EUROTECH
Imagine. Build. Succeed.

Securing Enterprise IoT Environments

An Executive Overview

white paper

Authors

Robert Andres
Chief Strategy Officer
Eurotech S.p.A.

Bob Emmerson
Industry Observer

www.eurotech.com
welcome@eurotech.com

Resume

The Internet of Things (IoT) divides into B2B and B2C sectors. This is a B2B paper, however, the term Industrial IoT (IIoT) is widely used and it is the one that Eurotech employs.

The paper starts with a holistic, executive overview of IoT security issues, what is needed to realize a secure environment, and the various security mechanisms that need to be implemented. In addition it considers the different ways that security can be compromised and the widely different reasons why attacks are made.

Executive

When the de facto barrier between the Operational Technology (OT) domain and the Information Technology (IT) is removed, OT domains appear to be seamless extensions to an enterprise's IT-centric network, which is a key Industrial IoT (IIoT) objective. However, this development also introduces a new set of security issues for enterprise management. In this paper these issues are addressed generically, focusing on the OT world and the interfaces to the IT world. In addition we demonstrate how security technologies and processes are implemented in Eurotech IIoT solutions in order to realize robust enterprise environments.

We do not examine security at the IIoT field level in detail, i.e. the smart edge devices and sensors, although many of the principles described elsewhere apply. Nor do we consider many of the best practices and common sense actions in detail, e.g. physical security. Instead, the focus is on securing the core IIoT infrastructure - software-defined multi-service edge gateways and the IIoT/M2M integration platform - as well as the various communication links.

We shall also explain that manageability is an essential part of the overall security solution. The software on the devices has to be maintained in a secure way: ideally this should be done using over the air updates.

NB: If you are unfamiliar with any of the security terms that are used in this paper you can find explanations in the "Key security related terms and abbreviations" section on page 19.

Cybercrime: a growth industry

This paper is titled "*Securing Enterprise IoT Environments*", but gaps in IT security have enabled cybercriminals to access tens of millions of records containing identifiable information as well as credit and debit card data. In earlier years security was enabled by a firewalled perimeter and virtual private networks (VPNs), but the widespread use of mobile phones, connected applications and the increased level of sophistication of the attackers has led to breaches in those fortified perimeters.

For example, there may be security vulnerabilities in operating systems or applications. In addition, employees might visit malicious websites and open a file that enables attackers to install malware, and once installed they can move around inside the perimeter. This security breach could be leveraged for accessing and manipulating data, harming the attacked company's business or leveraging its devices and infrastructure as a basis for attacks on other target companies.

Dissolving the barrier between the IT and OT domains in an IIoT solution that does not employ robust security mechanisms can be exploited in a similar way, i.e. attackers can gain access to individual devices or to all the systems in the OT infrastructure. This would, for example, enable attackers to launch DDNS and botnet attacks in very destructive ways, with obvious and legal consequences, particularly for companies that made it easy for the attackers.

Unfortunately we can expect more attacks being made in future, although many will not be reported. Moreover cybercriminals have access to very sophisticated technology, which is making cybercrime easier and more profitable.

The cybercriminals

At one end of the spectrum we have so-called script kiddies, who use programs developed by others to attack computer systems and networks for “fun”. At the other end we have individuals or organizations that are very sophisticated and sometimes they are very resourceful: they are known as hackers. So-called crackers are the individuals or organizations whose intentions are criminal. Their motives are primarily financial, but this group can even include governments who intend to conduct cyber warfare. Other motives include espionage, regular and industrial; sabotage; disruption of a company’s business and theft of intellectual property rights (IPRs).

Cybercriminals can employ the increased threat surface that comes from the billions of connected users and devices and the relatively poor security of the IoT devices that connect to the network and cloud services. This means that the challenge for the defenders against cybercrime is growing.

