one describes a subset of the all protocols described by the previous one. This series of canonical forms has taken into account all security features identified as requirements during our earlier interleaving attack analysis as well as additional requirements of simplicity, efficiency, flexibility and exportability. However the derivation was purely intuitive. It remains to test that these protocols are indeed secure. In the next section we present the method we used to test that they are secure against interleaving attacks. We have also shown formally in [Bird91] that one specific embodiment of the canonical form is secure against all attacks if reasonable cryptographic assumptions are met by the function $E()$.

3.2. Testing Resistance to Interleaving Attacks

For simplicity, we present the test of resistance of the canonical form against interleaving attacks only for the fifth canonical protocol defined earlier. Note that this test does not check for resistance to known plaintext attacks and for exportability since these are not addressed by the fifth canonical protocol. This test is thus not a proof of security against all attacks as presented in [Bird91].

To limit the complexity of the equations used for the test, we assume that functions $f()$ and $g()$ take just $N1$, $N2$, and D as arguments. The possible existence of additional arguments only complicates the expressions without adding any value to the test. Further we occasionally need to distinguish between the two possible values of D , which we note as AB and BA , referring to the direction of the first and second flow respectively.

We test that an intruder X attacking A or B cannot reconstruct or derive the cryptographic expressions needed in flows (2) or (3) by replaying or manipulating the results of passive observations or active interleaving attacks. Thus we start by considering what information a potential intruder could possibly glean through passive observations or interleaving attacks in the course of time.

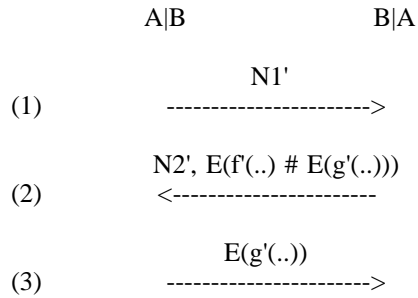


Figure 19. Reference session R1: a legitimate one

A first kind of observation it can make consists of recording legitimate past runs of the protocol between A and B, such as the reference session 1 depicted in Figure 19. In this and subsequent figures, the use of the prime (') notation indicates that the variables and functions are reference observations of the past. $f'()$ and $g'()$ are simply instantiations of $f()$ and $g()$ for parameters $N1'$, $N2'$, and D' as they could be observed in some past run of the protocol.

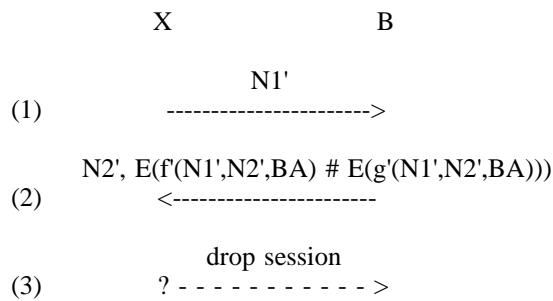


Figure 20. Reference session R2: X attacks B and fails

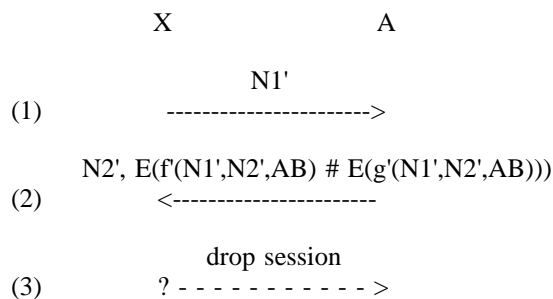


Figure 21. Reference session R3: X attacks A and fails

Similarly, X could collect information on the protocol actively by pretending to be A or B and attacking the other party (with no hope of succeeding for now) simply to see the other party's reaction and record more data on its responses. These two additional sources of information are represented as reference sessions 2 and 3 in Figure 20 and Figure 21.

