PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3703 di lunedì 25 gennaio 2016

Che cosa si intende per crittografia leggera

La crittografia leggera viene utilizzata quando esistono vincoli ambientali e di potenza di calcolo o di risorse energetiche, che non permesso un utilizzo di crittografia tradizionale. La serie normativa ISO/IEC 29192. Di Adalberto Biasiotti.

La serie normativa ISO/TC 29192 è una normativa internazionale, articolata in quattro parti, almeno per ora, che specifica le modalità con cui è possibile sviluppare una crittografia cosiddetta leggera, al fine di proteggere la **riservatezza dei dati**, l'autentica, l'identificazione, il non ripudio e lo scambio delle chiavi. La crittografia leggera è particolarmente adatta laddove esistono dei vincoli ambientali, legati ad esempio alla potenza di calcolo disponibile e a requisiti energetici assai impegnativi. I limiti che normalmente si incontrano, per sviluppare la crittografia leggera, che devono essere affrontati da questa serie normativa, possono essere i seguenti:

- la dimensione disponibile sul chip elettronico,
- l'energia disponibile,
- la dimensione della codice dei programmi e la dimensione della RAM,
- la larghezza di banda per la comunicazione dei messaggi,
- il tempo per lo sviluppo dei calcoli appropriati.

Tipici ambienti in cui si trova applicazione è per questo tipo di crittografia sono il contesto delle etichette RFID radio Frequency Identification, smart card, anche in applicazioni senza contatti, sistemi di monitoraggio della carica delle batterie, sistemi applicabili a sensori medicali, applicati su pazienti e via dicendo.
Di seguito offro una illustrazione delle quattro parti normative con gli obiettivi che sono stati soddisfatti dagli sviluppatori.
In particolare, la parte prima fa riferimento alle generalità, la parte seconda alla cifratura a blocchi, la parte terza alla cifratura in stream e la parte quarta ai meccanismi che utilizzano tecniche asimmetriche

ISO/IEC 29192-1:2012(E) Information technology ? Security techniques ? Lightweight cryptography ? Part 1: General
Questa parte della norma stabilisce i requisiti di sicurezza, i requisiti di classificazione e i requisiti di attuazione dei meccanismi che vengono proposti e meglio sviluppati nelle successive parti della norma.
È bene tener presente che la crittografia leggera fornisce un adeguato livello di sicurezza solo nel contesto per il quale essa è stata sviluppata. Ad esempio per una cifratura blocchi, con un blocco di n bits e una dimensione della chiave di k bits, quando si limita l'uso della cifratura a blocchi per cifrare non più di 2n/2 blocchi di testo in chiaro, utilizzando una singola chiave, è evidente che sarà disponibile una sicurezza di k-bit. Il livello di sicurezza diminuisce quando vengono trattati più di 2n/2 blocchi.
È bene sottolineare che vi possono essere delle sovrapposizioni in alcune tecniche di sicurezza tra la serie normativa in questione e serie normative già pubblicate come ad esempio ISO/IEC 18033, ISO/IEC 9798, and ISO/IEC 11770. L'esclusione di un particolare meccanismo non significa che questo meccanismo non sia adatto per la crittografia leggera. I criteri utilizzati per selezionare i meccanismi crittografici specificati nelle successive parti delle norme sono descritti nell'annesso A.
Come di consueto, questa prima norma offre i termini e definizioni che si applicano alle successive parti della serie normativa, oltre a stabilire i requisiti di sicurezza, i requisiti di classificazione dei requisiti di attuazione per tutti i meccanismi di cui si propone di intrusione nelle susseguenti norme.

La norma prende anche in considerazione la cifratura in stream e i meccanismi che utilizzano delle tecniche asimmetriche.

ISO/IEC 29192-2:2012 Information technology ? Security techniques ? Lightweight cryptography
Part 2: Block ciphers
Questa norma specifica illustra la cifratura a blocchi che è adatta per una crittografia leggera, che è stata specialmente sviluppata per essere attuata in contesti vincolati. Abbiamo già visto i requisiti illustrati nella prima parte della norma. Una cifratura a blocchi mappa i blocchi di n bit in corrispondenza di altri blocchi di n bit, utilizzando una chiave di k bit. È importante tenere presente che alcuni degli aspetti di questa norma potrebbero essere coperti da brevetti di specifiche aziende ed è pertanto necessario che chiunque utilizzi questa norma si accerti che possa avere una licenza all'utilizzo di eventuali diritti brevettuali. Il comitato tecnico si è accertato che i titolari dei diritti siano disponibili ad offrire licenza a prezzi competitivi.
Questa parte della norma illustra le due cifrature a blocchi che sono utilizzate per le specifiche applicazioni di crittografia leggera, vale a dire

- PRESENT: un sistema di cifratura blocchi con un blocco delle dimensioni 64 bit e una chiave di 80 o 128 bit,
- CLEFIA: un sistema di cifratura a blocchi con una dimensione del blocco di 128 bit e una dimensione della chiave di 128, 192 256 bit.

