ITU KALEIDOSCOPE
ONLINE 2021

6-10 December 2021

Research on security and privacy for IoT-domotics

Jinxue Cheng
China Mobile (Hang Zhou) Information Technology Co. Ltd, China

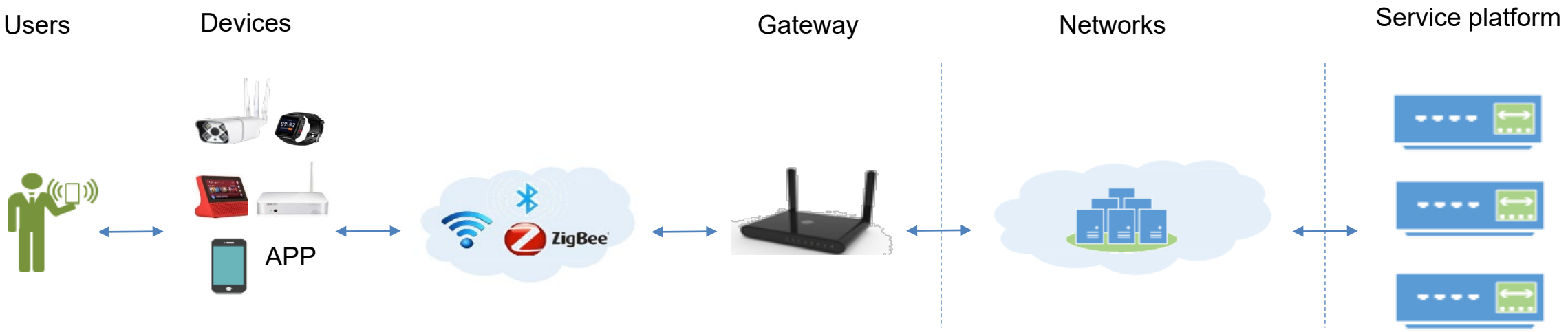
Session 3: Contributions to security

Paper S3.3: Research on security and privacy for IoT-domotics

Outlines of Contents

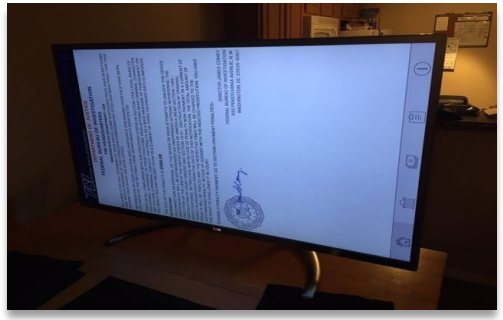
- Background
- IoT-domotics reference model
- Security and Privacy risks of IoT-domotics
- Security and Privacy controls of IoT-domotics
- Supporting control schemes
- Conclusion

What is the IoT-domotics?



Security& privacy incidents of IoT-Domotics

In January 2017, LG Smart TV users downloaded an app that claims to offer free movies. After installing the app on TV, users found that they were also installed with ransomware Police (also known as FLocker, Frantic Locker or Dogspectus) and were required to pay $500 as ransom.



Analysis of causes

- The provider does not take security restriction measures, which allows users to install malicious applications easily.
- Users are induced to access malicious applications due to lack of security awareness and common knowledge of TV applications

