SECURITY SCHEMES IN INTERNET OF THINGS (I0T)

Raja Rajeshwaṛi

Department of Computer Application, School of Information Technology,
Madurai Kamaraj University, Madurai

Abstract

The Internet of Things (IoT),is an environments ,in whichobjects,devices, people and anything with an identity to communicate with each other unqiueidentifiers.An enhanced version of machine-to-machine communication technology, was proposed to realize intelligent thing-to-thing communications by utilizing the Internet connectivity. In the IoT, "things" are generally heterogeneous and resource constrained. IOT evolves from wireless technologies but many other technologies such as the smart home control system etc can be supported.The main issues in IOT how to achiveInteroperability between theinterconnected devices . In this paper, we propose an inter-device authentication and system for devices with only encryption modules. In the proposed system, unlike existing sensor-network environments where the key distribution center distributes the key, each sensor node is involved with the generation of session keys. In addition, in the proposed scheme, the performance is improved so that the authenticated device can calculate the session key inadvance. In this paper some of the modals suggest authentication to IOT device and data.

Keywords: *Authentication, Security, IoT.*

Introduction

The Internet of Things (IoT) is a concept being increasingly supported by various stakeholders and market forces. The idea is to connect various devices or objects ("things") through wireless and wired connections and unique addressing schemes1and create a pervasive environment where a person can interact at any time with the digital world and physical world. It also encompasses virtual objects and, virtual machines having digital attributes and evolving personalities. IoT opens new exciting opportunities but also new questions on the interaction between the citizen and businesses operating in the digital world. Some of these questions include the capture, processing and ownership of citizen's data and the possible need to create new legislative or technical frameworks to exercise more control over such a large and complex environment while at the same time avoiding posing unnecessary constraints to IoT market development. Other questions refer to access and effects. These questions are related to various aspects: the governance, security and privacy aspects, which cannot be separated (in the opinion of the authors of this paper) from ethical aspects. Authentication and access control mechanism are capable of preventing unauthorized users from accessing the data of sensor nodes on the IOT perception layer and data security effectively.

Security Issues

The basic security issues in IOT,when two or more devices are communicatingwith each other,then devices involved in IOT.Internet of Things experts talk about two distinct

problems when IoTsecurityissues are brought up. Beyond that, Internet-connected machines and their data will lead to an exponential growth of the attack surface. The attack surface problem, at least as popularly understood: "More connected devices mean more attack vectors and more possibilities for hackers to target us; unless we move fast to address this rising security concern, we'll soon be facing an inevitable disaster."
Spoofed, altered & replayed routing information:

The most outstanding attack on routing is to alter, spoof, or just replayrouting information is known as false routing information. Malicious nodes simply, Drop data packets quietlyModify data contentGenerate false error messagesTraffic redirections

Selective Forwarding

A venomous node which behaves like black hole can compromise theother nodes by creating an illusion that it is still active by forwarding only selective packets and that data can be routed via it. To minimise the attack of selective forwarding in wireless sensor networks, multi path routing along with implementation of redundancies should be established with high reliable in routing

Sinkhole Attack

In the sinkhole attack, the intention of an adversary's aim is to decoy nearly all the congestion from a specified area which have been passed along with the endangered node, will have a chance to establish a false sinkhole with the adversary at the centre. If the enemy node does not introduce itself as the sink, the node closer to the sink will make more interruptions in the network because the traffic absorbed by enemy node will be more.

Sybil Attack

Node replicates itself and involves their existence in the differentlocations. In other words it is defined as a "malicious device illegitimately taking on multiple identifiers". The existence of this attack is at physical layer, data link layer and network layer.By verifying the identities of the valid nodes which having the unique key along with the base station the Sybil attack as been recovered. The shared key has been used for an encryption and also for the verification of link within the nodes of connections around the area.

Wormhole Attack

In the wormhole attack, an adversary burrows messages over a lowlatency link which have been received in one part of the network and plays back them in a different part. Wormhole attack is very difficult to detect because it uses out-of-bound channel to route packets. An adversary records packets or bits from whatever location in the mesh that can perforate them to another location and conveys them into the network.

Hello Flood attack

It is a novel attack against sensor networks. The unidirectionalconnections between nodes are highly utilized by this attack. Nodes broadcast hello packets with the help of routing protocols to announce themselves to their neighbours and a node inviting such a data packets may assure that it rests inside the (normal) radio range of the sender. Hello flood attack will taken part in the network layer.

