Project D : Trusted Camera

Working Version 2017-10-14 16/10/2017

Introduction

This project presents the design of a surveillance camera. There are a lot of different kind of users, features and requirements. This camera has a specific purpose, it is suppose to be easy to use and secure. So, it must be simple.

Description

This camera is a private consumer product focused on the kind of user who want something that is rather secure and that works automatically.

The user only have to care about using his phone application. If it doesn't work, the service desk must be called.

Assumptions

- The product is not protected by a locked box. However, it is located high on a wall. Someone can access to it.
- LTE module provides a proper bitrate. We don't care about bandwidth consumption.

Architectural overview

Security Target (ST): a surveillance camera allows to:

- Send the information to the user securely. Avoid eavesdropping.
- Get attested information about the firmware and the hash of the key to store video and SRTP.
- Update the firmware.
- Avoid physical tampering.

Target Of Evaluation (TOE): Physical device integrated by the hardware listed below:

- LTE Subsystem with USIM card reader.
- Special flash to hold an ID
- Camera
- PCB with flash memory
- ARM trustzone CPU

- RAM
- JTAG
- TPM
- Tamper sensor

Diagram of the system:

User device camera server



---

management interface
←---------->

---

key agreement ECDHE
←---------->
Authentication
←---------->
key exchange
←---------->
ENCRYPTED VIDEO
←----------*

The user device and the camera establish secure connection by opportunistic encryption. Then, the user device and the camera authenticate each other over the encrypted channel. Once both are authenticated they exchange a key for SRTP and the user device provides a key to the camera to encrypt the data on memory. Finally, data transmission starts.

The ARM trustzone keeps the firmware secure.

TPM manages the keys. The PIN to store the keys derives from the authentication.

Secure JTAG implementation using Schnorr Protocol avoid the misuse of JTAG. [1]

The key agreement is based on Elliptic Curve Diffie-Hellman with Ephemeral key because it has a good performance and it allows to keep the communications secret.

Security evaluation

theads\protection	ASLR/ input checking	SECURE BOOT	User and camera authentication	tamper sensor	ARM trustzone	TPM	Schnorr Protocol
executable foreign code	x						
Loading of unauthorized firmware		x					
Loading of SRTP keys of incorrect receiver.			x				
Opening camera device and replace flash memory contents with own code and configuration.				x	x		
Dishonest device repair personnel.					x	x	
Misuse of JTAG debug interface.							x
Loss of key or compromised				x	x	x	

camera (fallen into the hands of a stranger)							

References

1 Secure JTAG implementation using Schnorr Protocol
https://www.esat.kuleuven.be/cosic/publications/article-2321.pdf