*2011 International Conference on Economics and Finance Research*
*IPEDR vol.4 (2011) © (2011) IACSIT Press, Singapore*

# A Private Data Transfer Protocol Verification and Analysis Using Colored Petri Nets

Fengjing Shao
College of Information Engineering
Qingdao University
Shandong, China
sfj@qdu.edu.cn

Sheng Bin
College of Information Engineering
Qingdao University
Shandong, China
binsheng @ qdu.edu.cn

Gengxin Sun
International College
Qingdao University
Shandong, China
sungxmail@gmail.com

Rencheng Sun
College of Information Engineering
Qingdao University
Shandong, China
qdsunstar@163.com

***Abstract*—Focusing on the characteristics of the new high secure computer architecture, an embedded operating system with internal network structure is proposed and designed. The operating system contains two subkernels: local kernel and network kernel. In order to communicate between two subkernels securely, an inter-subkernel private data transfer protocol is proposed and implemented in this paper. Colored Petri Nets is used to verify the private protocol for eliminating weaknesses and inaccuracies of the effective security protocol.**

***Index Terms*—embedded operating system, data transfer protocol, computer architecture, protocol verification, colored petri nets***

## I. INTRODUCTION

With the development of computer network, the network security is becoming more and more important. A series of network security technologies have been used to protect the computer security, such as computer virus scan technology, intrusion detection technology [1,2], software or hardware encryption technology [3,4], secure computer architecture[5], etc.

Based on the traditional architectures of computer such as Von Neumann[6], network and local storage are connected to the same bus, which causes potential security issue because data in local storage might be taken if network intruder has the control of the system bus. Aiming at this security problem, many methods have been proposed, such as TPM (Trusted Platform Module) [7,8], information exchange and encryption[9]. Although these methods enhanced the security of computer, they could not address the fundamental problem due to the vulnerability of Von Neumann architecture.

A new high secure architecture of network computer is proposed by Fengjing Shao[10]. The new computer architecture has a single CPU and two physically isolated high-speed system buses (local bus and network bus), ensure only one bus can be connected to CPU at the same time, a Bus Bridge[11] is designed.

In this new architecture, computer system is divided into tow subsystems. All the network devices and other devices mounted on the network bus form into a network subsystem which connects with the Internet. All the storage devices and other devices mounted on the local bus form into a local subsystem which is isolated from the Internet. So even if the network intruder suddenly gets the whole control of network bus in network subsystem, only the temporary information of the network subsystem is exposed, while the local subsystem is left intact. Thus, hardware-level isolation can effectively ensure the security of sensitive data in local subsystem.

As the new secure computer architecture has one CPU and two subsystems, there should be a befitting operating system to support this architecture. In order to enhance the security of the computer architecture, an embedded operating system with internal network structure is designed, the operating system contains two subkernels: the local kernel and the network kernel. The two subkernels run individually in two subsystems, and they are coordinating relationship rather than subordinate relationship. The relationship between the operating system and the new high secure computer architecture is shown in Fig. 1.

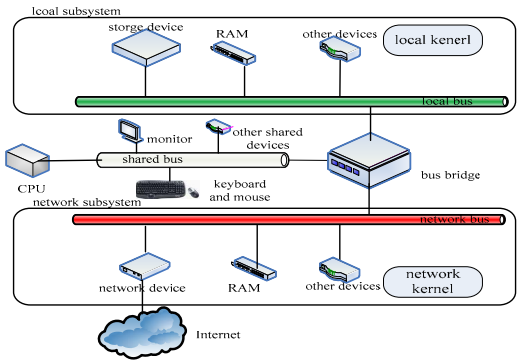

Figure 1. The operating system based on secure computer architecture

## II. COMMUNICATION MECHANISM OF OPERATING SYSTEM

The new high secure computer architecture combined with the embedded operating system can effectively prevent network intrusions from invading local subsystem. But at the same time, it also prevents the data that user gets from Internet in the network subsystem from entering the local subsystem, and the data that user wants to send to Internet in local subsystem from entering the network subsystem. In order to implement communication between two subsystems, there should be a secure communication mechanism of operating system. Currently there are many secure communication technologies in bus systems [12], but none of them can be used in the new high secure computer architecture. In order to communicate between two subsystems securely, an inter-subsystem private data transfer protocol is proposed and implemented. With the private data transfer protocol, data can be transferred between the two subsystems by shared transit cache and the network intrusion can still be isolated from the local subsystem.

