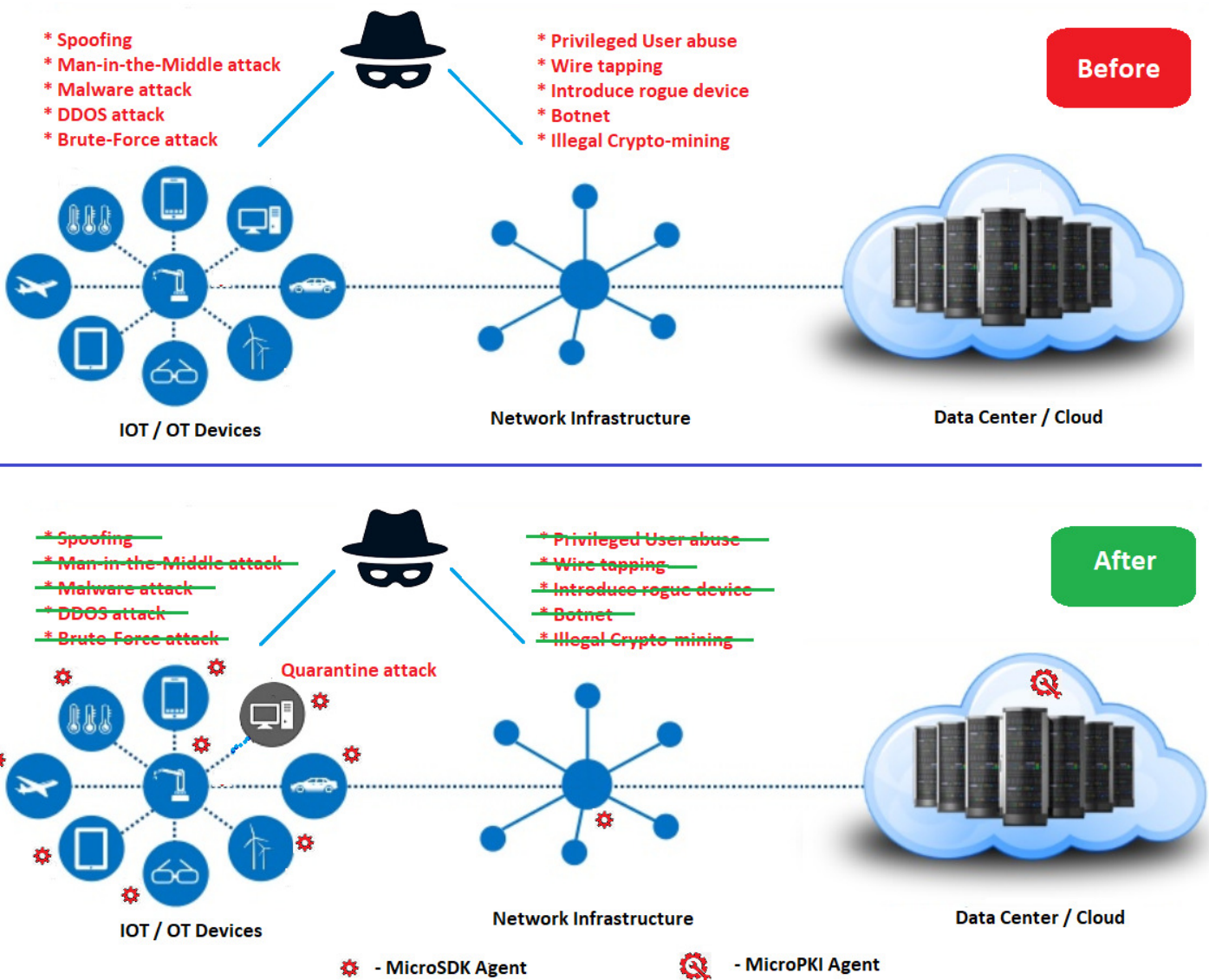


MicroPKI – IoT / OT Device and Network Security Software

Keep your mission-critical Devices and Network safe from prying eyes



For whom does it concern

- Are you part of the IT Security or OT Operations team in your organization?
- Do you manage IoT, SCADA, ICS, DCS, AMI, BMS, Monitoring, Security or “Smart” Infrastructures?
- Are you converging IT & OT, exploring Digital Transformation, Industry 4.0 or new Business Models?

Why

- Security at the Edge Devices was completely ignored thus far; such devices include PLCs, RTUs, Sensors, Actuators, HVAC, Automobiles, BMS Controllers, Home Appliances, Locks, Cameras, Baby & Patient Monitor, Industrial Instruments, Wearables, Toys, Entertainment Products, Security products etc
- Edge Devices have poor computing power, low memory, low battery life and low data transmit limit; some has an OS, some just bare metal; they use a variety of Micro-Controllers and Wireless Protocols; so how to bring “*One Common, Scalable Edge Security*” with so many layers of constrains?
- At best, some have Pre-shared Keys (AES) replicated over to 100s of thousands of devices; but this can be abused by an unhappy employee or hacked easily by dumping the firmware of just one device
- Thus, such weak Devices & Network are an ideal target of attack because it is a goldmine for hackers

Why Now

- Recent high profile attacks: Mirai botnet, Stuxnet, St.Jude’s Cardiac device, Owlet baby monitor etc
- Exploding IoT Malwares: 3,219 in 2016 to 121,588 in 2018, as per Kaspersky Labs
- \$ 3.9 Million – average cost of data breach in 2018, as per IBM Security; it led to job losses too

What is the Solution

- Install an Agent (MicroSDK) on your Devices & Gateways, and another Agent (MicroPKI) on Servers
- MicroSDK gets a unique Micro-Certificate with a Private & Public Key; this brings Digital Identity, Mutual Authentication, End - End Encryption (Perfect Forward Secrecy) and Over-the-Air (OTA) Administration
- MicroPKI enforces policies automatically by creating, updating, revoking millions of Device Certs OTA
- Isolate attacks, if they occur, and defend rest of your Devices and Network

What is Unique here

- ✓ Asymmetric Encryption with Elliptic Curve
- ✓ Symmetric Encryption of any choice (AES etc)
- ✓ Compressed SDK; 10 KB Flash, 2 KB RAM
- ✓ Agnostic to Chipset, OS / No OS, IP / No IP, Protocols
- ✓ TLS 1.3 / DTLS 1.2 equivalent Support
- ✓ CAVP FIPS 140-2 Level 1 Certified
- ✓ 130 byte Micro-certificate (Or X.509)
- ✓ Based on Public Key Infrastructure (PKI)

Refer to MicroPKI Datasheet, User Guide and API Docs for more technical details of the solution.

Who else is using

MicroPKI is being deployed in 110,000 Smart Street lamp posts in Singapore. So, you are in good company.

How to deploy

It's just a simple two step process:

1. Just introduce your Device Supplier to us via sales@usec.io; nothing more; we will collaborate with your Supplier to install MicroSDK on to your devices. Chances of us already working with your Supplier are quite high, since we have established partnership with world's leading OEMs.
2. Receive MicroPKI Service pack and Deployment Manual from sales@usec.io; A MicroSec Customer Success Engineer will contact you to do the server setup for you. You'll be up and running in 30 minutes.

What is the Investment needed

Based on No# Of Devices to be protected, billed annually

How to give it a try

To test how to protect from professional hackers, amateur tinkerers, unhappy staffs and sponsored attacks,

Call [+65 6931 4227](tel:+6569314227) or Write Now to sales@usec.io for a FREE Trial