Communication Security Problem and Solution In Safety-Related System

Yan Song1,2, Tianran Wang1, Aidong Xu1, 1. Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China
Kai Wang1 and Zhijia Yang1 2. Graduate University of Chinese Academy of Sciences, Beijing 100039, China

Abstract—Security in control system is an important issue. To safety-related system it is more critical. A safety-security communication measure to counteract nature or intend data modification is proposed, which based on refining characters of data with MD5 approach. And to some low speed network a 2-refine approach is introduced which based on MD5 and CRC. A confidential communication to secure all the data is proposed, too. Furthermore, the key distribution approaches named KDC and DKD are introduced.

Keywords- MD5, Safety-related system, Security

I. INTRODUCTION

Traditional control systems involve a “protection system” which is well known as safety-related system[1], such as Emergency Shutdown system (ESD) and other type protection system. Safety-related system aimed at how to reduce the risk and hazard to a rational and acceptable level. Meanwhile the safety-related system can’t protect the system and Equipment Under Control (EUC) from hacking or attacking.

The security problem of industrial control system has not got sufficient recognition for a long time, until the “Stuxnet” occur and destroyed some uranium enrichment infrastructure in Iran. A fact is proofed clearly that a well designed computer worm program or virus may intrude some target control network even if the control network is separate in physical.

Industrial control system’s security is an important issue in modern plant automation, because most control system in a bigger plant no more than an isolated island, but a subsystem of a bigger network. Protecting safety-critical systems traditionally relies on concepts that presume a probabilistic distribution for failures that does not hold for failures that does not hold for intelligent attacks.[2]

How to protect the whole network in a plant or even in an enterprise scope is more and more critical. Hacking and attacking may lead to critical data disclose, equipment damage and human injured. In plant automation control network, the safety-related system part (if there is) is the critical part, because the malfunction of safety protection system may lead a disaster, such as blast, poison gas leak and so on.

The information security problem is concern with two aspects: system security and network security [3]. Security in control system is same with information system. The security problem in safety-related system is discussed latter and some novel communication approach and system architecture are proposed.

II. SECURITY MEASURES IN SAFETY-RELATED SYSTEM

Security in safety-related system is an important issue in secure the control system [4]. The safety approach and security approach are developed by separated technical group, and less integration effort was made at the beginning. Security approach and safety approach have some intersection here, but there are more different between each other.

According to IEC 61784-3[5], safety communication must make sure the data deliver by user layer should be received no change by corresponding peer. An untrusted communication channel named black channel which consisted in the communication stack software, the physical wires and hardware, as shown in following.

The “black channel”[3] means there are no guarantee for correct delivering between two corresponding communication peers. The data may be changed 1 bit or more because of disturbance or internal fault. IEC 61784 give us a series
technical approach to conquer this weakness, they are known as safety approach. The safety approach may include Sequence No., Time Stamp, Relationship Key, CRC code, the communication faults can be conquered by them as following.

<table>
<thead>
<tr>
<th>TABLE I. SAFETY APPROACH AND CORRESPONDING ERROR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repetition</td>
</tr>
<tr>
<td>Repetition</td>
</tr>
<tr>
<td>Deletion</td>
</tr>
<tr>
<td>Insertion</td>
</tr>
<tr>
<td>Disorder</td>
</tr>
<tr>
<td>Corruption</td>
</tr>
<tr>
<td>Delay</td>
</tr>
<tr>
<td>Masquerade</td>
</tr>
</tbody>
</table>

As far as we knew, there are some intersection approach between safety and security. Relationship Key makes sure the data is sending and receiving by right role. The CRC ensure the data is not changed when sending. Sequence No. and time stamp protect the time order between originator and responder. But all safety approaches haven’t token attacking and hacking into account. CRC can be recalculated online after changing the data. SN and TP can be changed easily because they are sent with plant text and no one-way data consistency checking, where mean if you don’t have the “secret”, you can’t calculate the consistency checking code, such as MAC (Message Authentication Code) or HMAC (Hash Message Authentication Code). If the relationship key have no well way to update timely, the threat of key disclose is growing.

The safety and security approach must be integrated well and only by this way the safety-related system is “safe” enough.

A. Direction HMAC measure in safety communication (1-refine approach)

Message Authentication Code (MAC) is an authentication technology, MAC hires a crypto algorithm to create a fixed size short data block, which is a “character” of the message, the sender make MAC and send them with raw message, and receiver get the data and recalculate the MAC according to raw data. If they are equal, the message is right and sent by the unique sender.

The classic application measure is displayed as following:

\[ A \rightarrow B : Msg \ || \ C(Msg, Key) \] (1)

Formula (1) provides a plant text transmitting and a MAC, A and B share the key and no confidential is provided.

\[ A \rightarrow B : E_{k1}(Msg) \ || \ C_{k1}(E_{k1}(Msg, k1), k2) \] (2)

Formula (2) provides a cipher text transmitting and a MAC, A and B share the Key1 and Key2, confidence and authentication are provided by this measure.

\[ A \rightarrow B : E_{k1}(Msg, K2) \ || \ C_{k1}(E_{k1}(Msg, K2), K1) \] (3)

Formula (3) show an alternative way to achieve confidence and authentication, all information are transmitted by cipher and MAC inside.