In order to prevent the network intrusions from entering local subsystem from network subsystem via shared transit cache, a private inter-subsystem data transfer protocol is used to control the inter-subsystem data transfer.

The private protocol is a connection-oriented protocol, it can provide reliable end-to-end connectivity and ensure data to be transferred safely and inerrably between subsystems.

In the process of transferring data, data is packeted as file which is written into or read from shared transit cache. The private protocol format is in manner of data stream.

The protocol format is fairly straightforward, which is shown in Fig. 2, including File Structure Information (FSI), File Begin Token (FBT), File Size (FS), File Data (FD) and File End Token (FET).


FSI:File Structure Information; FBT:Begin Token; FS:File Size; FD:File Data; FET:File End Token; ET Transfer End Token

Figure 2. Private data transfer protocol format

## III. VERIFICATION OF PROTOCOL USING COLORED PETRI NETS

As a connection-oriented protocol, it must set up end-to-end connection before transferring data. Because of the demand of the new secure computer architecture, when using the private protocol for transferring data, both ends of connection should be identity authentication for validation of identity. A switch of transit cache can be used to control whether setting up connection of both ends, for the connection request which do not pass identity authentication, the switch would close transit cache and the connection request would be refused. It requires the establishment of a security authentication mechanism to meet the demand. In the private data transfer protocol, connection management based on signature verification is proposed and designed.

In the world of designing data transfer protocols, verification is a crucial step to eliminate weaknesses and inaccuracies of effective protocols. There are many models to verify data transfer protocols, including, Finite State Machines (FMS), Colored Petri Nets (CP-Nets), Cryptographic Protocol Analysis Language Evaluation System (CPAL-ES), etc. In this paper, we use CP-Nets model to design and verify the private data transfer protocol, and show how it can be used to analyze and improve the private protocol.

There are two courses for using CP-Nets: forward or backward analysis. As Ayda and Moon stated [13,14], the backward state analysis of a data transfer protocol includes three steps:

- Generating an explicit CP-Nets specification for the protocol;
- Identifying insecure states that may or may not occur;
- Performing a backward state analysis to test if each insecure state is reachable or not.

Our verification model mainly depends on their work with some minor changes and improvements. Our model consists of the following steps:

- Describe the protocol in a CP-Nets form;
- Write Acceptance Check Steps (ACS);
- Describe the intruder model;
- Propose and analyse the modified protocol.

Digital signature technology is proposed on the basis of public-key cryptosystem, It can ensure that only the sender can produce information which can not be faked by others, sender uses private-key to sign the message which would be sent, the information which had been signed is a proof of authenticity for a message which is sent by sender. Another important function of digital signature is to verify the integrity of data, because digital signatures can prevent third-party from forging or altering message which had been signed. The private protocol use digital signature technology based on public-key for adding authentication mechanism in the connection management process, therefore, security of protocol is increased and high security requirements of data transfer is met.

The private protocol adopts digital signature technology based on RAS algorithm. The first researchers to discover and publish the concepts of Public-Key Cryptography(PKC) were Whitfield Diffie and Martin Hellman[16], and The Diffie-Hellman key agreement protocol (also called exponential key agreement) was developed, The protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. The Diffie-Hellman key agreement protocol provided an implementation for secure public key distribution, but didn't implement digital signatures. After reading the Diffie-Hellman paper[15], three researchers at MIT named Ronald Rivest, Adi Shamir, and Leonard Adleman (RSA) began searching for a practical mathematical function to implement a complete PKC approach[16]. After working on more than 40

candidates, they finally discovered an elegant algorithm based on the product of two prime numbers that exactly fit the requirement for a practical public key cryptography implementation.

