CYBERUS KEY

A new security architecture for the IoT world.

Powered by CYBERUSLABS

INTRODUCTION

Internet of Things. Outlook.

There's little question the "Internet of Things" will eventually be enormous. Using Internet technology to make our homes and devices smarter is easy to understand, but is also a great challenge, both technological and social.

One of the the biggest enabler of the Internet of Things was the introduction of IPV6 in 2011. As IPV4 had only approximately 4 billion addresses, IPV6 has a total of 340 undecillion IP addresses. This number enables us to deal with growing industry and needs of Internet of Things in the years to come. International Data Corporation (IDC) estimates 200 billion connected devices by 2021, with more than 30 billion of them being autonomous devices.

But there is one very important factor – security and access control.

Today's vision of IoT does not provide, however, for the security and management of connected devices, which is a necessary condition of the IoT industry to realize its full potential.
Typically IoT devices operate over a LAN running ZigBee (IEEE 802.15.4) or similar wireless LAN protocols like Z-Wave, Thread and WeMo.

While these protocols can provide encryption for local devices, they do not currently have a mechanism to authenticate and govern the devices on the network.

The Cyberus Key User Authentication protocol originally designed to authenticate users securely, presents an ideal architecture to also authenticate connected devices and to govern their interaction with users and each other.

CYBERUS KEY system is a international multiple patent pending technology.
Copyright © Cyberus Labs 2016. All rights reserved.

CYBERUS KEY
USER AUTHENTICATION

CYBERUS KEY system is a international multiple patent pending technology.
Copyright © Cyberus Labs 2016. All rights reserved.

Powered by CYBERUSLABS

A NEW HOPE

The Cyberus Key User Authentication Protocol.

Cyberus Key is based on the use of a highly secure one-time password generation and encryption methodology. System allows a user to securely logon to a any website using a preinstalled application on a mobile device by securely transmitting an OTP between the device and the website via a laptop or desktop computer – authenticating that user's credentials instantly and securely by generating an "unbreakable" unique onetime password.

This short-lived HSM generated token (password) is transmitted via out-of-band link. Using the Cyberus Key authentication server, both sides of the transaction are instantly authenticated and a final approval is sent back to the Cyberus Key enabled network. The benefits are both on the user side and on the network's side. Both sides mutually recognize and authenticate each other and the authority of the user commanding over the IoT network is confirmed.

CYBERUS KEY system is a international multiple patent pending technology.
Copyright © Cyberus Labs 2016. All rights reserved.

Powered by CYBERUSLABS

PROTECTION

Cyberus Key - A Universal System.

Automated systems of connected devices in Internet of Things (IoT) that include i.e.: systems of the "intelligent houses" (connection of the household equipment, air condition, heating, power, light, entertainment) is a fast growing market. Cyberus Key offers a universal system of the authentication information exchange, that transmits and controls the answers of the devices, comparing encoded algorithms and signal sequences that carry one-time-passwords.

Cyberus Key proposes a mechanism which will add IoT device identification, authentication and will govern the types of interactions which can be legally performed by devices and to allow only authorized actions to be undertaken by IoT devices.

The Cyberus Key authentication protocol was designed to protect the Internet from bad human actors, it will now protect IoT from bad cyber actors and well as bad human actors. This same architecture will also allow Cyberus Key to predict anticipated device failures and can recommend device repair and replacement prior to any failure of critical components.

CYBERUS KEY system is a international multiple patent pending technology.
Copyright © Cyberus Labs 2016. All rights reserved.

SECURITY

CYBERUS KEY system is a international multiple patent pending technology.
Copyright © Cyberus Labs 2016. All rights reserved.

Powered by CYBERUSLABS

SECURITY

Connection And Authentication.

Connection between human authentication and Internet of Things - the creation of an effective user authentication mechanism may be available to include device authentication by use of the same authentication server.

This way Cyberus Key solves an emerging security problem related to device/device and human/device connectivity and interactivity. At present it is an emerging market without an existing unified solution. Cyberus Key system offers an innovative, unique and universal solution for any product or service based on IoT.

Cyberus Key Identification Server can formulate and enforce rules for automatic device interaction as well as authenicate users issuing commands to devices. That gives Cyberus Labs a significant scientific, technological and market advantage in providing a more universal and secure IoT authorisation system.

