MLIS2020: Some Security Issues on IoT Products with Home Network

Pan Lanlan (潘蓝兰)

abbypan@gmail.com

Guangdong OPPO Mobile Telecommunications Corp. Ltd., China

2020.09

1. **Offline Peer To Peer Connection**
   - Bluetooth vs WiFi Direct
   - Bluetooth
   - Wifi Direct
   - Application Level Authentication
2. **Communications Between Multiple IoT products**
   - Binding
   - Router Centered ECQV Implicit Certificate System
   - ECQV Implicit Certificate Provision
3. **Local Visit To Home Gateway Service**
   - Router Web Admin Page
   - Router DNS Service
   - Use TLS-PSK
4. **Conclusion**
   - Conclusion

Bluetooth vs WiFi Direct

https://www.dignited.com/23330/bluetooth-5-vs-wifi-direct-which-is-the-best-for-sharing-files-between-smartphones/

	Bluetooth 5.0	WiFi Direct
Peer-to-peer sharing	Yes	Yes
Speeds	1-3 Mbit/s	>54Mbits/s
Range	100m	46-100m
Energy consumption	0.01–1.0 W	2 to 20 watts
Frequency	2.4Ghz	2.4 or 5.0Ghz
Service discovery	Yes	Yes
Supported devices	Smartphones Smart TVs Laptops Smartwatches	Smartphones Smart TVs Laptops Smartwatches Desktop computers

