

Intro Broadcast Encryption

By- Ashutosh R. Chickerur

Initial Research

- Amos Fiat and Moni Naor were the first to pioneer the research in broadband encryption.
- The question was “IF two devices unknown to each other can agree upon a key and on a One-Way communication channel.

Answer – YES.

- IBM, INTEL, TOSHIBA, MATSHUSHITA developed CPRM(Content Protection for Recordable Media) technology.
e.g. : DVD players, DVD recorders, Compact disk players.

Present Broadband encryption in DVD's

- DVD players now-a-days use CS(Content Scrambler Systems).

CSS has been broken already. This cannot be fixed since its been embedded in all devices and shipped out to consumers.

How Broadband Encryption works

- Scheme based on KEY-MANAGEMENT-BLOCKS.
- KEY-MANAGEMENT-BLOCK:
 - A block of data sent in a broadcast or pre-recorded at the beginning of the block media.
- Each recipient reads the KEY-MANAGEMENT-BLOCK & “processes” it to get the management key and use it to decrypt the content.

How devices Decrypt..

- The key management block contains a 2500 x 16 matrix.
- Each device has 16 keys for each column stored in one of its memory chips.
- Max 2 keys for 2 different devices match, but all 16 never match.
- Positions(x,y) >>[process] << (16 DVD keys) = see movie.
- Each device has 16 keys, one for each column, If all match then BINGO... decrypt and use...

Example of a MAC Processing

- Snapshot Key management block

12	14	42	65
223	85	54	76
554	774	545	654
4563	987	789	287
4568	5472	3654	4587
1555	3333	2545	1425

- These are the keys and their positions that match for device 1

			65
223			
	987		
		2545	

- Snapshot of keys for device 1.

223	987	2545	65
-----	-----	------	----

- While the second set of device keys has 2 keys missing for device 2.

			65
	987		

- Snapshot of keys for device 2.

223	987	2545	65
-----	-----	------	----

Example of a Revocation of device keys

- Snapshot Key management block

12	14	42	65
223	85	54	76
554	774	545	654
4563	987	789	287
4568	5472	3654	4587
1555	3333	2545	1425

- Snapshot of keys for device to be deleted .

223	987	2545	65
-----	-----	------	----

- These are the keys and their positions after deletion of the device keys.

12	14	42	76
554	85	54	654
4563	774	545	287
4568	5472	789	4587
1555	3333	3654	1425
1111	2222	3333	4444

- The new keys are added at the end, as the device matching is not position dependent.

Improvements in broadcast encryption over CSS

- Instead of a matrix, a hierarchical tree structure can be used. The newer algorithm didn't provide much advantage over CSS in time/space .
- Dalit and naor later provided an optimized tree algorithm to provide time/space advantage.

Broadband Encryption(BE) Vs. Public Key Encryption(PE)

- Broadband Encryption is simple and fast whereas PK loads the processor with calculations. (Estimated approx. 1000 times more).
- PK makes forging digital-signs difficult coz of its intractable math code. Actual signer' private key has to be known to digitally sign a documents .
- PK has a link level handshake for Authorization.Keys are exchanged,hence making it easier to eavesdrop.Where as BE hides the keys deep into software making it difficult to detect.

Broadcast Vs. Public Key encryption (contd..)

- BE replaces the digital-sign with MAC(Message Authentication Code).
- To verify MAC devices share a secret key.For e.g. Management key.
- A central Authority has to be present for licensing the device keys and producing key-management-blocks for media.
- Hence BE is not completely optimal but provides advantages like-
 - Low overhead
 - Strong resistance for reverse-engineering of h/w devices
 - for keys can be controlled and made difficult.

Broadcast Vs. Public Key encryption (contd..)

- Some advantages of PK are-
 - No central licensing authority is required.
 - Some of the HOME- network use PK for content and media protection. Below are some schemes which use PK and BE for home networking.
- HOME-Networking : All devices connected inside a home. Eg : DVD players, TV, Computer, Stereo. And all these connected to the Internet.
- Broadcast encryption basically promotes One-to Many technology, but poor on peer-to-peer applications. But here are some examples which work well with Broadcast encryption.
 - The criteria is MAC's has to suffice.

