Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 907-912
doi:10.4028/www.scientific.net/AEF.6-7.907

Hybrid Encryption Scheme of EOC Traffic

Ren Xun-yi[1, a], Zhang Jun-feng[1, b], Yu yang[1, c], Wan Hai-ping[2, d]

[1]School of Computer, Nanjing University of Posts and Telecommunications, China

[2] Shandong Youth University of Political Science, China

[a]renxy@njupt.edu.cn, [b]xfzjf@139.com, [c]15051896636@139.com, [d]whp@sdyu.edu.cn

Keywords: EOC; encryption technology; security threat; hybrid encryption scheme

Abstract. To improve the security of EoC network traffic, the hybrid encryption scheme was presented. The relevant encryption algorithm was analyzed, and the hybrid encryption scheme was proposed for EOC downlink traffic encryption, in which ECC algorithm is taken to produce and encrypt session key, and Blowfish algorithm is improved to encrypt the broadband-authorized frame and downlink data. The security analysis show the encryption scheme can guarantee the integrity and confidentiality of the data in the EoC transmission process.

Introduction

Currently, EOC technology, slathered in the families of the United States, Japan, Korea and Europe, is comparatively ripe in coaxial network data transmission. It has also been decided in our country that thousands of billions will be invested to build the next-generation broadcast and television network and 200 million CATV users are planned to be transformed in 10 years. The market prospect is rather wide but the security problems reflected are very severe which are imperative to be resolved for their impacts on commercialization procedure. As a result, this paper study the security mechanism of EOC system from the point of traffic data encryption and propose a method in which ECO downlink traffic is encrypted with hybrid encryption scheme combined with the special circumstances and security requirements of EOC system.

It is with good adaptability and a flexible networking access scheme for that there is no need to transform the original CATV net line. EOC is a generalized conception. Technologies using telephone line, power line and television cable to transmit data and signals are called EOC. Early research on EOC technology is concerned with the applications of telephone line and power line on transmitting signals but recent studies are emphasized in the application of television cable on transmitting data. Although breakthrough point and technical method of all kinds of EOC technologies are various, they can all used in CATV network where data and signals are transmitted with coaxial cable [1-2].

Security Problems Faced by EOC

Bus-type or tree topology is usually adopted in EOC system, mainly presented that central office device send information to terminal device with downlink frame made up of Ethernet frame and each terminal device can receive all the data stream and then extract the specific data packages according to the its MAC address. However, it is the downlink method that leads to that there are following three security threats exist in EOC system.

(1) Eavesdropping. As the downlink data of EOC system transmit with broadcast, each terminal connected to the same central office device can receive all the downlink data. Set LLID (Logical Link Identification) for each connection according to IEEE 802.3 standard so that each terminal device only receive the data package belong to its LLID and the rest will be discarded and no longer forwarded. However, since LLID is set for distinguishing different connections, we can eavesdrop at downlink direction if only we set the working mode of the terminal network card registered in AVLN (Homeplug AV Logical Network) to promiscuous mode. That is, attackers can get all the information

in the downlink channel if only to invalidate filter rules of LLID. What is more serious that eavesdropping can not be detected by central office device since it is completely passive and it would not have a noticeable negative impact on the network structure or performance. Attackers can get AVLN information uninterruptedly without being discovered with the method such as the MAC address of adjacent terminal, with which the traffic information of the adjacent terminal can be inferred, which is undoubtedly against to the information confidentiality and would compromise it. So in order to isolate the user information and ensure the data privacy of each terminal, data encryption of each terminal at downlink direction is needed.

(2) Impersonation. Attackers can pretend to be the adjacent legitimate user with the MAC address of adjacent terminal gotten by Eavesdropping so that administrators believe that it's a legitimate user, which is most commonly used by attackers to break into the secure line. Attackers get the access to the resource accessible only for legitimate users by impersonation or send data to the network and get services illegally in the identity of legitimate user.