This attack will increases the delay since the messages are need to beroutedmulit-hop to their parent nodes. The avoidance of this attack can easily be kept off by verifying the bi-directionality of a link through identity verification protocol before considering the information produced by the link.

Acknowledgement Spoofing

Many of the protocols in the TCP/IP suite do not provide mechanisms for authenticating the source or destination of a message. They are thus vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. IP spoofing and ARP spoofing in particular may be used to leverage man-in-the-middle attacks against hosts on a computer network. Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable ofdeep packet inspection or by taking measures to verify the identity of the sender or recipient of a message.

Disclosure

Release of message contents to any process not possessing the appropriate cryptographic key.

Traffic analysis

Traffic analysis is a special type of inference attack technique that looks at communication patterns between entities in a system. "Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security."

Masquerade

A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The attempt may come from within an organization, for example, from an employee; or from an outside user through some connection to the public network. Weak authentication provides one of the easiest points of entry for a masquerade, since it makes it much easier for an attacker to gain access. Once the attacker has been authorized for entry, they may have full access to the organization's critical data, and (depending on the privilege level they pretend to have) may be able to modify and delete software and data, and make changes to network configuration and routing information.

Content Modification

In a session replay attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

In a denial of service (DoS) attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.In a distributed denial-of-service (DDoS) exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

Active attacks contrast with passive attacks, in which an unauthorized party monitors networks and sometimes scans for open ports and vulnerabilities. The purpose is to gain information about the target and no data is changed. However, passive attacks are often preparatory activities for active attacks.

Sequence Modification

The attributes of the sequence that can be modified include:

- Changing the increment between future values
- Establishing new minimum or maximum values
- Changing the number of cached sequence numbers
- Changing whether the sequence cycles or not
- Changing whether sequence numbers must be generated in order of request
- Restarting the sequence

Timing Modification

Delay and reply messages.in connection oriented applications. Timing attacks are practical in many cases:

- Timing attacks can be applied to any algorithm that has data-dependent timing variation. Software run on a CPU with a data cache will exhibit data-dependent timing variations as a result of memory looks into the cache. Some operations, such as multiplication, may have varied execution time depending on the inputs. Removing timing-dependencies is difficult in some algorithms that use low-level operations that frequently exhibit varied execution time.
- Finding secrets through timing information may be significantly easier than using cryptanalysis of known plaintext, ciphertext pairs. Sometimes timing information is combined with cryptanalysis to improve the rate of information leakage.

Replay Attack

A replay attack is an attack where an authentication session is replayed by an attacker to fool a computer into granting access. It may be any form or retransmission of a network data transmission but is usually used to gain authentication in a fraudulent manner.Ways to prevent replay attacks from succeeding are:

1. Assign a random large session token to a session and the sender of the password sends a password modified by the session token value. The session token may only be used once. The authentication information sent may be the hash of the password added to the session token and hashed again.
2. The authentication session considers the time the transaction takes place. The password may tied in with an approximate timestamp and modified accordingly.

Conventional Security Requirements for IOT

Authentication is the process of identifying users, computers, devices and machines in networks and restricting access to authorized persons and non-manipulated devices. Authentication processes typically rely on usernames and passwords, which are not particularly secure, require frequent changing and do not work with unattended devices. Cryptographic mechanisms are a more robust way of securing communication over the Internet of Things.

Confidentiality

IoT services may contain sensitive data; therefore, IoT connected objects data should be keptconfident. Confidentiality can be achieved through encryption. Different existing symmetricand asymmetric encryption schemes can be leveraged to ensure confidentiality. However,selection of a particular type of encryption is highly application and device capability dependent. To exemplify, consider a smart home environment that maintains the information aboutthe owner activity at the home. The owner will never welcome that anybody who comes tohis home will read the data just by viewing the activity monitoring device.

Integrity

IoT services exchange critical data with other services and also with the third parties (e.g., authorities, service providers, control centers etc.), which put forward stringent demand thatsensed, stored and transmitted data must not be tampered either maliciously or accidentally. Integrity protection of sensor data is crucial for designing reliable and dependable IoTapplications. This is ensured with message authentication codes (MAC) using one way hashfunctions. The selection of MAC technique again depends on application and device capabilities. Consider the example of smart home that is connected with the smart grid. The smartgrid provider deployed an electricity consumption monitoring service in order to produceelectric bill.

