An Approach for the Verification of Trusted Operation on Automatic Control System

Li-tian XIAO1,2,* , Meng-yuan Li2 and Nan XIAO3

1Beijing Special Engineering Design and Research Institute, Beijing 10028, China
2School of Software, TNList, KLISS, Tsinghua University, Beijing 10084, China
3China Aerospace Academy of System Science and Engineering, Beijing 10048, China

*Corresponding author

Keywords: Control system, Trusted operation, Trusted stamp, Verification protocol.

Abstract. The automatic control system is very important to space launch. Even if the control system has been tested, there is still no very effective method to ensure the trusted operation of the system. We propose an approach for the trusted operation and verification of control system. Based established control system model in the paper, the trusted elements of the core controller are configuration transformation and state transferring in the control system operation. The state transferring of each module inside each controller is stamped by the stamping method. The state stamps of output result are verified at the output port of each module. The trusted state transferring is used to ensure the credibility of the operation. The paper analyzes the approach’s security under environmental impact as well as independent and joint attack. The approach is tested by building a simulation platform. It is proved to be safe and reliable. Also, it is feasible to apply in launch site.

Introduction

Programmable Logic Controller is a kind of embedded system in the automatic control system. The controller’s trusted operation is vital to this kind of safety-critical applications. Conceptually, the trusted goal of the control system is to propose a running entity that can perform a special action surpassed the preset security rules, and how to verify the entity. Therefore, we need first ensure that the software and hardware systems can be quantified and verified by calculation. The critical core of a trusted system is the trusted computing. At present, trusted control system platform is mainly considered the security issues from the perspective of security architecture. The security of the user’s operating environment is ensured by the passive defense (i.e. security patching).

The paper proposes a control system model, and analyze the state change and transmitting of the control system. Based on the model, the security mechanism and the processes are set up by the critical elements for verifying the trusted operation. So the approach ensures the operation reliability and security of the whole system.

Related Work

Now, there are a few related papers and reports about the trusted research of control systems. The research of the related trusted system is mainly focused on the network, trusted computing and related software and hardware [1]-[8].

For the trusted guarantee of the complex software system under the network environment, the main research is establishing a new software technology hierarchy. Trusted technology system is constructed by quality assurance. In the research and development of trusted computing, trusted computing technology is combined with other information security technologies in the trusted computing field. In the research of software trusted evolution management, it is considered that the nature of trusted evolution is a software modification process driven by user expectation deviation. The researchers study how to improve the convergence speed and effect of software trusted evolution. The researchers on the architecture and key technologies of trusted networks propose a possible
control model for evaluating the enabling technologies of trusted networks. In the progress of trusted computing technology hardware, the software on the computing platform is measured by enhancing the hardware architecture of the existing open platform.

In the control system field, the technical features of the trusted control system are integrated existing defensive measures. The researchers utilize linkage mechanism between the inside firewall of control systems, the intrusion detection system and the trusted connection server. It can improve the overall defense and security capability of control systems [9][10], but it doesn’t have the trusted verification and cannot ensure the trusted operation.

The credible risks are very high in actual applications at the aerospace launch site. Certainly, measures have generally been taken for these keys in the control system. Some have adopted redundant or hot backup methods. Some have added monitoring points and fault handling software. Others are strict with the test inspection and control the identity of software users. But there is no trusted verification in control system, whether the state transmission can be trusted exists the risk on the information source and host as well as terminal. Therefore, the untrusted verified system exists risks on safe and reliable. Correlated trusted research lags behind the application needs in actual control systems. It still lacks typical solutions.

**Control System Modeling**

Control system receives and processes the various sensor signals of controlled devices. These sensor signals (Sigsen) include analog signals (AI) and digital signals (DI), e.g. they are from coders (Cod), location detectors (Loc), operation inductors (Opt) and moving sensors (Mov), etc. They are converted and stored into data input port (PI) by A/D and D/A. The set is

\[ \text{Sig}_{\text{sen}} = \{ \text{Al}_\text{Cod}, \text{Al}_\text{Loc}, \text{Al}_\text{Opt}, \text{Al}_\text{Mov}, \ldots, \text{Di}_\text{Cod}, \text{Di}_\text{Loc}, \text{Di}_\text{Opt}, \text{Di}_\text{Mov}, \ldots \}; \ P I \subseteq \text{Sig}_{\text{sen}}. \]