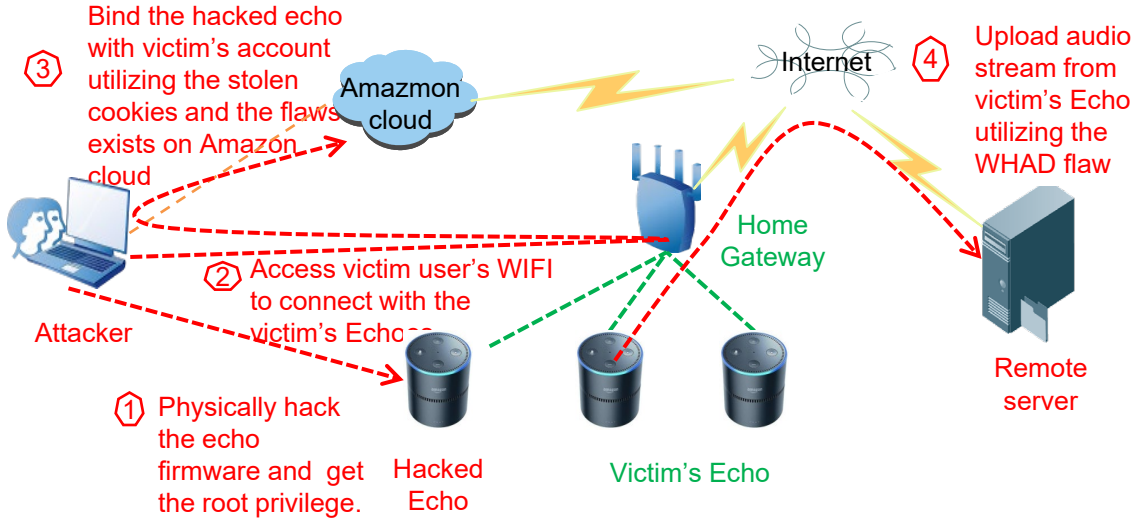
```
public String onDisableRequested(Context context, Intent intent) {
    new Handler().postDelayed(new Runnable() {
        public void run() {
            Object v0 = this.val$context.getSystemService("device_policy");
            if(((DevicePolicyManager)v0).isAdminActive(new ComponentName(this.val$context, DeviceAdmin
                    .class))) {
                this.val$context.startService(new Intent(this.val$context, DisableService.class));
                ((DevicePolicyManager)v0).lockNow();
                int v1;
                for(v1 = 1; v1 <= 20; ++v1) {
                    new Handler().postDelayed(new Runnable() {
                        public void run() {
                            this.val$dpm.lockNow();
                        }
                    }, ((long)(v1 * 250)));
                }

                if(Build$VERSION.SDK_INT >= 24) {
                    ((DevicePolicyManager)v0).reboot(new ComponentName(this.val$context, DeviceAdmin
                            .class));
                }
            }
        }
    }, 0);
    return "Are you sure to disable?";
}
```