Availability

Our envisaged IoT environment may comprise of sensor node hosted services. Therefore, it is extremely important that these IoT services be available from anywhere at any time in order to provide information (i.e., measured data, sensor alarm, etc.) continuously. There is no single security protocol that can satisfy this property. However, different pragmatic measures can be taken to ensure the availability. For example, in the aforementioned smart home if the attacker knows the consumption monitoring service, he can launch the denial-of-service (DoS) attack by just trying to send false service requests and the sensor nodes are incapable of handling huge number of requests due to resource limitations. Since any transmission (i.e., receiving or sending) consume power, the node will eventually run out of its battery.

In addition to these traditional security properties we also identify the following properties that need to be addressed by any IoT environment.

Authentication

It refers to the means used for the verification of one’s identity. In IoT context, mutual authentication is required because IoT data is used in different decision making and actuating processes. Therefore, both the service provider and service consumer needs to be assured that theservice is access by authentic user and service is offered by an authentic source. Furthermore,strong authentication mechanism needs to be deployed in order to prevent impersonation.Enforcing any authentication mechanism requires to register user identities and resourcelimitation of IoT objects poses stringent constraints to enable any authentication technique.

Authorization

It refers to the means of expressing the access polices that explicitly assign certain permissions to subjects. The IoT environment needs to provide fine-grained, re-useable, dynamic easy to use polices defining and updating mechanism. Thereby, it is imperative to externalizethe policy definition and enforcement mechanism of IoT services. Furthermore, the resourcelimitation of IoT sensor node restricts to employ such mechanism.

Access Control

This is an enforcement mechanism that allows only authorized users' access to the resources.The enforcement is usually based on access control decisions. Since, IoT is becoming omnipresent, privacy issue has become a real concern. For instance, consider the example ofsmart home that has smart power metering as IoT services and without a proper access control mechanism it could not only lead to disclosure of electricity usage pattern but it couldalso help adversary to deduce user related information such as when the user is at home,at office or travelling.

Authorization

Authorization or authorisation is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy.

Non Repudiation

Nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Interoperability of Security Enabled Internet of Things

The Communication and Real-World Access Layer

The layer provides an interface with an underlying IoT cloud. It implies an adapter orientedapproach to address the technological diversity regarding nodes and communication mechanisms. The layer provides different adapters to communicate with different type of nodesfor example Sun SPOT adapter to communicate with Sun SPOT nodes. The layer performnumber of tasks such that discovering nodes, receiving events from nodes and dispatchingthem to upper layers both for making sense of the events and sending them to their subscriber and invoking services hosted on the nodes.

The Semantic Overlay Layer

The semantic overlay layer acts as both the integrator and the interface between differentlayers. It provides the semantic model of an underlying IoT cloud by maintaining IoT ontology, sensor ontology, event ontology and service access polices. The layer also performsnumber of tasks such as facilitating create, read, update and delete (CRUD) operations onThe Service Virtualization LayerThe service virtualization layer provides web service interface for the functional aspects ofthe nodes in an IoT cloud. The layer perform various tasks such as translating virtual serviceinto web service definition, generating micro-formats of available web service.

The Application Layer

The application layer contains the real applications created using the data, semantics ofdata and application logics. Resolving the interoperability issues between different serviceprovider's platforms is the functionality of this layer.It is often required an application gateway to communicate with other systems and the Internet without IP-based network. Application gateways are complex to design and manage since they perform significant functional and semantic translation and carry an application-layer state [2]. A gateway device only needs to forward packets from or to the Internet, if the wireless network is according with the IP-based network architecture. Kernel could transmit IPv6 packets and run the routing protocol on the Internet side, while there are two approaches proposed in Ref. [17] to handle routing and 6LoWPAN logic. One case is that the 6LoWPAN logic is handled by the PC, the other is by the Micro control unit (MCU) in the IEEE 802.15.4 device. The former case is a good design for quick processing and large memory, while it is required to change the Linux kernel.