According to control logic, initial configuration, task and interrupt, the control program processes and responds to port data. Then it updates system configuration (V) and gives the corresponding control data to data output port. After A/D or D/A conversion, the control data are converted into analog signals or digital drive ones (AO or DO) for moving drive mechanism such as relays, valves, transmission and etc. Finally, it achieves real-time control, i.e.

\[ \text{Sig}_{\text{drv}} = \{ \text{AO}_\text{Rly}, \text{AO}_\text{Valv}, \text{AO}_\text{Trans}, \ldots, \text{DO}_\text{Rly}, \text{DO}_\text{Valv}, \text{DO}_\text{Trans}, \ldots \}; \ P O \subseteq \text{Sig}_{\text{drv}}. \]

The communication between controllers is dependent on the bus network port. Control system is constructed by the components such as Fig.1. A control system can be composed of multiple controllers. Controller system features are decided by \{PI, V, PO\}, i.e. controller’s action is controlled by input, output, and configuration. The description of the controller can be defined as a tuple:

\[ M = < V, v_0, P I, P O, R_{PI}, P M >, \]

where \( V \) is the finite state set of non-empty configuration inside the controller, \( P I \) is the finite set of non-empty input, \( P O \) is the finite set of non-empty output, \( R_{PI} \) is the mapping set of an input subset, \( v_0 \subseteq V \), where \( v_0 \) is the initial state of the control program.

\[ R_{PI} \subseteq \beta(P I) \subseteq \{ r_1 \}, \quad (i = 1, 2, \ldots), \]

which \( \beta \) is the transform function set of confirmed generalized verification. \( \beta \) filters an input subset that is effective in handling, \( r_i \) is the subset of \( P I \). \( P M \) describes the incomplete mapping of the control program.

\[ P M(a, b); \beta(V) \times \beta(PO) \times R_{PI} \rightarrow \beta(V) \times \beta(PO), \quad \text{where} \ a \in \beta(V) \times \beta(PO), \ b \in R_{PI}, \ v_0 \in \beta(V) \times \beta(PO). \]

**Trusted Elements in Control System**

Based on the control system model, ensuring the trusted state transferring in the controller is the key to ensure the credibility of the system operation. There are \( n \) states inside a controller. Each state transform is decided by \( M \). \( M \) is constructed by \{M1, M2, \ldots, ML\} inner states. It includes multiple states transferring labeled as \( \phi_i \) (\( i = 1, 2, \ldots, n \)). Each M1 may have several \( \phi_i \). Likewise, the state transformations combined multiple controllers is the same as individual controller inner states. The controller is abstracted by its operation states from the configuration of a controller, e.g. it is showed in Fig.2. So the trusted elements of the controller include input/output interface, configuration...
transformation, state transferring and programmable components. The network interface is outside the scope of the controller. We embed trusted verification computation in the controller to verify each input/output and state transfer.

The model M of the example consists of four submodule Mi (i=1,2,3,4). φ={φ1, φ2, φ3, φ4} is the verified property, which φi (i=1,2,3,4) is the state transferring property from the input set to output set. It needs to ensure that the transferring property is trusted from input to output.

A group of submodule Mi transforms configuration according to transferring path. We utilize the principle of digital signatures based on Schnorr protocol [11]. The module members are marked particular stamps for output and verified stamps for input.

The Trusted Stamp and the Verification Protocol

φ1, φ2, …φn are defined as n state transferring to a controller.

a). Generating a key pair. To choose two large prime p and q, q is the prime factor of p-1. q≥(2^{140}) and p≥(2^{512}), and the primitive a (a≠1) of rank q is chosen in GF(p) and satisfies a^q ≡ 1 mod p [11]. The one-way HASH function is chosen and makes function h→{0,1,…2^t-1}. They are promulgated and shared by all state members Mj (j=1,2,…L). Each φi chooses the private key Ki which is defined as a random number less than q on GF(q). The public key is

\[ U_i = a^{K_i} \mod p \ (i=1,2,…n). \]  

b). Generating state stamp. Assumed that T is the scan period of a response in the controller, state transferring has the performance time Ti (i=1,2,…n), where \( T = T_1 + T_2 + … + T_n \). The designed scan period should be abided, or else the design and Ti reset. T and Ti are the time mark of the system given to every member states. It requires that the submodule should finish their work and state transferring at the given times. When state stamp being calculated, the system automatically gets corresponding system unify-time for consistency. Every time Ti exists the differences in precise time because of different performances.

The process of state stamp is designed as below that n states transferring to result f.