The biggest security issue right now is the so-called advanced persistent threat (APT), which attacks specific high-value information. Industry estimates put the cost of data breaches caused by APTs at around $5 million per breach: the breach at Sony in 2014 is estimated to have cost over $160 million. In addition, IoT infrastructures and devices, simply because of scale and pervasiveness of technology and applications, will be targeted. In addition, new attack scenarios will appear. Unfortunately cybercrime is a growth industry: the returns are great, and the risks are low. And each and every business can be targeted at any time.

Security vulnerabilities in many places

The previous section indicated the massive size of the attack surface. Now we are going to consider it in more detail. Figure 1 focuses on the section of the IoT infrastructure that connects device hardware to business applications, but there are many ways an attacker can exploit vulnerabilities. The intrinsic fragmentation and inherent complexity of these infrastructures can open many doors.

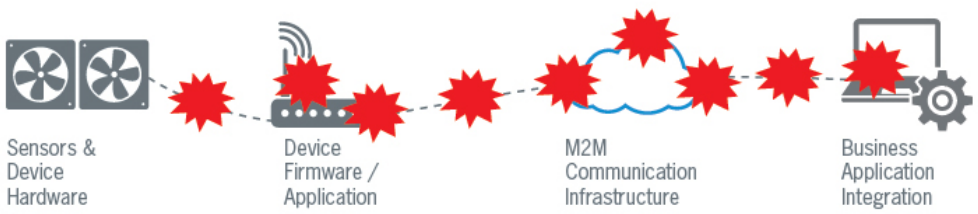

Figure 1. There are vulnerabilities inside the four domains as well as the interfaces, where very robust mechanisms are needed.

Appropriate levels of security in these IoT solutions can only be achieved if security is an integral and fundamental part of the overall architecture. IoT security has to be implemented end-to-end and in the individual elements. Best practice has to take into account the specific aspects of distributed, unattended, mobile systems/devices. And last, but not least, IoT security has to integrate easily and effectively with existing IT security measures.

Layered security

Eurotech solutions enable a seamless flow of data: they are end-to-end solutions. However, a single solution cannot enable end-to-end security: there is no silver bullet; it is essential to look at the entire system holistically and address security at each potential point of failure. In turn, this indicates that security must be a fundamental part of the overall architecture of an IIoT system, i.e. be designed in, not added afterwards.

Figure 2 shows how the functionality of the OT world is divided into three layers: (1) the field infrastructure where the devices that generate M2M data are located; (2) the communication infrastructure that transfers data to the IIoT Platform in the cloud; and (3) the IoT application infrastructure, the layer that enables integration with mainstream business processes.

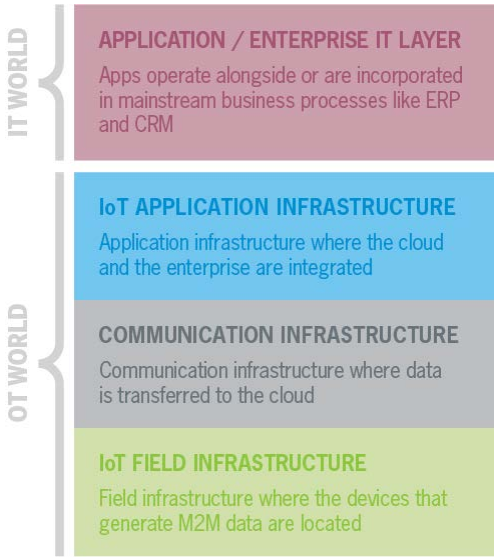

Figure 2. There are four basic potential attack vectors in this layered architecture.

At the top there is the interface between the OT world and the enterprise IT world. Security requirements at this level against eavesdropping and manipulation include: robust authentication, data protection and many of the best practice security measures taken from the IT world.

The IIoT/M2M integration platform, which is located in the cloud, has to be secured internally and also in the context of its place in the infrastructure, i.e. the network, cloud and data centers.

The multi-service edge gateway in the communication infrastructure needs robust internal protection in order to provide a secure execution environment. This includes securing the devices, sensors, actuators in the field infrastructure and their communication links to the gateway when applicable. NB: If there is a network link from sensors, actuators and devices to the IIoT platform then the security issues are fundamentally the same as those described in this document.