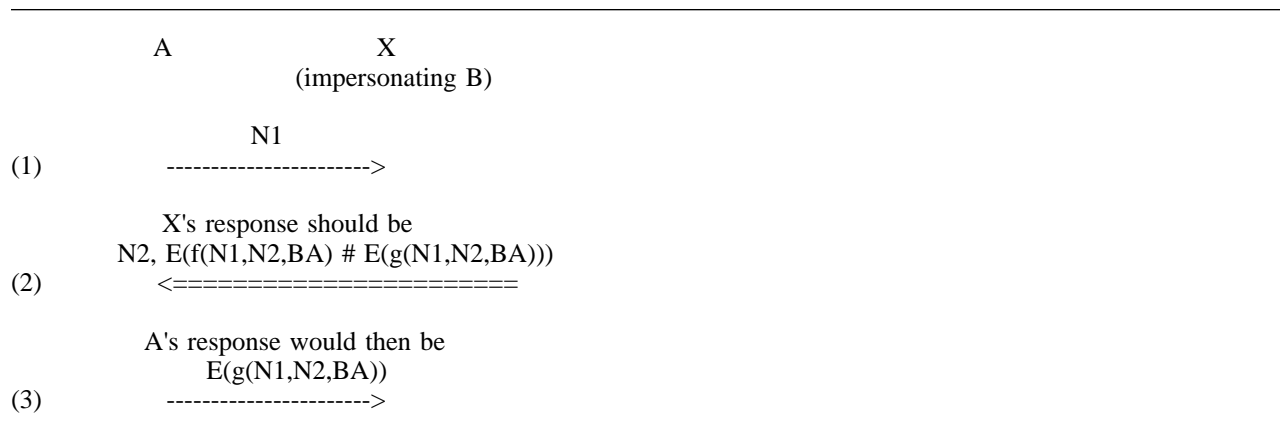


Figure 22. Attack session A1: X intercepts call from A (or B)

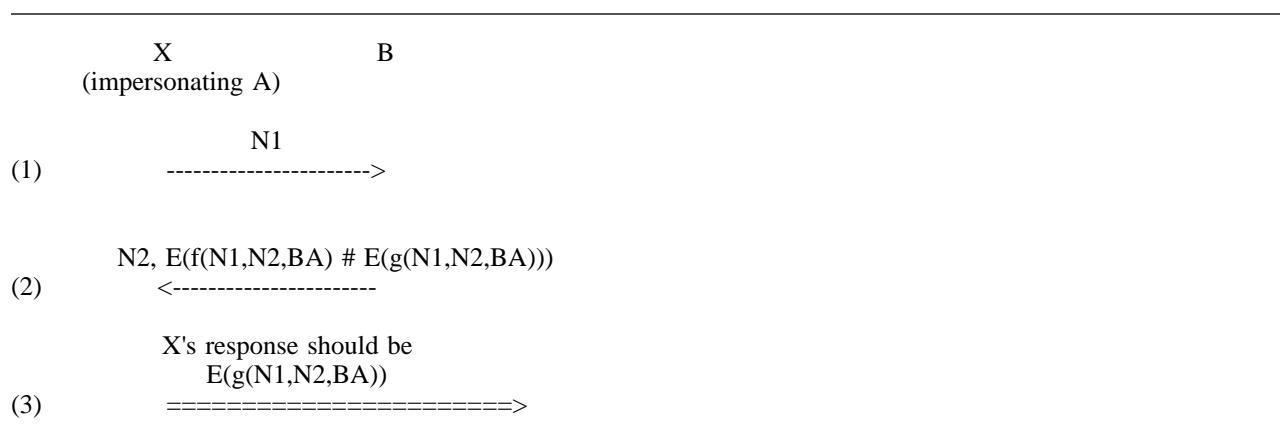


Figure 23. Attack session A2: X tries to calls B (or A)

Armed with any amount of knowledge about legitimate past runs or interleaved trial runs of the protocol, as defined above, the intruder could then try to attack the protocol in two ways represented in Figure 22 and Figure 23. In the first attack, X behaves passively, waiting for a call from A (or B, the derived equations would be similar) to intercept, while in the second it takes the initiative to call A (or B, the derived equations would also be similar). In the first attack, X is challenged to produce the cryptographic expression of flow (2), while in the second attack it is challenged to produce the one for flow (3).

In order to ensure security of the protocol against interleaving attacks, we must test that X cannot produce the necessary expressions based on interleaving attacks or simple manipulations of observations of the past, unless it was able to record the behavior of A and B for many possible combinations of $N1'$ and $N2'$, which we must assume is impossible. (If A and B have communicated that often, they should change secrets many times in the course of things!)