Fig: Bluetooth vs WiFi Direct

Bluetooth Low Energy Pairing

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

Pairing Methods: Numeric Comparison, Just Works, Passkey Entry, Out Of Band

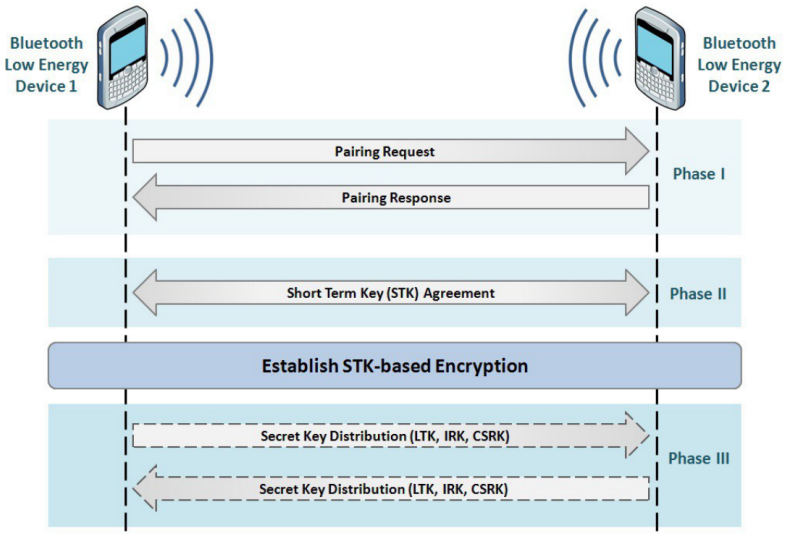

Fig: BLE Legacy Pairing

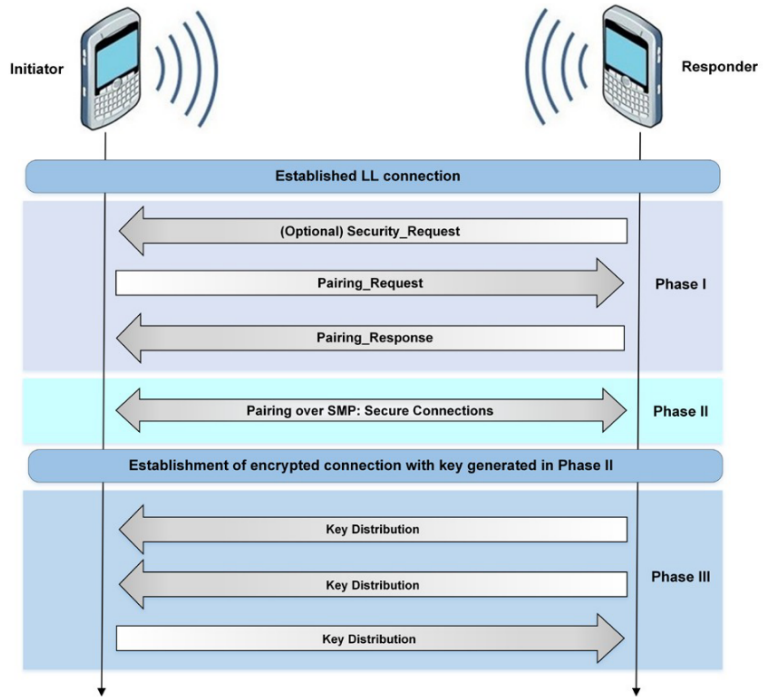

Fig: BLE Secure Connection Pairing

Bluetooth Attack

2019 Fixed Coordinate Invalid Curve Attack: it is a MitM attack which modifies the public keys ina way that lets the attacker deduce the shared secret.

2019 KNOB (Key Negotiation of Bluetooth) Attack: attacker forces two devices to use an 8-bit key, which can be brute-forced quite easily.

2020 BIAS (Bluetooth Impersonation Attacks) Attack: attacker completes secure connection establishment while impersonating Bluetooth master and slave devices, without having to know and authenticate the long term key shared between the victims.

Wifi Direct Connection

https://ieeexplore.ieee.org/document/7579020

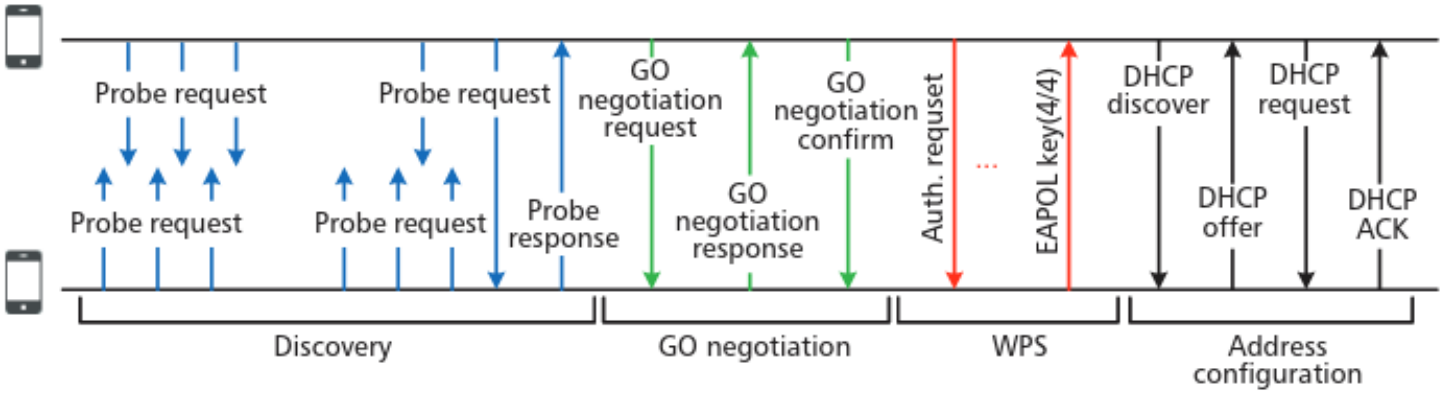

Fig: WiFi Direct Connection

Wifi Attack

2017 EvilDirect Attack: a rogue GO accepts the clients invitation requests beforethe legitimate GO, to hijack the wireless communicationsbetween the clients and the legitimate GO.

2017 Key Reinstallation Attacks (KRACKs): an attacker can force nonce resets by collecting and replaying retransmissions of message 3 of the 4-way handshake. By forcing nonce reuse in this manner, the encryption protocol can be attacked, e.g., packets can be replayed, decrypted, and/or forged.

2019 RTLWIFI driver vulnerability (CVE-2019-17666): The vulnerability triggers a buffer overflow in the Linux kernel when a machine with a Realtek Wi-Fi chip is within radio range of a malicious device. At a minimum, exploits would cause an operating-system crash and could possibly allow a hacker to gain complete control of the computer.

Application Level Authentication

For home network scenario, IoT product should add application level authentication over Bluetooth/WiFi Direct.

generate random password on initial binding (such as scan QR code) secure communication with balanced PAKE protocol.

