



Atalla key block

making triple-DES
truly secure

a white paper
from hp

combining key management with triple-DES to maximize security

contents

- DES is broken
- Triple-DES is secure
- Key management vulnerability
- How Triple-DES can be attacked
- The Atalla Key Block
- Conclusion

For the last two decades, cryptographic protection of keys and data in financial networks has been provided by the Data Encryption Standard (DES) encryption algorithm. Single-length DES has been shown to be vulnerable to an exhaustive key search attack in as little as 22 hours. The finance industry is moving to the Triple-DES algorithm for its presumed increased security. The DES algorithm itself remains secure, but requires the longer key length of Triple-DES to adequately secure banking assets. The security of the DES environment is compounded by legacy single-length DES systems coexisting with Triple-DES implementations.

In order to realize the increased security potential of Triple-DES, key management will need to assume primary importance. Standards-based Triple-DES key storage and key exchange are being implemented insecurely today. Perhaps surprising to many, such implementations are only slightly more secure than single-length DES. HP's Atalla Security Products Group has documented several attacks that revealed stored Triple-DES keys with significantly less effort than informed customers find acceptable.

In response, the Atalla Security Products Group has defined the new Atalla Key Block, which is designed to maximize security in a Triple-DES environment.

The Atalla Key Block from HP is flexible and extensible to enable the secure management, storage, and control of all keys used with Atalla banking products. The new Atalla Key Block is both simple and easy to implement, and the Atalla Security Products Group also provides tools for customers to migrate easily to the secure Atalla Key Block.

Atalla Security Products Group recommends that customers consider all facets of implementing Triple-DES security: operational usage, key management, key storage, and key exchange. The Atalla Key Block provides true Triple-DES-strength security in all

cases. But Triple-DES is not the last new algorithm in sight. The Atalla Key Block provides ease of use and extensibility for future needs such as the Advanced Encryption Standard (AES). Atalla Security Products Group recommends that customers start planning migration to the Atalla Key Block to accrue the benefits of full Triple-DES security.

DES is broken

key exhaustion attack breaks single-length DES encryption

The bank payments network links thousands of financial institutions to automated teller machines (ATM) and point-of-sale (POS) devices worldwide. It is estimated that between US\$2 and US\$8 trillion are securely transferred through this network daily. These transfers can occur only if the network is secure and trusted by banks and customers alike. A lynchpin to this public trust has been the DES, a bulk encryption algorithm developed in the early 1970s by IBM and adopted by the U.S. government in 1977. Over the past two decades, the Atalla Security Products Group has provided most of the hardware security modules (HSMs) protecting the DES algorithm and related keys that secure an end user's personal identification number (PIN). Atalla Security Products Group, in tandem with financial institutions and many different host vendors and application providers, has created the most trusted commercial network in the world.

The DES algorithm, or single-length DES, as specified by ANSI, National Institute of Standards and Technology (NIST), International Standards Organization (ISO), and other standards bodies, has served the industry well for many years. The algorithm remains secure, even though it is in the public domain. There are no shortcuts to break the DES algorithm. The key exhaustion attack, in which an attacker continually tries all possible key values, is the only known way to break DES. Figure 1 illustrates single-length DES. If you are attempting to break DES and you know the plain text data and the cipher text data, then you would test for the unknown key, or KS. The strength of DES encryption is measured by the amount of effort required to find a DES key. A single-length DES key has 56 bits. That means that two to the 56th key values would need to be tried in an exhaustive search of all possible key values in order for the correct one to be found. The strength of DES security, then, resides in the length of the DES key. Until recently, a 56-bit DES key was perceived as sufficient to secure the bank payments network.

Constant advances in computer technology, however, make single-length DES vulnerable to a key exhaustion attack. In January 1999, the Electronic Frontier Foundation (EFF) demonstrated that a motivated adversary with a specially designed computer connected to thousands of PCs via the Internet could break single-length DES in as little as 22 hours. Thus, the work effort to break a 56-bit DES key can be said to take 22 hours. The trade press made much of this event, but industry changes take time. This "DES cracker" is commercially available on the Web today for less than US\$200,000. Improvements in processor speed will continue to decrease the time, money, and effort required for an exhaustive key search of single-length DES. An algorithm to replace single-length DES is needed, or ATM and POS systems that rely on the security of the DES algorithm will remain perilously vulnerable.