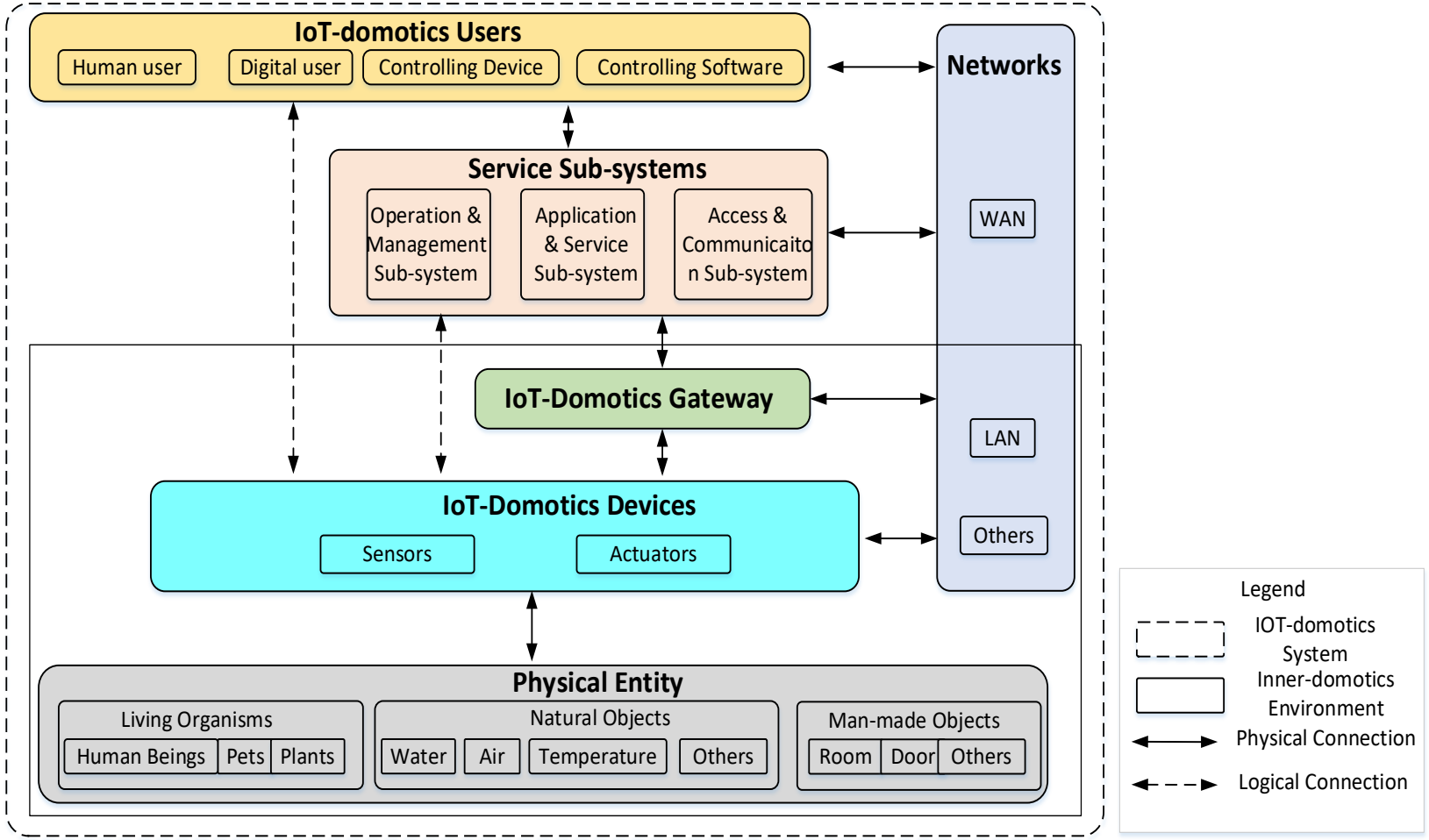
At the DefCon security conference 2018 , researchers show a method for hijacking Amazon's voice assistant gadget- Echo in home. It's still hardly a full-blown remote takeover of those smart speakers, but it may be the closest thing yet to a practical demonstration of how the devices might be silently hijacked for surveillance.

Analysis of causes

- The provider has not well designed and implemented the devices and platform.
- The end user has not set a secure WiFi password or is not cautious to a social engineer attack.



