

La pirateria della televisione a pagamento in Europa: storia, aspetti tecnici e proposte

Gioacchino Candilio

ABSTRACT: In this technical paper, the Author deals with the European pay-tv piracy. The study analyses the phenomenon from a historical and technical point of view and makes some suggestions to oppose it.

SOMMARIO: 1. Televisione a pagamento e pirateria. - 2. Il sistema per l'accesso condizionato. - 3. Breve storia della pirateria. - 4. Le tecniche per la visione abusiva. - 5. I motivi del successo della pirateria. - 6. Proposte per combattere la pirateria.

1. Televisione a pagamento e pirateria

La televisione a pagamento è un servizio ad accesso condizionato che consiste nella visione di programmi televisivi riservata ai soli utenti autorizzati in quanto paganti¹. Attualmente tale servizio viene erogato in due modalità: *pay-tv*, che permette la visione di specifici canali per un determinato periodo di tempo (tipicamente un anno) pagando il relativo abbonamento, e *pay per view*, che permette la visione di un singolo evento (un film, una partita o un concerto) pagando il relativo costo.

La tv a pagamento si avvale di un apposito sistema per l'accesso condizionato (*Conditional Access System, CAS*) che consente la cifratura del segnale audio/video da parte della stazione emittente e la sua decifratura da parte dei soli utenti autorizzati.

Le tv a pagamento sono soggette a continui attacchi crittoanalitici, o di altra natura, che hanno l'obiettivo di mettere in chiaro i programmi per consentirne la visione anche a coloro che non sono autorizzati in quanto non paganti.

Tali azioni non possono essere classificate in alcuna forma di hacking, né di tipo tecnologico, né, tantomeno, ideologico.

Il loro obiettivo non è quello di approfondire la conoscenza tecnica del sistema (hacking tecnologico), né quello di testare la sua forza nei confronti di un attacco (hacking etico) e, né, tantomeno, quello di rendere pubbliche e condivise informazioni o conoscenze riservate a pochi (hacking sociale).

Vanno invece considerate come azioni di cracking con chiari scopi commerciali consistenti nella vendita o nella modifica di sistemi per la ricezione non autorizzata delle tv a pagamento.

¹ L'Autore è Professore a contratto di Informatica presso l'Università di Bari e Foggia.

Le analisi svolte sia da società indipendenti sia dagli stessi operatori del settore risultano discordanti riguardo l'entità del problema, ma presentano tutte un quadro allarmante.

Nel 2003, in Europa (compresa quella dell'Est dove il fenomeno è in rapida crescita), sembra siano stati venduti sistemi per la visione abusiva per la ragguardevole cifra di un miliardo di Euro.

Le società televisive e i vari Stati hanno subito danni per svariati miliardi di Euro per mancati abbonamenti e per mancati introiti fiscali mentre i posti di lavoro persi per mancati investimenti sono stati diverse migliaia.

Analogamente, se non più grave, è la situazione di tutto il continente americano [Law04].

Da più parti si ritiene che un'attività così diffusa sia gestita da una rete internazionale di organizzazioni criminali, di cui fanno parte anche tecnici altamente qualificati e specializzati, che possono così realizzare lauti guadagni generando una pericolosità sociale molto bassa se non nulla. Tutte queste connotazioni hanno finito col rendere comunemente noto il fenomeno come pirateria della tv a pagamento.

In termini più propriamente tecnici, la tassonomia IBM [Abr91] definisce i pirati come attaccanti di classe III, ossia organizzazioni consolidate composte da tecnici con conoscenze specialistiche ma integrabili e con considerevole disponibilità di risorse che sanno analizzare in dettaglio sistemi, usare tecnologie e prodotti avanzati e progettare attacchi molto sofisticati.

La situazione attuale potrebbe divenire ancora più grave con la graduale introduzione della tv digitale terrestre che sta interessando quasi tutti i paesi dell'Europa occidentale e alcuni dell'orientale.

Questa nuova tecnologia, che affiancherà la tv digitale via satellite e via cavo, permetterà la trasmissione di programmi televisivi via etere utilizzando le antenne terrestri già esistenti.

Rispetto alla tv analogica terrestre, il numero di canali aumenterà in maniera considerevole e molti saranno a pagamento.

I Paesi interessati stanno effettuando sperimentazioni a livello nazionale, regionale o urbano, da tempo più o meno considerevole, per poter effettuare il definitivo passaggio dall'analogico al digitale in un arco di tempo molto ampio che va dal 2006 al 2010-2012.

Dopo la città di Berlino, che è stata la prima ad aver completato il passaggio nell'agosto del 2003, l'Italia dovrebbe essere il primo Paese a convertirsi completamente alla nuova tecnologia.

Infatti la Legge 3 maggio 2004, n. 112, recante norme di principio in materia di (ri)assetto del sistema radiotelevisivo, meglio nota come Legge Gasparri [Leg04], prevede che il passaggio debba avvenire entro il 2006.

