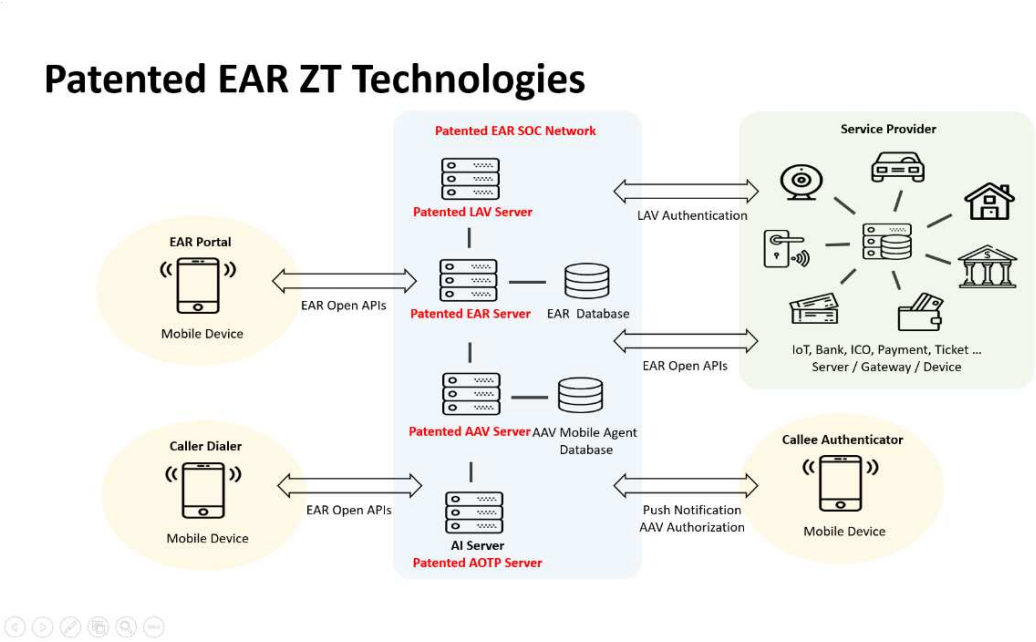
ZTSHELL

EAR Zero Trust Solution

The Sophisticated Combination of EAR and AOTP Technologies



Company Profile

OmniBud is an expert solution provider in IoT security system established in 2003. It is an B.V.I. registered company with the core R&D and hardware partners in Taiwan. OmniBud owns the unique EAR Zero Trust Solution named EAR ZT which consists of a portfolio of technologies with patents in major countries. The solutions are applicable in a wide range of areas, such as smart city, smart home, hospital, retail, banking etc.

The major patented technologies include:

- 3 Mode Active One Time Password Technology
- E.164 Authentication Routing Technology
- Access Authorization Verification Technology
- Legitimate Authentication Verification Technology
- E.164 Authentication Routing Security Operation Center Technology

Market Footprint

OmniBud products and services are available in Asia and expanding rapidly to the rest of the world.

Products and Solutions

Nowadays many applications require remote access to the IoT devices via public Internet, and most IoT devices in the market are light weighted and may not be equipped with strong enough security features. OmniBud can provide the unique multi-factor authentication together with dynamic firewall of generic terminal to protect application servers and IoT devices based on the well deployed patented technologies.

An example is the application of EAR ZT Service to surveillance IP cameras. Typical IP camera security only requires username and passwords for login. With EAR ZT Shell, the user will be authenticated by EAR ZT technologies based on Who, When, How and What conditions smartly and automatically instead of traditional username and password input manually. EAR technologies include EAR ZT Server, EAR ZT Terminal and EAR ZT Embedded Devices to fit various users' needs. Moreover, a designated user of the IP cam can remotely one time "allow" or "decline" access request from other users easily and securely by one click only AOTP Authenticator with AI integration flexibility. A user can do multi-factor authentication when logging on EAR ZT Services by one click only easily with AI integration choice too.

