International Journal of Computer Science Engineering & Technology
IJCSET
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)– NEW DELHI INDIA .
ISSN :2455-9091

SECURE FILE TRANSFER USING INTERMEDIATOR SYSTEM

[1] Mrs. R. Suganya, MCA., M.Phil., [2] D. Sangeetha
[1] Assistant Professor, [2] Student,
[1, 2] Department of CSE,
[1, 2] Sri Krishna Arts and Science College,
[1, 2] Coimbatore.

ABSTRACT: In the interest of protecting customer data or securing trade secrets many companies are modifying their mechanisms of transferring data across the Internet. In this paper, technical advances in ubiquitous sensing, embedded computing, and wireless communication are leading to a new generation of engineered systems called Cyber-Physical Systems (CPS). Cps promises to transform the way we interact with the physical world just as the Internet transformed how we interact with one another. Before this vision becomes a reality, however, a large number of challenges have to be addressed. Network quality of service (QoS) management in this new realm is among those issues that deserve extensive research efforts. It is envisioned that Wireless Sensor/Actuator Networks (WSANs) will play an essential role in CPS. This paper examines the main characteristics of WSANs and the requirements of QoS provisioning in the context of cyber-physical computing.

Keywords: [Cyber-Physical Systems, Network quality of service, Wireless Sensor/Actuator Networks.]

1. INTRODUCTION

Since the earliest days of computing, there have been mechanisms for transferring files from one system to another. Unfortunately, these mechanisms, such as the File Transfer Protocol (FTP) and email, have lacked built-in security features. As organizations became more security conscious and threats expanded, organizations needed ways to transfer files while ensuring their confidentiality, integrity and availability, as well as allowing for the monitoring and managing of them.

To help accomplish these goals, vendors have created a wide variety of file transfer products. In this guide, find out how secure file transfer products work and determine which may be the best fit for your particular environment.

At its most basic, file transfer technology is simply a mechanism to transport a file from one system to another system over a network. A secure file transfer adds security features to this transport, such as encrypting the file to preserve its confidentiality and integrity.

This prevents eavesdroppers on the networks between the systems from accessing the file contents and reading or modifying them. Secure file transfer also involves some sort of reliable delivery, even if it's just provided by TCP/IP conventions. Most secure file transfers are based on standard protocols

such as the Secure File Transfer Protocol (SFTP) or secure copy (SCP).

What makes file transfers confusing is that there are several ways to provide security. The most sophisticated type is known as managed file transfer (MFT), and it adds a wide variety of management, auditing, automation, security and reliability features to secure file transfers.

Another IT system that enables file transfer security is the file hosting service. Originally intended for end user collaboration, file hosting services also typically offer access control and encryption features that allow a user to email a link to a person that grants him or her secure access to a file hosted on the service.

In this existing system can't send the file securely. Generalizations of these embedding's from to proper subgroups are not known, in particular if the cofactor h is large. In this system can't revisit existing files, have already noted, no efficient embedding is currently known in the asymmetric pairing setting. The attackers can attack the information which would send by the sender.A glaring omission in the aforementioned papers is an examination of the effectiveness of these fault attacks on specific pairing-based protocols.

In this paper, technical advances in ubiquitous sensing, embedded computing, and wireless communication are leading to a new generation of engineered systems called cyber-physical systems (CPS). Cps promises to transform the way we interact with the physical world just as the Internet transformed how we interact with one another. Before this vision becomes a reality, however, a large number of challenges have to be addressed. Network quality of service (QoS) management in this new realm is among those issues that deserve extensive research efforts. It is envisioned that wireless sensor/actuator networks (WSANs) will play an essential role in CPS.

2. PROPOSED SCHEME

Polynomial-based compromise-resilient en-route filtering scheme,which can filter false data en-route effectively and achieve high resilience to the number of compromised nodes without relying on static routes and node localization. PCREF adopts polynomials for endorsing measurement reports to improve resilience to node impersonating attacks.

In the proposed system we implement a novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. When a report is transmitted from a sensor node to the controller, each forwarding node checks whether the forwarding reports actually carry valid MACs. If not, the report is considered a false one forged by the adversary and then dropped. Otherwise, the report is forwarded to the next forwarding nodes.

Achieve a high resilience.

Filter false injected data effectively.

3. SYSTEM IMPLEMENTATION METHODOLOGIES

3.1 CONTROLLER

- Destination Selection And Encryption
- Inter Mediator Way Selection
- Inter Mediator Selection and Encryption
- File Selection And Forward to Inter Mediator
- Decide The Destination Action

3.2 INTERMEDIATER

- Receive File with Destination IP
- Forward Received File To Destination

3.3 DESTINATION

- Receiving File From Inter Mediator
- Start And Perform Commend From Controller

3.4 DESTINATION SELECTION AND ENCRYPTION

Destination Means where the controller wants to send the data and controlling its Action. Encryption is used for avoid Data injection attack from hacker; Because If the path is Encrypted Means Hacker Cant able to inject false data.