(3) DoS(Denial of Service). If DoS attacks take place in a terminal of AVLN, attackers can send a large number of invalid information to the network that would result in computing resources consumption, network congestion and the destruction of the sensitive configuration information of the system, making that the network resource, MAC control frames and OAM frames are not available thus leading to that the network is not connective and all the standard service owned by legal end-users become invalid. More serious, the network connectivity of physical layer may even be destroyed such as that the use of strong laser signal can lead to the overflow of upstream channel and blocking of the physical-layer network.

Current Encryption Technology in EOC System

Data encryption can be divided into stream ciphers and block ciphers according to different encryption modes, where block ciphers have a wide range of important applications in the field of communication network and system security. Currently many kinds of working modes of block ciphers have been proposed such as cipher block chaining (CBC) mode, output feedback (OFB) mode, cipher feedback (CFB) mode, cascade mode (CM), block chaining (BC) mode, counter mode, plaintext feedback (PFB) mode and proliferation cipher block chaining (PCBC) mode, where the first four are common basic working modes. The modes above have their own characteristics and applications. Data encryption in satellite communications is usually in OFB mode and character data encryption is usually in CFB mode. However, CBC mode and CFB mode can be used for authentication system where the key length can be increased by block cipher cascade for multiple encryptions [2].

Security is the primary principle of password design with no exception of block cipher, which acquires that attackers can not decrypt the cipher by its internal structure. But in EOC system there is a need of real-time data transmission and more stringent requirements on computing resource. Commonly used AES can provide a good safety performance, but the resource occupancy is slightly large in the environment where the computing resource is limited. Therefore password researchers dedicate themselves to finding the equilibrium point of security and execution efficiency to design many lightweight block cipher algorithm which, on the basis of security, pursue higher efficiency to cope with the needs in special environments.

So as shown above, it's urgently needed to design a lightweight data encryption method suitable in EOC system which should have the following features: (1) It can be adapted to the special environment during the data transmission in EOC system; (2) It must be as simple as possible and the system consumption must be as small as possible due to the limited embedded resource; (3) The implementation and deployment must be as simple as possible; (4) Minimize a variety of increased costs to meet the business needs; (5) Ensure that the security is as high as possible on the base of the four requirements above.

Hybrid Encryption Scheme of EOC Traffic

The security of ECC algorithm is much higher than RSA [1] for that 160 bit ECC is equivalent to 1024 bit RSA and 210 bit ECC to 2048 bit RSA. Therefore, ECC algorithm is taken to produce and encrypt session key in the hybrid encryption scheme. Blowfish algorithm, designed by Bruce Schneier, is an unpatented symmetric block cipher algorithm and has been widely used in practice for fastness, compaction and variable key length. Based on the Feistel structure of 16 iterations, Blowfish algorithm takes 64-bit blocks and consists of two parts that are key expansion algorithm and data encryption algorithm. The variable key length is 32 bits to 448 bits. Blowfish algorithm is simple to implement and can save resource, thus suitable for the special circumstances of EOC system during data transmission [1]. However, there are several security defects: (1) Defect of equivalent keys. Since users' key length (448 bits at most) is less than the total length of P-array (32×18 = 576 bit), it's necessary to make recycling use of the keys to complete the XOR of users' key and P-array, it's which that may produce equivalent keys. That is, get P⊕K1 and P⊕K2 by XOR of K1, P and K2, P respectively. After Feistel encryption structure, update to get new sub-key arrays P1, P2, S1 and S2. Suppose K1 and K2 exist to meet that P⊕K1=P⊕K2, it's known from the steps of producing P-array and S-box that updated P-array and S-box must exist and P1≡P2, S1≡S2. Seen that the initialization effect with K1 and K2 are the same, where such keys like K1 and K2 are defined as equivalent keys. So it's inferred that the key point to determine that whether equivalent keys exist is to verify that if the XOR results of user key K and P-array are the same. (2) Hidden danger of P-array and S-box. The S-box used by the encryption process of Blowfish algorithm described in chapter 4.3.3 of this paper is the fractional part of the initial constant π, from which attackers can derive the S-box. Thus it can be regarded that the S-box is already known. Simultaneously, it's known from the steps and documents of producing P-array and S-box that the update and produce of P-array is related to the choice of original key array K, which has been explained in chapter 4.3.3. Save the updated P-array and S-box, usually in EEPROM or FLASH, before using Blowfish to encrypt. When an attack starts, the keys can be acquired if P-array and S-box can be gotten from the memory. So Blowfish encryption algorithm would lose its effects and would be easily broken [4]. (3) Repeated initialization. If not to save updated P-array and S-box and only reserve the original initialization results, safety performance will be greatly improved with dynamic calculation of sub-key array P and S-box and key verification by matching the calculated P-array, S-box and the stored original initialization results. But a lot of time would be wasted in the repeated calculation of sub-key array and the efficiency of the encryption algorithm would be reduced [3]. (4) Reverse calculation defect of key array K. It's shown from document 4 that key array K can be derived from the updated sub-key array in Blowfish algorithm, which makes that the security of Blowfish algorithm is greatly reduced [4]. Since Blowfish encryption is a symmetric key algorithm, encrypted data can be decrypted is the key is known, which determines its inherent disadvantages and brings the problem of key management.

