WHITEPAPER

MTE TECHNOLOGY:

The Compact Solution to Safeguard IoT Data

Document ID: ECLYPSES-1532395320-116
Version No.: 2.0

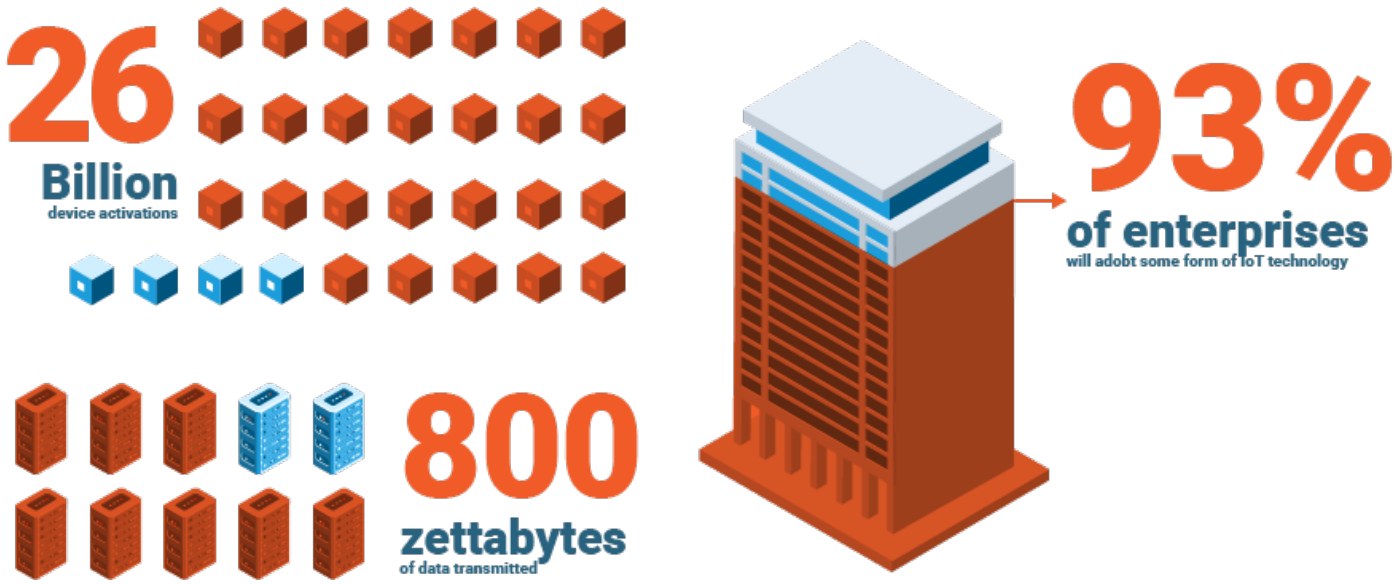
www.eclypses.com

Contents

Introduction: The Importance of IoT Devices

Internet of Things (IoT) devices use wireless sensor software to facilitate the automatic transfer of data from low-powered hubs to analytic engines. With the continuous rise of intelligent, connected technologies, IoT devices have become an integral part of everyday life. From smart home systems to healthcare equipment, businesses and consumers alike have come to depend on IoT technology to function efficiently.

In fact, it is estimated that 26 billion IoT devices were activated in 2019 alone. These devices are expected to produce a massive 800 zettabytes of data, most of which is sensitive. It is also anticipated that 93% of enterprises will adopt some form of IoT technology, using the collected data points to make informed businesses and manufacturing decisions. To ensure these enterprises remain protected, the transferred data must be managed in a confidential, valid, and secure manner.

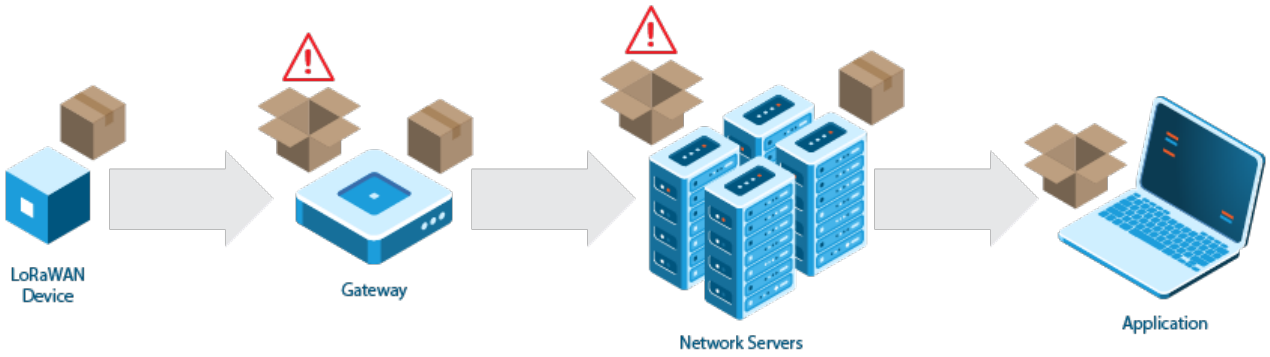


The Problem: IoT Data Security

Consumers want their IoT devices to be as compact, efficient, and cost-effective as possible. Yet, the same consumers also demand more security from their IoT devices. Unfortunately, this creates a dilemma for manufacturers, who must adhere to strict constraints that decrease profit margins and limit the room for typical safeguarding measures.