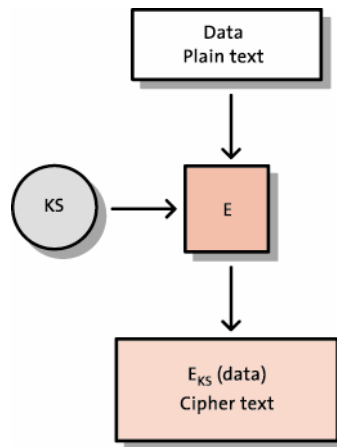


Figure 1. Single-length DES.

triple-DES is secure

operationally, longer keys mean more security

Although faced with the prospect of a vulnerable DES-based system, the financial industry knew the DES algorithm itself had proved to be strong. A ready alternative was the Triple-DES algorithm. Triple-DES is an extension of the DES algorithm but provides longer and therefore stronger keys. Banks have begun to move to Triple-DES because of its similarity and compatibility with DES. They also have a large installed base of DES devices and an already sizeable investment in DES-based applications.

As we shall see, the improvement in operational security from single-length DES to Triple-DES is real.

Triple-DES uses two 56-bit DES keys at different times during separate encrypt, decrypt, and reencrypt operations against a block of data (see figure 2). Use the first key, K_L , or Key Left, to perform a DES encrypt operation on the plain text data, then perform a DES decrypt operation on the result with the second key, K_R , or Key Right. The result of the second process is then DES encrypted using the K_L key again. An alternative is to use a separate 56-bit DES key for each DES operation. In either case, the resulting cryptogram will have been shaken and stirred. Hardware security module vendors, such as Atalla Security Products Group, have been implementing Triple-DES in their products for several years.

Customers who choose Triple-DES assume that the work factor for Triple-DES is at least 2112. Breaking the Triple-DES algorithm requires an exhaustive key search similar to the process of breaking single-length DES described earlier. The work effort involved is not just two times what is required to break single-length DES, but rather 256×256 , or 2112, the number of possible key combinations that must be compared to find the working key. If single-length DES can be broken in 22 hours, then a simple arithmetic extrapolation suggests that Triple-DES will be secure for approximately 2×10^{14} years (more than 200 trillion years). In reality, cryptography experts anticipate that Triple-DES will have at least a 10-year life span. Even a motivated adversary will not break Triple-DES in operation and will look elsewhere to launch a security attack.

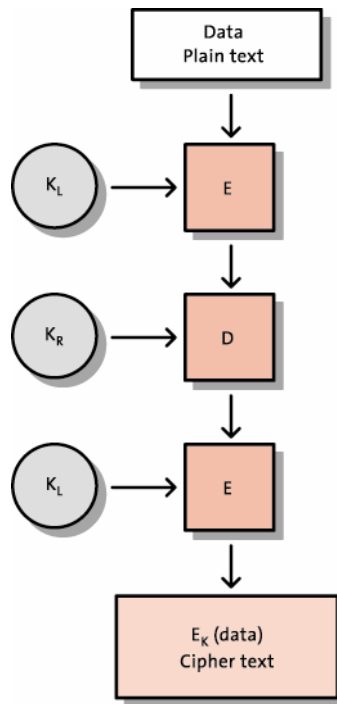


Figure 2. Triple-DES.