Details of how the field infrastructure is secured are outside the scope of this paper, apart from authentication principles and IP network security. However, the infrastructure employs intrinsic security measures at this level. For example, we minimize the "attack surface" by utilizing firewalls and by reducing communications from the devices and the gateways to a single outgoing connection that is message oriented in nature.

Basic IoT security architecture requirements

The foundation for secure solutions should be based on:

- Devices having a validated identity
- IoT platforms that have a validated identity
- Mutual authentication for communication
- Signed messages over an encrypted channel
- Secure execution environment
- Secure software management
- State-of-the art network & system security
- Role based access control
- Secure management access

In addition, the following best practices should be adopted:

- Build solutions based on open and industry standards
- Leverage proven IT/enterprise class security technologies

- Include security, scalability and resiliency in design from day one
- Encapsulate the complexity of an end-to-end security solution
- Continuously test and audit the system.

These are generic requirements and there should be no compromises. Needless to say these are all enabled in Eurotech solutions.

Different protocols at different levels

Enabling the requisite robust security entails working with different communication technologies. Typical examples in the Field Infrastructure are ZigBee, Bluetooth, Ethernet, Wi-Fi, RFID, but also Field Bus technologies like Modbus and CAN. As and when new protocols like LoRa go mainstream they will be enabled in order to ensure that solutions continue to deliver the optimum performance. Eurotech is a member of the LoRa Alliance.

At the next level Internet connectivity (at OSI Model Layers 1 & 2) is enabled by communication technologies like Cellular Networks, Satellite, Ethernet, Wi-Fi and xDSL.
The Application Infrastructure (starting with OSI Layer 5), which is layered above TCP/IP, employs communication protocols that address the specific needs of devices that are unattended, geographically dispersed, and often mobile.

Eurotech supports different protocols, but we advocate the use of MQTT (Message Queue Telemetry Transport), which is not only a lightweight protocol optimized for

M2M device communications, but also a heavyweight technology that enables IM-type messages to be used and files exchanged.

Figure 3. MQTT provides secure messaging between Everyware Software Framework (ESF), which is embedded in the gateway and Everyware Cloud. All MQTT traffic is encrypted over an SSL connection. Device management messages published by the cloud are signed to guarantee authenticity and message integrity.

Device and server authentication

The IIoT is predicated on data generated by remote sensors, actuators, and smart devices that will be integrated with business and mobile applications. To ensure that devices, systems and applications can trust their respective counterparts it is necessary to identify and authenticate the connected devices in the field as well as on the cloud/server side.

Secure authentication can be achieved in many ways. But when looking for a standards-based, proven and solid technology approach, solutions that leverage

digital certificates provide the highest level of security. One of the important standards is X.509, a cryptography standard for a public key infrastructure (PKI). It specifies, amongst other things, standard formats for public key certificates and their management.

X.509 certificate-based authentication is an effective way of identifying individual devices. Eurotech integrates X.509 with the powerful PKI functionality in the Everyware Software Framework and Everyware Cloud in order to issue and manage the certificates. They can also be used to sign application code that is deployed and executed in the IIoT devices and gateways in the field.