Mediaset ha già acquisito i diritti per la trasmissione in *pay per view* delle partite interne di alcune squadre di calcio di serie A, a partire dal 2005.

Nei paesi scandinavi, dove la sola Norvegia ha legiferato il passaggio entro il 2007, vengono già offerti alcuni canali a pagamento.

La Gran Bretagna è stata la prima nazione a sperimentare il digitale terrestre ed ha previsto la conversione entro il 2010.

Intanto, dopo il fallimento di ITV, la prima tv digitale terrestre a pagamento europea, è attiva Top Up Tv con un'offerta di una decina di canali tematici a pagamento. In

Francia, le prime tv a pagamento dovrebbero iniziare le trasmissioni nel settembre 2005.

La copertura della tv digitale terrestre è limitata al solo territorio nazionale di ogni singolo Stato al pari di quella via cavo e non all'intera Europa come quella via satellite ma i canali tematici a pagamento potrebbero risultare molto appetibili per la pirateria. Sarebbe opportuno cercare di limitare questo rischio con interventi urgenti di natura culturale, legislativa e tecnica.

2. Il sistema per l'accesso condizionato

La tv digitale europea fa riferimento allo standard *Digital Video Broadcasting* (DVB) [DVB][Ben03] definito dall'*European Broadcasting Union* (EBU) [EBU] tra il 1994 e il 1996 e diffuso dall'*European Telecommunications Standard Institute* (ETSI) [ETSI].

Esso definisce i protocolli della tv digitale via satellite (DVB-S), via cavo (DVB-C) e terrestre (DVB-T) e, parzialmente, anche l'accesso condizionato (DVB-CA package). Il DVB prevede che audio e video dei programmi da trasmettere siano rappresentati e compressi in formato MPEG-2.

La tv a pagamento richiede che la rappresentazione MPEG-2 sia cifrata col sistema *Common Scrambling Algorithm* (CSA) definito dal DVB (DVB-CSA) e costituito da un algoritmo simmetrico che prevede una prima cifratura a blocchi in modalità di concatenamento inverso di 64 bit ed una seconda a flusso di 8 bit.

Il CSA utilizza una chiave, chiamata *ControlWord* (CW), che viene cifrata con un altro sistema simmetrico non standardizzato che utilizza una chiave chiamata *ServiceKey* (SK).

A sua volta, la *ServiceKey* viene cifrata con un ulteriore sistema simmetrico non standardizzato che utilizza una chiave chiamata *UserKey* (UK).

La *ControlWord* viene modificata ogni due secondi e, una volta cifrata, inserita in un segnale di controllo chiamato *Entitlement Control Message* (ECM), la *ServiceKey* viene modificata ogni dieci secondi e, una volta cifrata, inserita in un segnale di controllo chiamato *Entitlement Management Message* (EMM) mentre la *UserKey* viene modificata raramente.

ECM ed EMM, che costituiscono il flusso dati per la decodifica, vengono opportunamente sincronizzati ed inviati col relativo flusso audio/video MPEG-2 cifrato.

Al contrario del CSA, i sistemi di codifica consistenti nella cifratura e gestione delle chiavi, degli abbonamenti in *pay tv* e degli eventi in *pay per view* non sono stati unificati e standardizzati, in quanto ogni operatore ha preferito, per motivi di sicurezza e commerciali, utilizzare il proprio sistema.

I più diffusi sono: Irdeto [Ird], Mediaguard della SECA (chiamato, in genere, Seca) [NagFr], Viaccess [Via], Nagravision [Nag], Conax [Con], Cryptoworks della Philips [Cry] e Videoguard della NDS (chiamato, in genere, Nds) [Nds].

La codifica Seca viene usata quasi esclusivamente dal gruppo francese CanalPlus, proprietario di emittenti in molti Stati europei, e l'Nds soltanto dal gruppo britannico Sky a cui, tra l'altro, appartiene anche Sky Italia.

Il DVB prevede che gli utenti della tv a pagamento possano rimettere in chiaro le chiavi ed il segnale audio/video ricevuti tramite un sistema composto da un ricevitore con decodifica chiamato comunemente decoder (*Integrated Receiver Decoder*, IRD), fornito dall'emittente o acquistato, e da una smart card fornita dall'emittente.

Il decoder deve supportare la codifica dell'emittente di cui si desidera la visione in modo che possa decodificare la *ServiceKey* e la *ControlWord*. Inoltre deve essere in grado effettuare il *descrambling* del flusso MPEG-2 (che poi decomprimerà per ottenere audio e video) con la *ControlWord* decodificata.

Infine deve essere dotato di un lettore (scrittore) di smart card in formato standard ISO 7816 [ISO]. La smart card costituisce il nucleo del sistema di accesso condizionato in quanto la sua EEPROM contiene la *UserKey* e i dati relativi all'abbonamento sottoscritto dall'utente quali, per esempio, i canali visibili e la data di scadenza.

Inoltre possiede un microprocessore in grado di effettuare la decifrazione della *ServiceKey* con la *UserKey* e della *ControlWord* con la *ServiceKey*.