First, defined \( x_0 = a^T \mod p \). φi has choose the random number di on GF(q). Calculating

\[ x_i = x_{i-1} \cdot a^{-Ti} \cdot a_{di} \mod p \]  

and \( x_i \) is sent to the submodule \( M_j \) (j=1,2,…L) related φi. When \( j=L, M_L \) send \( x_n \) to \( PO \). Then assuming \( y_0=0 \) and calculating is processed
\[ e = h(x_n, f), \quad y_i = y_{i-1} + (d_i + K_i) (\text{mod} \; q) \quad (i=1,2,\ldots,n). \]  

Finally, \( \{f, e, y_n\} \) is sent to PO and verified. \( \{f, e, y_n\} \) is the group state stamp of the result \( f \) signed by the state transferring \( \varphi_1, \varphi_2,\ldots, \varphi_n \) in the controller.

c). Verifying state stamp. The PO receives the group state stamp \( \{f, e, y_n\} \), then verifies the whole stamp with \( U_i \) of the state transferring. Calculating

\[ x'_n = a^{y_n} \left( \prod_{i=1}^{n} U_i \right)^e (\text{mod} \; p) \]  

and further verifying \( e = h(x'_n, f) \) whether or not comes into existence. If the verification equation comes into existence, the output is confirmed that the result is valid and can process the next performance. If the verification fails, the control system refuses the result.

The equation showed below is proved the validity of the state stamp scheme. Because it is based on (3) and (1), it has

\[ x'_n = a^{y_n} \left( \prod_{i=1}^{n} U_i \right)^e (\text{mod} \; p) = a^{y_n-1+(d_n+K_n e) (\text{mod} \; q)} \cdot (\prod_{i=1}^{n-1} U_i)^e \cdot (U_n)^e (\text{mod} \; p) = a^{y_n-1} \cdot a^{(d_n+K_n e) (\text{mod} \; q)} \cdot (\prod_{i=1}^{n-1} U_i)^e \cdot (a^{K_n} e) (\text{mod} \; p) = a^{y_n-1} \cdot (\prod_{i=1}^{n-1} U_i)^e \cdot (a^{K_n} e) (\text{mod} \; p) \]

The below equation can be obtained on the analogy of (3). \( x'_n = a^{y_n-1} \cdot a^{d_n} \cdot a^{d_{n-1}} \cdot \cdots \cdot a^{d_1} (\text{mod} \; p) \). Due to (2) and initial condition \( x_0 \), the equation is \( x_n = [x_0 / (x_0 \cdot a^{T_n-1})] \cdot [x_0 / (x_0 \cdot a^{T_{n-1}-1})] \cdot \cdots \cdot [x_0 / (x_0 \cdot a^{T_1})] (\text{mod} \; p) = x'_n \cdot (x_0 a^{T_0}) (\text{mod} \; p) = x_n (\text{mod} \; p) \). So \( e = h(x_n, f) = h(x'_n, f) \) is verified.

During the state stamp, every state transferring \( \varphi_i \) apply the below equation to verifying the validity of the stamp

\[ y_{i-1} \cdot x'_{i-1} = a^{T_{i-1}+T_{i-2}+\cdots+T_1} \cdot a^{y_{i-1}} \left( \prod_{j=1}^{i-1} U_j \right)^e (\text{mod} \; p) \quad (i = 2, 3, \ldots, n) \]

The validation is to judge whether or not \( x_{i-1} = y_{i-1} \cdot x'_{i-1} \) comes into existence. In fact (4) is a special example of (5). Similarly the validation can be capable of proof.

\[ x'_{i-1} = a^{T_{i-1}+T_{i-2}+\cdots+T_1} \cdot a^{y_{i-1}} \left( \prod_{j=1}^{i-1} U_j \right)^e (\text{mod} \; p) = a^{T_{i-1}+T_{i-2}+\cdots+T_1} \cdot a^{r_{i-1}} \cdot a^{r_{i-2}} \cdots \cdot a^{r_1} = x_{i-1} \]

The verification is considered that the group state stamp mentioned above is correct.

### Analyzing the Security of the Trusted Stamp Protocol

Because a majority of calculation needed to produce a stamp can be finished in the phase of pretreatment and be independent of massages that are ready to be stamped, the calculation can be processed in idles and not influence the stamp speed. For the same level of security, the stamp length based on Schnorr protocol is much shorter than other signature protocol[111]. The security of the stamp and authentication scheme is founded on the computational difficulty of discrete logarithm.

