Proceedings of the 7th International Conference on Applied Informatics
Eger, Hungary, January 28–31, 2007. Vol. 2. pp. 147–153.

The extension of CNS-logic for multi-channel protocols

Péter Takács

University of Debrecen, Faculty of Health College
e-mail: vtp@de-efk.hu

Abstract

The purpose of this paper is to examine multi-channel protocols. We present a way of building a logical theory for multi-channel protocols.

Keywords: cryptographic protocols, multi-channel communication, logical theory of protocols

MSC: 94A40, 94A60, 68P30

1. Introduction

The purpose of this paper is to generalize the result of T. Coffey, P. Saidha and T. Newe (CSN-model, see [1, 2]). Our aim is to present in short how the logical theory of multi-channel protocols can be built up.

- In the first part of the lecture we want to introduce what multi-channel protocols are.
- In the second part we want to present how we can examine the security protocols with the theory of mathematics and mathematical logic. We present the brief history of formal verification.
- In the third part we describe the CSN model.
- In the fourth part of the lecture we give a generalization of CNS logic able to deal with multi-channel protocol. We apply this method to MANA I. protocol. With this protocol the users can verify that the used devices share exactly the same data items.

We employ the notation of the CSN-model, and write only the used and changed elements of the logical system.

2. Multi-channel protocols

If we examine the traditional secret-key cryptographic systems, we can find the principle of multi-channels. We can share a security key across a protected channel to the partners, afterwards we can send encrypted messages across a public channel. Using more than one channel in a security protocol is not a new idea. Nowadays a user can use many comunication devices (for example: mobile phone with camera, internet pages, e-mail, fax, and so on). These examples mean using more than one channel in the course of communication, too. A new research area is formed to examine the possibilities. We take it that this research area will expand cryptography with many elements and ideas ([3]).

2.1. The MANA I. protocol

The initialisation of cryptographic devices is a procedure of equipping the components with suitable cryptographic parameters. This process sometimes is called *imprinting*. The next MANual Authentication Protocol (MANA) is an initialization part of many other protocols (see [4, 5]). With this simple protocol, the owner of both devices can verify that the two equipments share the same data exactly.

The notations are the next. Let A, B denote the components of the protocol (the two participant devices). Let K denote key. $m_K(X)$ is the check-value computed using key K and data string X. m is generally one-way hash function (see [4]). Let ch_1, ch_2 are the channels with distinct properties and t_i denotes the time. We assume device A has a display and device B has a keypad in this protocol.

The steps of protocol MANA I. are the next.

1-2. steps A and B try to agree on data string D. They use the public (wireless) channel ch_1. A sends D_A to B in time t_1 and B receives D_B in time t_2. This channel is unprotected. This notation postulates the possibility $D_A \neq D_B$.

3-4. steps Device A generates random key K and the check-value $m_K(D_A)$. Hereupon device A sends the check-value $m_K(D_A)$ and K to the device B using the protected channel ch_2 in time t_3. B receives the message in time t_4.

5. step Device B recomputes the value $m_K(D_B)$ with the received parameters and compares it with the value of the received $m_K(D_A)$. If the result of comparsion is true, device B sends sign $'1'$ to the device A using the protected channel ch_2 in time t_5. B sends sign $'0'$ otherwise.

6. step Device A receives the sent sign in time t_6. So A knows the comparsion made by B.

Notations:

- Detailed analysis of the protocol scheme can be found in [4]. It analyses the possible strategies of attackers and the problem of short check-values, too.

3. Examination of security protocols

Formal methods can be used in various phases of the design of a cryptographic protocols. These phases are specification, construction and verification. The verification is the most developed area of cryptographic protocols. We can classify formal verification into four types - using general modelling tools, using expert systems, using modal logics and using algebraic tools (see [6]).