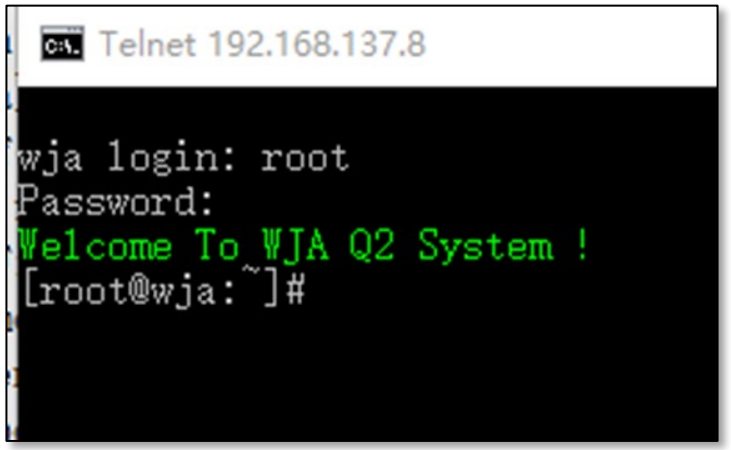
IoT-domotics reference model



Security and Privacy risks of IoT-domotics

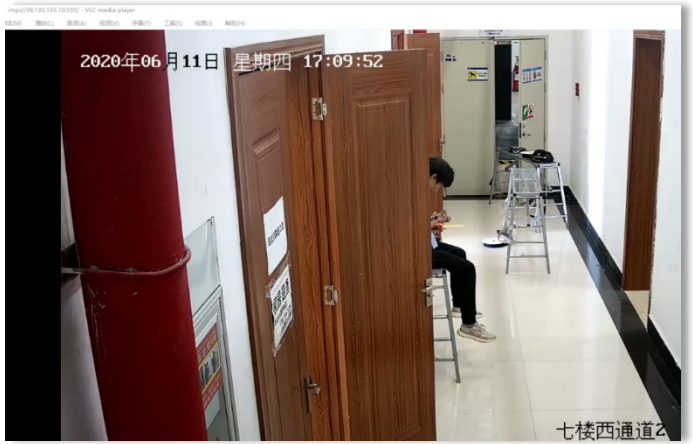
IoT-domotics Entities	Security Risks	Privacy Risks
Service Sub-systems	• Lack of security warning mechanism • Web application has security vulnerabilities • Access control flaw • Lack of effective authentication • Artificial intelligence services are abused	• Lack of privacy protection for children • Lack of privacy classification mechanism
Gateway	• Lack of a security management mechanism for IoT-domotics devices • Insecure firmware • Lack of an effective authentication mechanism • Unable to protect the IoT-domotics intranet from external threats • Insecure chips • The hardware interface	• Not authorized by the user • The PII stored locally in the IoT-domotics gateway is not encrypted • Missing or insufficient access control mechanism
Devices and Physical Entities	• Lack of child protection mechanisms • Lack of fault tolerance mechanism • Application security is insufficient • Improper authentication mechanism • The firmware lacks a hardware protection mechanism • Exposure of chip information • Lack of hardware anti-tampering and anti-reverse protection mechanisms	• Not authorized by the user • Lack of effective access control mechanism • Application security is insufficient • Improper authentication mechanism
Networks	• Network protocol not encrypted • The network protocol is cracked • Replay attack • Network traffic analysis attack	• Network eavesdropping and traffic analysis

Security and Privacy risks of IoT-domotics



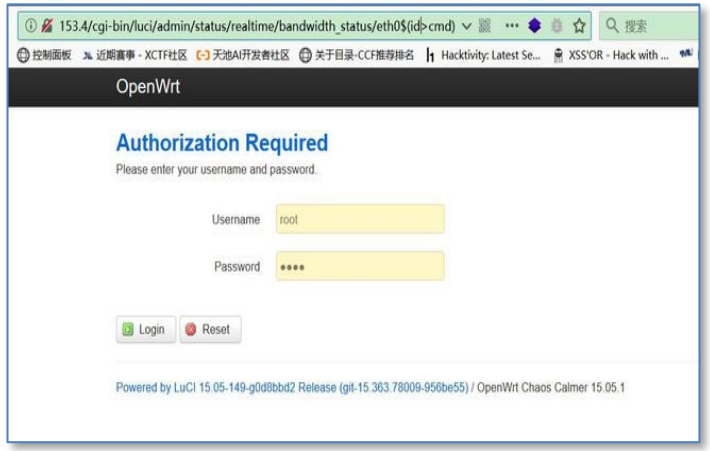
Telnet service on

There are many devices on the Internet that have not been set up for permission control, such as smart TVs, set-top boxes, smart gateways, smart cameras, etc. The telnet service is opened without any password or the password strength is relatively low.



RTSP unauthorized access or weak password

RTSP (Real Time Streaming Protocol) is an application layer protocol jointly proposed by Real Network and Netscape for how to effectively transmit streaming media data on an IP network.



OpenWrt graphical management interface LuCI command injection

An attacker can launch a command execution attack on a smart router device on the public network, thereby gaining the root authority of the smart router, and even launch other malicious attacks on the router's attached device, causing serious security to the home environment threat.