The specific steps of using hybrid encryption scheme to encrypt EOC traffic is described as follows:

Step 1 When the device communication of EOC system is established, the newly added re-powered terminal device need to be authenticated first, during which the central office device and terminal device share their public key by the exchange of certificates.

Step 2 The terminal device sends the frame applying for a session to the central office device to start the exchange of session keys.

Step 3 The central office device generates a random number RC and calculates GRC, used to initiate a session, and sends the information containing GRC to the terminal device.

Step 4 Similarly, the terminal device generates a random number RT and calculates GRT.

Step 5 The terminal device generates the session key of the terminal and central office with ECC algorithm in which KC-T=SKT (GRC) + RTPKC, where SKT is the private key of the terminal device and PKC is the public key of the central office device. Encrypt its ID with the session key to get EKC-T (IDT) and then send GRT and EKC-T (IDT) to the central office device.

Step 6 After calculating to get the session key in which KC-T=SKC (GRT) + RCPKT, where SKC is the private key of the central office device and PKT is the public key of the terminal device, decrypt EKC-T(IDT) received from the terminal device to verify its identity and confirm that the session key is shared.

Step 7 The central office device encrypts IDC with KC-T and then send it to the terminal device.

Step 8 After validating the decrypted IDC, the terminal device can determine that if the central office device shares the session key KC-T.

Step 9 Combining the session key with the MD5 value H(MAC) of the terminal MAC address as the user key K of the improved Blowfish algorithm, the central office device encrypts the broadband-authorized frame and downlink data frame. Only the terminal device with corresponding MAC address can decrypt to get the plaintext and then encrypt the uplink data to the central office device by the improved Blowfish algorithm with the same method.

Step 10 The central office device decrypts to get the plaintext of the uplink data with the improved Blowfish algorithm.

The steps above describe the process of using hybrid encryption scheme to encrypt EOC traffic, to which the pseudo code corresponding is described as Table 1.

