Lunds Tekniska Högskola

EITN50

Advanced Computer Security

Project E
Trusted Camera

October 19, 2017

1 Target of Evaluation

The trusted camera is a surveillance camera capable of protecting its operation and the data it streams, that can be mounted inside a building. The camera device has the following components: a camera, a PCB with ARM TrustZone CPU, RAM, flash memory, TPM, a JTAG debug interface, a LTE subsystem with USIM card reader, a sensor and a battery connected through a power management system. Access to camera footage and management options is handled through a management interface that requires login credentials to access.

This camera is considered a professional level product and the device life cycle can be seen in figure 1.

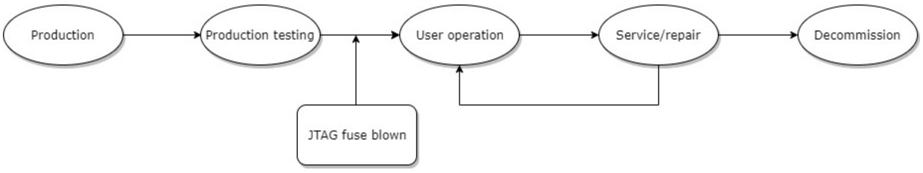

Figure 1: Life cycle for the camera device.

2 Security Target

2.1 Functional Requirements

- The cameras data is streamed with SRTP.
- Secure firmware updates of the camera.
- The camera has a unique identity.
- The camera has a flash memory used to store firmware and configuration data, as well as up to one hour of recorded video.
- User information and stored data is unaccessible for repair personnel.
- The stored user information and data stored on the flash memory should be easily wiped upon decommissioning of the device.
- The camera has a management interface where attested information such as the currently loaded firmware and the hash key used to protect the SRTP channel and stored video data is available.
- The camera housing has a tamper sensor.
- It is possible to handle hardware problems by applying software patches that overcome hardware errors and/or by applying fixes in the devices permanent ROM code.

2.2 Assumptions

A.Protect: The computer with access to the camera interface is protected.

A.Watch: The camera is presumably used in a public setting and the feed will be under constant surveillance through the interface.

A.Battery: The device battery can last for up to three days of operation on its own.

3 High Level Design

The high level architectural overview can be seen in figure 2.

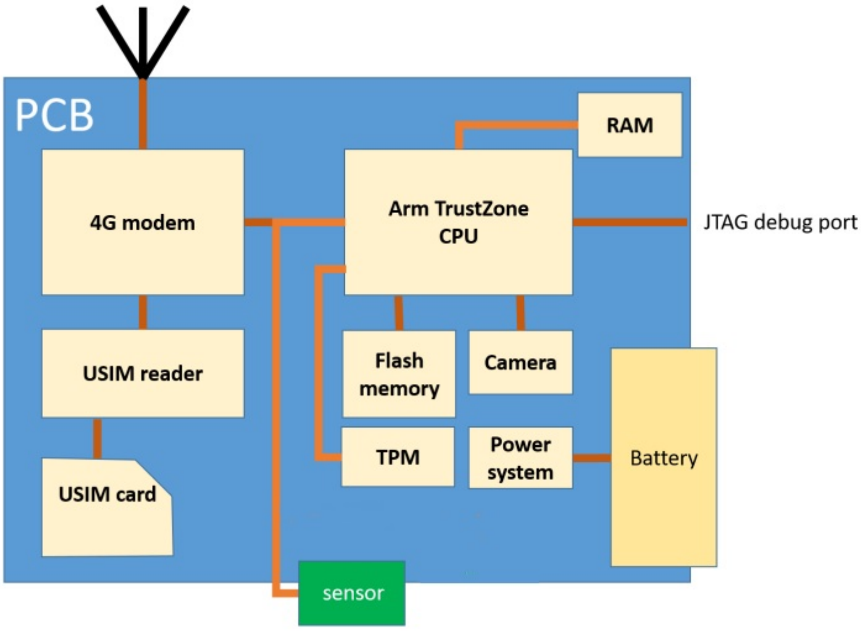

Figure 2: Architectural overview of the system.

3.1 Central Processing Unit

The CPU used for the camera device utilizes the trusted execution environment (TEE) ARM TrustZone technology. The TrustZone partitions the systems memory and CPU resources into a secure and a non-secure world and has an extremely small remote attack surface. There is practically no way of interacting with the TrustZone directly without kernel privileges. This means that arbitrary code would be ran in unprivileged mode and not have read, write or fetch access to memory that belongs to privileged mode [1]

3.2 Storage

An hour long recording using H.264 video compression with a resolution of 1280 x 720 and a frame rate of 30 FPS requires approximately 25.97 GB of storage capacity. Since the firmware and configuration is stored on the flash memory as well, a 64 GB SD card is used to allow for some leeway.