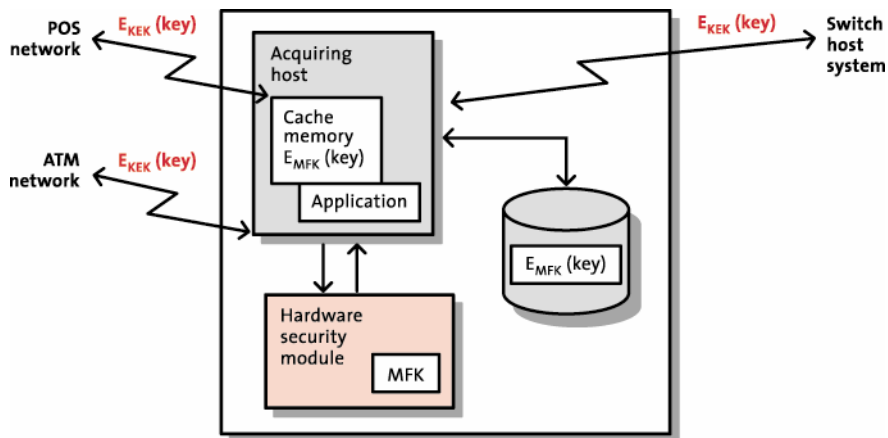


Figure 3. Secure key management is achieved by the host application and HSM working together.

key management vulnerability

stored or transmitted triple-DES keys are no more secure than single-length DES

The emphasis of this paper, and of the industry, has thus far been on the operational use of Triple-DES. If Triple-DES keys are generated, used once, and then discarded, there is no security issue. However, cryptographic keys also reside in two other states: stored in a host's memory or database and transmitted over networks to other systems.

In any case, Triple-DES keys outside an HSM are considered to be in a “hostile” environment and must be managed securely. If Triple-DES key management is implemented suboptimally, then Triple-DES is not substantially more secure than single-length DES.

Where should keys be stored? It may appear most safe to store keys in a physically secure HSM, but this is not practical. An HSM will never have enough key storage capacity for today’s needs. In practical terms, key storage is managed by a host application and the HSM working together (see figure 3). As shown in the figure, keys within the host domain (shown in green) are secure, while those outside the host domain (shown in red), though encrypted, may be less secure in enabling interoperability with other systems. Cryptographic systems store thousands of cryptographic keys for use in a wide variety of algorithms that are applied simultaneously for many different purposes. For example, a typical HSM may simultaneously support RSA signature generation, PIN processing, digital enveloping, and data encryption using DES, Triple-DES, RC4, and many other algorithms. Cryptographic keys must be protected throughout the cryptographic life of the data or process being protected. This life span of the data or process may be many years in the case of PIN protection in a consumer banking environment.

Within the ANSI X9.24 standard, the guideline for key protection is to encrypt the keys when they are in a hostile environment. However, this guideline is inadequate. ANSI X9.24 specifies that Triple-DES keys be encrypted under a Triple-DES key and stored as two DES keys (K_L and K_R), which are stored independently, side by side, in a database. Simply encrypting keys is not sufficient for the control, confidentiality, and integrity of underlying keys. With certain information and casual access to the HSM, an adversary can break up the Triple-DES key block and attack each stored 56-bit DES key independently (see figure 4).

In addition, keys must be shared among HSMs at a host site and transmitted to other systems. Secure key exchange, the transmission of cryptographic keys between disparate systems, has garnered even less attention by standards bodies. One applicable standard, ISO-8583, is really just a messaging standard, not a security standard. Even if they are suboptimal in a security sense, Atalla Security Products Group products must adhere to current interoperability standards. At the same time, Atalla Security Products Group must also provide customers with the ability to secure key management in the domain that they control.

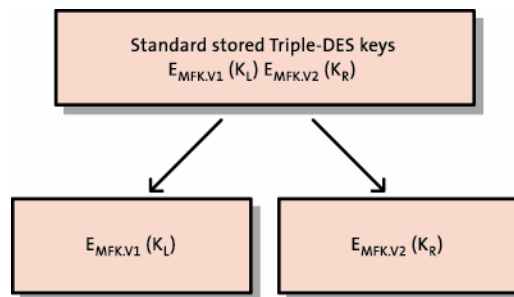


Figure 4. Triple-DES keys stored as independent 56-bit key components can be broken as readily as DES keys.