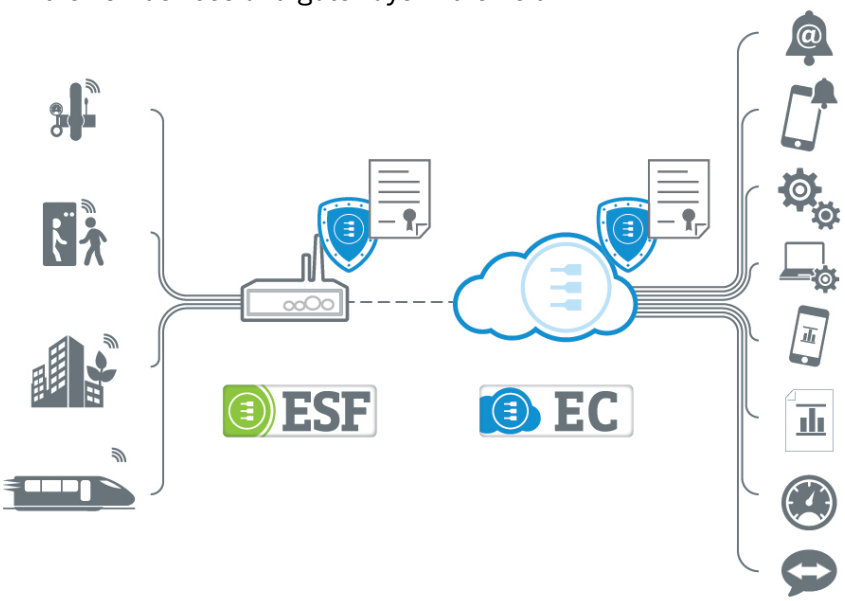

Figure 4. Integrated certificate management is enabled by X.509 certification deployed in the ESF and the cloud. This provides integrity, authenticity and non-repudiation of the data's origin.

Similar functionality is needed for the server. In addition, the ability to manage and execute applications remotely in the field is essential in many IIoT applications. For example, over-the-air provisioning and software updates have to be secured.

Data security

Data security is very important. Secure transmission of all data via encryption over an SSL connection is essential. All Console and REST API access must only be available over an encrypted HTTPS connection. State-of-the-art data centers that utilize the most current architectural and engineering approaches are ideal. All databases should be protected from external access through strict firewall rules. And data should be segregated by account.

Identity and access management

Confidentiality and integrity can be ensured through a role-based access control model and access control lists that follow the Principle of Least Privilege and are enforced through all the layers of the architecture. Each account manages a list of users and controls the user's credentials. Eurotech's Everyware Cloud, for example, has a configurable lockout policy per account, which may block a user's credentials after a certain number of failed login attempts. Logins to Everyware Console can be further protected through the use of a Two Factor Authentication (2FA).

Vulnerability management

Independent, certified security firms perform remote vulnerability assessments, including network/host and applications. Vulnerability scanning should be conducted regularly and after any major changes to the infrastructure and environment.

Remember, when thinking about IIoT security, although data security is essential, do not forget all of those other potential points of failure. From the most remote device in the field to the backend business system, every part of the IoT solution must be secure.

Mandatory requirements

Devices must not have open inbound ports from a TCP/IP perspective. We do this by specifically addressing the Internet traffic to the IIoT gateway/edge devices by aggregating all communication into a single outgoing connection that is message oriented in nature and SSL/TLS protected. We use the MQTT protocol, for data and device management. In general ports should be closed whenever it is possible. End-to-End Encryption is needed, not only for data but also for device management.

Robust authentication is essential; it's enabled by strong, well-understood technologies like X.509 Certificates and encrypted credentials. It is a solid foundation for many of the security services at the IIoT platform and the device level.

Device status and health monitoring, which is layered on top of MQTT, is an important additional security feature. MQTT level connectivity with individual devices is constantly monitored by the broker infrastructure, thereby enabling actions to be taken very quickly. In addition, the diagnostic capabilities of Everyware Cloud allow devices to be monitored at lower levels. For example, even the usage of system resources like CPU utilization can be used to identify issues taking place at the edge followed by remedial actions.

The Everyware Cloud and Everyware Software Framework provide user-friendly setup and upgrades.

NB: In legacy OT solutions a lack of support for old software, often for legal reasons plus a lack of affordable, practical ways of maintaining the software, means that OT solutions stay as they are, sometimes for decades. No security patches, etc. While in the past most of these devices were connected through private secured networks, now the Internet is used as the OT infrastructures backbone - with obvious security consequences.

Designed in security

As indicated earlier, security attacks are often made via the communication interfaces, therefore ultra-robust mechanisms are needed in the Multi-service IoT Edge Gateway and the Everyware Cloud. Earlier we indicated that security must be a fundamental part of the overall architecture.