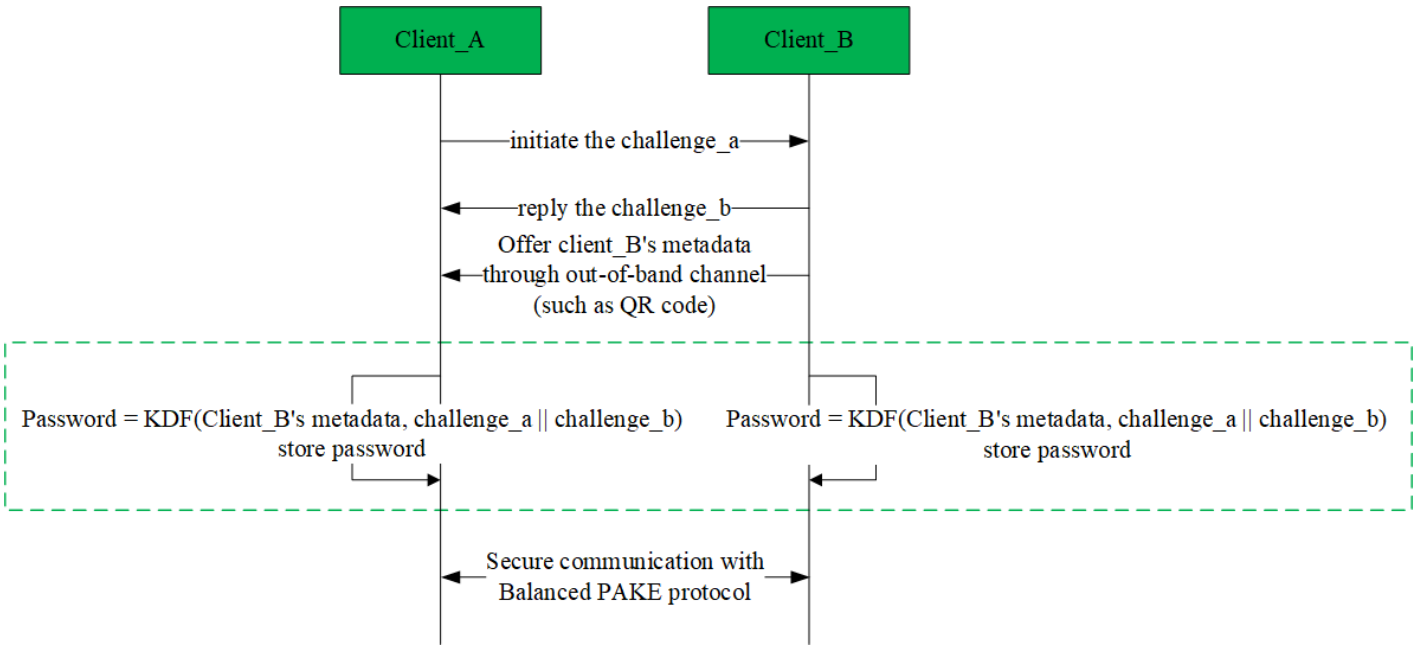

Fig: Application Level Authentication

Binding

User controls the actuators (such as Air Condition, TV, Light) with commanders (such as Mobile Phone, Smart Speaker).
Router isn't involved in the communications, just forwards the packets.
Different actuator products should be adapted to different commanders' platform.