The basic protocol of digital signature based on RSA is very simple. Roughly speaking, the protocol scenario is as follows:

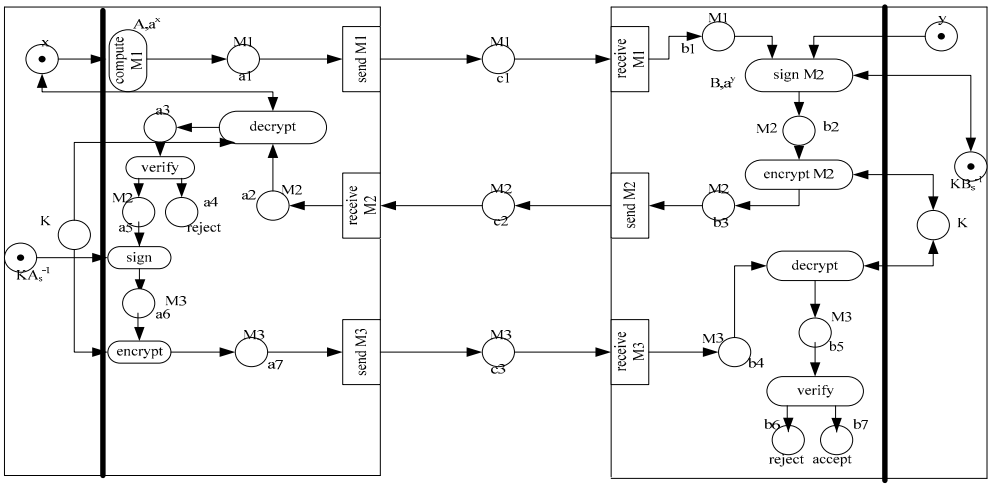


Figure 3. CP-Nets model for the private protocol

- The protocol initially is based on RSA in the first message from entity A to entity B. The entity A generates a random value x and compute the term $\alpha^x$ mod P where both α and P are known integers values for the two entities.
- In second message of negotiation, entity B generates a random value y, computes the shared key K. It sends an encrypted message enciphered with the computed key. The encrypted message itself is a signed message of B's private key. Upon entity A receiving the second message, the shared key is computed and it can verify that the signed message is from entity B after decrypting it with B's public key embedded in the message.
- Finally, the entity A signs a message with its private key. Then it sends the message encrypted with the shared key K.

The protocol messages as follows:

- A→B: A, $\alpha^x$ mod P
- A←B: $\alpha^y$ mod P,$E_k(S_{Bs}(\alpha^x, \alpha^y),B_p))$
- A→B: $E_k(S_{As}(\alpha^x, \alpha^y),A_p))$

Steps of protocol analysis is described using Colored Petri Nets as follows:

Step 1: model the private protocol using CP-Nets illustrated in the Fig. 3.

M1: A, $\alpha^x$ mod P

M2: $\alpha^y$ mod P,$E_k(S_{Bs}(\alpha^x, \alpha^y),B_p))$

M3: $E_k(S_{As}(\alpha^x, \alpha^y),A_p))$

Step 2: apply the Acceptance Check Step (ACS) to STS messages. We note that the general man-in-middle intruder can exist between the two entities or client-server. As the intruder works in the model, we forward to the step3. It is clear that the intruder cannot get the shared key between the two entities, but the intruder owns a key that can be shared in the secure transition between the two sides. The weakness of this model depends mainly on that both sides do not verify each other or there is no certification for the entities.

Step 3: add the proposed intruder side in the model as in the Fig. 4.