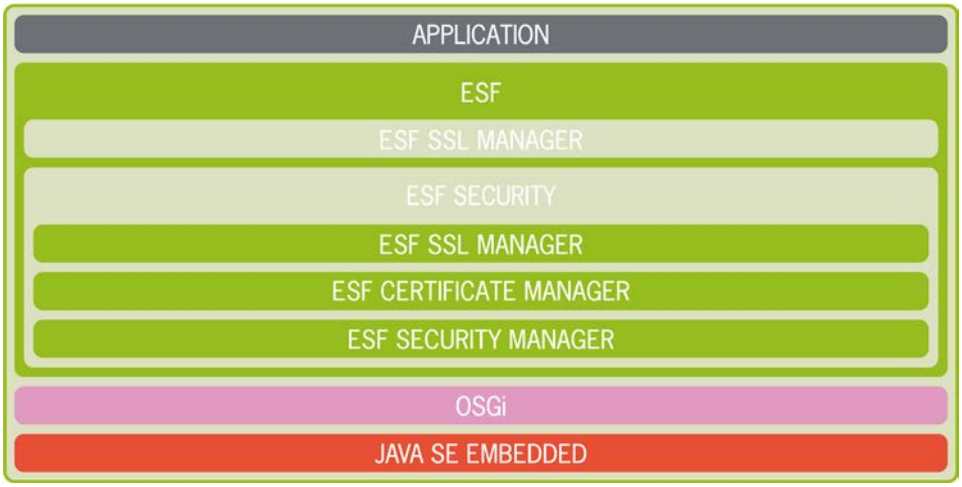

Figure 5. Security mechanisms are an integral component of the Eurotech's Everyware Software Framework (ESF), which in turn is embedded in the Multi-service IoT Edge Gateway.

The ESF architecture is based on different software layers, which allows developers to start writing the application on top of a solid, hardware abstracted platform. The OSGi (Open Services Gateway Initiative) layer provides a good foundation for securely managing software components (signed bundles).

The ESF Security layer encapsulates a comprehensive portfolio of security features and simplifies usage by the programmer/user. This approach abstracts and encapsulates many of the authentication/security aspects in the device and is supplemented by other measures like secure boot, appropriate hardware design and other measures, thereby ensuring proper protection of the solution in the field.

Everyware Cloud

Everyware Cloud unites the OT domain and the IT domain, which means that it is the single, most important interface. A success attack would enable access to the enterprise environment. Everyware Cloud also functions as an IoT integration platform that acts like an operating system for the infrastructure. On the operational technology side it provides all the data, device and embedded application management required to deploy and maintain distributed intelligent systems in the field. This schematic indicates how security is embedded in Everyware Cloud.

Figure 6. The Edge-to-Cloud-to-Application Security Architecture incorporates X.509 Certificate based authentication plus Integrated PKI Certificate management.

Security mechanisms in the cloud ensure that authorized traffic is secure and authenticated; that no unnecessary ports are open on the application/interface servers: that the infrastructure is secured.

Access control is centralized and authenticated via HTTPS/SSL. Role-based access control is employed as well as user management and roles and permissions.

A strict segregation of tenants down to a data level is another important element ensuring that other parties cannot access data and infrastructure.

Securing Edge-to-Cloud (communication security) allows traffic that is secure and authenticated. The broker/infrastructure/perimeter defense employs firewalls, all in-bound ports other than broker ports are closed and secure (encrypted and authenticated) MQTT messaging is employed.

The initial pairing and provisioning of an IoT device with the IIoT Integration Platform is another important security-related aspect.

Since remote device management is an important element of many IIoT solutions, Everyware Cloud offers a sophisticated VPN Service. This provides secure transparent communication channels with IIoT gateways and devices, but also network connected assets behind the gateways. Asset examples include industrial ovens, manufacturing machines, printers, medical diagnostic devices and air conditioners.

