

Re: Combine Secure 3DES Encryption with ability to count occurrence of known plaintext – how to accomodate both aims?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-01/1336.html>

From: David Wagner (daw_at_taverner.cs.berkeley.edu)

Date: 01/20/05

Date: Wed, 19 Jan 2005 23:46:22 +0000 (UTC)

a c wrote:

>The problem I have is the limited capabilities of the HSP. It's designed for
>banking use and HMAC is not part of the capabilities –and we cannot access
>the secret keys either for use with our own application, only Ansi Key Block
>cryptograms which are used as input to encryption and MAC functions (eg:
>3DES CBC).

As Paul Rubin says, you can use 3DES–CBC–MAC instead of SHA1–HMAC.
(I slightly prefer 3DES–OMAC or AES–OMAC, but the difference is unimportant
if the messages you are hashing are of a constant, fixed length.)

>Looking at the response from David Wagner (thanks) this has the advantage
>that it uses standard (for our equipment) crypto operations, but we have to
>update old records (update the velocity checking data with fixed IV after a
>fixed period).

Yes. Most databases should allow you to do this, I would have thought.

>The other issue is the number of transactions processed within 48 hours –
>more than 100,000 which would mean at any one time there would be 100000
>records encrypted in this less than optimum manner.

Yes. At 20 bytes a record, that is 2 MB, not even a penny worth of disk.
At 100,000 encryptions per 2 days, that is 0.5 encryptions per second, which
any HSP should be able to handle trivially. Hard for me to imagine that this
would be a bottleneck, unless I'm missing something.

>i've search, but can't find, a description of A/B switchover. Could I have a
>pointer please.

I have two sets, set A and set B. At the start of odd–numbered days,
I delete everything from set A and re–set it to the empty state. At the
start of even–numbered days, I delete everything from set B and re–set
it to the empty state. When I have a transaction, I add a timestamped

Re: Combine Secure 3DES Encryption with ability to count occurrence of known plaintext – how to accomodate both

ci.crypt: Re: Combine Secure 3DES Encryption with ability to count occurrence of known plaintext – how to accommodate bo

record of that transaction to both set A and set B. At any point, I can retrieve the transactions that have occurred within the past 24 hours by looking in one or the other of these sets (on odd-numbered days, I look in set B; on even-numbered days, I look in set A).

In your application, set A would have a key k_A and an IV iv_A associated with it; set B would have k_B and iv_B . When transaction T occurs, do this:
add (T, $E(k_A, iv_A, CC \#)$, timestamp) to set A, and
add (T, $E(k_B, iv_B, CC \#)$, timestamp) to set B.

When a set S is re-set, delete everything from S, securely delete k_S and iv_S , and pick a new key and IV. To count the number of transactions with a particular credit card number over the past 24 hours, pick the appropriate set to look at, say set S, compute the value $E(k_S, iv_S, CC \#)$, extract all records from set S that have this same ciphertext value and have a timestamp within the past 24 hours, and count.

If you want to count over a 48-hour period, then just double the time scale above.

Note: $E(k, iv, x)$ could be a deterministic encryption algorithm, or it could just be a keyed hash (a PRF) like SHA1-HMAC, 3DES-CBC-MAC, etc. It doesn't really matter, as you never

Re: Combine Secure 3DES Encryption with ability to count occurrence of known plaintext – how to accommodate