Leon S. Scaldeferri

Office of Information Security Research

NSA, R22

9800 Savage Rd.

Ft. Meade MD 20755-6000

(301) - 688 - 0293

Time Bounded Implications

Applied to Secure Services

* Encryption Overview

* Bit/Frame Count Integrity

*Time Delay vs. Buffer Size

*Absolute Time Delay

Leon S.Scaldeferri
FWUF

Encryption Overview[1]

Encryption:

$$P\ [f]\ K = C$$

Decryption:

$$C\ [f^{-1}]\ K = P$$

P = Plaintext Digital Data. e.g. voice, video, FAX, etc.

K = Key

C = Cipher Text

[f] = encrypt function; $[f^{-1}]$ = decrypt function

---

1. ref: G. J. Simmons (ed), "Contemporary Cryptology", IEEE Press, 1992.

Encryption Overview cont.

Stream Cipher: P_n (+) $K_n = C_n$; C_n (+) $K_n = P_n$

n= 1,2,3,.....N bits N= Message Length

(+) = Modular Addition base 2, (symmetric function)

Block Cipher: P_B [f] $K_B = C_B$; C_B [f] $K_B = P_B$

B= Block of bits/Frame; [f] = symmetric function. e.g. DES

Block size of P and K may be different.

PKC: P_B [f] $K_B = C_B$; C_B [f^{-1}] $K_B = P_B$

[f] and [f^{-1}] are non-symmetric functions, e.g. RSA

Given either [f] or [f^{-1}], the other is very difficult to find!

Bit/Frame Count Integrity

* Sync of K_n & C_n necessary in receiver for decryption.

* Loss of bit/block count Integrity will result in loss of crypto-sync.

* C bits/blocks must be received in the order sent.

* Lost/duplicate bits/blocks result in loss of crypto-sync.

* Re-sync's may take many seconds. To be avoided!

* Incorrect C bits/blocks result in incorrect P bits/blocks.

* Bit/block errors are acceptable, handled by upper Layers in ISO model, e.g. frame replay/interpolation.

* MAC must keep Frame count integrity, removing duplicates or adding blanks, to maintain bit/block count integrity in upper Layers.

Time Bounded Services

* Offer/expect data in a periodic/regular manner, e.g voice, FAX.

* Large uncertainties in acceptance/arrival requires large data buffers to smooth out data.

* Data Frames will be offered in a continuous manner without ACK/ NACK.

examples:	frame rate	bits/frame
IS-54 (dig. cell.)	25/sec	318+OverHead
GSM	216/sec	60+**OH**
DECT	100/sec	320+**OH**
QCDMA	50/sec	160+**OH**

OH = error coding + sync bits

Absolute Time Delay

* Interactive services, e.g. conversations, interactive video, require short absolute delays.

* For human interactive events, typically less than 100 msec.

Unnoticeable: < 100 msec

Noticeable: 100 msec < T < 300msec

Objectionable: > 300 msec

* For telecommunication systems.

Transparent: < 5 msec

Possible impact: 5 msec < T <10 msec

Impact design, e.g. echo cancellers: > 10 msec