Looking ahead

Cybercriminals are increasingly operating as syndicates: they conduct research and buy services from each other. Cybercrime has become a well-financed global industry, fueled by the value of the data that is being generated. The biggest security issue right now is the advanced persistent threat, which attacks specific high-value information. These attacks are well concealed and they only need to establish a single connection, which can come via an employee's device after visiting a malicious website and opening a file.

One response is to employ scalable stream analytics in the edge cloud, which detects attackers, and to share this information in the cloud and network provider communities. Another is to provide multiple levels of encryption. However, the only way to effectively fight the cyber war is to make the cost of illegally accessing information much higher than the value of that information to the attacker.

Traditionally enterprise security employed perimeter based security, but APT doesn't respect this approach and this has resulted in solutions that combine endpoint, perimeter and network-based security. In future we can expect to see security analytics being deployed on a massive scale, allowing the network activity in virtually all devices to be recorded and stored. This will enable real time APT detection and mitigation, as well as forensic analysis. In addition, SDN (Software Defined Networks) will provide dynamic flexibility, allowing networks to quickly and automatically adapt to security threats.

These are the kind of developments that are coming to IT and IIoT domains, but meanwhile approaches to security will have to change if companies wish to comply with the General Data Protection Regulation (GDPR), which obligates European companies to adopt preventative security measures that lower the risks of data breaches and mitigate the consequences after an incident occurs. All organizations controlling the processing of personal data will have to notify both authorities and affected individuals when a data breach incident occurs- and face the damage caused to their reputation and bottom line.

Summary and conclusions

The security technology measures outlined in this paper are a solid basis for IIoT infrastructures. We have emphasized the need to implement end-to-end security: to look at the entire system holistically and address security at each potential point of failure. In turn, this indicates that security must be a fundamental part of the overall architecture of an IIoT system, i.e. be designed in, not added afterwards.

Eurotech IIoT solutions are compliant but we are also vigilant: when the security bar goes up, when new threats emerge, so does our response and that of the Industry. Cybercriminals can take advantage of the huge opportunity that comes from billions of connected users and devices. But through technology and cooperation, by employing analytics in the edge and the cloud, attacks can be detected in real time, and by sharing information throughout the industry, the pendulum will start to swing away from the attackers and towards the users.

Key security related terms and abbreviations

NB: Security is a moving target, so it is advisable to have an independent certified security firm perform remote vulnerability assessments at regular intervals, e.g. every quarter, or when there is a major change in the infrastructure and the environment.

APT: advanced persistent threat is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention is to steal data rather than to cause damage to the network or organization.

APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.

Botnet: a is a jargon term for a collection of software robots (bots) that operate automatically and independently. The term is often associated with software that sends unsolicited email automatically, i.e. spam but also DDoS attacks.

CAN: Controller Area Network is a standard for a serial data bus widely used, for example, in vehicles. It enables real-time communication at up to 1Mbps.

DDNS: a method of automatically updating a server in the Dynamic Domain Name System.

DDoS: Distributed denial-of-service attacks try to disable services for the intended user. The difference between a regular denial of service attack and a distributed DoS attack is that multiple computers simultaneously carry out the attack.

Firewall: a software or hardware system that protects the resources of a network or system against abuse from outside.

HTTPS: HyperText Transfer Protocol Secure is an extension to the HTTP protocol, designed to secure data exchange. When using HTTPS the data is encrypted.

LoRa: is a low-power, wireless networking protocol that enables low cost, secure two-way communication in the IoT solutions. Eurotech is a member of the LoRa Alliance.

Malware: any software that is used to disrupt computing systems, collecting sensitive information, or to gain access to computer systems. The word is a contraction of malicious software. The biggest cause of a malware infection is through holes in software.

Modbus: is a serial communications protocol used to communicate with PLCs that enables communication among devices and sensors, for example a system that measures temperature, pressure and humidity.