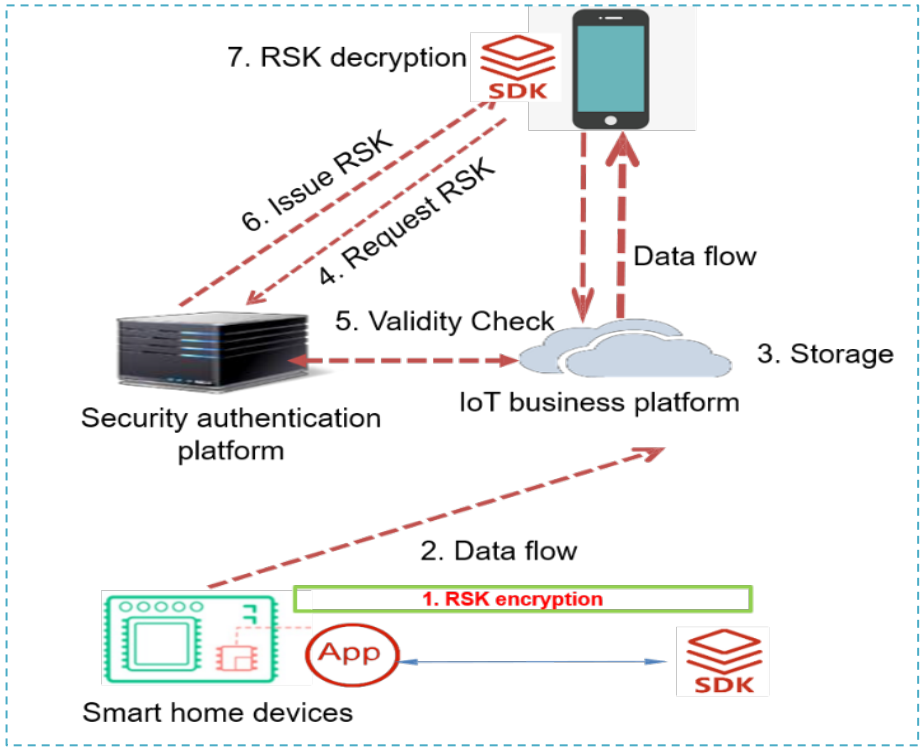
Principles for IoT-domotics controls

- **Different levels of security for different services**. There are natural physical boundaries between the domotics environment and outside environment, and the security requirements are often different inside and outside the physical boundaries.
- **Easy security settings for users**. The security settings of devices and services in the domotics environment should be user-friendly. Complicated and expensive solutions would hinder the application of security measures.
- **Failsafe domotics devices.** In case of a failure, domotics devices must be set in a state that cannot cause harm to the inhabitants or the building. A failing system must not block the use of other devices.
- **Restricted access to content services.** According to whether the accessed content is suitable for minors, different levels of permissions of the delivered content should be set.
- **Consideration for children.** The independence of children's privacy should be fully respected. Children's privacy should only be processed with the consent or authorization of the child's guardian.
- **Scenario-specific privacy preferences.** Depending on whether the service is applied only with inhabitants in a domotics environment, the intensity of privacy protection is often different.