La *ServiceKey* e la *ControlWord* vengono trasmesse alla *smart card* dal suo lettore che, successivamente, riceve la *ControlWord* decifrata dalla smart card e la trasmette al decoder che provvede al *descrambling* del flusso MPEG-2.

La complessa gestione gerarchica delle chiavi definita dal DVB ha una validità molto generale in quanto, non costituendo standard, viene adattata da ogni sistema di codifica in funzione della propria strategia di gestione.

Le variazioni più comuni riguardano la frequenza con cui viene generata una nuova *ControlWord* e il relativo ECM e una nuova *ServiceKey* e il relativo EMM.

Gli ECM hanno una frequenza molto alta e vengono generati all'incirca ogni dieci secondi mentre gli EMM molto bassa e vengono generati sporadicamente con frequenza oscillante fra uno e trenta giorni.

Considerato che i sistemi di codifica sono diversi e l'acquisto di un decoder con codifica integrata potrebbe risultare vincolante per l'utente, il DVB ha definito *simulcrypt* e *multicrypt*.

La prima tecnica prevede la contemporanea cifratura delle chiavi con codifiche diverse; l'altra prevede l'adozione dello standard *Common Interface* (DVB-CI) in cui il decoder è dotato di uno o più slot PCMCIA dove inserire i *Conditional Access Module* (CAM) che supportano i vari sistemi di codifica e dispongono di uno slot per l'inserimento della smart card.

3. Breve storia della pirateria

La prima società europea ad offrire un pacchetto di canali (*bouquet*) a pagamento fu la britannica Sky Tv nel 1990 (negli Stati Uniti il primo *bouquet* fu proposto da Hbo nel 1986 con codifica VideoCipher violata dopo soli sei mesi).

Le trasmissioni avvenivano via satellite in analogico e, sebbene riservate alla sola Gran Bretagna, erano ricevibili in quasi tutta l'Europa.

La codifica veniva effettuata col Videocrypt, un sistema ibrido in cui lo *scrambling* (del solo video in quanto Sky preferiva lasciare l'audio in chiaro) veniva effettuato con la tecnica analogica del taglio e rotazione (ogni linea dell'immagine viene tagliata in due

parti che vengono ruotate e scambiate; la divisione avviene in un punto casuale diverso per ciascuna linea) mentre la generazione, codifica e gestione delle relative chiavi con tecniche digitali [Coh91].

Nel 1994, il tedesco Markus Kuhn [Kuhn], un giovane informatico esperto di sistemi per l'accesso condizionato, riuscì a mettere in chiaro l'intero bouquet in vari modi: operando sull'algoritmo di scrambling senza l'ausilio delle chiavi (in questo caso l'immagine veniva visualizzata solo in bianco e nero), con una smart card "clonata" che emulava perfettamente quella originale e, infine, sostituendo la smart card con un PC dotato di apposito software e collegato al decoder [Videoc]. Kuhn diffuse i risultati della sua ricerca attraverso le BBS ed Internet ed il fenomeno della visione abusiva cominciò a prendere piede in tutta l'Europa occidentale (si consideri che l'abbonamento poteva essere sottoscritto solo da residenti in Gran Bretagna in quanto i diritti televisivi acquisiti da Sky erano limitati a quell'area geografica). Sky sostituì la card serie 08, ormai violata, con la 09 ma senza alcun successo.

Le conoscenze tecniche diffuse da Kuhn stimolarono la creazione di diversi gruppi di studio delle codifiche delle tv a pagamento via satellite che operavano in stretto contatto scambiandosi i risultati delle loro ricerche.

La sinergia portò alla forzatura del sistema D2-MAC/Eurocrypt [Eur92][Len91], utilizzato dall'operatore scandinavo Viasat e dal francese CanalPlus, nonostante cifrasse le chiavi col DES [NBS77].

Analoga sorte toccava alla codifica Nagravision [Kud94] [Kuh98] utilizzata dalla tedesca Premiere e da alcuni canali spagnoli.

Nel 1995 Sky introdusse la serie 10 apportando notevoli modifiche alla generazione, codifica e gestione delle chiavi e riuscì a mettere fuori gioco tutti i crittoanalisti; anche la successiva e ultima serie, la 11, resistette ai vari tentativi di forzatura.

Nel 1996 cominciarono le trasmissioni digitali via satellite con il conseguente progressivo abbandono della tecnica analogica.

La prima società europea ad offrire un bouquet digitale a pagamento via satellite fu la francese Canal Satellite Numérique (CSN) del gruppo CanalPlus nel 1996.

Le trasmissioni venivano codificate col sistema Mediaguard realizzato dalla società SECA, appartenente allo stesso gruppo, riprendendo alcuni concetti del D2-MAC/Eurocrypt.

Seguirono, subito dopo, l'italiana D+ e la tedesca DF1 che codificavano le trasmissioni col sistema Irdeto.

