International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 03, March 2017
ISSN: 2455-3778
http://www.ijmtst.com

Intrusion Detection in Industrial Automation by Joint Admin Authorization

Apune Sagar Sambhaji[1] | Prof.Kishor Honwadkar[2]

[1,2] Department of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Maharashtra, India.

To Cite this Article
Apune Sagar Sambhaji and Prof.Kishor Honwadkar, "Intrusion Detection in Industrial Automation by Joint Admin Authorization", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 03, 2017, pp. 25-29.

ABSTRACT

Intrusion response is a more important part of security protection. In industrial automation systems (IASs) have achieved maximum and availability attention. Real-time security policy of intrusion response has big challenge for intrusion response in IASs. The loss caused by the security threats may even increase the industrial automation. However, traditional approach in intrusion detection pays attention on security policy decisions and removes security policy execution. Proposed system presents a general, real-time control depends on table driven scheduling of intrusion detection and response in IASs to resolve the problem of security policy like assigning rights to use the system. Security policy created of a security service group, with every kind of security techniques supported by a realization task set. Realization tasks from different task sets can be combined to form a response task set. In this approach, first, a response task set is created by a non dominated genetic algorithm with joint consideration of security performance and cost. Then, the system is re- configured via an integrated scheduling scheme in which system tasks and response tasks are mapped and scheduled together based on a GA. Additionally, this system proposed Joint Admin Model (JTAM) model to control over unauthorized access in industrial automation system. Furthermore, proposed method shows result of industrial automation for security mechanism. Security policy helps to authenticate user request to access industrial resources.

KEYWORDS: *GA, Outsider Attack, Insider Attack, Anomaly Detection, Authentication, Authorization*

I. INTRODUCTION

There are number of fact used to prevent of various attacks such as web proxy attack, insider attack, outsider attack etc. First, insider attack includes access to resource such as data and computer systems, and services inside the organization networks as they are having valid credentials. Second the actions of insiders initiate at a trusted network, subject to thorough security checks in the same way as external actions are. For instance, there is often no internal firewall within the organization network. Third, insiders are often highly trained computer experts, who have knowledge about the internal configuration of the network. For access control, authentication and authorization of users, they use various local passwords. Several passwords allow different user to access the device for various purposes. Proposed system works to ensure different users role along with smart device taken into account for authorization and authentication to have access to the system. In the distributed environment for application or data access control is more challenging task, as security management by a single central authority might not be possible or could be more resource overhead.

Intrusion response systems (IRSs) can be classified into three types:

1) Manual IRSs ;

2) Semiautomatic IRSs; and
3) Automatic IRSs. IASs have high availability demands, It means the manual and the semi-automatic intrusion response will not implement the security protection requirements for IASs.
Automatic intrusion response has been a thesis topic in the IT domain for several years. Designed multi attribute genetic algorithm (GA) approach for handling a multi attribute decision problem in intrusion response. These works focus on security policy decision and ignore the security policy execution, i.e., instant intrusion response.