Advantages

- **EAR Zero Trust Stops Major IoT Attacks at Once**

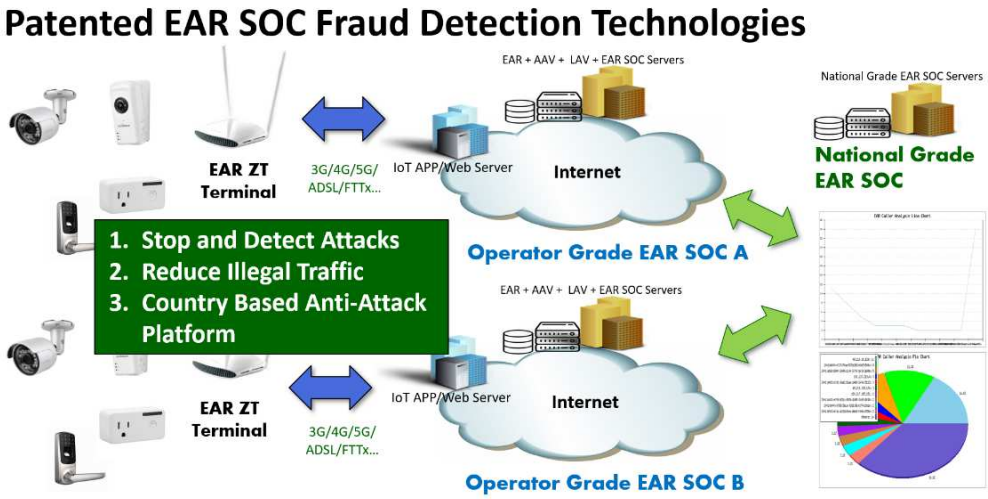
  - Stop Attacks of Service Registration with Fake Mobile Number
    SMS AOTP for Service Registration is used to upgrade compromised SMS OTP to stop and detect attacks.

  - Stop IoT Device Hacking of Compromising Username/Password
    3 Mode AOTP (AI/APP/SMS AOTP) MFA Login is used to stop and detect attacks of Username/Password compromising attacks.

  - Stop IoT Device Attacks of Using Unauthorized Username/Password
    Callee AAV is used to perform Callee one time authorization to stop and detect attacks of Using Unauthorized Username/Password.

  - Stop IoT Device Attack of IP Connection Directly
    All direct IP connecting attacks are blocked by EAR ZT Terminal to stop and detect these major type IoT attacks.

  - Stop IoT Device Access by Random EAR Number Dialing
    Because E.164*Thing Code formatted is not predictable as E.164 number, EAR ZT Platform can block and detect random EAR Number dialing happening on PSTN.



- **Generic EAR ZT Terminal Enables Easiest Security**

  - Device Flexibility
    EAR ZT is composed of multiple ZT systems with EAR ZT Terminal to protect IoT Devices or Application Platform connected to EAR ZT Terminal. There is no IoT Device or Application Platform upgrade needed to enable EAR ZT Shell.

  - Network Flexibility
    EAR ZT provides flexible deployment to protect IoT devices and application platforms on both Internet and Intranet by ADSL/FTTX/4G/5G network. There is no Network limitation to enable EAR ZT Shell.

  - Real-time Attack Detection
    Patented EAR SOC aggregates failed EAR, AAV and LAV related data to analyze and detect attacking sources to initiate corresponding response instantly when attackers try to compromise IoT Devices or Application Platforms.

  - Global Connectivity
    Based on E.164 ownership numbering plan, EAR ZT keeps the business to local Operators and ISPs in different countries as value adding services to increase the ARPU and meet the regulation and security requirement of local government when IoT services are provided by Operators and ISPs.

1. Fulfill Security Liability
2. Attract Customers Care About Privacy & Security
3. Extra Zero Trust Shell Service & Application Revenue
4. Increase ARPU of Mobile Operators

- **Web based UI and APIs Enable Service and Integration**

  - Web Based UI Enables Standard EAR ZT Service to End Users
    End users can use EAR ZT Services by Web based UI with no need to download extra APP but by simply Clicking Hyperlink or Scanning QR Code. We provide Web based UI customization for Service Providers to save cost and time with good user experience and flexibility.

  - Open APIs Enables Flexible Integration to Application and IoT Platforms
    Application Platform Providers and IoT Platform Providers can use EAR ZT Open APIs to integrate EAR ZT services into their products and services to save cost and time with integration flexibility for different vertical industries.

Network Structure and Security Policy

- **EAR ZTNA**

  - EAR Zero Trust Network Architecture is the unique structure includes various ways of building up EAR ZT Networks meet the requests of the Zero Trust Guideline published by NIST.

- **EAR DOCP**

  - EAR Device Oriented Cybersecurity Policy defines series of roles and rules based on EAR ZTNA and makes the operation procedure and data flow meet the requests of the Zero Trust Guideline published by NIST.

- **3 Mode AOTP**

  - Regardless of the way a user gets the OTP: from OTP Tokens, from OTP generation software installed in computers or mobile phones, from SMS or from Email, if the OTP can be input through any computer or any internet access terminal, there will be a logical defect when OTP can be intercepted by others which leads to frauds and arguments.
  - After considering the balance of security, convenience, popularity and digital proof ability, EAR ZT chooses 3 Mode AOTP as the MFA tool which authenticates both OTP and the device sends it to upgrade the compromised SMS OTP which authenticates OTP only and is listed as “not recommend” MFA tool by NIST.
  - 3 Mode AOTP consists of SMS AOTP/APP AOTP/AI AOTP of different authentication strength to fits the needs of different occasions and scenarios.

Please contact OmniBud Support Team for technology and business details.

Email: support@omnibud.com

Website: www.omnibud.com