The test of security rests on the ability to show that the cryptographic expressions of flow (2) in the first attack (noted A1.2) and flow (3) in the second one (noted A2.3) cannot be derived from any of the cryptographic expressions in flows (2) or (3) of any of the reference sessions (noted R1.2 and R1.3, R2.2, and R3.2) or of the on-going attack session itself. In other words, X cannot break the protocol if it cannot solve any of the following nine equations:

- (1) $A1.2 = R1.3$, where $N2$ is free and $N1 \triangleleft N1'$
- (2) $A1.2 = R1.2$, where $N2$ is free and $N1 \triangleleft N1'$
- (3) $A1.2 = R2.2$, where $N1'$ and $N2$ are free

but $N1'$ cannot depend on $N2'$
 and $N1' \nleftrightarrow N1$ or $N2 \nleftrightarrow N2'$ as this would
 be a trivial interceptor-repeater attack
 where X is just a passive observer
 between A and B , who have actually
 authenticated one another in real-time

(4) $A1.2 = R3.2$, where $N1'$ and $N2$ are free
 but $N1'$ cannot depend on $N2'$

(5) $A2.3 = R1.3$, where $N1$ is free but cannot depend on $N2$

(6) $A2.3 = R1.2$, where $N1$ is free but cannot depend on $N2$

(7) $A2.3 = R2.2$, where $N1$ is free but cannot depend on $N2$
 and $N1'$ is free but cannot depend on $N2'$

(8) $A2.3 = R3.2$, where $N1$ is free but cannot depend on $N2$
 and $N1'$ is free but cannot depend on $N2'$

(9) $A2.3 = A2.2$, where $N1$ is free but cannot depend on $N2$

When checking alternative protocols, including some of the simpler ones mentioned earlier in this paper, we were often able to solve one or more of the equations above and from this to construct an attack on the protocol. However, as we argue below, it is not possible to solve these equations for protocols having the canonical form under proper assumptions about $f()$ and $g()$.

Equations (1) and (9) are unsolvable because solving them would require the ability to break the encryption itself, which is assumed to be impossible.

Equations (7) and (8) are unsolvable because solving them would require knowing the values of $E(g'(..))$ in reference session 2 and 3, which never appear anywhere since those reference sessions could not complete.

Equations (5) and (6) are unsolvable because solving them would require that $N1$ be a function of $N2$, which contradicts the fact that $N2$ is determined by the attacked party **independently from and after** $N1$ is picked by X .

Because of the cryptographic separation between the $f()$ and $g()$ terms in equations (2), (3), and (4), these equations would be solvable only if the intruder could either:

(in case (2)) find $N2$ to solve equations

$$(2a) \quad f(N1, N2, BA) = f(N1', N2', BA)$$

$$(2b) \quad g(N1, N2, BA) = g(N1', N2', BA)$$

where $N1 \nleftrightarrow N1'$, or

(in case (3)) find $N2$ and $N1'$ to solve equations

$$(3a) \quad f(N1, N2, BA) = f(N1', N2', BA)$$

$$(3b) \quad g(N1, N2, BA) = g(N1', N2', BA)$$

where $N1 \nleftrightarrow N1'$ or $N2 \nleftrightarrow N2'$, or

(in case (4)) find $N2$ and $N1'$ to solve equations

$$(4a) \quad f(N1, N2, BA) = f(N1', N2', AB)$$

$$(4b) \quad g(N1, N2, BA) = g(N1', N2', AB)$$

In case (4), which is in effect a parallel session attack on A , if X selects $N1'=N1$ and $N2=N2'$, equations (4a) and (4b) are not solvable since $f()$ and $g()$ yield different results for different direction indicators by definition, all other parameters being equal. Thus, it remains to show that equations (4a) and (4b) are unsolvable in cases where $N1' \nleftrightarrow N1$ and $N2 \nleftrightarrow N2'$. However, in these cases, all pairs of equations (2a/b), (3a/b) and (4a/b) boil down to the same single pair of equations

- (a) $f(..) = f'(..)$
 (b) $g(..) = g'(..)$

which must not be simultaneously solvable for any $N2$ with the condition that $N1' \neq N1$ or $N2 \neq N2'$.

These two remaining equations thus represent criteria that functions $f()$ and $g()$ must meet to ensure resistance of the canonical protocol to interleaving attacks. They express that, given that $N1'$ cannot be equal to $N1$ and $N2$ cannot be equal to $N2'$, $f()$ and $g()$ must be such that the two equations never accept the same solution in $N2$. To put it in other words, the fewer points there are in the $\{N1, N1', N2, N2', D, D'\}$ space where $f()=f'()$ and $g()=g'()$, the better the resistance of the protocol will be to A1 attacks. (A2 attacks are strictly impossible since equations (5-9) are strictly unsolvable in any case.)