Successivamente vennero introdotte la codifica Viaccess dal gruppo francese ABSat, la Conax dal gruppo scandinavo Canal Digital, la Nds dal gruppo britannico Sky ed, infine, nel settembre del 1997, la Nagravision dal gruppo spagnolo Via Digital.

Nel 1998, dopo soli due anni dall'avvento della tv digitale a pagamento, la pirateria era già in grado di forzare tutte le codifiche, come peraltro ampiamente previsto [McC96].

La prima a cedere è stata Irdeto, seguita nell'ordine da Seca, Viaccess e Nagravision.

Questi sistemi sono stati irrimediabilmente compromessi e, nel 2002, le società che li hanno realizzati hanno introdotto una seconda versione che ha richiesto il cambio di smart card.

In particolare, Nagravision2, chiamato Aladin, è basato su IDEA [Lai90], uno dei più forti cifrari simmetrici esistenti. Nel 2003, Seca2 è stato parzialmente ma

costantemente forzato mentre Irdeto2 e Viaccess2 lo sono stati solo sporadicamente e per brevi periodi.

La situazione attuale vede compromessi Seca2 per quanto riguarda i bouquet italiani e spagnoli e Conax per il bouquet scandinavo. Irdeto2, Viaccess2 e Nagravision2 non sembrano attualmente soggetti a forzature ma l'unico sistema ancora completamente integro è Nds, sebbene in America sia stato aperto (va considerato che l'Nds americano sembra essere meno forte rispetto a quello europeo) [Law04].

4. Le tecniche per la visione abusiva

Come abbiamo già detto nei precedenti paragrafi, gli attacchi alle tv a pagamento sono spesso coronati da successo e, cosa ancora più grave, i risultati possono essere facilmente riprodotti dal punto di vista tecnico e resi immediatamente disponibili anche a persone senza alcuna preparazione ed esperienza specifica.

La tecnica più comune per accedere abusivamente alle tv a pagamento è quella di "clonare" la smart card.

In realtà, essa non viene riprodotta in tutte le sue caratteristiche, sia per le difficoltà tecniche sia per i costi delle apparecchiature necessarie ad effettuare il reverse engineering.

Viene invece realizzata una smart card, chiamata trick card, con architettura hardware (processore e memorie) diversa da quella originaria ma in grado di emularla in quasi tutte le sue funzioni.

Sulla trick card vengono caricati il sistema operativo per la sua gestione, il software di emulazione della codifica e le *ServiceKey* in chiaro.

Sono state sviluppate anche trick card capaci di autoaggiornare le chiavi, periodicamente modificate dalle televisioni, o in grado di resistere agli *Electronic Counter Measure* (ECM), comandi inviati dalle emittenti nel tentativo di metterle fuori uso e consistenti in un cambio di chiavi imprevisto o nella cancellazione della EEPROM.

A volte, gli ECM vengono resi inefficaci grazie a un *blocker*, un dispositivo che si interpone tra la card e il suo lettore.

Le operazioni di scrittura del software e delle chiavi sulle trick card vengono effettuate mediante dei semplici dispositivi elettronici chiamati "programmatori", collegabili alle porte di un PC e gestibili con software in ambiente grafico di semplice ed immediato utilizzo.

Trick card (senza alcun software ad eccezione del sistema operativo) e relativi programmatori vengono legalmente venduti a prezzi irrisori nei negozi di elettronica mentre software per la programmazione, file e chiavi sono facilmente ma illegalmente reperibili su Internet.

Un'altra tecnica ampiamente sperimentata ma non generalizzabile è costituita dalla modifica dei decoder.

Le modifiche dell'hardware, per quanto efficaci, non sono molto diffuse perché sono complesse e possono essere effettuate solo da esperti, mentre le modifiche del software sono molto semplici e possono essere effettuate anche da persone con scarse conoscenze.

In genere, viene sostituito il firmware originale del decoder in modo da trasformarlo da monocodifica a multicodifica o, come si dice in gergo, allcam.

Ad esempio, un decoder con codifica Irdeto integrata sarà in grado di gestire anche le codifiche Seca, Viaccess e Nagravision.

Il firmware può anche essere integrato con altri software, detti in genere “emulatori”, in grado di aumentare ulteriormente il numero di codifiche o di bouquet rimessi in chiaro.

Il caricamento del firmware o di altri software sul decoder viene effettuata con un PC dotato di un semplice programma in ambiente grafico fornito a corredo del decoder stesso.

Con analoghe modifiche hardware e software è possibile trasformare CAM, in genere Irdeto, in allcam chiamati freecam.

Le difficoltà tecniche di tali interventi sono state completamente superate dall'introduzione ufficiale sul mercato di CAM allcam in cui il firmware può essere modificato con un semplice programmatore collegato ad un PC e gestito da un software con interfaccia grafica.

Gli allcam stanno avendo un enorme successo commerciale (attualmente sono disponibili una decina di questo tipo di CAM) e i più evoluti possono memorizzare nella propria EEPROM sia un emulatore che le chiavi rendendo addirittura inutile l'uso della trick card.