3.5 INTERMEDIATOR WAY SELECTION

Controller Has Need to decide which way the file has travel. There Is Two option Available Inter Mediator one and Inter Mediator two. This will be used for send if any Error occurs in Mediator, Controller Send the Data to Destination Without fail.

3.6 INTERMEDIATOR SELECTION AND ENCRYPTION

In this after select the mediator controller set the destination and encrypt.

3.7 FILE SELECTION AND FORWARD TO INTERMEDIATOR

After finishing all of this controller will select file to send to destination. File added then controllers send that file to inter mediator

3.8 RECEIVE FILE WITH DESTINATION IP

Intermediate receiving file from the Controller. Forward to destination, inter mediator having destination information .

3.9 RECEIVE FILE FROM INTERMEDIATOR

Destination receive file from destination and it's not perform any action without controller permission

3.10 DECIDE THE DESTINATION ACTION

Destination need command for perform action, so it's send request to controller for command. Controller will control all action of destination so its send command to destination

3.11 START AND PERFORM COMMEND FROM CONTROLLER

See the diagram below it shows the concept, in this destination has send request to controller and then controller send command to destination

4. EXPECTED OUTCOMES

The test process is initiated by developing a comprehensive plan to test the general functionality and special features on a variety of platform combinations. Strict quality control procedures are used. The process verifies that the application meets the requirements specified in the system requirements document and is bug free. The following are the considerations used to-develop the framework from developing the testing methodologies.

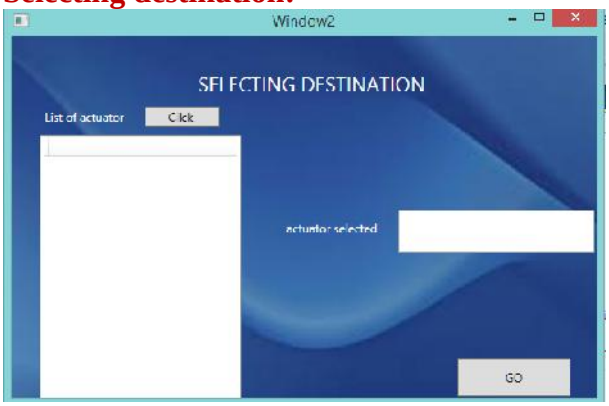
The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner.

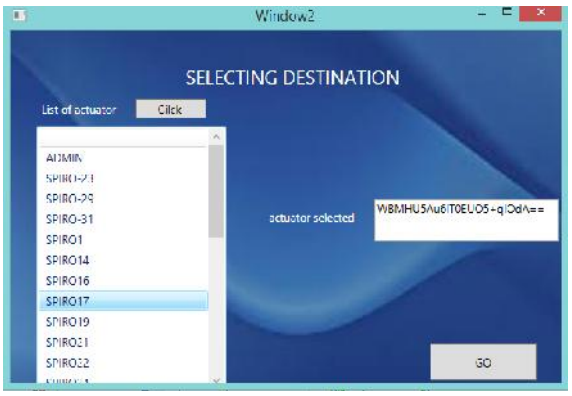
5. SNAPSHOTS

Snapshot is nothing but every moment of the application while running. It gives the clear elaborated of application. It will be useful for the new user to understand for the future steps.

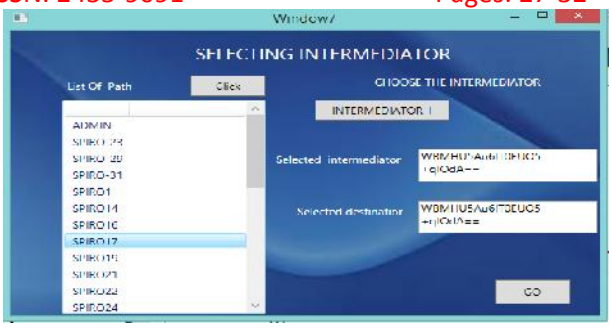
Login Page.

Selecting destination:



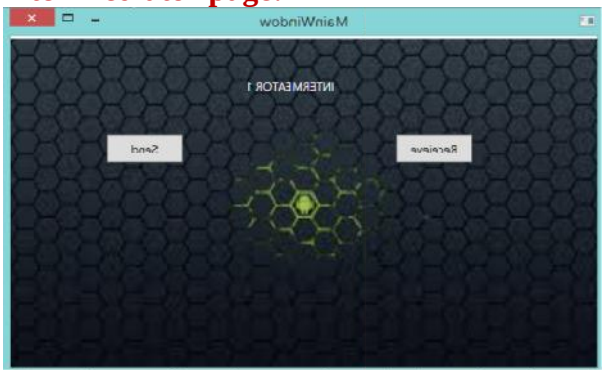


Selecting Intermediate:



