An Investigation of the Security of Smart Doorbells

Bauhaus-Universität Weimar

Marcus Jan Almert, Nathalie Lang, Stefan Lucks

first.middle.lastname@uni-weimar.de

Introduction

- IoT devices offer convenient features but they also introduce cyber-security risks to traditionally ”dumb” equipment
- Our security investigation focuses on the device group of smart doorbells
- Smart doorbells live stream their camera feed, issue notification if motion is detected and offer two-way audio calls with visitors
- They require a constant internet connection and are accessed and set up by an companion app which requires an account
- Investigated devices for this research: Victure VD300, Eken V5, Eken V7, and Tuya DDV-202

Methodology

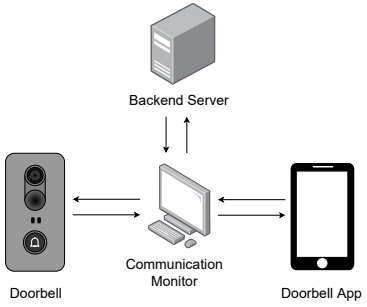

Figure 1. Network analysis setup.

Firmware and App Analysis

- Firmware extraction from flash memory chips
- Search for default credentials, encryption keys, and authentication procedures
- Reverse Engineering

Network Analysis

- Network traffic between doorbell, app and backend server is relayed through a communication monitor
- Wireshark and Mitmproxy to capture and analyze network traffic

Network-based Attacks

Attack	Vulnerability	Consequence
Person-in-the-middle	Unencrypted HTTP communication	Leakage of data, e.g. settings, pictures, account information, and account credentials
URL-Manipulation	Unauthorized access to backend API servers	Leakage of user data, e.g. email address, pictures, voice recordings, settings and notifications
Credential extraction	Doorbell hosts HTTP-server which uses default login credentials extractable from the firmware	Access to settings, live pictures, doorbell log, reboot and factory reset commands and firmware updater
Denial of Service	Doorbell, app and backend server use slow-DoS vulnerable MQTT version	Unavailability of critical infrastructure needed for doorbell usage

Hardware-based Attacks

Attack	Vulnerability	Consequence
Local storage tempering	Unencrypted removable storage	Access to pictures and videos
Reset button abuse	Easily accessible reset button	Data loss and doorbell unaccessible
Network settings tempering	Doorbells can be added to other networks by using QR codes	Data leakage through person-in-the-middle attacks
Camera covering	System crashes when camera sensor is covered	Bootloop