M1: A, $\alpha^x$ mod P

M1$^{\backslash}$: A, $\alpha^z$ mod P

M2: $\alpha^y$ mod P,$E_{k2}(S_{Bs}(\alpha^z, \alpha^y),B_p))$

M2$^{\backslash}$: $\alpha^z$ mod P,$E_{k1}(S_{Bs}(\alpha^z, \alpha^x),B_p))$

M3: $E_{k1}(S_{As}(\alpha^x, \alpha^z),A_p))$

M3$^{\backslash}$: $E_{k2}(S_{As}(\alpha^z, \alpha^y),A_p))$

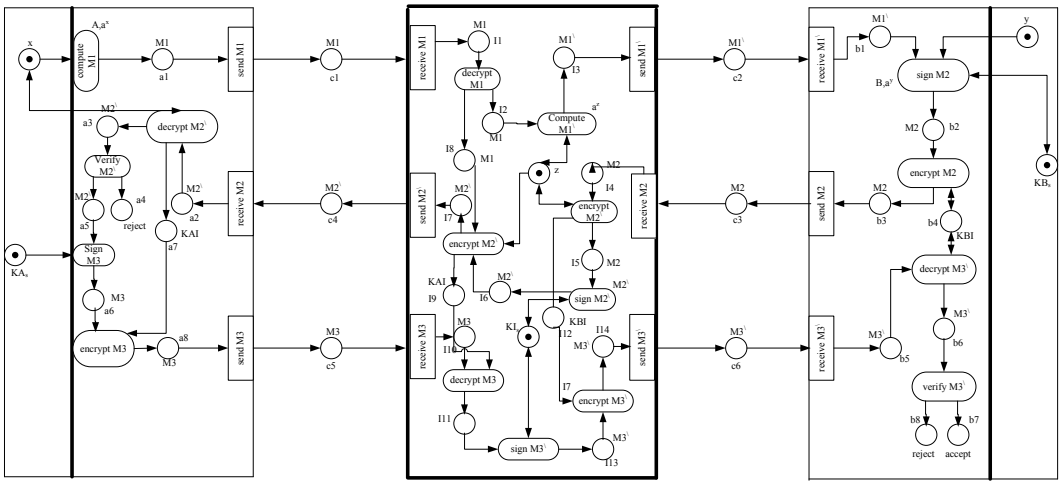


Figure 4. CP-Nets model for intuder in the private protocol

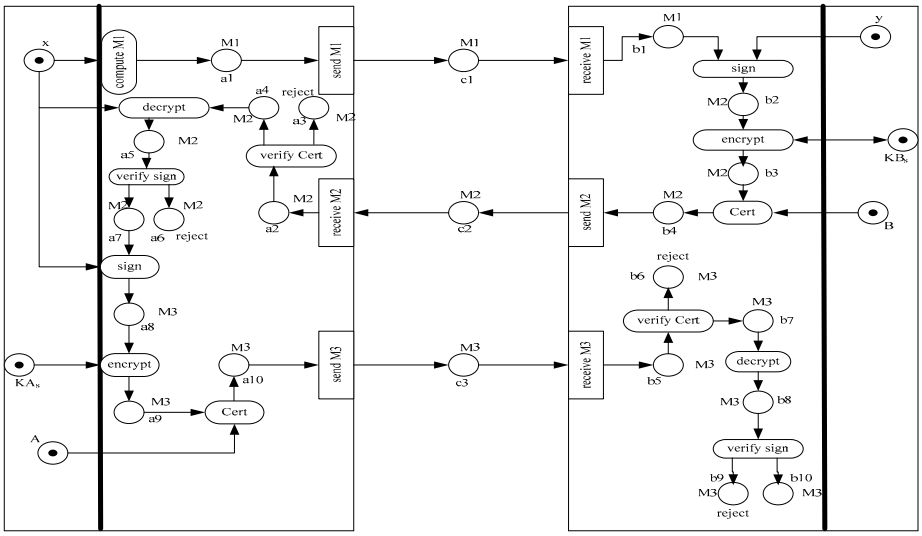


Figure 5. CP-Nets model for the modified private protocol

By analyzing the private protocol as in Fig. 4, we find that man-in-middle attack has the ability to direct the negotiation between communications of both ends. The intruder shares K1 with sender and K2 with receiver, so the intruder can modify the outgoing messages from sender to receiver and vice versa.