The general sheme for analyzing cryptographic protocols with modal logic tools are the following. At first: we formalize the protocol (namely we decribe steps of the protocol with formal logic). Secondly: we specify the initial assumptions. Thirdly: we specify the goals of the protocol. At the fourth step: we apply the logical postulates. The fifth step is: comparing the results with the goals. The main aim is to deduce the protocol goals from formal protocol and from initial assumptions.

In this scientific area the first momentous result was BAN logic in 1990 (see [7]). BAN logic has been extended in many directions (see [6]). Next we examine the Coffey-Saidha-Newe (CSN) model. It was presented in two scientific papers (see [1, 2]). The firs paper described the model of public-key systems and the second paper investigated the secret-key systems.

Next we will sum up the CSN model and afterwards extend this model by the idea of multi-channel.

4. The CNS model

The language of CSN model includes formal signs for describing statements, entities, functions and operators.

For example: ENT the set of all possible entities in the protocol $ENT = \{\Sigma, \Psi, \ldots\}$; K propositional knowledge operator of Hintikka - $K_{\Sigma,t}x$ means that Σ knows statement x at time t; L knowledge predicate - $L_{\Sigma,t}x$ means Σ knows and can reproduce object x at time t; B belief operator - $B_{\Sigma,t}x$ means Σ believes at time t that statement x is true; S emission operator - $S(\Sigma, t, x)$ means Σ sends message x at time t; R reception operator - $R(\Sigma, t, x)$ means Σ receives message x at time t.

This system uses the classical logical connectives: conjunction, disjunction, complementation, implication. We can use the universal and existential quantifiers, sign of the membership of a set and set exclusion and the symbol of logical theorem.

The logic incorporates rules of inference ($R1$ to $R7$). For example $R1$ is the Modus Ponens, $R2$ consists of the Generalization rules, etc.

$$R3: \ from\ (p \wedge q)\ infer\ p$$

The logic also includes standard propositional rules of natural deduction. Two types of axioms are used in this logic: logical and nonlogical axioms.

Logical axioms are general statements valid in arbitrary models while nonlogical axioms are system specific. In this case they apply to public-key systems

and secret-key systems. These axioms describe emission and reception of messages and use of encryption and decryption on these messages.

The original Coffey-Saidha logic ($A1$ to $A10$) is capable of analysing a wide variety of public key cryptographic protocols (see [1, 2]). The second part of the axioms ($A11$ to $A15$) enables to describe symmetric key protocols (see [2]). For example axiom $A3(a)$ is the following

$$A3(a) \quad \exists t\ \exists x\ \exists i\ \ i \in \{ENT\}\ L_{i,t}x \rightarrow \forall t',\ t' \geqslant t\ \ L_{i,t'}x.$$

This means that knowledge once gained cannot be lost.

$$A5(a)\ \ \exists t\ \exists x\ \ (S(\Sigma, t, x) \rightarrow L_{\Sigma,t}x \wedge \exists i, i \in \{ENT/\Sigma\}\ \ \exists t',\ t' > t\ \ R(i, t', x)).$$

This means if Σ sends a message x at time t, then Σ knows x at time t and some entity i other than Σ will receive x at time t' subsequent to t. And

$$A6(a)\ \ \exists t\ \exists x\quad (R(\Sigma, t, x) \rightarrow L_{\Sigma,t}x \wedge \exists i,\ i \in \{ENT/\Sigma\}\ \ \exists t',\ t' > t\ \ S(i, t', x)).$$

This means: if Σ receives a message x at time t, then Σ knows x at time t and some entity i other than Σ has sent x at time t' prior to t.

5. The extension of the CSN-model

We can apply the CSN system to a wide area of protocols, but we do not use it in case of multi-channel protocols. We extend the original CSN model.

5.1. The language

- Let denote the channels ch_1, ch_2, ... , ch_i.
- ENT_{ch_i} denote the entities who can use the channel ch_i. $ENT_{ch_i} \subseteq ENT$.