Enabling end-to-end secure communication between wireless sensor networks and the internet:

In the paradigms of the Internet of Things (IoT) as well as the evolving Web of Things (WoT) and the emerging Wisdom Web of Things (W2T), not only can the data collected by the sensor nodes (i.e., the things) in the wireless sensor networks (WSNs) be transmitted to and processed at Internet nodes and subsequently transformed into information, knowledge, wisdom and eventually into services to serve humans, but human users can also access, control and manage the sensor nodes in the WSNs through nodes in the Internet. Since data are the basis for enabling applications and services in W2T, it becomes imperative that enabling technologies for end-to-end security be developed to secure data communication between Internet user nodes and sensor server nodes to protect the exchange of data. However, traditional security protocols developed for the Internet rely mostly on symmetric authentication and key management based on public key algorithms, thus are deemed to be unsuitable for WSNs due to resource constraints in the sensor nodes. Specifically, acting as the server nodes in this scenario, sensor nodes cannot take on the heavy duty like regular servers in the Internet.

Authentication Systems in Internet of Things

Authentication Systems in Internet of Things this paper analyes the various authentication systems implemented for enhanced security and private reposition of an individual`s login credential.

Efficient and Secure Source Authentication Multicast

One of the main challenges of securing multicast communication is source authentication, or enabling receiversof multicast data to verify that the received data originated with the claimed source and was not modified enroute. The problem becomes more complex in commonsettings where other receivers of the data are not trusted and where lost packets are not retransmitted.

Dynamic user Authentication scheme for wireless sensor networks

We consider user authentication (UA) for wireless sensor networks. UA is a fundamental issue in designing dependable and secure systems. Imagine that a wireless sensor network is deployed in an intelligent building, a hospital, or even a university campus, to allow legitimate users to send queries and retrieve the respective result at any of the sensor nodes. Importantly, the system needs to provide a means of user authentication to verify if the user is valid. We propose a dynamic strong-password based solution to this access control problem and adapt it into a wireless sensor network environment.

Authentication and key establishment in dynamic wireless sensor networks

When a sensor node roams within a very large and distributed wireless sensor network, which consists of numerous sensor nodes, its routing path and neighborhood keep changing. In order to provide a high level of security in this environment, the moving sensor node needs to be authenticated to new neighboring nodes and a key established for secure communication. The paper proposes an efficient and scalable protocol to establish and update the authentication key in a dynamic wireless sensor network environment. The protocol guarantees that two sensor nodes share at least one key with probability 1 (100%) with less memory and energy cost, while not causing considerable communication overhead.

Improved authentication and integrity verification in WSN

Message authentication is one in all the foremost effective ways in which to thwart unauthorized and corrupted messages from being forwarded in wireless device networks (WSNs). For this reason, several message authentication schemes are developed, supported either symmetric-key cryptosystems or public-key cryptosystems. Polynomial-based theme was recently introduced. However, this theme and its extensions all have the weakness of an intrinsic threshold determined by the degree of the polynomial once the amount of messages transmitted is larger than this threshold. During this paper, we propose to scalable authentication theme supported elliptic curve cryptography (ECC).

Conclusion

Authentication is critical for the security and integrity of schemes in internet of things. In this paper, we have surveyed the various authentication techniques that are proposed by research .however, the issues and requirements on authentication and security remains the same .traditional authentication methods are not suitable for system in IOT. So new and morden authentication and security methods need to be created keeping in mind the IOT environment and properties.

References

1. M.A. Chaqfeh, N. Mohamed, Challenges in middleware solutions for the internet of things, in: 2012International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, 2012, pp. 21–26.
2. S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011, Chennai, India, 2011, pp. 1 – 5.
3. M.C. Domingo, An overview of the internet of underwater things, J. Network Comput. Appl. 35 (6)(2012) 1879–1890.• [16] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architecturalelements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
4. Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. NetworkComput. Appl. 42 (0) (2014) 120–134.
5. Y. Zhao, Research on data security technology in internet of things, in: 2013 2nd InternationalConference on Mechatronics and Control Engineering, ICMCE 2013, Dalian, China, 2013, pp. 1752–1755.
6. T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, Dtls based security and two-way authenticationfor the internet of things, Ad Hoc Netw. 11 (8) (2013) 2710–2723.
7. R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in thecontext of the internet of things, Comput. Electrical Eng. 37 (2) (2011) 147–159.
8. W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, A pairwise key predistribution scheme forwireless sensor networks, ACM Trans. Inf. Syst. Secur. (TISSEC) 8 (2) (2005) 228–258.
9. D. Liu, P. Ning, Establishing pairwise keys in distributed sensor networks, in: CCS '03 Proceedings ofthe 10th ACM Conference on Computer and Communications Security, Washington, DC, USA, 2003, pp. 52–
10. F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical En-RouteFiltering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, Mar. 2014