We can choice a method above, but all of them need a crypto algorithm, such as DES or AES or 3-DES, which are all time consumed.

MAC is based on crypto algorithm and there are some reason that crypto algorithm is not very acceptable:

1. The processing speed is slow and CPU-time cost is huge, industrial control device’s ability is not very strong as PC system.
2. Some crypto algorithm is protected by patient or by the country.
3. Popular crypto algorithm is designed for big data block, not for protocol data unit.
4. Efficient crypto algorithm is difficult to obtain.
5. May offend the real time restrict of industrial control system.

Another measure can be taken as an authentication approach, the hash function.

Hash function is a one-way function, which mean from A, calculate hash (A) is easy but from hash (A) deduce the “A” is very difficult, which named computationally infeasible. The input of hash function is scalable message M, the output is a fix-size hash code about M. The classic hash algorithms are MD5, SHA-1 and RIPEMD-160.

Authentication based on hash function is faster than one based on crypto algorithm.

In the industrial control context, hash-based message authentication code is recommended according former discuss.

The hash algorithm we choice is MD5, which is a fast one in common hash algorithm.

As figure 2 shown, original messages may include SN, Time Stamp and other safety communication measures, but HMAC is used as error-detecting code, and attach at whole message to be send.

The 1-refine characters approach mean refine the data characters by HMAC only. Nature or intend modification of data can be detected well by HMAC. 1-refine characters approach safe-sec communication way is shown as following:

\[ Msg = Header \ || \ Data \ || \ SN \ || \ TS \ || \ HMAC(Header \ || \ Data \ || \ SN \ || \ TS, Ks) \] (4)

In formula (4), Ks is a private communication Session Key, which is described in Part C. According to table 1 and formula (4), 1-refine character approach based communication way can
conquer the following errors: Repetition, Deletion, Insertion, Disorder, nature data Corruption, delay, Masquerade and intend data modification.

CRC is replaced by HMAC, but there are some problems still. HMAC based on MD5 will produce 128 bit or 16 Bytes MAC, meanwhile CRC 16 is 16 bits and CRC-32 is 32 bits or 4 bytes. A long error detect code may lead to a more consume of network resource and may reduce the real time ability. But in some critical application, a predictable delay may be acceptable than un-security. Cause once the delay time and jitter’s principles are known, there are always counteractive measures can be taken. In modern control device, especially smart control devices, the CPU’s ability usually is redundant. Classical CPUs are ARM7, ARM9 and so on. ATMEL ARM7TDMI CPU can handle MD5 algorithm well. HMAC will cost more time of CPU than CRC, but the time cost is not big between HMAC and CRC. Direct using HMAC is recommended to some high speed control network, because the extra 16byte can be ignored to high speed control network such as real time Ethernet. The following diagram show the CRC based safety measure and HMAC based safety security measure.

![Diagram](image)

**B. In-Direction HMAC Safe-Sec Measure (2-refine character approach)**

As discussed above, some high speed control network can use HMAC measure directly, because there is enough transfer ability to deal with the additional 14 bytes than CRC measure. But in CAN bus, Foundation Fieldbus and other low speed control network, the additional 14 bytes are too big to accept. CAN bus data frame has 16 bytes or 128 bits only, if the HMAC is put in, there no space for data and frame control word. To FF H1 or FF SIS, the situation is better, but additional 14bytes are a heavy burden, too.

It is well known that both CRC and MAC can refine the characters of data to be transferred, and because CRC can be calculated online, that mean if an intruder modified the data and recalculate the CRC according to new data, the receiver can’t tell if it was modified or raw. An acceptable measure is “twice refine characters of information”. The basic formula is as following:

\[ \text{Msg} = \text{Data} \mid \text{SN} \mid \text{TS} \mid \text{CRC}\{E[\text{Hash}(\text{Data} \mid \text{SN} \mid \text{TS}, \text{Key})]\} \]

The algorithm is as following:

1. Generate serial number and time stamp;
2. Attach data to pdu;
3. Attach SN, TS to pdu;
4. Calculate \( h=\text{Hash}(\text{Data}, \text{SN})[\text{TS}] \);
5. Calculate \( E(h, \text{Key}) \);
6. Calculate \( \text{CRC}(E(h, \text{Key})) \);
7. Sending the pdu.

According to the “twice refine characters “ algorithm, the basic idea is using CRC to refine the HMAC’s characters. This algorithm has refine the characters twice, first, the HMAC is calculated, and the HMAC can not be recalculated without the secret “Key”, and for transfer efficient, the CRC of HMAC is calculated after HMAC was generated. By this way, the HMAC can be “compressed” into 4 bytes, and the security or safety abilities are not reduce distinctly.