Some classic PK and BE examples for content protection in home networking

- DTCP (Digital Transmission Content Protection)
 - Straightforward Public-key cryptography application
 - Solves the problem of content protection on digital bus.
- Algorithm:
 - 2 Handshake protocols to let participants authenticate each other and establish session keys
 - > Protected content doesn't flow in the network until authentication is complete. Both authentication protocols are based on the elliptical curve certificates and Diffie-Hellman key exchange.
 - > The full authentication procedure requires both the devices to exchange and check signatures on each others certificates.
 - > Next the Diffie-Hellman key exchange results in calculating the session keys.
 - > Revocation of devices are done by listing the certificates of devices in system renewal messages, distributed by licensing agency.
 - > AT LINK LEVEL DTCP FACES REVERSE ENGINEERING THREAT.
 - > DOES NOT SOLVE THE PROBLEM OF PROTECTING REDISTRIBUTED DATA

OCCAM: END TO END CONTENT SECURITY

- **OCCAM(Open conditional Content Access Management)**
 - **General approach to system security by CISCO**
 - **Protects content on the network and on storage media.**
 - **Based on hierarchical public key infrastructure with central authority called OCRA**
(OCCAM Certification and Revocation Authority).
 - **OCRA assigns device ID's and private keys to device manufacturers.**
 - **Maintains a database of public key certificates.**
 - **The device wishing to view the content asks the content owner a ticket. The ticket contains an encrypted content key, encrypted by the querying device's public key.**
 - Only the device can decrypt the key and view the content.**
 - this necessitates the need to connect to a central authority(At least at the beginning of the transaction). This helps the content provider in checking if the device is on the revocation list.**
 - **DOES NOT WORK IN A DISCONNECTED ENVIRONMENT.**
 - **DOES NOT HELP IN REDUCING THE OVERHEAD OF NETWORK TRAFFIC.**
 - **BUT HELPS IN CONTENT PROTECTION ON STORAGE TOO.**

xCP Cluster- An broadcast encryption protocol

- **Developed by IBM – a Broadcast encryption based technology.**
 - **Algorithm :**
 - **Devices agree upon a common key management block.All protected content is encrypted with the management key.Only compliant devices can process the content associated with the cluster they belong to.**
 - **Any compliant devices can join and leave the cluster.They have to verify the MAC,that is all.**
 - **Devices need not have to converse with other devices for content keys.If they spot the key management block(which is a simple file on the network),they are good to go.**
 - **This design is based on trust too.The compliant devices will not perform forbidden tasks.Like a DVD recorder will not record data if the content specifies “don't copy”. This differs from the previous DTCP protocol, since DTCP will not channel content to any device which says “recorder.**
 - **IF ANY DEVICE PERFORMS FORBIDDEN TASKS< THE KEYS WILL BE REVOKED.**

Where Broadband encryption fails

- Few Examples where Broadband encryption fails
 - Electronics funds transfer
 - Since Public Key system does identifies the actual principal involved, where as broadband encryption authenticates the members in a given group. This non-refutable property renders broadband encryption unapplicable.
E.g.: The sender and receiver has to know and authenticate each other if they have to deal in funds transfer. Else no one knows who is getting the money.
 - This is ok in content protection, where a break of DVD will not hurt as much as a heist from a bank account.

Examples (contd..)

- Secure Socket Layer.
 - Public key cryptography has another important application involving link-level security for communications channel.
 - SSL offers businesses encryption, authentication and verification services like HTTPS, ssh etc.
 - SSL requires handshakes prior to communications, and loads the processor with computations.

Conclusion

- Broadband encryption is fundamentally different from Public Key Encryption.
 - Broadband encryption guarantees that the other principal involved in the communication belongs to the same group, where as public key encryption actually verifies the identity of the user.
 - In Both cases the guarantees are only strong as much as the system's functional revocation mechanism.