From Fig. 4, the private protocol and the attack can be explained below:

- The intruder intercepts the message M1, stores everything and sends it's own data instead of sender's data to the receiver as in $M1^{\backslash}$.
- The receiver then gets the shared key K2 with the Intruder. It then signs a message by it's private key, encrypts it with the shared key, and supposes to send M2 to sender.
- The intruder intercepts M2 then stores receiver's data and decrypts it to get the receiver public key then verifies the signature. Also, the intruder signs a new message using it's secret key, encrypts it with the shared key K1 with the sender, and sends it to the sender.
- The sender receives the message $M2^{\backslash}$, decrypts it to get the public key from it, and validates the signature in the message for acceptance or rejection. Upon the above, the sender signs, encrypts a new message M3, and believes that it could be sent to the receiver.
- The intruder intercepts the message M3, decrypts to get the public key, and validates the signature. Upon the above, the intruder can fabricate the new message $M3^{\backslash}$ and impersonate the receiver by it.

- The receiver decrypts M3\ and validates the signature. Upon that, it decides to accept or reject the negotiation.

From the analysis above, it is clear that the intruder can now eavesdrop, modify or delete all subsequent messages. To prevent such attacks, each communication end should certify the outgoing messages and verify the incoming messages, and the certification must be done with all exchanges between the sender and the receiver.

The modified private protocol is specified as follows:

- The sender A selects a random secret integer $r_A$ and sends to receiver B the message M1. Upon receiving M1, B selects a random secret integer $r_B$, computes the shared secret $K = (\alpha^{rA})$ , and sends message M2 to A.
- Upon receiving M2, A uses Cert(B) to verify the authenticity of B's signing key $P_B$, verifies B's signature on the message $(\alpha^{rA}, \alpha^{rB})$, computes the shared secret $K = (\alpha^{rB})^{rA}$ , and verifies the MAC on $S_B(\alpha^{rA}, \alpha^{rB})$ . A then sends message M3 to B.
- Upon receiving M3, B uses Cert(A) to verify the authenticity of A's signing key $P_A$ , verifies A's signature on the message $(\alpha^{rA}, \alpha^{rB})$, and verifies the MAC on the $S_A(\alpha^{rA}, \alpha^{rB})$. If at any stage a check or verification performed by A or B fails, then that entity terminates the protocol run, and rejects.

Fig. 5 illustrates an intruder between the sender and the receiver. once again, we study the case of man-in-middle attack. We show that the intruder can not modify the outgoing messages from the sender to the receiver and vice versa.

M1: A, αrA

M2: Cert(B), αrB, SB(αrA, αrB), MACk(SB(αrA, αrB))

M3: Cert(A), SA(αrA, αrB), MACk(SA(αrA, αrB))

By analyzing the modified private protocol, we find that man-in-middle attack does not have the ability to control the negotiation between the sender and the receiver. The intruder neither shares K1 with the sender nor K2 with the receiver. Also, presentation using CP-Nets, Fig. 6 shows that the modified private protocol is secure.