ISO/IEC 29192-3:2012 - Information technology ? Security techniques ? Lightweight cryptography ?
Part 3: Stream ciphers
questa terza normativa illustra dei generatori di chiavi particolarmente adatti per la cifratura in estrema leggera, da utilizzare in contesti vincolati. Una cifratura in stream un meccanismo di cifratura che usa un generatore di una serie di chiavi, per generare una serie di chiavi che vengono utilizzate per cifrare un testo in chiaro bit per bit o a blocchi.
È importante tenere presente che alcuni degli aspetti di questa norma potrebbero essere coperti da brevetti di specifiche aziende ed è pertanto necessario che chiunque utilizzi questa norma si accerti che possa avere una licenza all'utilizzo di eventuali diritti brevettuali. Il comitato tecnico si è accertato che i titolari dei diritti siano disponibili ad offrire licenza a prezzi competitivi.
La norma illustra due generatori specifici di chiavi per cifratura in stream, vale a dire:

- Enocoro: una generatore di una flusso di chiavi, di tipo leggero, con una dimensione della chiave variabile tra 80 e 128 bit,
- Trivium: un generatore di un flusso di chiavi con una dimensione della chiave di 80 bit.

ISO/IEC 29192-4:2013(E) Information technology ? Security techniques ? Lightweight cryptography
Part 4: Mechanisms using asymmetric techniques
Questa parte della norma illustra tre meccanismi di cifratura leggeri, basati su crittografia simmetrica. I tre meccanismi hanno funzionalità diversi, diverse infrastrutture di supporto e differenti profili di prestazione.

Il primo meccanismo, costituito da un meccanismo di autentica unilaterale, basato su logaritmi discreti su curve ellittiche, ed è chiamato **crypto GPS**; si tratta di uno schema di identificazione asimmetrico di tipo leggero; nella letteratura che ho scritto criptografica questi schemi sono generalmente descritti come sistemi interattivi di prova di conoscenza. Anche se esistono diversi modelli di questi schemi, le risorse di calcolo che devono essere utilizzate quando si usa cretto GPS sono relativamente basse. Questa è molto importante ed ecco il motivo per cui questo schema e adatto ad una strategia di attuazione che viene spesso illustrata come basata su "coupons", o se preferite tagliandi. Questi sono, in sintesi, i risultati offerti da una elaborazione di modeste impegnati impegno, off line, con il cupo utilizzati ogni qualvolta vengono chiamati in causa dallo schema cretto GPS. Lo schema risultante, il ruolo dell'elemento di convalida basato da uno su un apparato con modeste capacità di elaborazione, come ad esempio una targhetta i VDI, offrendo una soddisfacente compromesso tra sicurezza e prestazioni.

Il secondo meccanismo **ALIKE - authenticated lightweight key exchange** - è invece un meccanismo asimmetrico per l'autentica e lo scambio delle chiavi. È una variante dello schema RSA ed offre un'autentica unilaterale ed una funzionalità aggiuntiva vale a dire uno scambio sicuro delle chiavi. Questo meccanismo offre dei vantaggi attuativi significativi, rispetto a soluzioni simili a simmetriche convenzionali come RSA.

Il terzo meccanismo è uno schema basato sulla firma legata all'identità. In questo schema una soggetto terzo affidabile viene

coinvolto nelle calcolo delle chiavi separate di firma. Questo schema offre notevoli vantaggi attuativi su altri schemi, illustrati nella letteratura crittografica.
È importante tenere presente che alcuni degli aspetti di questa norma potrebbero essere coperti da brevetti di specifiche aziende ed è pertanto necessario che chiunque utilizzi questa norma si accerti che possa avere una licenza all'utilizzo di eventuali diritti brevettuali. Il comitato tecnico si è accertato che i titolari dei diritti siano disponibili ad offrire licenza a prezzi competitivi.

Adalberto Biasiotti