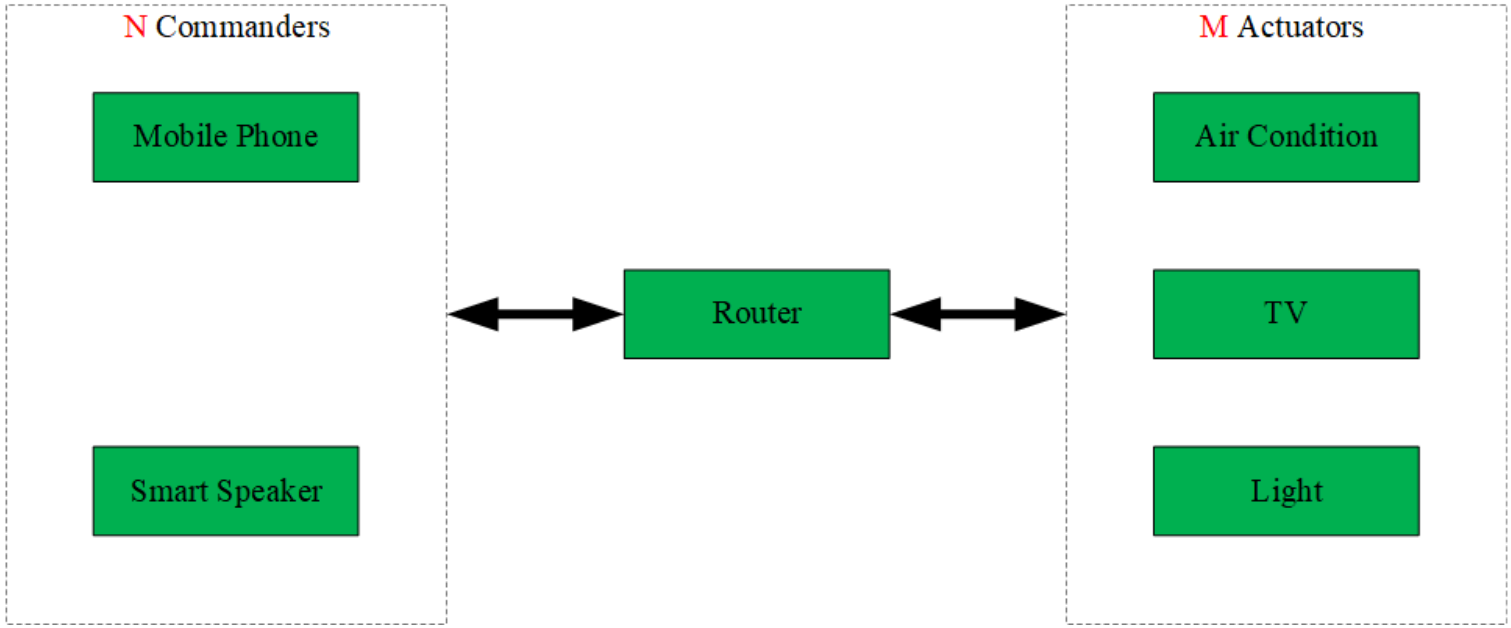

Fig: N Commanders and M Actuators: (N x M) initiate binding

Router Centered ECQV Implicit Certificate System

User controls the actuators (such as Air Condition, TV, Light) with commanders (such as Mobile Phone, Smart Speaker).
Router acts as the center credential distributor of the home network.
Both N Commanders and M Actuators request ECQV Implicit Certificate from Router for initiate binding.