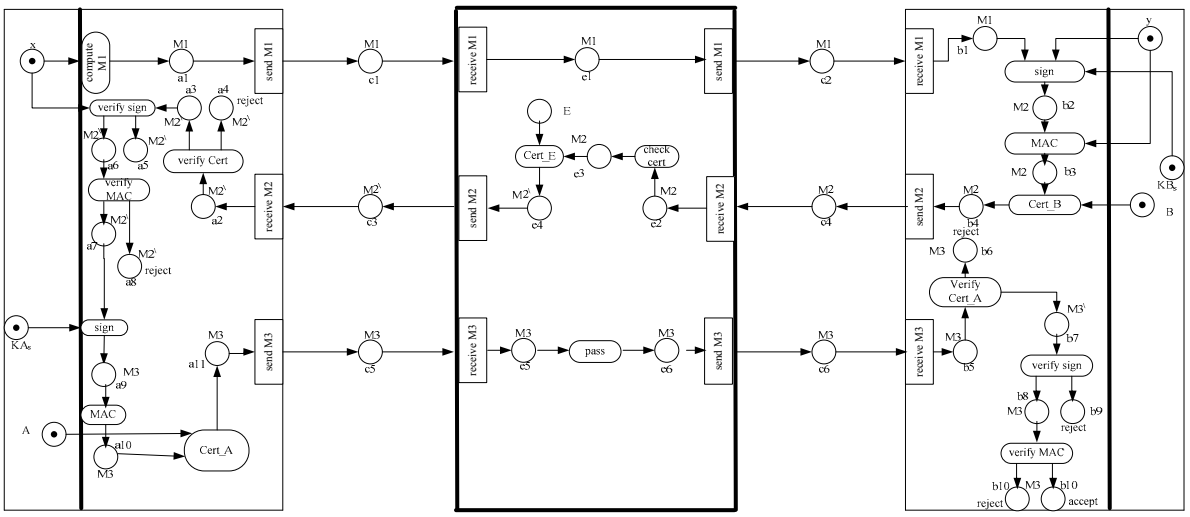


Figure 6. Modified private protocol intruder model

## IV. . CONCLUSION

In the new high secure computer architecture, in order to prevent the network intrusions from entering local subsystem from network subsystem via transit cache, in the embedded operating system, a inter-subkernel private data transfer protocol is designed and used to control the inter-subkernel data transfer. We use Colored Petri Nets to verify and improve the private data transfer protocol and prove that the private data transfer protocol can ensure data to be transferred safely and inerrably between subkernels.

## ACKNOWLEDGMENT

This work was supported in part by the High-Tech Research and Development Program of China (863 Program) (2006AA01Z110) and and the Development Project of Science and Technology of Qingdao (09-2-3-19-chg).

## REFERENCES

[1] Abdoul Karim Ganame, Julien Bourgeois, Renaud Bidou and Francois Spies, "A global security architecture for intrusion detection on computer networks," Computer & Security, Vol. 27, pp. 30-47, March 2008.

[2] Ben Rexworthy, "Intrusion detections systems – an outmoded network protection model," Network Security, Vol. 2009, pp. 17-19, June 2009.

[3] Niansheng Liu, Donghui Guo, "Security analysis of Public-key Encryption Scheme Based on Neural Networks and Its Implementing, " International Conference on Computational Intelligence and Security, pp. 1327-1330, 2006.

[4] Prayag Narulaa, Sanjay Kumar Dhurandhera, Sudip Misrab and Isaac Woungangc, "Security in mobile ad-hoc networks using soft

encryption and trust-based multi-path routing," Computer Communications, Vol. 31, pp. 760-769, March 2008.

[5] Igor Podebrad, Klaus Hildebrandt, Bernd Klauer, " List of Criteria for a Secure Computer Architecture," 2009 Third International Conference on Emerging Security Information, Systems and Technologies.

[6] John von Neumann, First Draft of a Report on the EDVAC. Moore School of Electrical Engineering, University of Pennsylvania, June 30, 1945.

[7] Trusted Computing Group (TCG), Trusted Platform Module (TPM) Specification Version 1.2 Revision 103, https://www.trustedcomputinggroup.org/specs/TPM/, July, 2007.

[8] IBM Research Report, the role of TPM in enterprise security. 2004.

[9] Chuanjin, Wei,Qingbao, and Li,Yan Bai, "The research and realization of network teriminal information switch mechanism", Control &Automation, Vol. 21, 2005.

[10] Shuangbao Wang, Fengjing Shao, and Robert S.Ledley, "Connputer—a framework of intrusion-free secure computer architecture", Security and Management 2006, pp. 220-225, 2006.

[11] Tiedong Wang, Fengjing Shao, Rencheng Sun, He Huang. "A hardware implement of bus bridge based on single CPU and dual bus architecture," International Symposium on Computer Science and Computational Technology, Shanghai, China, December 2008.

[12] Sascha Mühlbach, Sebastian Wallner. "Secure communication in microcomputer bus systems for embedded devices," Journal of Systems Architecture, Vol. 54, pp. 1065-1076, November 2008.

[13] A. M. Basyouni, "Analysis of Wireless Cryptographic Protocols," Master's Thesis,Queen's University Kingston, Ontario, Canada, 1997.

[14] HeeChul Moon, "A study on formal specification and analysis of cryptographic protocols using Colored Petri Nets," Master's Thesis, Kwangju institute of science and technology, Korea. 1998.

[15] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," Information Theory, Vol 22, pp. 644-654, November 1976.

[16] RL Rivest, A Shamir, L Adleman , "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol 21, pp.120-126, 1978.