Va rilevato che, in genere, questi CAM non vengono venduti con alcuna codifica a bordo in quanto il produttore non ne possiede i diritti e il firmware per trasformarli in allcam viene prodotto da terze parti indipendenti.

L'ultima frontiera relativa agli allcam è costituita da un programmatore universale in grado non solo di programmare vari tipi di CAM ma di trasformare un CAM di un tipo in un altro più potente in quanto dotato di un maggior numero di funzioni, anche inerenti la decodifica.

Naturalmente la disponibilità di ricevitori e CAM allcam, ha portato allo sviluppo di trick card multicodifica (x in 1).

Attualmente è molto diffusa la 6 in 1, una sola trick card è in grado decodificare ben sei codifiche diverse.

Stravolgendone completamente la filosofia, anche l'Open Source è divenuto uno strumento, peraltro elitario, della pirateria.

Sono in commercio decoder con sistema operativo Linux che, oltre a consentire modifica del firmware, allcam, emulatori e memorizzazione delle chiavi, permettono anche di modificare, aggiornare, estendere le funzioni del sistema operativo e di sviluppare software di decodifica in maniera relativamente semplice.

Questi programmi possono poi risiedere sull'hard disk del decoder, senza alcun problema di memoria, ed essere eseguiti quando servono.

Alcune di queste macchine sono anche dotate di scheda di rete e possono essere collegate ad Internet; sfruttando questa possibilità, è stato sviluppato un programma che permette l'aggiornamento automatico delle chiavi prelevate da appositi siti.

Naturalmente questi ricevitori vengono venduti con software assolutamente “innocuo” ma, anche in questo caso, è possibile reperire facilmente su Internet, firmware, add-on e software vari che li trasformano in potenti sistemi per la visione abusiva.

Un discorso del tutto analogo può essere fatto per le schede di ricezione della tv via satellite su PC. La differenza sostanziale, rispetto a un decoder, sta nella maggiore potenza di calcolo di un PC che permette di aumentare notevolmente la capacità di decrittazione.

Inoltre è possibile utilizzare una scheda che non preveda il *descrambling* in quanto questa funzione può essere eseguita dal PC.

Un'ultima tecnica, anche se di livello molto basso in quanto estranea alla crittoanalisi, è la riattivazione di smart card scadute o sostituite, o la maggiorazione dell'abbonamento su smart card attive (per esempio, da base a full).

In questo caso, vanno individuate le locazioni di memoria della EEPROM della smart card in cui si trovano le informazioni relative al numero di card e alla data di scadenza o al tipo di abbonamento e sostituite con un numero e una data validi o con un altro tipo di abbonamento.

La card va generalmente usata in combinazione con un *blocker* per evitare eventuali disattivazioni da parte dell'emittente.

Al contrario di tutte le altre sinora descritte, questa tecnica è piuttosto complessa e può essere messa in atto solo da specialisti.

5. I motivi del successo della pirateria

La storia della crittologia insegna che si susseguono periodi (anche interi secoli) in cui hanno la meglio i crittografi o coloro che vogliono mantenere un segreto e altri in cui prevalgono i crittoanalisti o coloro che vogliono svelare un segreto.

La crittologia moderna, dall'introduzione del DES, avvenuta nel 1977, ad oggi, ha visto la netta prevalenza dei primi grazie alla scoperta di crittosistemi molto forti come lo stesso DES o l'RSA [Riv78].

I sistemi per l'accesso condizionato, in particolare quello della tv a pagamento, costituiscono un'eccezione a causa di deficienze tecnologiche e strategie di gestione inadeguate.

Sia il *Common Scrambling Algorithm* che i sistemi di codifica non sono stati resi pubblici dalle aziende che li hanno sviluppati e le sole conoscenze disponibili sono state fornite, in maniera non ufficiale, da coloro che li studiano (una panoramica degli algoritmi pubblici di *scrambling* si trova in [Bha02]).

Questa scelta è stata motivata col non voler fornire informazioni ai pirati e col mantenimento del segreto industriale, ma induce a ritenere che tali crittosistemi non siano poi così forti.

Questo alla luce del principio di Kerckhoffs [Ker83], alla base di tutta la crittografia moderna, secondo cui la sicurezza di un sistema dipende dalla segretezza delle chiavi e non dell'algoritmo.

In ottemperanza a tale principio, tutti gli attuali crittosistemi sono pubblici e possono essere sottoposti a studi che ne evidenziano le eventuali debolezze permettendo di eliminarle.

Il non rendere pubblici i sistemi per l'accesso condizionato della tv a pagamento li ha posti in una situazione singolare in cui essi sono forzati senza che le società che li

hanno realizzati sappiamo ufficialmente con quali tecniche e, quindi, senza possibilità di apportare modifiche per rafforzarli.

La documentazione non ufficiale di cui disponiamo, fa ritenere che, alla luce delle attuali tecnologie elettroniche ed informatiche, la crittografia delle tv a pagamento sia effettivamente debole in quanto prevalentemente basata su chiavi a 64 bit.