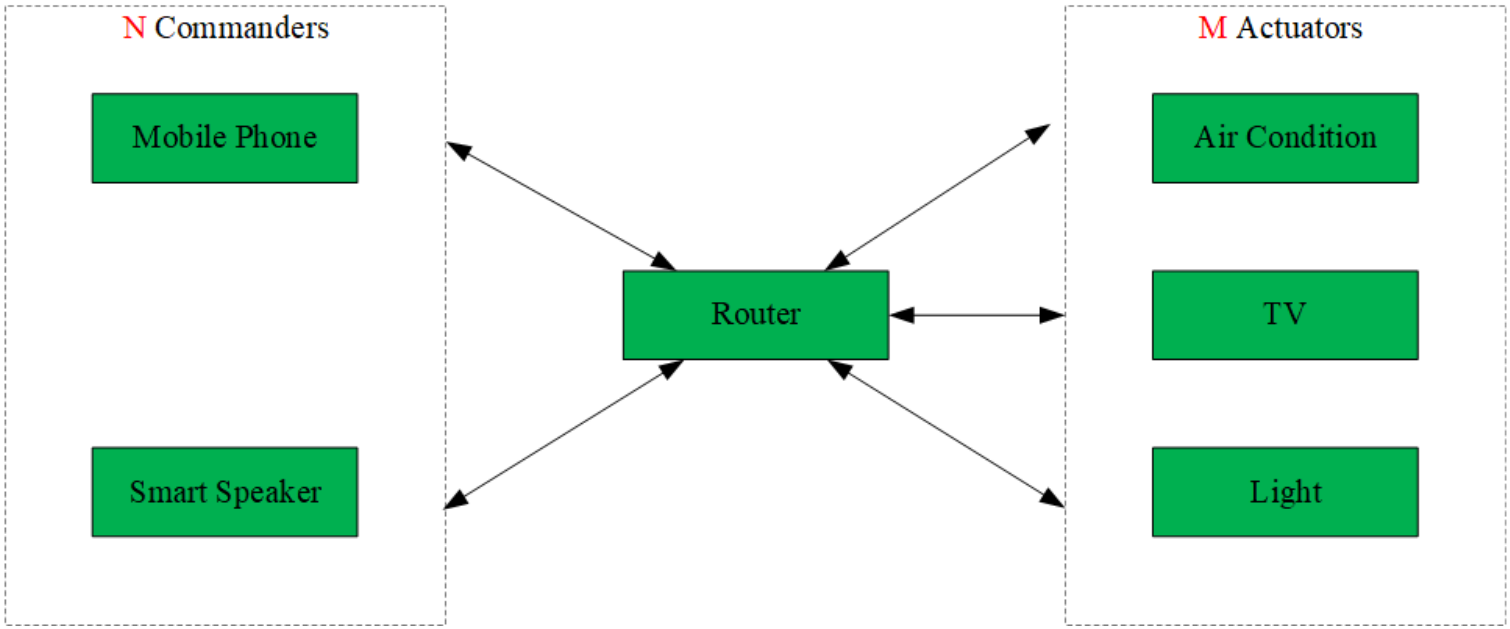

Fig: N Commanders and M Actuators: (N + M) initiate binding

ECQV Implicit Certificate Provision

https://www.secg.org/sec4-1.0.pdf
U: IoT Products
CA: Router

U		CA
$k_U \in_R [1, \ldots, n-1]$		
$R_U := k_U G$		
	$\xrightarrow{U,\, R_U}$	
		$k \in_R [1, \ldots, n-1]$
		$P_U := R_U + kG$
		$Cert_U := Encode(P_U, U, *)$
		$e := H_n(Cert_U)$
		$r := ek + d_{CA} \pmod n$
	$\xleftarrow{r,\, Cert_U}$	
$e := H_n(Cert_U)$		
$d_U := ek_U + r \pmod n$		
$Q_U := eP_U + Q_{CA}$		

Fig: Router Generate ECQV Implicit Certificate For IoT Products

Router Web Admin Page

Home Gateway (Router) doesn't deploy X.509v3 Certificate which is issued by public CA.
To avoid the browser's invalid certificate alarm, router's web service has to accept local client's visit without TLS connection.
Even worse, some router may set the Web Admin Password same as Wi-Fi Password.

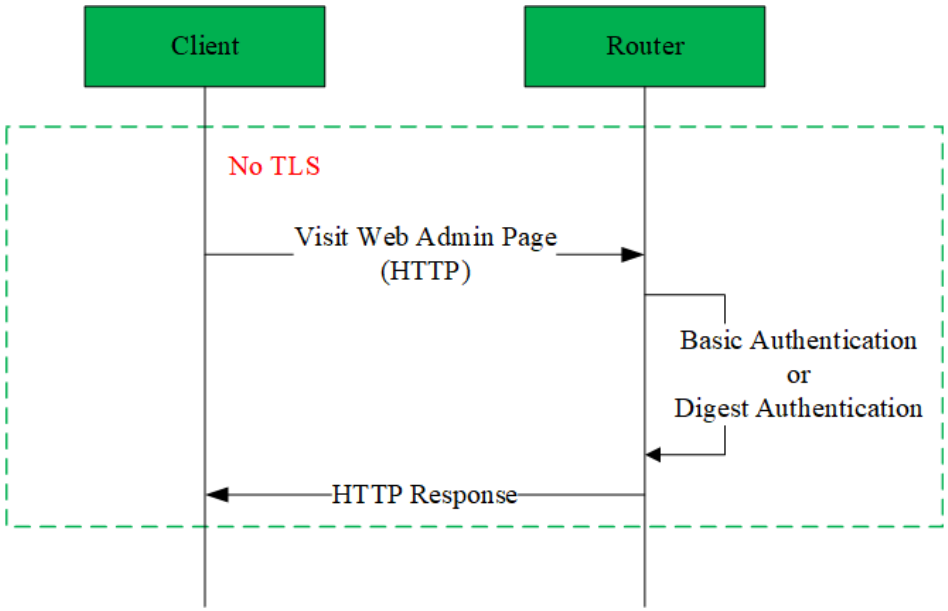

Fig: Local Visit to Router Web Admin Page Without TLS

Router DNS Service

Router offer DNS forward resolver service for local clients.
Default router's DNS service is in plaintext.