Whether $f()$ and $g()$ functions meeting these criteria exist and can be found, and how good they are, are legitimate questions. The existence and quality of such functions are best substantiated by the examples given in the next section.

3.3. Specific Examples

Example With Two Encryptions

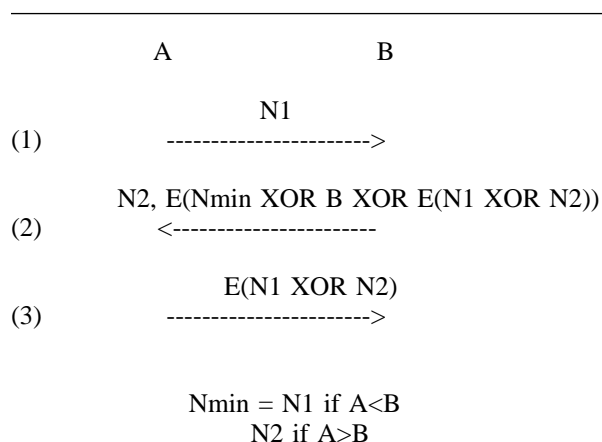


Figure 24. Secure protocol with two encryptions

Figure 24 shows an example of a perfectly secure protocol using only two encryptions, where $f()$ is the exclusive-or of the name of the responder with the nonce of the party with the lower address (or name), while $g()$ is the exclusive-or of the two nonces. The name B appearing in flow (2) is assumed to be no longer than nonces and is used here as the direction indicator D. Since this protocol uses only two encryptions, it does present the disadvantage of allowing an intruder to build up tables of known-plaintext-ciphertext pairs. However, the protocol is otherwise secure. Indeed, assuming use of 64-bit DES, the equations $f()=f'()$ and $g()=g'()$ are solvable simultaneously for only $1/2^{64}$ of the points in the $\{N1, N1', N2, N2', D, D'\}$ space, meaning that the probability that an intruder can take advantage of such a point is no higher than the probability that it can guess the right encryption for any other point. This can be seen as follows: if nonces and party names were assumed to be one bit long, the two equations would be simultaneously solvable for 4 out of the 8 points of the $\{N1, N2, D\}$ space, meaning the intruder would have a one out of two chances to succeed. Using 64-bit nonces and names, this 1/2 chance of success is of course raised to the power 64, which is equal to the statistical 'solidity' of DES in the first place.

Example With Three Encryptions

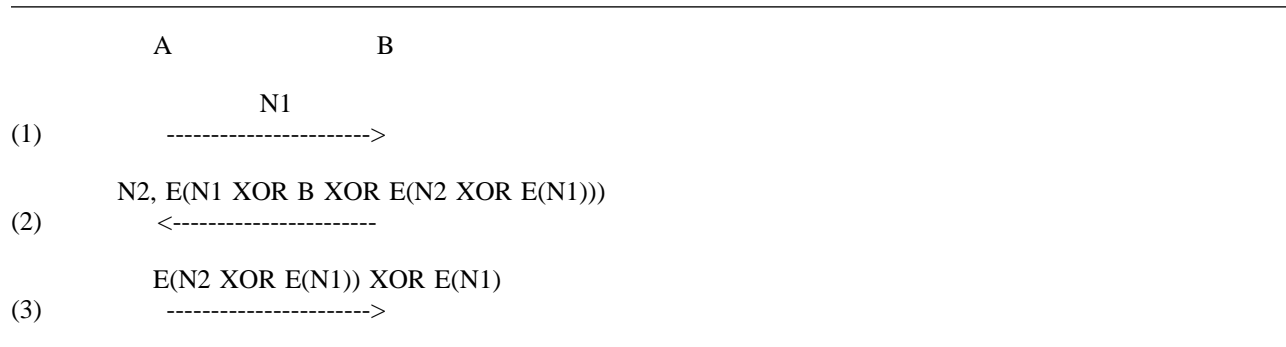


Figure 25. Secure protocol with three encryptions

By adding an extra block encryption operation inside $g()$, and re-using its result by exclusive-oring it with the message of flow (3), one gets a protocol that has the added advantage of resistance to known-plaintext attacks. This is depicted in Figure 25 That protocol is otherwise also secure against all the usual attacks because its function $g()$ is the exclusive-or of $N2$ with $E(N1)$, and since $E(N1)$ does not appear anywhere in cleartext, an intruder can never obtain or derive $g()$ from past observations, and thus can never solve the equation $g()=g'()$. A protocol very close to this one was even shown secure in a broader sense in [Bird91].

