Proc. IEEE 34th Annual 2000 International Carnahan Conference on Security Technology, Ottawa, Canada, October 2000, pp. 238-241.

A 6805-based Security System for Broadcasting Stock Information[*]

Chung-Huang Yang

National Kaohsiung First University of Science and Technology

Taiwan, REPUBLIC OF CHINA

chyang@ccms.nkfust.edu.tw

http://www.nkfust.edu.tw/~chyang/

Abstract: This research describes the design and implementation of secure stock information broadcasting systems using Motorola's 68HC05B6 single-chip microcontroller as the embedded security devices. In-band technology is used to transparently insert encrypted stock information into TV channel(s) and send to households. The implemented conditional-access system uses Data Encryption Standard (DES) and triple-DES to provide high levels of communication security.

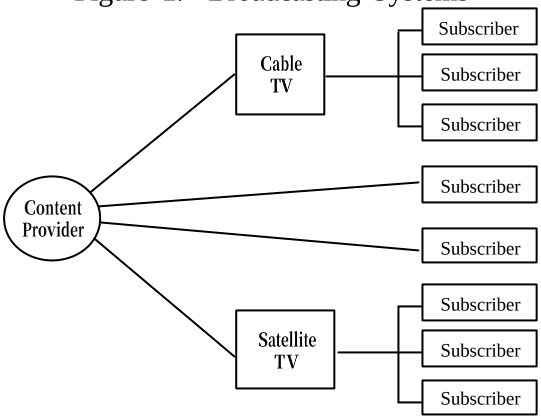
INTRODUCTION

The fast growing stock market in Taiwan has generated thousands of individual shareholders who buy or sell stocks. In general, individual shareholders will go to securities brokers or connect to the Internet to learn stock trading information. However, both would require valuable time or communication fee.

Since the advent of pay-TV in the 1950s, scrambling transmission of television broadcasting signals has generated a great deal of interest. Broadcast communication allows central source to simultaneously distribute the same message to many receivers. Due to broadcast nature, some form of security becomes essential in very many applications. The term "conditional-access" is frequently used to describe systems that enable the individual control over the access to services, programs, etc.

In a typical conditional-access control system [1-6], a group of channels are transmitted in the scrambled form and all the decoders in each subscriber's home receive the same signal consisting of scrambled or encrypting components and access control parameter. Successful descrambling occurs only in the homes of those who have been authorized. A conditional-access system is user transparent and could be very secure. It is capable of providing pay-per-view service or send personalized message service to individually addressable subscribers.

Figure 1: Broadcasting Systems



Strong scrambling or encrypting operation is generally based upon the usage of a cryptographic algorithm controlled by a secret *key*, changed at very frequent intervals, while a decoder at subscriber's home would reproduce the original data of certain programs (or services) if a correctly encrypted descrambling key ("*session key*") was received. Without knowing the secret keys, the pirate is assumed to have the complete knowledge both about the nature of the signals under transmission and also about everything of the decoder that is invariant and key independent. But with regarding the security, no general criterion at the present time

[*] This research was supported in part by the Chilong Data Products Corp., Taipei, Taiwan

has been developed to certify the system security, and many schemes have been proposed and then broken. The only way of cryptanalysis (attacking) is by trial and error, subjecting the system to all known techniques.

In practice, for reason of security, a set of secret keys is resident in the key manager device or inside IC card. Each subscriber will have a decoder which has a unique ID stored on the security module and identical scrambled information will be received by every decoder. Furthermore, in such an addressable system, the decoder could be completely activated or deactivated according to subscriber's status or the program (service) in use.

STOCK MARKET

The stock market in Taiwan has been very volatile [7-9]. Individual investors make up most of the very high market volume. The stock trading information comes from Taiwan Stock Exchange [7]. During trading hours, investors may obtain real-time trading information from the electronic quotation display in boardrooms of the securities brokers. Stock information includes the bid and ask price, the last trade price, cumulative traded volume of individual stock, and a collection of market statistics, etc.

Individuals usually make dozens of trades a year in each of their accounts. They will go to stock trading agencies to learn about stock status or they need to connect to the Internet to receive such trading information. Both would require quite a lot time or communication fee that motivates this research.