Note: $E_{MFK.V1}(K_L)$ = left half of key encrypted under master file key with variant 1; $E_{MFK.V2}(K_R)$ = right half of key encrypted under master file key with variant 2.

how triple-DES can be attacked

a generic example

The banking environment is becoming more and more complex. Banks are asking for better efficiencies, new capabilities, and new algorithms, such as RSA public key cryptography. NIST has chosen an AES to replace DES. But even though single-length DES has been shown to be vulnerable, it is still the most widely used cipher today. As financial institutions migrate to Triple-DES, they create networks in which single-length DES and Triple-DES must coexist in the same system. Mixing different key lengths, key types, and algorithms creates the opportunity for new kinds of attacks.

It is commonly understood that internal attacks account for upwards of 80 percent of all bank fraud today. Disgruntled employees, contractors, and vendors may all have the necessary inside information and access to attack stored Triple-DES keys. As we've learned, an adversary will not attack Triple-DES in operation, but rather will modify and manipulate the encrypted 56-bit key components stored outside the HSM.

Figure 5 provides an example of an attack on Triple-DES keys. Let's assume the adversary targets the Triple-DES key, K1, which consists of two single-length DES keys, K1L and K1R. K1L and K1R are encrypted under Triple-DES and stored on the host database as C1 and C2, so together they are C1C2. A second stored Triple-DES key is C3C4.

In an attack, the adversary gets the hardware security module to use part of a Triple-DES key, C1, as a single-length DES key to obtain a plain text/cipher text pair. The person now goes offline to their own facility and performs a 2^{56} search (in just 22 hours) to uncover the key, K1L.

Armed with knowledge of K1L, the adversary attacks another key, K2, by substituting C1, the cryptogram of this known K1L, into the C3 portion of the cryptogram for K2 to create a modified key, C1C4.

The adversary then gets the hardware security module to encrypt some plain text with this modified key. This plain text/cipher text pair, P/C, is then taken offline, and the adversary mounts an exhaustive attack against the key, K. This is only a 2^{56} search to uncover K2R because the adversary already knows K1L.

The work factor to uncover the two parts of a Triple-DES key is thus two times 2^{56} . Another measure of Triple-DES security is 2×22 hours, or only 44 hours. In security terms, this reflects a negligible increase in security from single-length DES to Triple-DES.

On a larger scale, the adversary can continue breaking keys to create a working but illegitimate database of bad keys. The result is that all sensitive information in the host database can be successfully accessed or corrupted. Does this mean that Triple-DES should not be used?

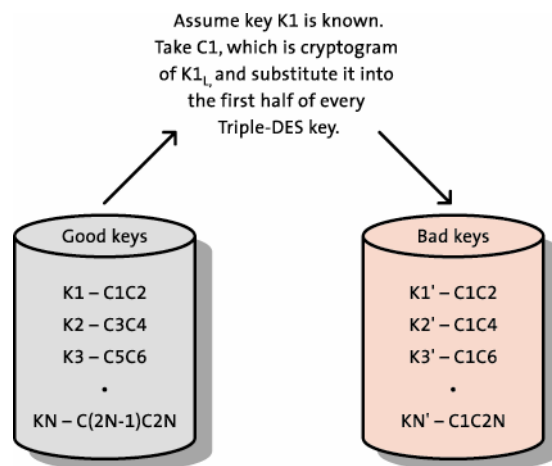


Figure 5. An attack on Triple-DES keys.

the Atalla key block

protects triple-DES keys as well as all others

The basic structure that an HSM uses to achieve secure key management is the key block. A key block is a data structure used to store or exchange cryptographic keys within hostile environments. A bad key block design will leak key information and provides an attractive point of attack for knowledgeable adversaries. However, a good key block design has the following attributes:

- Keys are encrypted using a secure algorithm with an appropriate key size
- Control information allows hardware security modules to determine correct key usage
- A secure mechanism is provided to detect any modification or manipulation of the control information and encrypted keys

Today's single-length DES keys are stored in a database using a Triple-DES key protection key called the master file key (MFK). Similarly, the key that protects keys during transmission is a key exchange key (KEK). A variant mechanism provides control information that determines and enforces correct key usage. Thus, only the first two of the three prime attributes of a secure key block design are met with today's systems.