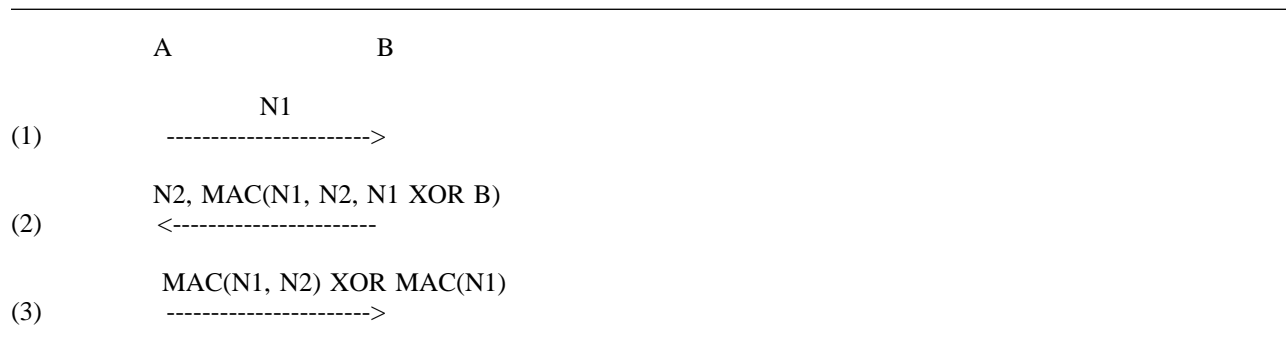


Figure 26. Secure protocol with three MAC operations (three encryptions)

The above protocol can of course be expressed in terms of MAC operations rather than encryption operations to underline its exportability, as represented in Figure 26.

Example With Four Encryptions

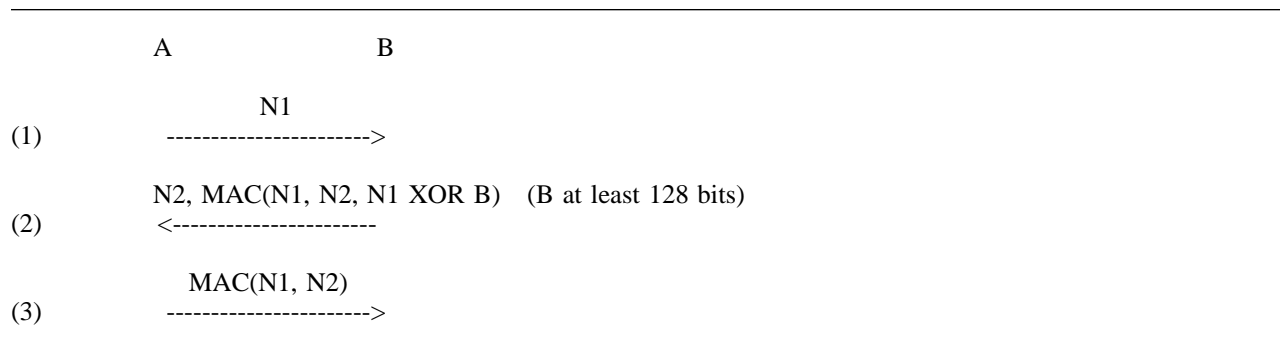


Figure 27. Secure protocol with two MAC operations (four encryptions)

By a similar minor extension, one can easily produce a protocol suited for environments where hardware support for MAC computations is available and the cost of invoking that hardware is more important than the cost of an individual block operation: this protocol uses at least six encryption operations (only four if optimized to re-use two) but only two invocations to the MAC hardware, as depicted in -- Fig 'MAC4' unknown -- Four of the encryption operations come from the operations on N1 and N2 while the remaining two (or more) come from operations on the expression (N1 XOR B). The XOR in this expression denotes an operation whereby the nonce N1 is XOR'ed repeatedly with each successive cleartext block in the name B to add randomness to that name between different executions of the protocol. The name B must be padded to at least two cryptographic blocks to protect flow (2) against known-plaintext attacks that would otherwise be possible. The protocol is then as secure as the previous one and for the same reason that g'() cannot be obtained by any intruder.