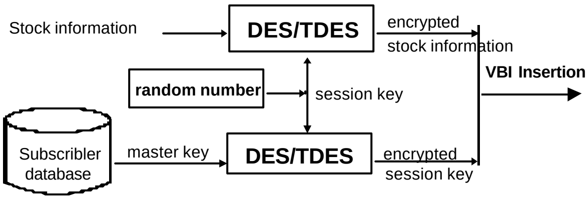
SECURE STOCK INFORMATION BROADCAST SYSTEM

Our goal is to find an effective and efficient mechanism to implement a conditional-access system for broadcasting stock trading information. In Taiwan there are over five million cable-TV (CATV) homes, which represent about 80 percent of the total number of television households. Currently most CATV network in Taiwan has over 90 channels to choose from. The increase in the number of homes with CATV and lots of cable channels render CATV as the best candidate for stock information delivery. Stock data could be encrypted then converted into analog signals and transmitted in the active portion of available TV lines, the unused lines in vertical blanking interval (VBI). The similar technique is used for closed caption or teletext [10].

The very nature of broadcasting is that the programs and data are transmitted in downlink direction and the subscriber needs some assurance that the data is from the alleged service provider. Therefore, in addition to protection from pirates, one-way authentication is also needed to verify the origin of services.

The session key cannot be sent with broadcast signal in the clear form, it must be encrypted with another key. Encryption of our conditional-access system is based on the private-key cryptography of NIST's DES or Triple-DES [11] and our system is capable of selecting addressable geographical area as well as providing personalized message service. The main idea is to encrypt the stock trading data with periodic session key while separately encrypt the session key directly or indirectly for authorized subscribers. The following figure illustrates the involved operations.

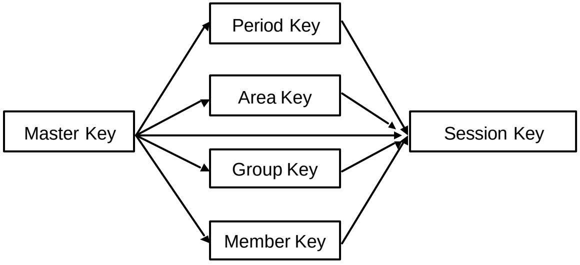
Figure 2: Broadcasting of Stock Trading Information



Large amounts of stock information are broadcasting and protected through the use of dynamically generated session keys, the data-encrypting keys. Session keys are in turn encrypted and guarded by the key-encrypting key, the master key, stored in a physically secure device at subscriber's decoder. The master key stored in each security device is unique to each subscriber for reasons of system security. But to encrypt and distribute the session key to each subscriber would be impractical, since there may be a huge number of subscriber. In order to overcome this problem a hierarchy of cryptographic key is deployed.

A three-level key hierarchy is illustrated in figure 3. At the top level is the master key; a unique distribution keys each stock information decoder. In the middle level are the group keys (or period key or area key or member key), common to each group of subscribers. The lowest level keys are session keys that are associated with the broadcast stock information for a short period of time. The group key is used to carry the session key and itself carried by the master key. As a consequence, only a small number of group keys, encrypted session keys, need to be broadcasting. This would significantly reduce the operational difficulties in distributing the session keys to huge number of subscribers.

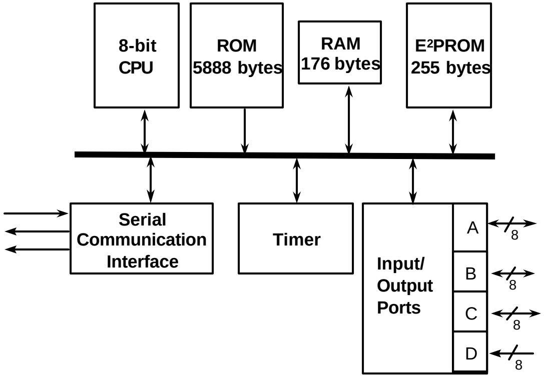
Figure 3: Hierarchy of Cryptographic Keys



THE SECURITY DEVICE

In order to make low cost approach, we select an embedded device instead of smart card approach. We select the Motorola 68HC05B6 [12] microcontroller that offers an 8-bit microprocessor, 6K-byte ROM, 256-byte EEPROM, 176-byte RAM, a timer, a serial communication interface, and four general-purpose input/output ports. Figure 4 shows the block diagram of this chip. The EEPROM area is where we store unique ID and cryptographic master keys for subscribers.

