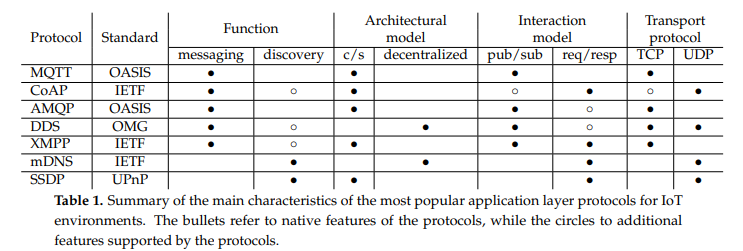
# Summary 2

Paper 6

“Security of IoT application layer protocols: challenges and findings”

Giuseppe Nebbione\* and Maria Carla Calzarossa

* This paper offers a comprehensive analysis of the security risks and 47 challenges affecting the most popular application layer protocols employed in IoT environments. In 48 particular, the paper examines and classifies the potential security threats and attacks outlined in the 49 protocol standards.
* “*IoT technologies are becoming pervasive in public and private sectors and represent 2 nowadays an integral part of our daily life. The advantages offered by these technologies are 3 frequently coupled with serious security issues that are often not properly overseen or even ignored. 4 The IoT threat landscape is extremely wide and complex and involves a large variety of hardware and 5 software technologies*.”.
* In the complex IoT world, application layer protocols play a key role. In fact, they are at the 45 basis of the communications among applications and services running on different IoT devices and 46 on cloud/edge infrastructures.
* To gain some further insights of whether/how security threats have materialized 50 and of their actual impact, these threats are also studied under a different perspective, that is by 51 analyzing the Common Vulnerabilities and Exposures (CVE) collected by MITRE for products and 52 services devising the various protocols
* The paper gives some background to the IOT threat landscape, citing studies stating almost 25% of cyberattacks against businesses will be IOT based.
* Application layer protocols: the paper states different application layer protocols and tells us where they are used majorly.



* The choice of the application protocol depends on the nature of the IoT systems and their requirements. MQTT and CoAP are particularly suitable for services requiring data collection (e.g. sensor updates) in constrained environments. On the contrary, AMQP, DDS and XMPP address specific service requirements, namely, business messaging, instant messaging and online presence detection and real-time exchanges, respectively. In terms of service discovery, mDNS and SSDP are the protocols of choice for IoT environments.
* MQTT: MQTT security threats have been investigated and a proposed model to identify the ability of threats was put together, DDos attacks can be carried out by sending large messages, unauthorized messages can also be sent aimed to damage the device.
* Mitigations

1. Authentication of users and devices
2. Authorization of access to server resources
3. Integrity of MQTT control packets and application data
4. Privacy of MQTT control packets and application data

Use of lightweight Elliptic Curve Cryptography along with a control packet version called Spublish were highlighted as being effective for better security

* CoAP : CoAP shares many characteristics with the HTTP protocol but it has been specifically designed for constrained devices with limited energy, processing power, storage space and transmission capabilities hence has lower security.

CoAP supports the usage of the Datagram Transport Layer Security (DTLS)

* Security threats of CoAP-enabled devices are:

1. Message parsing
2. Proxying and caching
3. Bootstrapping
4. Key generation
5. IP address spoofing
6. Cross-protocol exchanges

* Mitigations for CoAP:

The mitigations proposed by these works mainly focus on two aspects:

1. Access control mechanisms
2. Secure communication

A proposed approach discussed is based on the authentication of CoAP nodes and the usage of tickets to grant access to resources.

Improvements of the DTLS protocol have also been studied from the perspective of the cryptographic algorithm. In particular, the integration of DTLS over CoAP based on Elliptic Curve Cryptography helps in minimizing the computation overhead and ROM occupancy.

* DDS protocol is also discussed, whose vulnerabilities such as the handshake protocol used for permission attestation sends clear text information about participant capabilities, thus allowing attackers to discover potentially sensitive reachability information on a DDS network.
* Xmpp protocol is also discussed, with vulnerabilities mainly referring to the authentication and message validation processes along with insufficient controls on memory operations and inappropriate certificate verification.

Paper 7

“Evaluating Security Threats for each Layers of IoT System”

M.Junaid Arshad

* In this paper we will see the a) layer base architecture for the IoT b) attacks can be performed c) solution for that attacks and try to make sure the security of our data on each layer
* In this paper a review of all types of attacks and effects of that attack on each layer is carried out.
* We focus on the Application Layer related review.
* For the Application layer the major threats are

1. Sniffing Attack: A sniffer application is introducing by the attacker into the system which collect all the information from the network about the devices and communication
2. Data Leakage: At application level the security risk of data stalling is increase if the attacker knows the vulnerabilities of the application.
3. DoS/DDoS Attack: In DDoS attack create the environment where the requests are overloaded and make the system down or halt for real users
4. Malicious Code: If the attacker knows the vulnerability of the application then he can upload an malicious code while up-gradation of application

* In the Application Layer we have already seen the protocols used such as XMPP, CoAP, AMQP and MQTT
* To make the communication secure different type of authentication methods are used such as RSA and Elliptic curve cryptography.
* As a security measure Authentication is discussed:

“*An advance method of authentication is used in which a key is use for authentication of device. A secure Vault is used to store all the keys. While Developing the IoT device a secure vault is shared with IoT device and also with the server*”

* The paper also references to other papers who also approach the security aspect of IoT devices.
* In conclusion this paper is presenting the explanation of layered base IoT structure Security measurements with some possible solution for the networks are also discussed here which make the IoT network more secure.