4. Conclusion

We first described a few examples of interleaving attacks on simple two-way authentication protocols to derive a set of security criteria that protocols should meet to resist such attacks. Based on these examples, we suggested that the design of such protocols is not a trivial exercise. Thus we set out to derive intuitively as simple as possible a canonical form for two-way authentication protocols that were tested against interleaving attacks, yet are simple enough to be usable within the lower layers of a networking architecture. We gave several practical and elegant examples of such realizable protocols.

From the last of these examples, one might sweepingly conclude that plain MAC operations on sufficiently large numbers of authentication parameters such as nonces and names of involved parties meet all requirements. Admittedly, this conclusion is no real surprise and may sound intuitive. The interest of the design methodology, the canonical protocol and the test of security we have developed is however three-fold:

1. The methodology we used has shown that while using MAC operations should work intuitively, the choice and order of the arguments to these operations cannot be arbitrary. There are certain requirements for asymmetry and variety. Many protocols in use today are so complex that they probably meet these asymmetry and variety requirements, but at the cost of many unnecessary and expensive cryptographic operations. On the other hand, several of today's simplest protocols are actually too simple, do not meet the asymmetry and variety requirements and thus do not resist certain attacks. Thus we have put a lower bound on the number and the form of terms that a MAC-based authentication protocol must contain to be secure.
2. The canonical form we have developed covers far more than just DES MAC-based protocols. It clearly suggests that there is a wealth of other possible functions and protocols to achieve secure two-way authentication. Specifically, there is no requirement to use any cryptographic function at all. Any simple one-way function would do [Gong89]. For instance, one could use an MD4 function [Rivest90], suitably seeded with a secret prefix to implement the MAC functions of the canonical form.

3. Finally, the kind of security test that we provided on the canonical protocol has never been made before for any existing protocol we are aware of.

The canonical two-way authentication protocol described in this paper actually forms the basis for a family of modular and parametrized security protocols offering such functions as key distribution, single network sign-on, password management, and related security services in a distributed environment. The entire family benefits from the test of security provided with the basic authentication protocol. All protocols allows optional use of time-stamps instead of nonces, require minimal overhead and minimal-size tokens (tickets and authenticators), are amenable to use for securing network mechanisms at any architectural layer, and rely strictly on exportable data integrity mechanisms such as one-way functions rather than on confidentiality mechanisms. A prototype implementation of the protocol family using DES MAC technology has been implemented on AIX, IBM's Unix product [Molva92]. It is available both in TCP/IP and SNA environments. Further details on the entire protocol family will be documented in a later publication.