II. REVIEW OF LITERATURE SURVEY

It includes the brief overview of existing work of various techniques used for authentication and authorization of different users and devices: At the time the authentication is achieved by applying the standard SSL authentication protocol (SAP). However, it is low efficient for SAP, which is based on standard X.509 certificate-based PKI authentication framework. But all the time it is not possible to provide SAP protocol for authentication [1]. To overcome this problem, next presented novel mutual authentication & key management mechanisms tailored for the SG communications. The savings in resource consumption as the result of our mechanism can be used to handle more data delivery and/or to increase the security of the system by refreshing the keys more often, which brings to SG the opportunity to utilize keys of smaller sizes, further reducing resource consumption in the system [2]. The problem arises in earlier system is overcome in next generation. The analysis of the proposed protocol shows that the protocol is able to prevent various attacks. The transmission of symmetric key to the mobile users is efficiently managed by the protocol. Here's the concept of OTP which is send on users mobile phone is used but it has poor communication overhead and computation overhead. In our system all the problems will be recovered and defeat all the insider and outsider attacks and improve the efficiency of communication overhead and computation overhead [3].This system proposed a user authentication and authorization scheme for accessing many different types of devices in the SG. This scheme can be easily applied to different user-roles, such as auditors, researcher, etc., who access different devices in the SG system, as each user-role is computed dynamically based on attribute-based access control. Our scheme enables two-factor authentication so that a rogue device could not re-use the previous captured information of a legitimate user [4]. A bilinear pairing cryptography-based shared secret key is generated between the user and the device for further secure communications within a session. The proposed scheme is efficient in terms of both, communication and computation overheads in comparison with the existing schemes, and is able to defeat many well-known outsider attacks as well as insider attacks[5]. User authentication has done by administrative authority which is time consuming process for security authentication and authorization. Public key cryptography technique is used to protect user access for the system but the approach generates a huge overhead. An extension of distributed network protocol to the secure authentication considers multiple users at the master site [6]. This scheme presumes that both, the master station and the substation, share a common secret key, which is used to generate a session key. Furthermore, there exists a substation-level authentication scheme in the literature where IEDs and other resource-constrained devices can be authenticated by any remote users with the help of the substation controller. However, they considered remote access of the IEDs using passwords shared among users, lacking message integrity check, batch verification, and prevention against attacks [7]. This approach is based the analysis and profiling of the application in order to create a succinct representation of its interaction with the database. Such a profile keeps a signature for every submitted query and also the corresponding constraints that the application program must satisfy to submit the query. Later, in the detection phase, whenever the application issues a query, a module captures the query before it reaches the database and verifies the corresponding signature and constraints against the current context of the application. If there is a mismatch, the query is marked as anomalous. Defeats different outsider attacks as well as insider attacks, including man in middle attacks, replay attacks, impersonation attacks, integrity violations, attacks by customer, known key attacks, and repudiation attacks. It also prevents insider attacks where (i) a user accesses the device with the credential of his/her friend or family member without notifying him/her, and (ii) a rogue device is installed by a legitimate engineer in the network.

III. SYSTEM ARCHITECTURE

In proposed industrial automation system for automatic intrusion response is designed to implement.

1. User Registration
2. Policy Creation
3. Intrusion Detection
   a. User Verification
   b. Policy Verification
   c. Attack verification
4. Response Generation
   a. Response Policy
   b. Response Decision
   c. Response Action
5. Automation Log

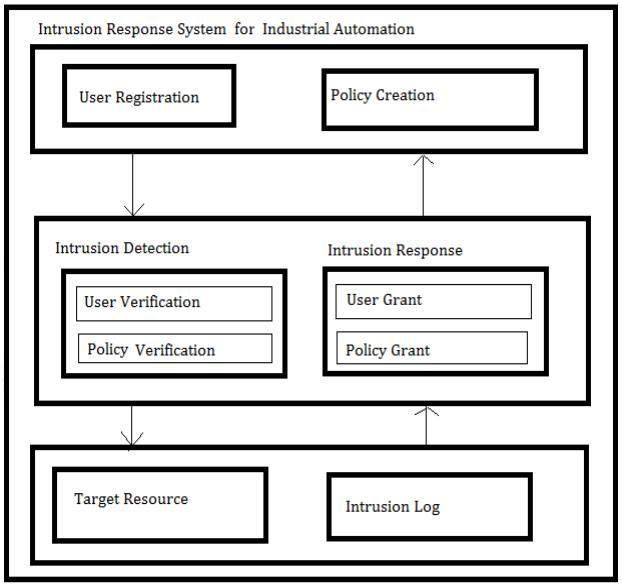

Fig.1: System architecture of intrusion detection in industrial automation

Our approach to an ID mechanism consists of two main elements, specifically tailored to an intrusion detection system and an anomaly response system. The first element is based on the construction of database access profiles of roles and users, and on the use of such profiles for the AD task. A user request that does not conform to the normal access profiles is featured as anomalous. Profiles can record information of different levels of details.

The main idea in JTAM (Joint Admin Model) is that a policy object is jointly administered by at least k automation system administrator, that is, any modification made to a policy object will be invalid unless it has been authorized by at least k administration. Proposed work present design details of JTAM which is based on a cryptographic threshold signature scheme, and show how JTAM prevents malicious modifications to policy objects from authorized users.

IV. SOFTWARE REQUIREMENT SPECIFICATION

Proposed design is planned to implement above requirement using following system configuration.