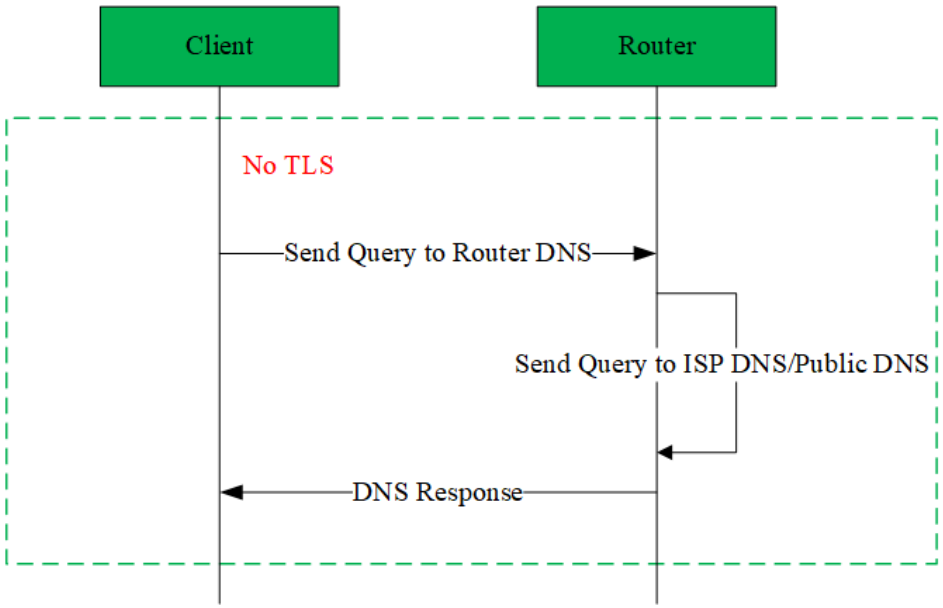

Fig: Local Visit to Router DNS Service Without TLS

Use TLS-PSK

Router can reuse Wi-Fi password or setup specific password for TLS :

- tls-psk = kdf(Wi-Fi User Name, Wi-Fi User Password)
- tls-psk = kdf(Wi-Fi Password)
- tls-psk = kdf(TLS Specific Password)

Client can make secure connection with Router if its system support TLS-PSK.

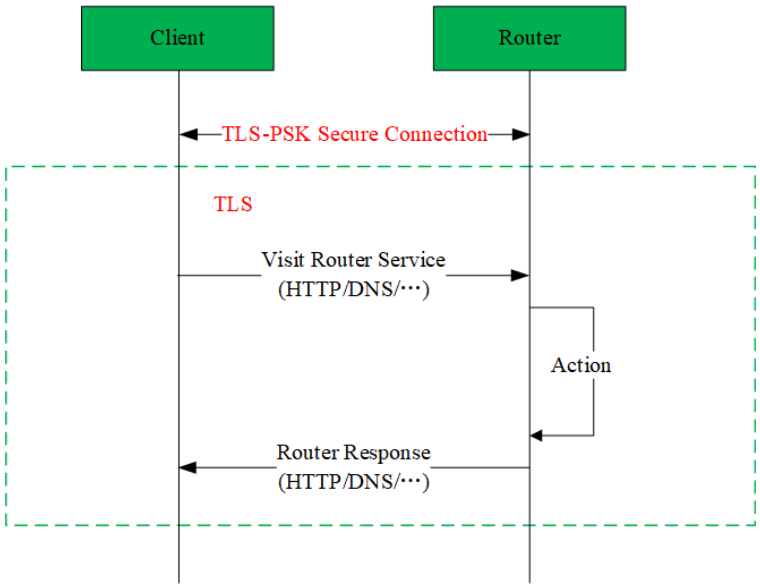

Fig: Local Visit to Router Service With TLS-PSK

Conclusion

Smart home network should be based on a platform that can secure control smart IoT products.

We should build up the open IoT ecosystem with secure design.