Ricordiamo che il DES, che aveva una chiave di 64 bit di cui solo 56 effettivi ed 8 di controllo, nel 1999, è stato violato con un attacco di forza bruta impiegando meno di ventiquattro ore anche se con macchine dedicate e ingenti risorse di calcolo [DESC3].

La potenza di calcolo degli attuali PC e la possibilità di distribuire un attacco di forza bruta su molte macchine operanti in parallelo consentono di rompere un simile cifrario in modo molto semplice, rapido e poco costoso.

Le *ControlWord*, che sappiamo avere una lunghezza di 64 bit dalla documentazione ufficiale del DVB, non sono soggette a questo tipo di attacco in quanto modificate con una frequenza altissima. Invece le *ServiceKey* vengono cambiate con una frequenza molto bassa e rimangono attive per un tempo che va da uno a trenta giorni.

Peraltro, i sistemi più evoluti prevedono *ServiceKey* di 128 bit ma le emittenti, per scelte che non sono note (forse per problemi tecnici), non sempre si avvalgono di tale possibilità.

Inoltre, sebbene in letteratura non vi sia riscontro, sembra ragionevole ritenere che le *ServiceKey* siano generate con algoritmi pseudocasuali e relativi semi, ambedue noti ai pirati.

Questo permetterebbe di definire le chiavi future con largo anticipo senza dover ricorrere a tecniche più complesse o dispendiose come un attacco di forza bruta.

La smart card costituisce un punto debole dell'intero sistema per l'accesso condizionato in quanto soggetta ad attacchi di varia natura che ne consentono la lettura e, addirittura, anche la scrittura [And96][And97].

L'evoluzione tecnologica ha sicuramente aumentato la sicurezza delle smart card [Köm99] [Moo02] ma non al punto da renderle immuni da intrusioni.

Una ricerca ha evidenziato che tutti i cifrari finalisti del concorso per la definizione dell'Advanced Encryption Standard [NIS01], il nuovo cifrario simmetrico standard che ha sostituito il DES, mostrano una vulnerabilità più o meno accentuata ad attacchi effettuati con la recente e sofisticata tecnica dell'analisi di potenza [Cha99].

La cosa assume aspetti ancora più significativi se si considera che uno dei requisiti richiesti ai candidati all'AES era proprio quello dell'implementazione sicura su smart card.

Le attuali tecnologie per la progettazione e realizzazione di smart card non sembrano poter garantire la sicurezza necessaria a mantenere un segreto su vasta scala.

Un'altra debolezza dei sistemi per l'accesso condizionato delle tv a pagamento è costituita dalla possibilità di rilevare costantemente il flusso cifrato in ingresso al decoder e il corrispondente decifrato in uscita dal decoder con un semplice analizzatore logico o *logger*.

Considerato che si possono rilevare un numero a piacere di coppie testo cifrato-testo in chiaro, sarebbe possibile effettuare un attacco di tipo matematico-statistico con testo (in chiaro o cifrato) scelto [Qia97][Sla04].

In realtà, questa tecnica viene utilizzata per analizzare il traffico tra la smart card ed il suo lettore e definire in maniera dettagliata tutte le interazioni esistenti tra i due dispositivi.

Manchevolezze nella gestione del sistema per l'accesso condizionato da parte delle emittenti possono favorire le azioni di cracking.

Il sistema non è costituito soltanto dai vari dispositivi e dai relativi software ma prevede anche operazioni, opportunamente pianificate, da attivare periodicamente o al verificarsi di determinati eventi.

Il cambio delle chiavi, la disattivazione di trick card mediante *Electronic Counter Measure* o la sostituzione delle smart card sono parte integrante del sistema e devono essere realizzate nei modi e nei tempi previsti in modo da prevenire o eliminare rapidamente la visione abusiva.

Non sempre le emittenti mettono in atto tali azioni in quanto non sono disposte a sopportarne i relativi costi, tempi e sforzi organizzativi.

Il cambio delle *ServiceKey* avviene con una frequenza molto bassa che può arrivare addirittura a trenta giorni e la sostituzione delle smart card viene in genere effettuata solo quando il sistema è stato completamente forzato da tempo.

Il cambio di smart card comporta la modifica della *UserKey* e di tutti gli algoritmi di decifratura delle chiavi e rende quindi inservibili la gran parte delle conoscenze eventualmente acquisite dai pirati sul sistema di codifica.

Per questo motivo le smart card dovrebbero essere cambiate anche quando lo stesso risulti ancora integro.

Come per tutti i sistemi elettronico-informatici, un'ulteriore possibilità di attacco è costituita dalla presenza di bug nella progettazione e realizzazione dell'hardware o del software del sistema per l'accesso condizionato.

In genere, questi errori sono sfruttati per forzare la lettura e la scrittura della smart card.

Va infine ricordato che la visione abusiva può essere facilitata dalla natura stessa del sistema di trasmissione o di quello per l'accesso condizionato.