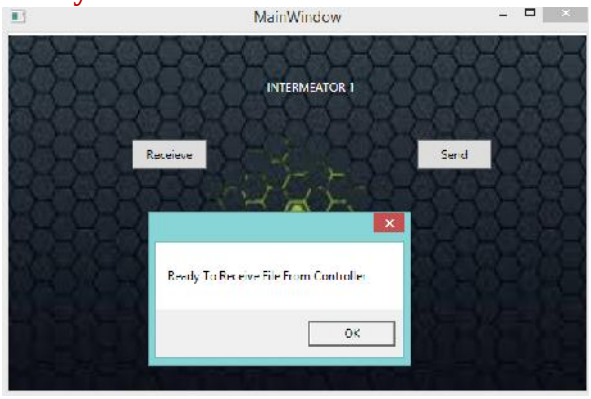
File Upload:

Inter mediator page:



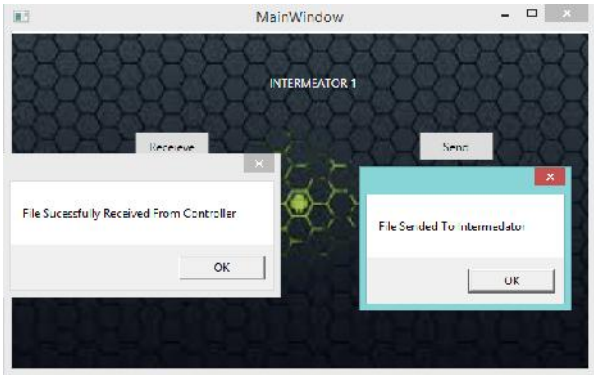
The above fig shows the design for inter mediator main page.

Ready for receive:



The above fig shows the design inter mediator is ready for receive file from the controller to forward to destination

File Received



This figure shows the Inter mediator receive file from the controller and its ready to forward.

CONCLUSION

In this project as demonstrate system based on a Polynomial-based Compromise-Resilient En-route Filtering scheme (PCREF). That can be filtering the false data en route effectively and this method can achieve more resilience to more no of compromised nodes without relying on static routes and node localization.

This algorithm adopts polynomials for endorsing measurement reports to improve resilience to node impersonating attacks. Each node stores two types of polynomials: authentication polynomial and check polynomial, derived from primitive polynomials, and used for endorsing and verifying the measurement reports, respectively.

This project developed a cluster-based primitive polynomial assignment to limit the effect of compromised nodes to a small area. Via both theoretical analysis and simulation experiments, our data shows that our developed scheme achieves better filtering capacity and resilience to a large number of compromised nodes in comparison with the existing schemes. This project results gives more resilience for compromised nodes.

In future there are still some possible extensions of our current work remaining. Using this additional Mediator, controller can't miss any fault occurrence for transfer data to destination, so at max the additional inter mediator offline if any urgency time it will used.

REFFERENCE

[1] CPS Week [Online]. Available: http://www.cpsweek2010.se/

[2] F. Wu, Y. Kao, and Y. Tseng, "From wireless sensor networkstowards cyber physical systems," Pervasive Mobile Comput., vol. 7,no. 4, pp. 397–413, Aug. 2011.

[3] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towardssurvivable cyber-physical systems," in Proc. 1st Int. Workshop Cyber-Phys. Syst. (WCPS), 2008, pp. 495–500.

[4] M. Pajic, A. Chernoguzov, and R. Mangharam, "Robust architecturesfor embedded wireless network control and actuations," Trans.EmbedsdedComput.Syst., vol. 11, no. 4, article no. 82, Dec. 2012.

[5] Cyber Physical Networks(CPN) Research Lab. [Online]. Available: http://cpn.berkeley.edu/.[6] A. Albur and A. G. Exposito, Power System State Estimation: Theoryand Implementation. Boca Raton, FL: CRC Press, Mar. 2004.

[7] H. Chan and A. Perrig, "Security and privacy in sensor networks,"Computer, vol. 36, no. 10, pp. 103–105, 2003.

[8] Y. Younan, P. Philippaerts, F. Piessens,W. Joosen, S. Lachmund, andT. Walter, "Filter-resistant code injection on arm," in Proc. 16thACMConf. Comput. Commun. Security (CCS), 2009, pp. 11–20.

[9] K. Xing and X. Cheng, "From time domain to space domain:Detecting replica attacks in mobile ad hoc networks," in Proc. 29thConf. Inf. Commun. (INFOCOM), 2010, pp. 1595–1603.

[10] Q. Yang, J. Yang, W. Yu, N. Zhang, and W. Zhao, "On a hierarchicalfalse data injection attack on power system state

estimation,"inProc. IEEE Global Telecommun. Conf. (GLOBECOM'11), 2011,
[11] http://www.codeproject.com/
[12] http://www.code-project.eu/
[13] http://www.oracle.com/technetwork/java/javase/downloads/index.html?ssSourceSiteId=ocomcn