The example of an attack on Triple-DES keys demonstrates that encrypting keys is a necessary but not altogether sufficient step in protecting stored keys in a changing banking environment. In response, Atalla Security Products Group has defined a key block structure that was designed to maximize security in a Triple-DES environment.

The Atalla Key Block structure is defined to support single-, double-, and triple-length DES keys; public keys; AES keys; and others (see figure 6). The figure depicts an Atalla Key Block consisting of three parts:

- 8-byte clear header containing attributes of the key
- 48-byte key field containing the Triple-DES cipher block chaining (CBC) mode cipher text of the key (the encrypted key field)

- 16-byte Triple-DES message authentication code (MAC) over header and cipher text field

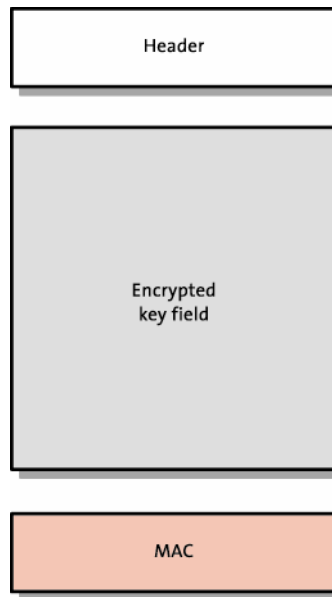


Figure 6. The new Atalla Key Block.

Key attributes such as algorithm and key usage are stored in the clear header. Before a key in the Atalla Key Block format is used in an Atalla HSM, the content of the header block is validated to ensure that the correct usage is enforced. Clear attributes are stored in byte values in fixed positions that allow for easy problem determination.

The key field contains the key data and is Triple-DES encrypted with a specific variant of the master key to protect the key values. A DES key can be generated with a length of 8 bytes, 16 bytes, or 24 bytes. Regardless of the actual key, the encrypted key field is padded to 48 bytes to disguise the existence of weaker, single-length DES keys.

The MAC across both header and key field cryptographically binds them together to prevent any alteration.

The Atalla Key Block structure results in several security benefits, and prevents an attacker from

- Changing any attribute of any key
- Changing any bits of any key
- Using part of a key as an entire key
- Rearranging any part of a key
- Substituting parts of a key into another key
- Identifying weaker keys

These benefits accrue to the use of other algorithms as well as to DES and Triple-DES.

More information on attacking Triple-DES

- Atalla Security Products Group has documented 11 attacks against Triple-DES. There are certainly more instances that remain undocumented.

- The documented attacks apply to all modes of Triple-DES key blocks: electronic code book (ECB), CBC, and output feedback (OFB).
- In ECB mode: Different variants on the key encrypting the left and right halves of a Triple-DES key do not prevent attacks.
- In CBC and OFB modes: Different initialization vectors (IVs) on each key do not prevent attacks.
- All cryptographic devices do not completely solve the problem highlighted by these attacks.

conclusion

summary and recommendations

The Atalla Key Block is a superior solution to the problem of vulnerable Triple-DES security caused by the weak key management prescribed by current standards bodies. At the same time, the new key block is flexible and extensible enough to apply to other algorithms, key lengths, and key types—even to new ones not yet created. For example, it will provide an easy migration path from Triple-DES to the AES.

The Atalla Key Block is simple, easy to understand, and implemented by users without a security background. Atalla Security Products Group also provides tools for users of the existing Atalla key management scheme to migrate easily to the new key block.

Atalla Security Products Group recommends that customers migrate to the Atalla Key Block when they migrate to Triple-DES to ensure they gain all the security benefits intended by a move to Triple-DES. Atalla Security Products Group offers the Atalla Key Block at no charge to users of its hardware security modules.

For more information on the secure Atalla Key Block or to request the Atalla Key Block Migration Guide, contact atallanewsletter@hp.com.

For more information go to www.hp.com/go/nonstop.

July 2002. All product names mentioned herein may be trademarks of their respective companies. HP shall not be liable for technical or editorial errors or omissions contained herein. The information is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A. 02-0390

©2002 Hewlett-Packard Company