For this reason, many IoT devices lack proper security for users. Standard encryption methods are unfeasible because they require extensive and costly computing resources. As another option, security chips may offer a layer of protection, but also increase the complexity and cost of the IoT device. Due to these restrictions, data is instead forced to the cloud for analytics and storage, creating massive vulnerabilities.

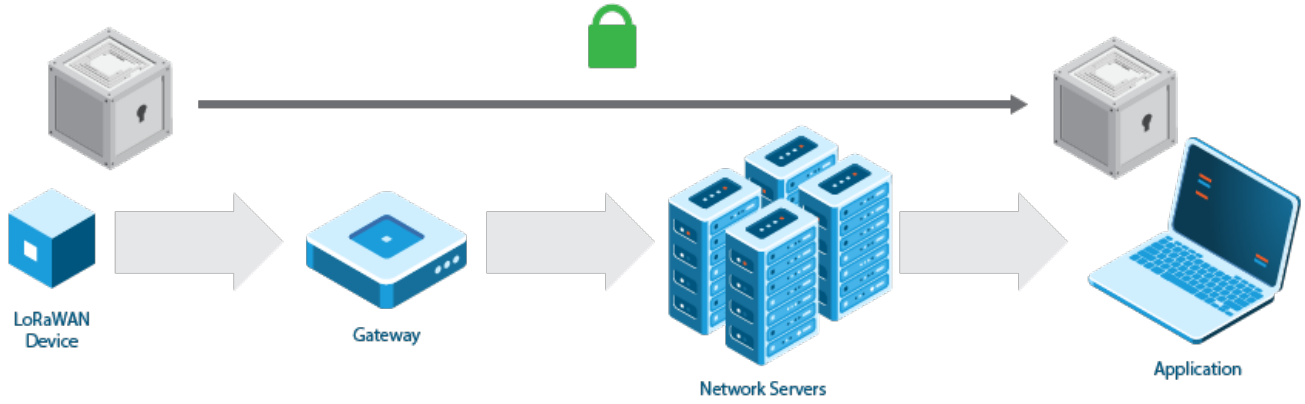
Without standard protections, security at the device level is limited. It becomes easy for a hacker to access the connected network, which can lead to identity fraud for consumers or ransomware attacks for corporations. There is also no true end-to-end payload protection when dealing with the IoT network infrastructure. As data travels through the gateway and then to the cloud, the data must be unsecured at each step in the process and then re-secured before reaching its next destination. The data owner must place a lot of trust in third party entities (such as network operators or cloud hosts) to keep the transferred information safe.



Due to these constraints, device manufacturers were originally left with two choices: (1) increase the cost and complexity of devices to utilize acceptable encryption or (2) leave the device susceptible to security threats. However, with MTE technology, manufacturers now have a third option: (3) embrace an alternative security approach that protects communication between any device at a fraction of the processing footprint.

The Solution: MTE Technology

The data received at the opposite end of an IoT network should be just as reliable when reading it off the original device. In order to guarantee this reliability, Eclypses designed a unique approach to data security, specifically with resource constraints in mind. Now, manufacturers can continue to produce the same hardware, while also providing the highest level of security possible to consumers. Eclypses offers manufacturers true end-to-end payload protection with its MicroToken Exchange (MTE) technology, protecting the integrity, confidentiality, and authenticity of all IoT-related data.



Defining Random Stream of Values

MicroToken Exchange (MTE), a patented technology, is a proprietary algorithm that substitutes each piece of transmitted data with randomly generated values. The data transmitted is purposely corrupted and replaced with random streams of values on each side, making it undiscoverable and secure from inception. Each value is unique and only valid once, ensuring the outcome of the packet is never the same. Therefore, only the intended recipient will be able to accept and decode the sequence.

Benefits include:

- 256-bit security strength for quantum-resistant data confidentiality
- An economically small footprint (as little as 4KB)
- Low RAM requirements (as little as 3.2KB)
- Minimal latency (as little as 18 µs)
- Low processing requirements (easily runs on microcontroller platforms)

How MTE Technology Functions

Random streams of values are created from the random bits assembled by NIST-approved deterministic random bit generators (DRBG) within the MTE library. Each side of the MTE pairing produces the same stream of random bits. Seed values, which can be burned into each device during the manufacturing process, are determined by the calling application and are used to initialize the MTE technology. Both devices run in a synchronized state and communicate securely with MTE. Matching seed values eliminate the use of public encryption keys that are vulnerable to quantum attacks.