Bibliography

- Abadi91** M.Abadi, M.Tuttle, "A semantics for a logic of authentication", Proc. ACM Symp. on Princ. of Distr. Comp. (1991) 201-216.
- Bauer83** R. K. Bauer, et al., "A key distribution protocol using event markers," ACM TOCS 1 3 (1983) 249-255.
- Bellovin90** S.M.Bellovin, M.Merritt, "Limitations of the Kerberos authentication system", ACM CCR 20 5 (Oct.90) 119-132.
- Biham90** E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Crypto-systems", Proc. Crypto'90 (Jun.90).
- Bird91** R. Bird, et al., "Systematic design of two-party authentication protocols," Proc. Crypto 91, Santa Barbara, CA (Aug.91) 44-61, available as "Advances in Cryptology", J. Feigenbaum (Ed.), Lecture Notes in Comp. Sc. 576, Springer Verlag (1991).
- Burrows89** M. Burrows, et al., "A logic of authentication", Proc. 12th ACM SOSOP, ACM OSR 23 5 (Dec.89) 1-13.
- Cheng90** P-C.Cheng, V.D.Gligor, "On the formal specification and verification of a multi-party session protocol", Proc. IEEE Symp. on Res. in Sec. and Priv., Oakland, CA (May 90) 216-233.
- Denning81** D. E. Denning, G. M. Sacco, "Timestamps in key distribution systems", CACM 24 8 (Aug.81) 533-536.
- DES77** "Data Encryption Standard", FIPS 46, NBS (Jan.77).
- Gong89** L.Gong, "Using one-way functions for authentication", ACM CCR 19 5 (Oct.89) 8-11.
- Gong90** L. Gong, R. Needham, R. Yahalom, "Reasoning about Belief in Cryptographic Protocols", Proc. IEEE Symp. on Res. in Sec. and Priv., Oakland, CA (May 90) 234-248.
- Ianson90** C.I'Anson, C.Mitchell, "Security defects in CCITT Recommendation X.509 - The Directory Authentication Framework", ACM CR 20 2 (Apr.90) 30-34.
- ISOSC27** "Entity Authentication Using Symmetric Techniques", ISO-IEC JTC1.27.02.2(20.03.1.2) (Jun.90).
- ISO8732** "Banking - Key management (wholesale)" ISO 8732, Geneva (1988).
- ISO9594** "OSI Directory - Part 8: Authentication Framework", ISO 9594-8, Geneva (1988).
- Molva92** R. Molva, G. Tsudik, E. Van Herreweghen, S. Zatti, "KryptoKnight authentication and key distribution system," submitted to ESORICS 92, Toulouse, France (23-25 Nov.92).
- Morris79** R.Morris, K.Thompson, "Password security: a case history," CACM 22 11 (1979) 594-597.
- Needham78** R. M. Needham, M. D. Schroeder, "Using encryption for authentication in large networks of computers," CACM 21 12 (1978) 993-998.
- Otway87** D. Otway, O. Rees, "Efficient and timely mutual authentication", ACM OSR 21 1 (Jan.87) 8-10.
- RSA83** R. L. Rivest, et al., "A method for obtaining digital signatures and public-key cryptosystems," CACM 21 2 (1978) 120-126 & CACM 26 1 (1983) 96-99.
- Rivest90** R. Rivest, "The MD4 Message Digest Algorithm (Version 2/17/90, Revised)", ISO/IEC JTC1/SC 27/WG20.2 N193 (Apr.90).
- Spafford89** E.H.Spafford, "The Internet worm program", ACM CCR 19 1 (Jan.89) 17-57.
- Steiner88** J. G. Steiner, et al., "Kerberos: an authentication server for open network systems", Proc. Usenix Conf. (Winter 88).
- Stubblebine92** S.G.Stubblebine, V.D.Gligor, "On message integrity in cryptographic protocols", to appear in Proc. IEEE Symp. on Res. in Sec. & Priv., Oakland, CA (May 92).

Figures

<u>id</u>	<u>File</u>	<u>Page</u>	<u>References</u>
OWAA	2PP SCRIPT	4	1
OWAB	2PP SCRIPT	4	4, 5
TWA4	2PP SCRIPT	5	5
TWA3	2PP SCRIPT	5	3
ORACLE	2PP SCRIPT	6	5
ISO	2PP SCRIPT	7	5, 9
PARALL	2PP SCRIPT	7	6
TWAX	2PP SCRIPT	8	7
OFFSET	2PP SCRIPT	8	7
CAN1	2PP SCRIPT	11	8
CAN2	2PP SCRIPT	12	9
CAN3	2PP SCRIPT	12	9
CAN4	2PP SCRIPT	13	10
CANON	2PP SCRIPT	14	11
CANXOR3	2PP SCRIPT	14	12
CANMAC3	2PP SCRIPT	15	12
CANXOR4	2PP SCRIPT	15	12, 12
CANMAC4	2PP SCRIPT	16	13
REFAB	2PP SCRIPT	17	13, 14
REFXB	2PP SCRIPT	17	14
REFXA	2PP SCRIPT	17	14

IBM

		17	21	
				17
ATKAX	2PP SCRIPT	18	22	
				18
ATKXB	2PP SCRIPT	18	23	
				18
ENC2	2PP SCRIPT	20	24	
				20
ENC3	2PP SCRIPT	21	25	
				21
MAC3	2PP SCRIPT	21	26	
				21
ENC4	2PP SCRIPT	22	27	
MAC4	?	?	?	
				22

Footnotes

<u>id</u>	<u>File</u>	<u>Page</u>	<u>References</u>
RTP	2PP SCRIPT	1	1
			1
WRC	2PP SCRIPT	1	2
			1, 1, 1, 1
ZRL	2PP SCRIPT	1	3
			1, 1

Revisions

<u>id</u>	<u>File</u>	<u>Page</u>	<u>References</u>
1	2PP SCRIPT	i	9, 9, 9, 9, 9, 10, 10, 10, 14, 14, 16, 16, 18, 18, 22, 22, 23, 23

Processing Options

Runtime values:

Document fileid	2PP SCRIPT
Document type	GDOC
Document style	DEFAULT
Profile	EDFPRF30
Service Level	0000
SCRIPT/VS Release	3.2.1
Date	92.09.04
Time	14:09:25
Device	PSA
Number of Passes	2
Index	NO