We need to sign the channels in the formalization: extend the CSN logic with channel signs and examine the result of this extension in system of axioms. We need to describe the channel properties in the system, too.

- Let denote $CH(ch_i, sec)$ channel ch_i secret or protected channel and let denote $CH(ch_i, pub)$ public channel. If a channel is protected we can set the users can use the channel: ENT_{ch_i}.

If we look into the system we see that we have to introduce a channel index to reception predicate R and to emission predicate S. The original R operator is $R(\Sigma, t, x)$. It means entity Σ receives message x at time t.

- Let the new R operator be the next: $R(ch_i, \Sigma, t, x)$. It means entity Σ receives message x at time t from the channel ch_i.

The original S operator is $S(\Sigma, t, x)$. It means Σ sends message x at time t.

- Let the new S operator be the next: $S(ch_i, \Sigma, t, x)$. It means entity Σ sends message x at time t to the channel ch_i.

5.2. Rules of inference

We do not change the set of rules of inference.

5.3. Axioms

We have to apply the new additions only in the axioms $A5$, $A6$, $A8$, $A12$, and $A15$. Due to the lack of space we do not list the full axiom system. We can find these in [1, 2]. The used axioms in this paper are the next.

If channel is secret only the authenticated users can use it ($A5(a)$ and $A6(a)$ are the original axioms).

$$A5(b)\ \exists t \exists x\ S(ch_i, \Sigma, t, x) \rightarrow L_{\Sigma,t}x \wedge \exists i, i \in \{ENT_{ch_i}/\Sigma\}\ \exists t',\ t' > t\ \ R(ch_i, i, t', x)$$

$$A6(b)\ \exists t \exists x\ R(ch_i, \Sigma, t, x) \rightarrow L_{\Sigma,t}x \wedge \exists i, i \in \{ENT_{ch_i}/\Sigma\}\ \exists t', t' > t\ \ S(ch_i, i, t', x)$$

We need a new axiom: every message is send only once.

$$A16\quad \exists t \exists x\ \ S(ch_i, i, t, x) \rightarrow \neg(\exists t', t' > t\ S(ch_i, i, t', x))$$

6. The examination of the MANA I protocol

With these extensions we can start the examination of protocol MANA I.

6.1. Logic descrition of the MANA I

The formal protocol is the next:

1. step $S(ch_1, A, t_1, D_A)$

2. step $R(ch_1, B, t_2, D_B)$

3. step $S(ch_2, A, t_3, \{K, m_K(D_A)\})$

4. step $R(ch_2, B, t_4, \{K, m_K(D_A)\})$

5. step $S(ch_2, B, t_5, x)$

6. step $R(ch_2, A, t_6, x)$

6.2. Initial assumptions

In addition we can describe the channel properties and other important properties of the protocol in the 'Specification of the initial assumptions' phase.

1. $CH(ch_1, pub)$, $CH(ch_2, sec)$
2. $ENT_{ch_2} = \{A, B\}$

3. We use the m function and $\forall x, y\ (m_K(x) = m_K(y) \rightarrow x = y)$.
4. $L_{\Sigma,t}x \ \wedge \ L_{\Sigma,t}y \ \rightarrow \ L_{\Sigma,t}m_x y$. This means Σ can use the m function.
5. $L_{\Sigma,t}x \ \wedge \ L_{\Sigma,t}y \ \rightarrow \ L_{\Sigma,t}(x = y) \vee L_{\Sigma,t}(x \neq y)$. This means Σ can compare two data strings. Let $'0'$ denote the case $x \neq y$ and $'1'$ the case $x = y$. So Σ send $'0'$ if the compare fail and send $'1'$ if the compare true.

6.3. The goal of the protocol MANA I

Finally by the extension of CSN-model we can state and prove our theorem.