Every time data is obtained by the MTE library, random streams of value are randomly mapped to the 256 possible bytes. Since each byte of data is substituted randomly and values are never duplicated within a packet, there are no possible patterns for a cybercriminal to observe.

Once a full packet is transmitted, all values are deleted, including the unused values. This process ensures the mapping of values is instantly obsolete – for a 16 byte token, there would be a one in an undecillion chance for that specific value to appear in the mapping again.

Why MTE Technology is the Ideal Solution

In addition to protecting users against data exposure, with its unique and secure cryptographic algorithm, MTE technology also provides a barrier from man-in-the-middle manipulation attacks. When using IoT devices, it is extremely important that data arrives to its destination in a correct and timely fashion. Cybercriminals commonly manipulate the behavior of devices by injecting false, delayed, or repeated packets into the communication stream.

MTE offers a checksum verification element that detects errors to protect against these damaging attacks. The checksum is shuffled into the raw data and the MTE technology is implemented. If MTE decodes a manipulated packet, the checksum will be incorrect and therefore will discard the erroneous data. If MTE receives a packet it does not understand, it will likewise eliminate the data and provide the user with an error message.

MTE can also protect users from delayed or irrelevant data by building timestamps directly into its packets, allowing the calling application to determine how long a packet takes to arrive. If the data packet arrives outside of the expected range of time, it is thrown out.

While other solutions, such as a hash-based message authentication codes (HMAC) or the Diffie-Hellman, do exist, these both require an additional layer of processing and memory requirements that low level devices cannot support. MTE is a compact and cost-effective solution that protects data from many forms of attack, which gives consumers the best of both worlds. With MTE technology, manufacturers no longer have to weigh cost and convenience against data protection – they can have it all.

MTE Technology in Action

The following is a breakdown how MTE technology can safeguard an IoT device from a harmful cyberattack in 3 different scenarios:

Scenario 1

Imagine someone needs to use a mobile app to transfer sensitive information or transactions on a jailbroken/rooted phone. With a deeper level of access into the OS, the phone is more susceptible to viruses and manipulation by cybercriminals.

Possible Attack: A cybercriminal alters the mobile app through a virus and now has the ability to manipulate and capture sensitive data. This has an enormous impact on any mobile app that protects the integrity of the user's information.

MTE Prevention: With the use of the MTE jailbreak/root detection add-on, the seed values of MTE are manipulated with every jailbreak/root check. This process intentionally corrupts the communication of jailbroken/rooted phones, so the receiving server will no longer be able to understand the communication from any compromised device.

Scenario 2

A smart city sensor is collecting sound data within a city and transmitting it over a LoRa network. This sensor gives the police the ability to triangulate gunshots and respond faster to the correct location. Due to limitations, the device uses static keys that a cybercriminal has now decoded, breaking into the LoRa communication.

Possible Attack: The cybercriminal knows what each packet is transmitting and intercepts a packet from the sound sensor that communicates a gunshot location. Since the keys are static, he can hold onto this packet and inject it into the communication stream at a later time, alerting police to gunshots that do not exist. This could allow the criminal to commit another crime, such as a bank robbery, while the police force attends to a fake gunshot alert.

MTE Prevention: The MTE library realizes the packet is missing through its optional sequencing feature and catches up to the state of the sound sensor. The receiving library will not be able to decode the hijacked packet because the values are no longer valid. MTE also uses a timestamp to deem the second reading as outside of the valid range of time. The delayed data is immediately discarded.

Scenario 3

Someone uses their banking web portal on an unsecure WiFi network and a cybercriminal is listening in on the communication. Because the cybercriminal has broken through the network protection layer, this person can easily identify sensitive information and tell what the packets are communicating.

Possible Attack: A cybercriminal mimics the online banking web portal and continuously replays a packet containing a transfer request to an account owned by the criminal. The replayed packet causes unauthorized transfers of money into the criminal's account from the user's account. This is repeated until the cybercriminal is satisfied, or the account is drained.

MTE Prevention: MTE immediately replaces any values with a new one, making it highly unlikely for the values to ever be used again. After the first packet is delivered successfully from the online portal, the mapping is completely erased, which ensures the packet cannot be replayed.

Conclusion

When we examine a breach in IoT data security through a real-world lens, the devastating effects are apparent. Data protection is of the utmost importance and manufacturers deserve a simple solution that allows them to instill confidence in their customers without having to make sacrifices to their products. Eclypses developed MTE technology as a means to safeguard data by offering true end-to-end payload protection without producing a large footprint. Low-level devices may now offer the same level of security as any other platform.

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today's environments, called MTE.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies and websites. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses' patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

With a focus in the mobile sector, this technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT US

info@eclypses.com
www.eclypses.com
(719) 323-6680