Formatting values used:

Annotation	NO
Cross reference listing	YES
Cross reference head prefix only	NO
Dialog	LABEL
Duplex	YES
DVCF conditions file	(none)
DVCF value 1	(none)
DVCF value 2	(none)
DVCF value 3	(none)
DVCF value 4	(none)
DVCF value 5	(none)
DVCF value 6	(none)
DVCF value 7	(none)
DVCF value 8	(none)
DVCF value 9	(none)
Explode	NO
Figure list on new page	YES
Figure/table number separation	YES
Folio-by-chapter	NO
Head 0 body text	(none)
Head 1 body text	(none)
Head 1 appendix text	Appendix
Hyphenation	YES
Justification	NO
Language	ENGL
Layout	1
Leader dots	NO
Master index	(none)
Partial TOC (maximum level)	4
Partial TOC (new page after)	INLINE
Print example id's	NO
Print cross reference page numbers	YES
Process value	(none)
Punctuation move characters	,
Read cross-reference file	(none)
Running heading/footer rule	NONE
Show index entries	NO
Table of Contents (maximum level)	3
Table list on new page	YES
Title page (draft) alignment	RIGHT
Write cross-reference file	(none)

DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
+++EDF078W Unable to start headfont HELVETICA. (Page 0 File: 2PP SCRIPT)
DSMMOM397I '.EDF#INIT' WAS IMBEDDED AT LINE 310 OF '.EDF#MAIN'
DSMMOM397I '.EDF#MAIN' WAS IMBEDDED AT LINE 179 OF 'EDFPRF30'
DSMMOM397I 'EDFPRF30' WAS IMBEDDED AT LINE 0 OF '2PP'
+++EDF089E Font 'ISIL GOTHIC' required. (Page 0 File: 2PP SCRIPT)
DSMMOM397I '.EDF#FTPS' WAS IMBEDDED AT LINE 1260 OF '.EDF#INIT'
DSMMOM397I '.EDF#INIT' WAS IMBEDDED AT LINE 310 OF '.EDF#MAIN'
DSMMOM397I '.EDF#MAIN' WAS IMBEDDED AT LINE 179 OF 'EDFPRF30'
DSMMOM397I 'EDFPRF30' WAS IMBEDDED AT LINE 0 OF '2PP'
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
+++EDF078W Unable to start headfont HELVETICA. (Page 0 File: 2PP SCRIPT)
DSMMOM397I '.EDF#INIT' WAS IMBEDDED AT LINE 310 OF '.EDF#MAIN'
DSMMOM397I '.EDF#MAIN' WAS IMBEDDED AT LINE 200 OF 'EDFDITYP'
DSMMOM397I 'EDFDITYP' WAS IMBEDDED AT LINE 2 OF '2PP'
+++EDF089E Font 'ISIL GOTHIC' required. (Page 0 File: 2PP SCRIPT)
DSMMOM397I '.EDF#FTPS' WAS IMBEDDED AT LINE 1260 OF '.EDF#INIT'
DSMMOM397I '.EDF#INIT' WAS IMBEDDED AT LINE 310 OF '.EDF#MAIN'
DSMMOM397I '.EDF#MAIN' WAS IMBEDDED AT LINE 200 OF 'EDFDITYP'
DSMMOM397I 'EDFDITYP' WAS IMBEDDED AT LINE 2 OF '2PP'
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMLNB724W UNABLE TO START FONT '@IBML12' FOR .DV.
DSMMOM395I '.EDF#TIPG' LINE 600: &@sec
DSMMOM397I '.EDF#TIPG' WAS IMBEDDED AT LINE 24 OF '2PP'
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMLNB724W UNABLE TO START FONT '@IBML12' FOR .DV.
DSMMOM395I '(RHEVEN)' LINE 320: &*sec
DSMMOM397I '(RHEVEN)' WAS IMBEDDED AT LINE 70 OF '.EDF#DUPL'
DSMMOM397I '.EDF#DUPL' WAS IMBEDDED AT LINE 70 OF 'EDFBODY'
DSMMOM397I 'EDFBODY' WAS IMBEDDED AT LINE 26 OF '2PP'
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMKDF478E INVALID FONT SPECIFIED WITH .BF.
DSMMOM395I '2PP' LINE 27: .bf sss
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.
DSMPEF372E FONT LIBRARY MEMBER 'EDFC0395' NOT FOUND.