![Diagram](image)

**C. Confidential security measure in safety-related system**

Safety and security are two attributes of dependability, along with availability and reliability[7]. To protect this two attributes, whole data encrypting maybe needed sometime. Part A and Part B has given a non-confidential but authenticated way to communication safely and securely. But sometimes there are confidential requirements in safety communication of control network, maybe the formulas or the

---

(sponsors)
processes are unique to protect, or other reasons. So, the whole information of pdu may need to be encrypted, too.

The encryption measures are rather lot. There are public key cryptography and symmetric cryptography can be chosen, both of them are considerable well known. Public key cryptography such as RSA or elliptic curve cryptography need more time cost than classics symmetric cryptography. In wireless sensor network there is a tinysec architecture which make use of symmetric cryptography. Both of them is available to control network in theory, but the time cost, CPU cost, network cost should be taken into account.

Cause safety related control network not only has security and safety attributes, but also other important attributes such as reliability, real time ability, robust ability, etc. Symmetric cryptography was chosen as a basic confidential measure in safety related control network according to the real time and process speed. Appropriate symmetric cryptography can provide good and efficient confidential ability meanwhile doesn’t take too much CPU time and network capability.

Confidential communication between two peers is easy to realize with symmetric cryptography. Every peer has a data structure named key ring, which keep all other peer’s communication key. Blowfish was chosen as the basic symmetric algorithm, cause blowfish has a high secure level and is faster than DES, 3DES or AES. The blowfish is easy to realize with software way. Blowfish was designed by Bruce Schneier. This algorithm has the following merits:

1. Fast. Using 32bit CPU it fast as encrypting a byte only need 18 tick time.
2. Small enough that only need 5K RAM.
3. Strong.
4. Simple. The algorithm’s structure is sample and the key length is scalable.
5. No patent restrict.

The Blowfish algorithm and other classical symmetric key algorithm’s speed is shown as following [3].

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Tick/round</th>
<th>Round sum</th>
<th>Encrypting a byte tick</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blowfish</td>
<td>9</td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>RC5</td>
<td>12</td>
<td>16</td>
<td>23</td>
</tr>
<tr>
<td>DES</td>
<td>18</td>
<td>16</td>
<td>45</td>
</tr>
<tr>
<td>IDEA</td>
<td>50</td>
<td>8</td>
<td>50</td>
</tr>
<tr>
<td>3DES</td>
<td>18</td>
<td>48</td>
<td>108</td>
</tr>
</tbody>
</table>

The Key distribution measures can be ether Key Distribution Center (KDC) or Distributed Key Distribution measure (DKD).

KDC is a centralized approach need a “center” to distribute session key. The KDC approach provides a convince way to deal with huge network, besides that, KDC approach is a transparent measure to the communication peers, but every time the initiation of communication KDC’s action must take place.

Distributed Key Distribution (DKD) approach is another better to control network or safety-related control network. To an end system has N endpoint there are at least \([N(N-1)]/2\) master keys. This approach is too complex to huge network system, but to the (safety-related) control network it can work well. So the key distribution method we choose the DKD approach. The DKD approach is shown as following:

1-refine characters algorithm make use of HMAC , which based on MD5 and symmetric, the HMAC’s speed is slow than CRC. A test between CRC and HMAC has been down on PC. The parameter is shown as following:

| Key | —— | 30 | VC 6.0 | Intel Core2 Quad |
| PlantText | 528 | 528 | VC 6.0 | Intel Core2 Quad |
The time parameters are taken from CPU directly by ASM language. Repeating the test for 100 times, and we get the following picture.

![Figure 7. 1-Refine algorithm VS. CRC](image)

As fig.7 shown the CRC is a little faster than 1-refine algorithm, but it is acceptable, spending more time and gain more secure by using 1-refine algorithm.

2-refine algorithm refine the characters twice, first by HMAC and then by CRC, the time cost is shown as following. Parameters’ setting listed in table 3.

![Figure 8. 2-Refine algorithm VS. CRC](image)

Secure problems of safety related system are discussed and a HMAC based safe communication named 1-refine approach is introduced. 1-refine approach is suitable to high speed control network such as real time Ethernet. To low speed control network, 2-refine approach was proposed which refine characters of data by HMAC and refine the HMAC’s characters by CRC, the character code is compressed from 32 bytes to 4 bytes. 2-refine approach can keep the safe data from modification by nature or by intruder. A confidential measure using blowfish algorithm to protect data’s secret is proposed, and two key distribution ways are discussed, too. Finally, 1-refine and 2-refine approach’s speed are evaluated by PC, the result shown both of them is a little slow than CRC, but they are acceptable and suitable.

IV. CONCLUSION

ACKNOWLEDGMENT

This work is supported by the Natural Science Foundation of China under contract 61004068.

REFERENCES