Table 1. Hybrid Encryption Scheme

```
Process mix_Encrypt(DeviceNode Center, DeviceNode Terminal)
    //Initialization phase
    Rawsocket_create(); //build the device communication Rawsocket
    //Authentication, exchange information like the keys
    SSL_Authenticate(Center,Terminal);
    //Handle the information, produce a random number RC
    RC  Num_Rand();
    GRC Computer_Rand(); //calculate GRC to initiate the session
    //Send the information containing GRC to the terminal device
    //Similarly, the terminal device produce the random number RT and calculate GRT
    RC Num_Rand();
    GRT Computer_Rand();
    //Generate the session key of the central office device and terminal device with ECC algorithm
    (Re_Initialize the Device, KC-T)  ECC_Encrypt(SKT, GRC, RT, PKC);
    //Encrypt its ID to get EKC-T(IDT) and send GRT, EKC-T(IDT) to the central office device
    EKC-T(IDT) ECC_ Encrypt(KC-T, IDT);
    Center Device GRT + EKC-T(IDT);
    //The central office device calculate the session key KC-T with the received information
    KC-T ECC_Encrypt(SKC, GRT, RC, PKT); // SKC is the private key of the central office device and PKT is the public key of the
terminal device
    //Decrypt EKC-T(IDT) derived from the terminal device to verify its identity
    Num_ID ECC_Decrypt(EKC-T(IDT));
    if (Num_ID == IDT)
    then continue;
    else return(error);
    //The central office device encrypt IDC with KC-T and then send it to the terminal device
    Terminal Device EKC-T(IDC);
    //Validate the decrypted IDC to determine that if the central office device shares the session key KC-T
    Num_ID ECC_Decrypt(EKC-T(IDC));
    if (Num_ID == IDC)
    then continue;
    else return(error);
    while (Rawsocket_create) and (data transmission is not finished)
    //Combine the session key with the MD5 value H(MAC) of the terminal MAC address as the user key K of the improved
Blowfish algorithm
    H(MAC)  Compute_MD5(MAC);
    K  KC-T + H(MAC);
    Blowfish_Encrypt(Data); //The central office device encrypts the broadband-authorized frame and downlink data frame
    Terminal Device Encrypted_Data;
    Blowfish_Decrypt(Data); //The terminal device decrypt to get the plaintext and then encrypt the uplink data with the same
method
    Center Device Blowfish_Encrypt(Data); //Transmit data to the central office device
    Blowfish_Decrypt(Data); //The central office device decrypt to get the plaintext
    end while
    Rawsocket_close(); //Close Rawsocket
    //Ending stage, clean up the cache information
    Process_Close();
return (true);
```

Analysis of the advantages of encryption schemes

He Yimin, etc proposed a method of registration authentication and communication encryption mainly applied to EOC system in document [6], in which registration encryption method is used to decrypt and store the encrypted authenticated keys with a unified public key that will be used to encrypt and decrypt interactive data communication by client and central office [6-8].

The hybrid encryption scheme is to combine ECC and Blowfish algorithm, improve Blowfish algorithm and generate the session key with the encryption strength and high efficiency of ECC algorithm. What's more, generate the key K of Blowfish algorithm with the MD5 value of terminal MAC address to improve the security of K, which can eliminate the application problems brought by Blowfish algorithm only. Add MD5 codes to Shellfish open source codes to implement the encryption. Now it is to elaborate the advantages of hybrid encryption scheme with the comparison of Blowfish process before and after improvement.

(1) Eliminate the hidden trouble of equivalent keys. Seen from the analysis of Blowfish security flaws and figure 3, the hidden trouble of equivalent keys exists when separately use Blowfish encryption algorithm in loop key expansion. Attackers can circularly extend completely equivalent keys to reduce the security of Blowfish encryption. While in this hybrid encryption scheme of this paper, connect the session key produced by ECC algorithm and the MD5 value H(MAC) of terminal MAC address as the initialized key of Blowfish algorithm. The key K after connection is unique for the security and uniqueness of the scattered value of current MD5 algorithm. Even if having got the equivalent key, attackers can not acquire the same P-array and S-box after initialization update. Thus the hidden trouble of equivalent keys is radically eliminated.