Recorded video stored in the camera's flash memory should not be accessible to an attacker even if the camera is compromised. This is achieved by implementing a device-specific key, which can only be accessed by authorized code. The key should be integrity protected and stored in a protected memory area on the processor chip. Additionally an implementation of a cryptographic mechanism should be provided.

The device also has a 512 MB static random-access memory (SRAM) stick which acts as a CPU cache.

3.3 Hardware Security Modules

The system contains a long term evolution (LTE) subsystem consisting of a universal subscriber identity module (USIM) card reader and a 4G modem that utilizes the secure real-time transport protocol (SRTP). SRTP needs an external key management protocol to establish initial keys [2], therefore the datagram transport layer security extension is used with SRTP (usually referred to as DTLS-SRTP) to secure unicast data transfers.

The advantage of DTLS compared to the SDES key management protocols is that keys will not need to be negotiated in a plain text key exchange. SDES negotiates keys and security parameters in plain text it is completely reliant on SRTP for the encryption, message authentication and integrity required for secure data transfer, while DTLS provides much higher security on its own.

Even though SDES is still widely used and slightly more interoperable and easier to implement than DTLS, DTLS is on the rise since it is the more secure alternative [3] [4].

The data stream itself will be protected by SRTP which uses the AES block cipher and the HMAC-SHA1 authentication transform.

3.4 Trusted Platform Module

The printed circuit board (PCB) is equipped with a discrete v1.2 TPM. The TPM provides functions for secure remote attestation of platform configuration, secure storage of sensitive data and implementation of a verified boot [5].

The TPM handles encryption of video data which is then stored inside the secure world part of the ARM TrustZone environment.

3.5 Joint Test Action Group

The system contains a JTAG that is provided with a security fuse. This fuse acts as a one time programmable device which cannot be re-enabled once it has been "blown".

3.6 Sensor

The camera has a sensor that is used to detect if the device case is open or closed. In the event of an unauthorized opening an alarm is activated at the remote control interface. Whenever a camera unit is sent for repairs the sensor is deactivated in preparation for the operation. Once the repairs are complete the sensor is set to the default mode.

3.7 Power Supply

The device is equipped with a battery that is normally connected to a charger, but can last for three full days of normal operation on its own. In the event of sudden power loss an alarm is activated at the remote control interface.

4 Security

4.1 Security Considerations

4.1.1 Threats

T.Insert: Bugs allowing insertion of executable foreign code through the remote management interface.

T.FW: Loading of unauthorized firmware.

T.SRTP: Loading of SRTP keys of incorrect receiver.

T.Open: Opening of the device and replacing the flash memory contents with own code and configuration.

T.Repair: Dishonest device repair personnel.

T.JTAG: Misuse of JTAG debug interface.

T.Keyloss: Loss of key or otherwise compromised camera.

T.Bruteforce: Bruteforce attacks against account passwords. **T.PowerAnalysis:** Power analysis.

T.PowerLoss: Power loss.

T.MITM Man-in-the-middle-attacks.

4.1.2 Security Objectives

O.Sanitize: Sanitize all input fields in the remote management interface.

O.Firmware: Require the firmware to be cryptographically signed.

O.DTLS: SRTP uses the key management protocol DTLS (DTLS-SRTP) for establishing keys.

O.Fuse: Disables the JTAG interface port.

O.Detect: Detect unauthorized opening of the camera casing.

O.Blacklist: Keys that may be compromised are blacklisted.

O.TZ: Inclusion of the ARM TrustZone TEE.

O.TPM: Inclusion of a discrete TPM (v1.2).

Table 1: Map of security threats and security objectives.

	O.Sanitize	O.Firmware	O.Detect	O.TZ	O.TPM	O.DTLS
T.Insert	X			X		
T.FW		X		X	X	
T.Open			X			
T.Repair				X		
T.SRTP						X
T.MITM						X

Table 2: Map of security threats and security objectives, continued.

	O.Fuse	O.Blacklist	A.Watch	A.Battery	O.StrongPass
T.JTag	X				
T.Keyloss		X			
T.PowerAnalysis			X		
T.PowerLoss				X	
T.BruteForce					X

4.2 Security Evaluation

Tables 1 and 2 shows an overview of security threats and the security objectives that counteract them. Here follows a more detailed description of how the threats are being handled.

4.2.1 Foreign Code Execution (T.Insert)

To prevent foreign code execution through bugs in the remote management interface the relevant memory addresses should be Read/Write only. All input fields and parameters should be properly sanitized. Additionally, the TrustZone would not allow foreign code to be ran in the secure world.