Operating System- Windows7
Coding Language – Java, JSP, Bootstrap
Framework – Spring MVC, Hibernate, JPA

V. MATHEMATICAL MODEL

Industrial automation for intrusion response system (MATHEMATICAL MODEL)

Let us consider S as a system for Authentication and authorization for industrial authentication S= {……

INPUT: Identify the inputs

F= {f1, f2, f3 ….., fn| 'F' as set of functions to execute commands.}

I= {i1, i2, i3…|'I' sets of inputs to the function set}

O= {o1, o2, o3….|'O' Set of outputs from the function sets}

S= {I, F, O}

I = {user credential, secret hash values, security policy}

O={users authorization , intrusion response, anomaly log}

F={policy matching, User role assignment, Public key cryptography}

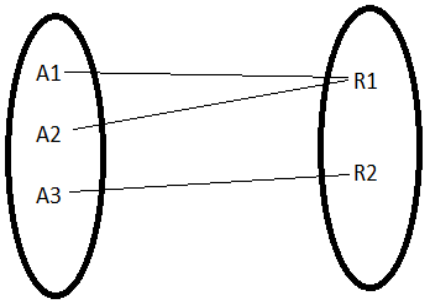

Fig.2: Industrial system Authentication and authorization

A1: Admin authenticated User
A2: Authorized Person
R1: Industrial authorization action/alarm
A3: Wrong or incorrect user detail
R2: Prevent user from accessing industrial data
Above mathematical model is NP-Complete

VI. ALGORITHM

Algorithm: Digital Signature Generation

Step1. Select random sequence of at least 160 bits and call it seed. Let g be size of seed in bits.

Step2. Calculate U = SHA-1[seed] XOR SHA-1[(seed+ 1) mod 2 g].

Step3. Form q from U by setting the Most Significant Bit (the 2^{159} bit) and the least significant bit to 1. In terms of Boolean operations, q = U OR 2^{159} OR 1. Note that $2^{159} < q < 2^{160}$.

Step4. Use a robust testing algorithm to test whether q is prime 1.

Step5. If q is not prime, go to step 1.

Ste 6. Let counter = 0 and offset = 2.

Step7. For k = 0,..., n let Vk = SHA-1[(seed + offset + k) mod 2^g]. A robust test is one where the probability of a non-prime number passing the test is at most 2^{-80}

Step 8. Let W be the integer $W = V0 + V1 * 2^{160} + \ldots + V_{n-1} * 2^{(n-1)*160} + (V_n \bmod 2^b) * 2^{n*160}$ and let $X = W + 2^{L-1}$. Note that $0 \le W < 2^{L-1}$ and hence $2^{L-1} \le X < 2^L$.

Step9. Let c = X mod 2q and set p = X -(c -1). Note that p is congruent to 1 mod 2q.

Step10. If $p < 2^{L-1}$, then go to step 13.

Step11. Perform a robust test on p.

Step 12. If p passes the test performed in step 11, go to step 15.

Step13. Let counter = counter + 1 and offset = offset + n + 1.

Step14. If counter $\ge 2^{12} = 4096$ go to step 1, otherwise (i. e. if counter < 4096) go to step 7.

Step15. Save the value of seed and the value of counter for use in certifying the proper generation of p and q.

Signature Verification

Before getting the digitally signed message the receiver must know the parameters p, q, g, and the sender's public key y.

We will let M′, r′, s′ be the received versions of M, r, and s. To verify the signature the verifying program must check to see that 0 < r′ < q and 0 < s′ < q and if either fails the signature should be rejected. If both of the conditions are satisfied then we will compute.

$w = (s')^{-1} \bmod q$

$u1 = ((SHA(M'))w) \bmod q$

$u2 = ((r')\ w) \bmod q$

$v = (((g)^{u1}\ (y)^{u2}) \bmod p) \bmod q$

Then if v = r′ then the signature is valid and if not then it can be assumed that the data may have been changed or the message was sent by an impostor.

VII. RESULT ANALYSIS

Proposed implementation is evolved by digital signatures computation assigned to user in the form requested policy authentication. Proposed system verifies the accuracy of signature authentication by computing signature hash value and policy authentication time.