Figure 4: Block Diagram of the MC68HC05B6



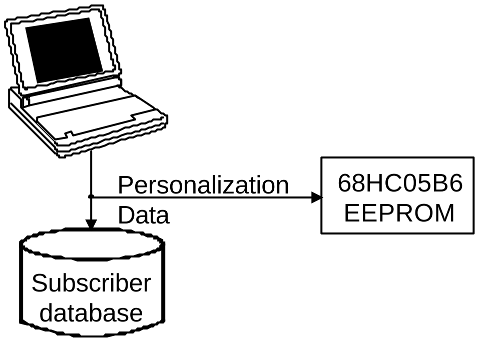
The vendor provides an in-circuit simulator kit that is an extremely economical tool, suggested retail price of US$99 [13], for developing and debugging target systems incorporating the 68HC05 microcontroller under Windows 95 environment. A one-time programmable device, 68HC705B16, with suggested list price of US$6.45, is also available for fast prototype development.

Performance of implemented DES algorithm is under 15ms per encryption or decryption, which is appropriate for key management. Here we list main functions of the customerized 68HC05B6:

1. Personalization (initialize built-in EEPROM data)
2. Setup group/period/member/area keys
3. Decryption of session key (via 56-bit DES algorithm)
4. Encryption and decryption of input data (via 56-bit DES algorithm)
5. Validation of message authentication code (when receive any new program from the content provider)
6. User PIN verification/alternation
7. Triple-DES encryption/decryption (i.e., 112-bit key)
8. Misc. (setup and test serial communication speed, communicate with host, etc.)

Finally, a personalization station is required to manage the issuing of security devices. It loads a unique ID and cryptographic keys onto the 68HC05B6 device, initialize the interface mode of device, and stores related information into subscriber database. Also it needs to handle key generation, storage, replacement, revocation, etc. during lifetime of the security device. We developed a personalization program under Windows 98 environment using Borland (Inprise) C++Builder development tool.

Figure 5: Personalization Station for the 68HC05B6



CONCLUSIONS

The objective of a conditional-access system is to ensure that certain broadcasting information is available only to authorized subscribers. Here we describe our implementation efforts for broadcasting stock information where low-cost 68HC05B6 devices with DES cryptographic firmware are used to ensure high levels of broadcast security.

REFERENCES

1. CCIR Report 1079-1, *General Characteristics of a Conditional-Access Broadcasting System*, 1986.
2. K. Lucas, "HDB-MAC, A Conditional-Access HDTV Transmission Format", *Proc. AIAA*, pp. 209-216, 1990.
3. A.G. Mason, "A Pay-Per-View Conditional Access System for DBS by Means of Secure Over-Air Credit Transmissions Having a Short Cycle Time," *International Broadcasting Convention*, 1984, pp. 282-288.
4. D. Angebaud and J. Giachette, "Conditional Access Mechanisms for All-Digital Broadcast Signal," *IEEE Trans. Consumer Electronics*, Vol. 38, No. 3, August 1992, pp. 188-194.
5. V. Lenoir, “Eurocrypt, A Successful Conditional Access System,” *IEEE Trans. Consumer Electronics*, Vol. 37, August 1991, pp. 432-435.
6. B. M. Macq and J.-J. Quisquater, “Cryptology for Digital TV Broadcasting,” *Proc. IEEE*, Vol. 83, June 1995, pp. 944-957.
7. Taiwan Stock Exchange, http://www.tse.com.tw.
8. Taiwan Securities Industry Risk Analysis, Taiwan Ratings Corporation, http://www.taiwanratings.com/analysis/securities.htm.
9. Rong-I Wu, “Financial Restructuring and Economic Perspectives in the East Asia: Country Perspectives of Taiwan,” Taiwan Institute of Economic Research, 1999, http://www.tier.org.tw/11english/Leader-publications/02.htm
10. Electronic Industries Association, EIA-516, *Joint EIA/CVCC Recommended Practice for Teletext: North American Basic Teletext Specification (NABTS)*, 1988.
11. National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard, October 25, 1999, http://csrc.nist.gov/ fips/fips46-3.pdf
12. MC68HC05B6 Technical Data, Rev. 4, Motorola Ltd., May, 1998, http://mot-sps.com/mcu/documentation/pdf/b6r4.pdf.
13. M68ICS05B In-Circuit Simulator (ICS) Kit, Motorola Ltd., http://208.21.175.62/device/device_detail.cfm?Device_Number=68HC705B16.