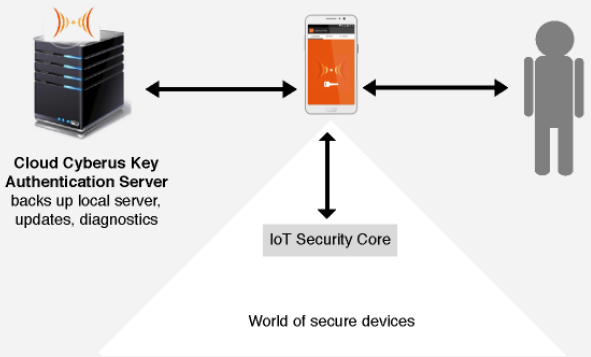


Fig. 1
Overview of the secure IoT pyramid with Users at the top, originating all authorized actions and device rules.

CYBERUS KEY system is a international multiple patent pending technology.
Copyright © Cyberus Labs 2016. All rights reserved.

SOLUTION

Cyberus Key User Authentication Basics.

The basic authentication protocol used by Cyberus Key in its original user-operator's authentication design, relies on the fact that both of the parties to the logon transaction have been registered on the Cyberus Key Authentication Server as legitimate, authenticated entities. This allows Cyberus Key to authenticate both sides of the transaction and creates a link between a user session resulting from the logon and the user's mobile device.

As mentioned above, Cyberus Key technology is based on the use of One-Time-Password. The OTP authentication protocol is a variant of the One Time Pad, or Vernam Cypher mathematically proven to be unbreakable by Claude Shannon (the father of modern Information Theory) at MIT.

Now, Cyberus Key may do the same for identification of the devices in the IoT environment.

CYBERUS KEY system is a international multiple patent pending technology.
Copyright © Cyberus Labs 2016. All rights reserved.

Powered by CYBERUSLABS

POTENTIAL

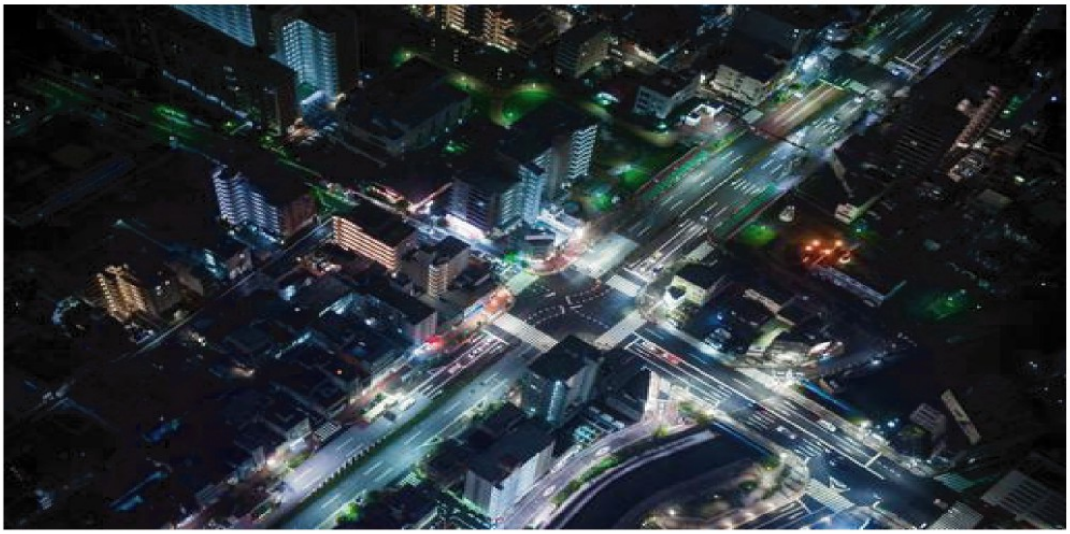
For The Secure Future.

Also in case of the IoT network the may act in the similar way to allow mutual identification and authentication in both cases – between authorised user that controlles the environment and authorised devices within the network. Similar core authentication mechanism may be used also for IoT environment preventing the attacer from taking control over the network.

As Cyberus Key uses in its original version the sonic signal to transmit OTP it is also designed in the way that OTP may be transmitted in Mobile Only version using pseudo Out-of-Band connection.

A Cyberus Key concept of identification and authentication may also be translated into various protocols that are in use for communication between devices in IoT environment.

This way Cyberus Key may be the critical element for the IoT world's security architecture.



CYBERUS KEY system is a international multiple patent pending technology.
Copyright © Cyberus Labs 2016. All rights reserved.

Powered by

CYBERUSLABS

SECURE WORLD

Cyberus Labs Sp z o.o.
ul. Królewska 65a/1
30-081 Kraków, Poland
Email: biuro@cyberuslabs.com
Phone: +48 692.437.857
www.cyberuslabs.com

CYBERUS KEY system is a international multiple patent pending technology.
Copyright © Cyberus Labs 2016. All rights reserved.