Syntax to Signature Verification: -

ON {Event}
IF {Condition}
THEN {Initial Action}
CONFIRM {Confirmation Action}
ON SUCCESS {Resolution Action}
ON FAILURE {Failure Action}

Proposed accuracy is measured by verification of signature time computation.

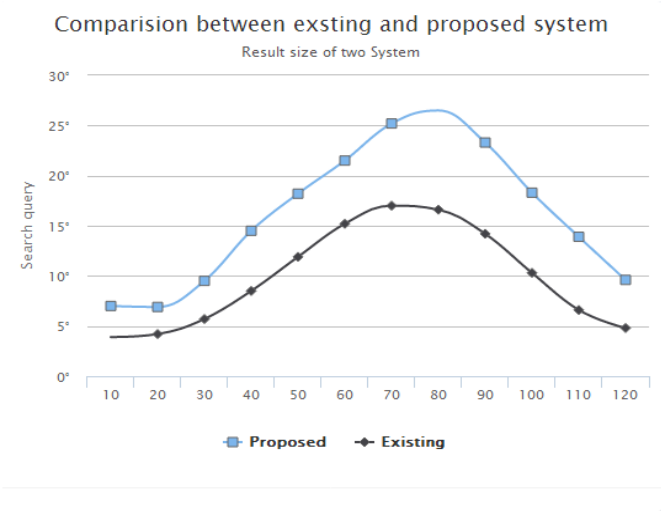

Fig.3: Accuracy for industrial automation

VIII. COMPARISON WITH SIMILAR SYSTEM

Proposed industrial automation intrusion response system is compared with existing implementation for different attributes.

Attribute	**Existing**	**Proposed**
User Security	User credentials	User credentials + Keyed Hash values
Approach	-Manual IRS -Semiautomatic IRS -Automatic IRS	-Automatic IRS -Digital Signature -JTAM Model
Algorithm	Genetic Algorithm	NaïveBayes Algorithm
Control	Operator	Automatic, JTAM model
Accuracy	70%	90%
Cryptogrphy	AES ,DES	Digital Signature

IX. CONCLUSION

Proposed system has been implemented for industrial automation protection of industrial automation system, security policies are created from the security policy decision is complex and varied. From the above simulation results, it can be seen that the proposed real-time control approach of intrusion response is an effective method to guarantee the smooth, timely execution of the security policy without effect on system control performance. To cover wide variety of security requirements for protection of automotive services, the security policy is formalized as a group of security services with different types. This system reduces the execution of the response tasks, an integrated scheduling strategy based on the Genetic algorithm is designed to map and schedule the system tasks and response tasks together. Inclusion of heterogeneous user in addition, to this technique focused on security policy enforcement, and did not discuss security policy generation.

REFERENCES

[1] C. Zimmer, B. Bhat, F. Mueller, and S. Mohan, "Intrusion detection for CPS real-time controllers," in Cyber Physical Systems Approachto Smart Electric Power Grid (Power Systems), S. K. Khaitan, J. D. McCalley, and C. C. Liu, Eds. Berlin, Germany: Springer, 2015, pp. 329–358.

[2] R. Mitchell and I.-R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 5, pp. 593–604, May 2014.

[3] C. Alcaraz and S. Zeadally, "Critical control system protection in the 21st century," Computer, vol. 46, no. 10, pp. 74–83, Oct. 2013.

[4] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part II: Attack detection using enhanced hydrodynamic models," IEEE Trans. Control Syst. Technol., vol. 21, no. 5, pp. 1679–1693, Sep. 2013.

[5] M. Mantere, M. Sailio, and S. Noponen, " Network traffic features for anomaly detection in specific industrial control system network," Future Internet, vol. 5, no. 4, pp. 460–473, Dec. 2013.

[6] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks," IEEE Trans. Control Syst. Technol., vol. 21, no. 5, pp. 1963–1970, Sep. 2013.

[7] J. Reeves, A. Ramaswamy, M. Locasto, S. Bratus, and S. Smith, "Lightweight intrusion detection for resource-constrained embedded control systems," in Critical Infrastructure Protection V (IFIP Advances in Information and Communication Technology), vol. 367, J. Butts and S. Shenoi, Eds. Berlin, Germany: Springer, 2011, pp. 31–46.