(2) Effectively avoid the problem of repeated initialization. P-array and S-box but not user key is stored in Blowfish algorithm without being improved that need 4KB storage space, which is suitable to the occasions where user key doesn't changes frequently. Inputting wrong keys when encrypting would also result in initialization, which would lead to useless and repeated initialization, a waste of time and reduction of the algorithm efficiency. In the improved scheme of this paper, MD5 algorithm is used to validate that if user key already exist so as to avoid repeated initialization. Meanwhile, that a few iterations and fast computation of MD5 does not have some important impacts on encryption and decryption speed of Blowfish algorithm. What's more, time-consuming due to repeated initialization is much more than hash time of MD5 function. So the improved scheme in which P-array and S-box are generated based on security key and saved for data encryption is faster than that without being improved. It's also not necessary to frequently change the user key, which brings convenience to the encryption process and users' use and improves the efficiency of the algorithm.

(3) Effectively solve the hidden trouble of terminal MAC address impersonation in EOC system. Known from the analysis and description of security threats of EOC system, attackers can get the MAC address of adjacent terminal by eavesdropping and pretend to be legitimate adjacent user to acquire illegal services. If AES algorithm currently used by EOC manufactures is cracked, terminal MAC address can be directly acquired. While encrypting EOC traffic data with hybrid encryption scheme, the data got by attackers with eavesdropping is encrypted and the MAC address of adjacent terminal can only be acquired by decryption. Since the key of Blowfish algorithm is dealt with by ECC and MD5 algorithm and encryption strength is enhanced in hybrid encryption scheme, improved Blowfish algorithm is needed to be cracked during the cracking process and the MD5 value is also needed to be cracked to get the MAC address of terminal device. Currently cryptography experts have proved the existence of collision of MD5 algorithm, but there is not a quick and effective method to crack it so that MD5 algorithm is still safe enough in application fields. Consequently, the method of using hybrid encryption scheme to encrypt EOC traffic data proposed in this paper can effectively solve the hidden trouble of terminal MAC address impersonation of EOC system.

Conclusion

This paper improve the security of EOC system, related algorithms including ECC and Blowfish is analyzed besides the security defects of Blowfish algorithm. Improving Blowfish algorithm combined with the special conditions of EOC network, the method of using hybrid encryption scheme to encrypt EOC traffic is proposed, which can ensure the data integrity and confidentiality during transmission. Finally the security of the encryption scheme is analyzed. The future work is focus on the security issues of EOC system from other aspects to put forward a complete set of security system and corresponding security solutions and promote the EOC development to be faster and safer.

Acknowledgement

Supported by National Natural Science Foundation of China (61073188)

References

[1] William Stallings. Cryptography and Network Security -Practice Principles[M]. Translated by Liu Yuzhen, Wang Lina, etc. Beijing: Publishing House of Electronics Industry, 2004.

[2] Wang Yinglai. Application of EOC Base on Homeplug AV in the Transformation of Two-way Radio and TV Network in Xinjiang. China Digital Cable TV, 2009 (7): 719-722.

[3] Shang Huayi, Yao Guoxiang, Guan Quanlong. Hybrid Encryption Based on Blowfish and MD5[J]. Application Research of Computers, 2010, 27(1): 231-233.

[4] Zhong Qianchuan, Zhu qingxin. Blowfish Cryptography Analysis. Journal of Computer Application, 2007, 27(12): 2940-2941.

[5] Zhang Zhong. Comparison and Evaluation of EOC Systems of Radio and TV Network. International Broadband Network, 2010(4): 85-88.

[6] He Yimin, Gu Yaping, Zhu Yunbin. Research of Registration Authentication and Communication Encryption in EOC System. Technical Acoustics, 2010, 29(6): 434-435.

[7] Li Zongjie. Research of Data Security in EPON. Jiaozuo: Henan Polytechnic University, 2010.

[8] Kuo-Feng Hwang, Chin-Chen Chang. A Self-Encryption Mechanism for Authentication of Roaming and Teleconference Services. IEEE Transactions on Wireless Communications, 2003, 2(2): 400-407.