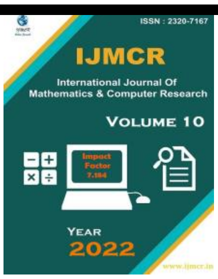
International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 10 Issue 04 April 2022, Page no. – 2644-2645

Index Copernicus ICV: 57.55, Impact Factor: 7.184

DOI: 10.47191/ijmcr/v10i4.01



Fully Decentralised, Post-Quantum Secure Networks

Wayne Henderson[1], Mykhailo Magal[2], Christopher P. Autry[3]
[1,2,3] Iothic Ltd, Quad One, Becquerel Avenue, Harwell, Oxfordshire OX11 0RA

ARTICLE INFO

Published Online:
03 April 2022

ABSTRACT

The Fourth Industrial Revolution, Industry 4.0, promises trillions of dollars of value creation by connecting billions of sensors and actuators to analytical engines, thereby creating the Industrial Internet of Things (IIoT). This revolution will push decision making to the edge and connect the edge to the center. The revolution faces three major technical challenges: interoperability between devices, security of edge devices and legacy infrastructure. This paper describes an implementation of a fundamentally new authentication and encryption technology ("dOISP™), that allows devices to connect regardless of operating system and transport technology. With dOISP™ a network manages its own security without use of certificates or Trusted Third Parties or any centralized or externalized source of trust and without human intervention – the network itself maintains a distributed source of trust that changes continuously and always assumes that authentication must be refreshed for every session. This technology enables the acceleration of Industry 4.0 initiatives thereby increasing their net present value as well as reducing the organizational costs of network security and reducing the risk of successful attack.

Corresponding Author:
Wayne Henderson

KEYWORDS: Decentralized networks; Authentication and Encryption; Post-quantum security; Security of Edge Devices; Industry 4.0 and IIoT; Interoperability

I. INTRODUCTION

In 2018 the World Economic Forum and McKinsey & Company estimated the value-added potential of Industry 4.0 at $3.7tn [1]. Previously, McKinsey pointed out that 40% of that value comes from unlocking data captured in IoT devices but not used [2]. Unlocking the data requires secure interoperability between devices. This poses three big technical challenges: security giving confidence that critical information cannot be stolen, tampered or prevented from arriving; interoperability, enabling diverse devices to connect; legacy infrastructure which may be low on computational resources. Authentication is a critical first step in secure communication, whereby a message that is claimed to originate from a device can be bound to that device, so that the receiving device knows the provenance of information or instructions. Next comes an integrity check, so that the receiver can be sure the message has not been tampered with. Finally, encryption so that third parties cannot overhear or see the message content. These characteristics make up the requirements of a secure communication protocol, to which can be added the need for availability, so that devices can communicate when they need to. Extensive research into authentication of ad-hoc networks [3] reveals some building blocks from which a fully decentralized secure communication protocol can be built for IoT networks. By locating this protocol between layers 4 and 6 of the OSI stack, and using an appropriate address protocol, interoperability can be achieved. As long as the protocol is not heavy on resources, this interoperability enables legacy infrastructure to be included in an IoT network without significant replacement or integration costs. This paper describes just such an implementation of a protocol, called "dOISP™".

II. TECHNICAL DESCRIPTION

dOISP™ combines a set of cryptographic primitives configured in a way so that the certificate-less approach of authentication described in [3] can be deployed into a self-managed network.

A. *Authentication requires three (3) parties, or nodes*

Three devices (or Three Groups of Devices). Whenever two devices, A and B, seek to start a session, a third device, P, is recruited to facilitate the authentication. The only requirements on this third device are that they are part of the network and that they have previously authenticated with at least the intended receiver in the session, B. The selection of P is arbitrary within these constraints. This triangle creates three independently encrypted channels in which each device will check that authentication values received from the other two devices are correct. The third device also checks that the sequence of exchanges, the time delay of exchanges, and the memory of values calculated over the course of authentication by the two initiating devices, A and B, show no signs of interference.

B. Shared Secrets

When initially provisioned, devices share their secrets created by devices themselves. Some of these are drawn fresh from device characteristics in every session; some are partial one-way secrets between two specific devices created at the most recent session.

C. Commitment Check

Each device checks that it shares the same session secrets with each other device using a hash commitment with a nonce. Only the hash digest is exchanged and each device checks that all three digests are correct.

D. Independently Encrypted Channels

Each device creates its own strong symmetric keys to encrypt authentication communication, so that there are three independent keys for the three links between devices.

E. Short-lived authentication

Authentication and the corresponding encryption keys are only valid for one session. Any new correspondence between devices requires a new authentication.

F. Strong primitives: SHA3-256, AES-256-CBC, NTRU-KEM

SHA3-256 hash function takes an input and produces a fixed length digest. This is used in the Commitment Check and elsewhere. AES-256-CBC are strong symmetric keys used to encrypt packets during authentication, and then new keys are generated to encrypt payload packets. NTRU-KEM is used to generate NTRU asymmetric keys used to securely exchange shared secret by sending and receiving devices, the shared secret is to be used as AES-256-CBC key to confidentially exchange authentication keys.

G. Unique Session Code

Once authenticated, A and B create a unique session value, called CMV, that is a hash of values created and checked in the A-B-P cell during the session. This value is not known by P. CMV is used to create an HMAC code to prove by A and validate by B the authenticity and integrity of the message in the payload packet.

H. Boot Check

Every time a device boots it will run a check on its stored secrets and a hash check on its code. This will raise an alert if anything has changed.

I. Entropy

Entropy from any device's specific random number generator (RNG) is supplemented by entropy drawn from peer devices by means of a seed with which the device's own RNG is updated with extracts of random data peeled from encrypted peer communications. As the size of the network of the device's peer list increases, the entropy available to that device also increases.

III. DISCUSSION

The requirement for three assets means that a relatively unpredictable third asset must participate in authentication. All three assets must derive the same hash digests in the Commitment Check and demonstrate that result to the others. As links are independently encrypted, at least two strong 256-bit AES keys would need to be simultaneously broken for a Man in the Middle attack.

As some secrets are one-way, one-time secrets, no single node knows enough secrets to complete authentication, and no set of secrets learned in one session can be used to complete authentication in a future session.

As the devices manage the security lifecycle after initial provisioning and check secrets themselves, there is no need for central server or third-party connectivity.

As encryption is one-time, using strong encryption keys (NTRU and AES-256-CBC), the technology is resistant to known quantum computer combinatorial attack.

IV. CONCLUSION

Extending research conducted into authentication of ad-hoc networks, dOISP™ delivers decentralised authentication and post-quantum secure interoperability without need for certificate, third-party access or human involvement after provisioning.

REFERENCES

1. Leurent, H., de Boer, E. 2018. The Next Economic Growth Engine, Scaling Fourth Industrial Revolution Technologies in Production. World Economic Forum in collaboration with McKinsey & Company.
2. Dobbs, R., Manyika, J., Woetzel, J., 2015. The Internet of Things: Mapping the Value Beyond the Hype. McKinsey Global Institute, McKinsey & Company.
3. Roscoe, A. W., Nguyen, L. H. 2008. Authenticating ad-hoc networks by comparison of short digests. Science Direct, Information and Computation 206 (2008) 250-271.