Theorem 6.1. *Suppose the last step in protocol MANA I device A receives* $'1'$ *sign then the parameters in the two devices are equal. We can rewrite this theorem with logical signs:*

$$R(ch_2, A, t_6, '1') \rightarrow D_A = D_B$$

Proof. We can separate the proof into two phases.

First phase. The starting point is $R(ch_2, A, t_6, '1')$. We can apply the first initial assumption and the Axiom $A6(b)$:

$$R(ch_2, A, t_6, '1') \rightarrow L_{A,t_6}('1') \wedge \exists i, i \in \{ENT_{ch_2}/A\} \exists t', t' < t_6 \ S(ch_2, i, t', '1').$$

We use the second initial assumption $ENT_{ch_2}/A = \{B\}$ and rule R3 to take

$$\exists t', t' < t_6 \ \ S(ch_2, B, t', '1').$$

According to Axiom $A16$ and in addition B sends messages only once in the ch_2 secret channel, so it must be $t' = t_5$. Hereby $S(ch_2, B, t_5, '1')$. Namely B sends $'1'$ sign to A at time t_5.

Second phase. In the third step of protocol A sends message to B:

$$S(ch_2, A, t_3, \{K, m_K(D_A)\}).$$

We can apply the Axiom $A5(b)$ and $A3(a)$. Like in the first phase we can prove

$$L_{B,t_5}K \quad \wedge \quad L_{B,t_5}m_K(D_A).$$

B receives D_B in the second step. By the Axiom $A6(b)$

$$L_{B,t_5}D_B$$

We can use the fourth initial assumption. A knows and can repoduce the check-value

$$L_{B,t_5}m_K(D_B)$$

and B can compare the two check-values $m_K(D_A)$ and $m_K(D_B)$. But B sends $'1'$ as result of the comparison, so $m_K(D_A) = m_K(D_B)$ must be true. On the other hand - refer to the third initial assumption - it may be true only if $D_A = D_B$. $\square$

7. Summary

We examined multi-channel protocols. We complemented the CSN model with a mark-system of multi-channel protocols, with new axioms and verified the MANA I protocol successfully.

We think the idea of the multi-channel protocols will extend the traditional cryptographic protocol model. It can be used to describe more realistic protocols used nowadays in banking and communication sector. If we examine this area we can construct new useful and interesting cryptographic protocols.

Acknowledgements. The author would like to thank Sándor Vályi for consulting the proof of the protocol.

References

[1] Coffey, T., Saidha, P., Logic for verifying public-key cryptographic protocols, *IEE Proc. Computers and Digital Techniques* Vol. 144. No. 1., (1997), 28–32.
`http://www.ece.ul.ie/Research/DataComms/papers/CS97\_IEE\_CompDigTech\_Logic.pdf`
Visited: 2007.05.14.

[2] Newe, T., Coffey, T., Formal verification logic for hybrid security protocols, *Comput. Syst. Sci. and Eng.*, Vol. 1 (2003), 17–25.
`http://www.ece.ul.ie/Research/DataComms/papers/NC03\_CSSEJournal\_Formal\_Logic.pdf`
Visited: 2007.05.14.

[3] Wong F-L., Stajano F., Multi-channel protocols, A, *Proceedings of Security Protocols Workshop, LNCS, Springer-Verlag* (2005).

[4] Gehrmann, C., Mitchell, C. J., Nyberg K., Manual authentication for wireless devices, *Cryptobytes*, 7(1) (2004), 29–37.

[5] Goeman, S. (ed.), Specification of Prototypes - D11, IST - 2000 - 25350 - SHAMAN *Public Report*, (2002), 26-29.

[6] Buttyán, L., Formal methods in the design of cyptographyprotocols (State of the Art), *EPFL SSC Technical Report*, No.SSC/1999/038. (1999).

[7] Burrows, M., Abadi, M., Needham, R., A Logic of Authentication, *Research Report 39.*, Digital System Research Center (1989).

Péter Takács
Sóstói Street 2-4.
H-4400 Nyíregyháza
Hungary