There is randomness influence on trusted operation caused by environment or components performance. Because of state stamping, it is easy to verify these trusted problems during system operation. It will not cause a particular trusted problem. However, intentional attack on the controller is the biggest risk of the trusted operation. The following analysis of the protocol is faced with the trusted operation security under attack.

### The Security on Exterior Independence Attack

The security of every single stamp is same as the Schnorr’s[12]. The attack on group stamp has the modes mentioned below. Under the mode a), b), c), d) and e) the computational difficulty is the equivalence of calculating discrete logarithm on \( GF(p) \).

a). Anyone can obtain the value \( p, a \) and \( U_i \). Someone tries to obtain \( K_i \) from \( U_i = a^{K_i} \text{ mod } p \). It is impossible to obtain the private key \( K_i \) that the attacker is directly started with generating the key.

b). Someone tries to obtain \( K_i \) or random number \( d_i \) by \( U_i \), \( x_i \), and \( y_i \).

c). Someone tries to obtain \( K_i \) or random number \( d_i \) by the public information \( \{f, e, y_n\} \) or \( \{f, e, y_i\} \) and the verification equation (5).

d). An attacker may try to choose randomly an integer \( K'_i \) and then solve \( d_i \) by calculating \( y_i \).
e). The attacker has known \( x_0, x_1, \ldots, x_i \) and tries to solve \( y_i \) or has also known \( y_i \) to solve \( d_i \) which are met the equation \( x_i = a^{T-T_1-T_2-\cdots-T_{i-1}} \cdot a^{y_i} \prod_{j=1}^{i} (U_j)^{\phi}(\mod p) \), who wants to make the whole group stamp met verification equation by using of calculating a part of group stamps.

An attacker may try to personate or change \( \phi_i \) under the condition of unknowing \( K_i \). Because the time mark \( T_i \) is added to the scheme and different every time, it is different from history and current information. It means that \( x_i \) of the same \( \phi_i \) is different every time and \( e \) is different too. The history stamp \( y_i \) cannot be utilized.

**Analyzing the Security of United Attack**

The united attack is that the obtained some stamps are united to solve other stamps of module group. It is not repeated here to the analysis of security similar exterior independence attack.

If a part of stamps is united to forge one or several stamps, they need one or several \( K_i \). If \( k \) stamps are united to forge \( h \) stamps of \( \phi_i (k+h \leq n) \) and make the group stamp valid to the verification during the state stamping, the verification equation needs to be met. They also face the computational problem of discrete logarithm. The replace attack is a kind of forging attack that has much danger. Because the security of \( \phi_i \)’s stamp is the equivalence of Schnorr’s protocol, the replace attack is invalidated in the scheme of the paper.

It can be summed up the discussion that it is secure to the group stamp based on the computational difficulty of discrete logarithm. According to conclusion proved by the theory of computational complexity, \( 2^t \) is the difficulty of breaking the protocol (the probability is \( 2^{-t} \), and Schnorr suggested \( t \geq 72 \)). The attacker can calculate for several years to forge a stamp [11][12][14]. But time mark is added into the scheme and enhanced the capability of anti-attack. In the state stamp, every module verifies the previous stamp and then stamping after the verification is correct. So the capability of anti-attack is enhanced further.

**Conclusion**

In the experiment, we build a simulation environment to verify the operation of the protocol. A desk computer connects the controller with the interface of input/output and network. The computer sends out input driving at the input port of the controller. Each state transferring of the controller is uploaded through the network interface, which is stamped and returned to the controller. Finally, the computer accepts the output result and the verification module verifies the stamps. For accumulative total about 10000 state transferring, the calculating speed of the stamping and the verification is at most the microsecond order of magnitude or faster. The millisecond level control is enough to deal with at launch sites. With the controller performance improvement, the application of this protocol has a larger capacity.

We create a guarantee mechanism for trusted operation on the control system and design the trusted stamp and the verification protocol. The approach ensures the trustworthiness of the state migration, so as to obtain the credibility of the system. The trusted state transferring ensures the system trusted operation. In the next step, the actual algorithm of state stamp and verification will be optimized. It needs to study how to embed the algorithm chip into the controller. Although theoretical and experimental methods are feasible, there are still many issues to be studied in actual applications.

**Acknowledgement**

This work was funded by the project of General Technology on Test and Launch partially sponsored by the 973 program. We would like to thank Tsinghua’s Prof. Yu Liu who provided us with the helpful suggestions and some research resources in the research.

**References**