4.2.2 Firmware (T.FW)

In order to update the device firmware it is a requirement that it is cryptographically signed. Whenever a new firmware version is released a hash is calculated and appended to the code. When an update attempt is initiated the processor calculates its own hash of the image. If the hash matches one signed by a certificate it trusts, the image is loaded. During production a code is embedded in the CPU that allows it to verify a signature from a trusted company. ARM TrustZone has a secure boot scheme that provides precisely these kind of checks. It does so by applying RSA Probabilistic Signature Scheme protocol. By including a public Key of a trusted firmware manufacturer in the device it can be used to verify that a binary has not been modified as well as that it was provided by a trusted entity. While the public key does not inherently need to be kept confidential, it is in our best interest do so since it could be replaced by a public key that belongs to an attacker. Storing the public key inside ARM TrustZone secure world area is sufficient protection against such an attempt [6].

4.2.3 Physical Tampering (T.Open)

The device has a tampering sensor that makes sure that the camera casing remains closed, which prevents the threat of an attacker opening the device and replacing components to inject their own code or configurations. If the sensor is activated an alarm is triggered in the management interface.

4.2.4 Dishonest Repair Personnel (T. Repair)

A camera in need of hardware repairs is an attractive attack vector for a malicious entity, for example a dishonest repair technician. Once the repairs are complete the technician can run various system checks through the user interface by using specific for such purpose login credentials. This approach limits access privileges and prevents unauthorized access to sensitive data.

ARM TrustZone secure world and non-secure world separation can further divide areas of access between repair personnel and legitimate users.

4.2.5 SRTP key protection (T.SRTP, T.MITM)

The key management protocol DTLS provides secure key exchange with perfect forward secrecy (PFS). PFS ensures that the session keys derived from a set of long-term keys will not be compromised if one of the long-term keys is compromised in the future. Additionally, DTLS-SRTP can compare the hash of each sides certificates and/or identities/MAC addresses during the handshake to bind these to the connection and ensure both that the camera is actually communicating with the device it wants to and that no man in the middle attacks can occur [2].

4.2.6 JTAG debug port (T.JTAG)

The JTAG is equipped with a fuse that once blown renders the JTAG interface unusable. This fuse is blown right after end-of-line production testing of the PCB is complete, which ensures that the JTAG port cannot be enabled again. This may obstruct repair work on the device but we found this a reasonable trade-off for securing the camera, considering that the JTAG port is a high risk aspect of the product.

4.2.7 Loss of Key (T.KeyLoss)

Should a key used for authentication become compromised it is to be added to a blacklist of ”bad keys”. Whenever an authentication is initiated said list is checked for a match on the received key. In case of a match the authentication attempt is denied and nothing else happens.

4.2.8 Power Supply (T.PowerLoss, T.PowerAnalysis)

If the camera loses power the tampering sensor would be disabled, making the camera vulnerable. The battery is usually connected to a charger, but this charger could potentially be disconnected or a sudden power outage could occur. This risk is mitigated by having a battery that lasts up to three days, which gives ample time to detect problems and charge the battery before it runs out. If the power would be cut completely an alarm is triggered in the management interface.

Power analysis is a non invasive side channel attack that could potentially be used to extract cryptographic information from a system by studying the current used by the device. However, since the device in question is a camera the perpetrator would most likely end up being recorded while connecting the oscilloscope and performing the analysis. This makes it seem like an unlikely threat that does not require any particular defense in this case.

4.2.9 Strong Passwords (T.BruteForce)

Brute force attacks against user accounts are hindered by requiring a strong password consisting of at least 10 characters that are a combination of uppercase and lowercase letters, numbers and special symbols. This method can further be augmented by restricting the number of login attempts with a time-out after a certain amount of login attempts.

5 Conclusion

Overall we are happy with our design of a secure camera, although we had some trouble at the beginning of figuring out how to define each components purpose. The project presented several different security areas that had to be taken into account when considering threats. All threats presented in this document are handled in a way that keeps the production costs of the camera low, as well as maintenance costs.

6 Peer Reviews

TBD.

7 Improvement Sheet

TBD.

References

[1] D. Rosenberg, 'Reflections on Trusting TrustZone'

[2] 'The Secure Real-time Transport Protocol (SRTP)', https://tools.ietf.org/html/rfc3711, 2017-10-15

[3] 'WebRTC MUST implement DTLS-SRTP but... MUST NOT implement SDES?', https://webrtchacks.com/webrtc-must-implement-dtls-srtp-but-must-not-implement-sdes/, 2017-10-15

[4] 'Options for Securing RTP Sessions', https://tools.ietf.org/html/rfc7201, 2017-10-15

[5] 'Trusted Platform Module (TPM)', https://trustedcomputinggroup.org/work-groups/trusted-platform-module/, 2017-10-15

[6] 'ARM developer ARM Security Technology Building a Secure System using TrustZone guides and articles Technology', http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.prd29-genc-009492c/CACGCHFE, 2017-10-15