La tv via satellite, che è la più soggetta agli attacchi, prevede una trasmissione di tipo simplex ossia unidirezionale dalla stazione emittente ad ogni singolo ricevitore.

La mancanza di un segnale di ritorno nel protocollo di comunicazione non rende possibile l'identificazione e la conseguente disattivazione delle trick card.

Inoltre un serio rafforzamento di una codifica potrebbe richiedere il cambio del decoder o della CAM con costi considerevoli non sempre sopportabili.

6. Proposte per combattere la pirateria.

La pirateria delle tv a pagamento costituisce un'attività illegale molto diffusa che comporta gravi perdite finanziarie ed occupazionali.

L'Unione Europea, gli Stati che vi appartengono e gli operatori del settore hanno effettuato alcuni interventi di natura legislativa e tecnica che non sembrano aver intaccato il fenomeno, visto il suo espandersi.

L'insuccesso di questa azione ed il previsto aumento del numero di tv a pagamento, a seguito del passaggio al digitale terrestre, fanno ritenere necessari ulteriori interventi.

Il primo è di natura squisitamente culturale.

I soggetti danneggiati dalla pirateria dovrebbero promuovere iniziative che portino a considerare la visione abusiva “inaccettabile” sia dal punto di vista legale sia finanziario.

Attualmente, quest’opera di sensibilizzazione, che ha valenza anche per altri generi di pirateria (software, musica, film), viene svolta di rado e con poca convinzione; il problema emerge, quasi sempre in maniera sensazionalistica, solo quando viene sgominata un’organizzazione di pirati o introdotta, aggiornata o forzata una codifica, senza che questo comporti significative ricadute in termini educativi o di presa di coscienza.

Quella culturale è una strada molto lunga che richiede tempi considerevoli ma, al di là di ogni retorica, è l’unica a garantire risultati consolidati e duraturi.

Non si potrebbe spiegare altrimenti quanto accade in Scandinavia, dove il numero di abbonati alle tv a pagamento rimane molto alto pur in presenza di una pirateria in grado di offrire la visione abusiva di tutti i *bouquet* degli operatori locali senza alcuna interruzione temporale.

Il secondo è di natura legislativa.

L’Unione Europea, sotto la spinta delle società di tv a pagamento, ha emanato nel 1998 la direttiva 98/84/EC [EC98] sulla protezione legale dei servizi basati sull’accesso condizionato, in cui le attività e i sistemi che consentono la visione abusiva vengono dichiarati illegali.

In Italia, la direttiva è stata definitivamente recepita con la legge n. 2442 del 15 gennaio 2003 [Leg03] che ha integrato il decreto legislativo n. 373 del 15 novembre 2000 [DL00].

Le leggi emanate a seguito della direttiva nei Paesi appartenenti all’UE hanno consentito di smantellare le piccole organizzazioni di pirati e di chiudere i siti Internet residenti su server, situati negli stessi Stati, che distribuivano software e chiavi.

Le grandi organizzazioni, invece, hanno continuato ad operare e a gestire siti in Paesi non appartenenti all’Unione Europea (in particolare dell’Europa dell’Est e dell’ex Unione Sovietica) dove la materia non è regolamentata.

Un’azione legislativa parziale, promossa solo da alcuni Paesi, non sembra in grado di combattere la pirateria.

Un’armonizzazione legislativa che consideri illegale la visione abusiva nel maggior numero di Paesi o, meglio ancora, in tutto il mondo, rimane la sola strategia per ridurre in maniera significativa il fenomeno.

L’ultimo intervento riguarda l’aspetto tecnico.

Abbiamo ampiamente dimostrato che l’attuale sistema per l’accesso condizionato non è in grado di garantire sicurezza ma, al momento, non sono disponibili alternative più efficaci.

Le proposte di sistemi per l’accesso condizionato più sicuri [Jai02][Nar03][You00] o di tecniche per la scoperta di “traditori”, ossia di utenti autorizzati che rendono pubbliche le chiavi per consentire la visione abusiva ad altri, [Tre03] non hanno ancora trovato attuazione.

Pertanto le uniche soluzioni proponibili riguardano il potenziamento e la corretta gestione dell’attuale sistema per l’accesso condizionato.

In primo luogo va adottata una crittografia forte a 128 bit invece degli attuali 64.

L'AES, che, come abbiamo visto nel par. 5, è a rischio di forzatura quando implementato su smart card, potrebbe però essere un buon candidato in quanto pubblicamente riconosciuto resistente ad attacchi di forza bruta e di tipo matematico/statistico.

In secondo luogo, le emittenti dovrebbero mettere in atto tutte le operazioni programmate per la corretta gestione del sistema per l'accesso condizionato, come il cambio molto frequente (più volte al giorno) delle *ServiceKey* e quello periodico (ogni sei-dodici mesi) delle smart card.