Paper 8

“Security Threats in the Application layer in IOT Applications”

Prof. Dipti Jadhav, Prof. Nikita Kulkarni.

* This paper represents the overview of Security principles, Security Threats and Security challenges at the application layer and its countermeasures to overcome those challenges
* The most widely used application layer protocol is MQTT. The security threats for Application Layer Protocol MQTT is particularly selected and evaluated
* This paper main focus is on the Internet of Things Security threats at the Application layer.
* There are many application layer protocols for different Internet of things applications. Depending upon the application and rate of data transmission, time, heterogenous infrastructures and smart devices available, particular protocol is selected. The main aim of these protocol is to identify, track, monitor and manage the smart devices present in the network.
* The important security goals of the Internet of things is to provide a reliable connection, and proper authentication mechanisms and provide confidentiality about the data to each device connected in the whole network
* The data can be accessed by the permitted user only. Data confidentiality can be achieved by data encryption mechanism where each bit of data is converted into cipher text and followed by two-step verification process, in which two devices/components allows access only if both the devices pass the authentication test, and a biometric verification in which the person is uniquely identifiable.

The ECC technique is very useful in this regard.

* Security measures: Authentication: The authentication process restricts any malicious user from accessing the data, this process defends by integrated identity identifications. The cloud computing and virtualization are the main technology that are more prone to attacks. Insider threats for cloud computing and data theft, DOS attacks for the virtualization are most feared attacks. Proper authentication technics should be employed.
* Intrusion Detection: Intrusion detection technics produce the alarm on any suspicious activity in the system and provide an administer solutions for many threats by uninterrupted monitoring and cloud computing and virtualization technologies.
* Data security: The encryption methodologies is incorporated for data security.
* In conclusion: This paper briefly mentioned about the security goals, security threats and security challenges and probable solutions for securing the Internet of things system.

Topic Chosen: Elliptic Curve Cryptography.

Overview:

In 1985, Koblitz and Miller introduced Elliptic Curve Cryptography (ECC) as potential solution to conventional public key cryptographic algorithms for example, RSA (Rivest, Shamir & Adleman, 1978). Similar to ElGamal techniques with the group FP, elliptic curves based cryptography algorithms uses elliptic curves defined over finite fields. The equation of elliptic curve on which all the mathematical operations are defined is:

An elliptic curve represents a set of pair of (x,y) satisfying the equation defined where value of ‘a’ and ‘b’ gives a different elliptic curve. All point pairs (x,y) and point ‘O’ at infinity lies on the elliptic curve.

Point doubling is a process performed on the Elliptic curve by which, given a point Pt = (xp,yp) and a multiplicand N we can figure out the point Pn = 2 \* Pt (by drawing tangent at Pt , finding the point where the tangent to Pt cuts the elliptic curve, and mirroring this point about the X axis we get the point 2Pt) (*Note: Only even multiples can be found for this method*)

Point Addition is a process by which 2 points on the curve can be added to find the third point

(P1 (x1,y2) and P2 (x2,y2) being points on the curve, we can find the line joining these two points. This line cuts the elliptic curve once more and yields the point -P3, on taking the mirror image of P3 about the X axis we get the point P3 = P1 + P2 )

Using these two methods we can find Pn = N \* Pi (where N can be odd or even) this is called Point Multiplication.

These methods on this curve can be used as a trapdoor function, because generating the point Pn from N and point Pi is easy**, but getting the value of N, from Pi and Pn is very difficult**.

Therefore N can be a Private Key known only to a owner device. Pn can be a public key for that device and Pi can be a generator point known to all. Hence even though an attacker knows the generator point and Public key we can guarantee that it is very difficult to find any private key and when compared to the RSA method ECC requires less space.

* For Generating keys

Device 1 chooses a secret number (usually a large prime number) ‘r1’ which is used as a Private key.

G is a generator point (xg,yg) on the elliptic curve, Known to all devices in the network.

A Public Key ‘P1’ for Device 1 can be generated by the process (where G is a Generator point (xg,yg) on the curve and \* is point multiplication)

A similar Public Key ‘P2’ for Device 2 can be generated by the process (where r2 is the private key for Device 2 and G is same as above)

Now the Public Keys of all Devices can be shared with one another.

* Process of Sending a message:

Suppose Device 1 wants to send a message ‘m’ to Device 2 (*Note: they both have each other’s public keys*)

Device 1 uses the Public Key ‘P2’ of Device 2 to encrypt his message, he does this by:

Multiplying his private key ‘r1’ with ‘P2’ (Public Key of Device 2) giving a secret point ‘S’ (Using Point Multiplication & Addition)

Now he sends encrypted message ‘M’ to Device 2

Where (Here M is Encrypted message, m is actual message and S is Secret point)

Since Device 2 has the public key P1 (of Device 1) and its private key ‘r2’

Device 2 can simultaneously find the value of ‘S’ since

Upon receiving the encrypted message M from Device 1,

To get the actual message ‘m’ Device 2 will simply subtract S from M to get m

Or

This method of encryption is useful because getting the private key ‘r1’ or ‘r2’ is very difficult because the Point Multiplication function ( \* ) on the elliptic curve is a One way function.