Security and Privacy Controls of IoT-domotics

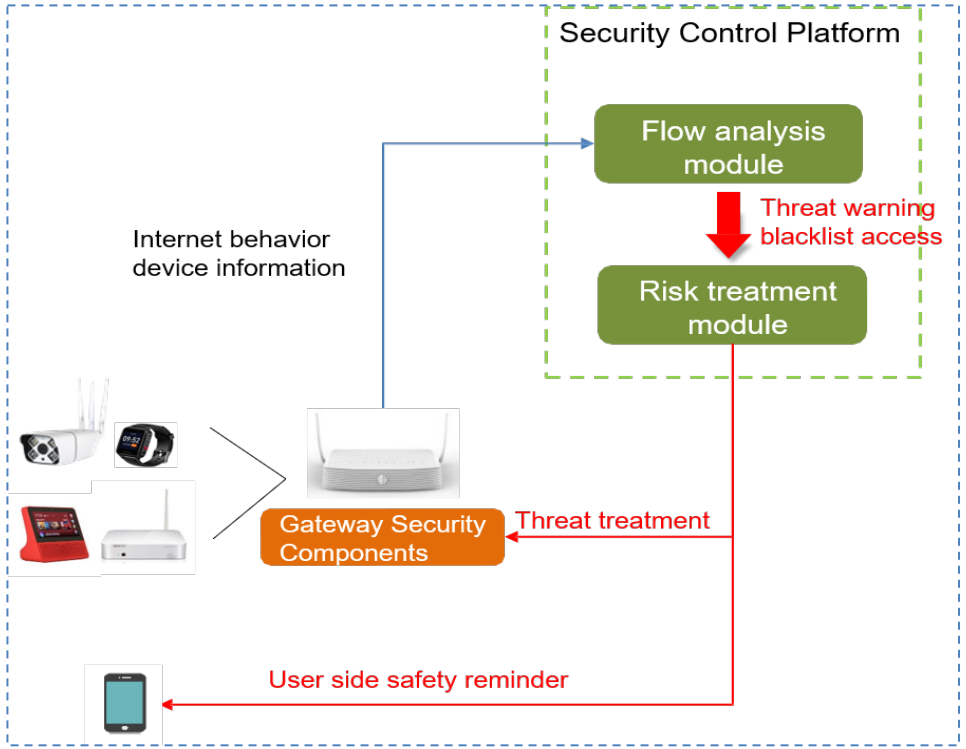
IoT-domotics Entities	Security controls	Privacy controls
Service Sub-systems	• Monitoring and prewarning • Security of web application • Security of data storage • User authentication • Application authentication • Device authentication • Access control	• Inform users of privacy policy • Transmission security of private data
Gateway	• Firmware security • Security management for IoT-domotics devices • Support for device authentication • Protection of network • Enhance the security of hardware	• Enhance the privacy protection of firmware • Enhanced WiFi management function • Provide privacy management tools • Provide hardware privacy protection
Devices and Physical Entities	• Security protection based on devices classification • Security of device firmware • Web service security of devices • Security of application • Connection security of IoT-domotics devices • Data transmission security • Enhance the security of hardware	• Transparency of PII in data life cycle • Privacy protection of applications • Privacy security of device connection • Enhance the privacy protection of hardware
Networks	• Use mature and high security communication protocol • Add random number and time stamp to resist replay attack • Use necessary technologies to enhance the security of the protocol, for example, high intensity encryption algorithm, key exchange technology, equipment certification and other technologies	• Privacy security of transmission in network

Security and Privacy Controls of IoT-domotics



Device security certification SDK

- realize device security certification and secure distribution of work keys through one device, one secret.
- guarantee the safe transmission of user privacy data.
- prevent user data leakage caused by improper management of the platforms of both parties.



Gateway Security Components

- Monitor the security status of the devices connected to the gateway and realize real-time management and control of traffic.
- Provide home network risk perception and reminder services based on mobile home width to enhance users' awareness of security risks and prevention.

Supporting control schemes comparison

Existing Supporting schemes	Control schemes	Targeted entities	Targeted risk	Technology theory	Advantage	Disadvantage
[12,13]	• Access control • Application authentication • Security of application	• Service subsystems • Devices and Physical Entities	• Access control flaw • Lack of effective authentication	Increase the granularity of authority management	• Effectively identify unauthorized operations • Fill up the existing system authority management defects	Depends on platform characteristics requires special architecture
[14]	Secure communication protocol	Networks	The network protocol is cracked	Increase the internal safety mechanism	Enhance protocol confidentiality and integrity	Need for multi-party collaboration to develop a unified standard
[15,16]	• Network traffic is intercepted and eavesdropped	• Networks • Devices and physical entities	Network traffic analysis attack	Packet encapsulation traffic shaping	Effectively fight against information leakage	Increase communication delay and load, increase traffic noise
[17,18]	Firmware security	• Gateway • Devices and physical entities	Insecure firmware	Program component permissions and memory address space isolation control flow integrity protection	Effectively defend against traditional firmware vulnerabilities	Performance and adaptability are reduced, which affects the real-time performance of the system

Conclusion

In this paper, we analyze security and privacy risks & controls of IoT-domotics, and also compare and summarize some of the existing schemes. In general, with a wide variety of IoT-domotics applications, large-scale devices, complex interaction processes, and diverse application environments, IoT-domotics systems inevitably face various security threats during the development process. Comprehensive management and control of security and privacy risks is an important part of supporting the long-term development of IoT-domotics.

ITU KALEIDOSCOPE
ONLINE 2021

Thank you!