MQTT: a lightweight communications protocol but it's also a heavyweight technology. IM-type messages can be used and files exchanged, which means that transportation is payload agnostic. MQTT has the following attributes:

- Message oriented
- Publish &.Subscribe
- Hierarchical Namespace

In addition, MQTT has three QoS levels.

OSGi: Open Services Gateway initiative. The *OSGi specification* describes a modular system and a service platform for the Java programming language that implements a complete and dynamic component model, something that does not exist in standalone Java / VM environments.

The technology is a set of specifications that define a dynamic component system for Java. They enable a development model where applications are (dynamically) composed of many different (reusable) components. The specifications enable components to hide their implementations from other components, while communicating through services, which are objects that are specifically shared between components. This surprisingly simple model has far reaching effects for almost any aspect of the software development process.

PKI: Public Key Infrastructure is widely recognized as one of the strongest authentication mechanisms. It's a technology that binds public keys with the respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. A third-party validation authority (VA) can provide this information on behalf of the CA. The binding is established through the registration and issuance process.

It's a system for the creation, storage, and distribution of digital certificates that verify that a particular public key belongs to a certain entity. PKI digital certificates map public keys to entities, securely store these certificates in a central repository and revoke them if needed.

Public key cryptography is a technique that enables users to securely communicate on an insecure public network, and reliably verify the identity of a user via digital signatures. It is also the underlying technology used in modern secure payment systems.

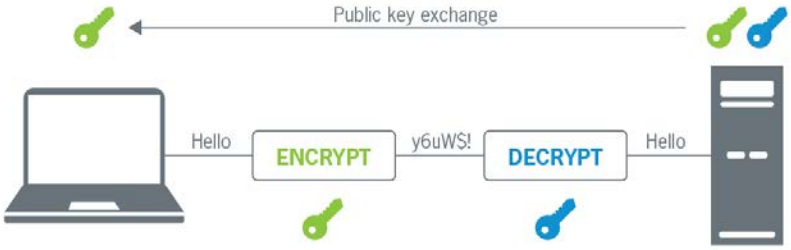

Figure 7. Public-key cryptography uses a separate key for encryption and decryption. Anyone can use the encryption key (public key) to encrypt a message. However, decryption keys (private keys) are secret. This way only the intended receiver can decrypt the message.

REST: REpresentational State Transfer is an architectural style, and an approach to communications that is often used in the development of Web services. The use of REST is often preferred over the more heavyweight SOAP (Simple Object Access Protocol) style.

Role based access control: is an approach to restricting system access to authorized users according to roles and rights/privileges associated with their roles. In this context access is the ability of an individual user to perform a specific task, such as view, create, or modify a file or data set. Roles are defined according to job competency, authority, and responsibility within the enterprise.

Tenant segregation: Multi-tenancy in cloud results in an effective sharing of resources and services to run software instances serving multiple consumers and client organizations (tenants). It means physical resources (such as computing, networking, storage) and services are shared. In this environment security requires

strict logical segregation (at the respective layers) rather than the physical separation of resources.

Secure boot: is a technology where the system firmware checks that the system boot loader was signed by an authorized cryptographic key.

Software Defined Networking (SDN): this is an approach to networking that allows network administrators to manage network services through abstraction of higher-level functionality. This is done by decoupling the system that makes decisions about where traffic is sent (the control plane)) from the underlying systems that forward traffic to the selected destination (the data plane).

SSL (Secure Sockets Layer): is a standard security technology for establishing an encrypted link between a server and a client. It allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text, which is vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information. More specifically, SSL is a security protocol. Protocols describe how algorithms should be used; in this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.

TLS (Transport Layer Security): is a protocol that provides secure connections at the transport layer of the Internet. The standard is used on top of standard Internet transport protocols (TCP/IP) and provides a secure base for application protocols such as HTTP (web traffic) or SMTP and IMAP (mail exchange). TLS uses certificates to provide assurance about the identity of both communicating parties before communication takes place.

X.509: is an ITI-T standard for a public key infrastructure. It specifies standard formats for public key certificates, certificate revocations lists, attribute certificates and a certification path validation algorithm.