BIBLIOGRAFIA

[Abr91] Abraham D. J., Dolan G. M., Double G. P., Stevens J. V., Transaction Security System, IBM Systems Journal, vol. 30, n. 2, 1991, pp. 206-229

[And96] Anderson R., Kuhn M., Tamper Resistance - a Cautionary Note, The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, USA, November 1996, pp. 1-11

[And97] Anderson R., Kuhn M., Low Cost Attacks on Tamper Resistance Devices, Security Protocols, 5th International Workshop, Paris, France, April 1997, pp. 125-136

[Ben03] Benoit H., Manuale della televisione digitale. MPEG-1, MPEG-2 e principi del sistema DVB, Hoepli, 2003

[Bha02] Bhargava B., Shi C., Wang S., MPEG Video Encryption Algorithms, citeseer.ist.psu.edu/621665.html

[Cha99] Chari S., Jutla C. J., Rao J. R., Rohatgi P., A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards, Second Advanced Encryption Standard Candidate Conference, Rome, Italy, March 1999, pp. 133-147

[Coh91] Cohen M., Hashkes J., A system for controlling access to broadcast transmissions, European Patent Application 0428252A2, 22 May 1991

[Con] www.conax.com

[Cry] www.cryptoworks.com

[DESC3] <http://www.rsasecurity.com/rsalabs/challenges/des3/>

[DL00] D.L. 373, 15 novembre 2000, www.parlamento.it/parlam/leggi/deleghe/00373dl.htm

[DVB] www.dvb.org

[EBU] www.ebu.ch

[EC98] Document 398L0084, Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, Official Journal L 320, 28/11/1998, p. 54-57

[ETSI] www.etsi.org

[Eur92] Access control system for the MAC/packet family: EUROCRYPT, European Standard EN 50094, CENELEC, December 1992

[Ird] www.irdetoaccess.com

[ISO] www.iso.ch

[Jai02] Jain P. C., Joshi S., Mitra V, Conditional Access in Digital Television, 2002, citeseer.ist.psu.edu/519542.html

[Ker83] Kerckhoffs A., La cryptographie militaire, Journal des sciences militaires, vol. IX, Janvier 1883, pp. 5-38, Février 1883, pp. 161-191

[Köm99] Kömmerling O., Kuhn M., Design Principles for Tamper-Resistant Smartcard Processors, Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, USA, May 1999, pp. 9-20

[Kud94] Kudelski A., Method for scrambling and unscrambling a video signal, United States Patent 5375168, 20 December 1994

[Kuhn] www.cl.cam.ac.uk/~mgk25/

[Kuh98] Kuhn M., Analysis of the Nagravision Video Scrambling Method, August 1998, www.cl.cam.ac.uk/~mgk25/nagra.pdf

[Lai90] Lai X., Massey J., A proposal for a new block encryption standard, Advances in Cryptology-EUROCRYPT '90, Berlin, Germany, May 1990, pp. 389-404

[Law04] Lawson D., Video Piracy, Scrambling News, 2004

[Leg03] L. n. 2442, 15 gennaio 2003, www.camera.it/_dati/leg14/lavori/stampati/sk2500/frontesp/2442.htm

[Leg04] www.comunicazioni.it/it/index.php?IdPag=836

[Len91] Lenoir V., EUROCRYPT, a successful conditional access system, IEEE Transactions on Consumer Electronics, 37(3), August 1991, pp. 432-436

[McC96] McCormac J., European Scrambling Systems 5, Waterford University Press, 1996

[Moo02] Moore S., Anderson R., Kuhn M., Improving Smart card Security Using Self-Timed Circuit Technology, The Eight IEEE International Symposium on Asynchronous Circuit And Systems, Manchester, UK, April 2002, pp.120-126

[Nag] www.nagravision.com

[NagFr] www.nagra.fr

[Nar03] Narayanan A., Rangan C. P., Kim K., Practical Pay TV Schemes, 2003, citeseer.ist.psu.edu/634115.html

[NBS77] National Bureau of Standards, FIPS PUB 46, 1977 January 15, Data Encryption Standard (DES)

[Nds] www.nds.com

[NIS01] National Institute for Security and Technology, FIPS PUB 197, 2001 November 26, Advanced Encryption Standard (AES)

[Qia97] Qiao L., Nahrstedt K., Tam I., Is MPEG encryption by using random list instead of zigzag order secure?, IEEE International Symposium on Consumer Electronics, Singapore, December 1997

[Riv78] Rivest R., Shamir A., Adleman L., A method for obtaining digital signatures and public key cryptosystem, Communications of the ACM, vol. 21, n. 2, 1978, pp.120-126

[Sla04] Slagell A. J., Known-Plaintext Attack Against a Permutation Based Video Encryption Algorithm, 2004, citeseer.ist.psu.edu/673231.html

[Tre03] Trevathan J., Ghodasi H., Overview of Traitor Tracing Schemes, 2003, citeseer.ist.psu.edu/681933.html

[Via] www.viaccess.com

[Videoc] www.cl.cam.ac.uk/~mgk25/tv-crypt/

[You00] Kim Y., Yu J., Won D., An Efficient Satellite CAS Using Password-Based Protocol, 2000, citeseer.ist.psu.edu/337205.html

