Attacks on GSM-devices

Aleksandr Kolchanov, pyrk1@yandex.ru
Theory part
GSM-alarms
Smart homes

BASIC LAYOUT

- RELAY BOARD
- GSM MODULE
- DTMF DECODER
- MICRO-CONTROLLER
- OFFLINE
- ONLINE
- Mobile Application
- Android

24 April 2012
SMART HOMES
Access control systems
Industrial GSM controllers

16 Relay output GSM Controller
DC12V power input
Phone calling and SMS remote control

GSM Environment Condition Monitoring Solution

Air-Conditioner
Smoke Detector
Temp. & Humidity Detector
AC Power Detector
Strobe Siren
Motion Detector
Door Contact
Water Leakage Detector
GSM electric sockets
Smartwatches for kids
Controlled devices

User (or hacker) can remotely connect to devices and perform actions

- Controlled alarms
- Electric sockets
- Locks
- Smart homes
- Spy devices
Managed devices

User (or hacker) can remotely connect to devices and change important settings

- Controlled alarms
- Several locks
- Smart homes
- Smartwatches
Uncontrolled devices

User (or hacker) can’t remotely connect to devices and perform actions

- Passive alarms (just will send SMS or make a call)
- Several GSM-trackers (will send SMS)
Unmanaged devices

User (or hacker) can’t remotely connect to devices and change important settings

- Some alarms
- Several locks
- Some controllers
A bad surprise :

If you don't know, how to manage this device, it does not mean, that this device is unmanaged.

- Hidden SMS-commands and password
- Remote reset
- Additional hidden commands
Attacks
Bypass an authorization

Make a call to device or send SMS and try to do something

- Caller ID check
- SMS phone number check
- Password
- Nothing
Attacks on mobile operators

Sometimes it can be easy and effective

- Block SIM-card
- Spend all money
- Change tariff
- Intercept SMS and find passwords
Strange attacks

- Incoming call attack: some devices can’t send alarm signal during another call
- Attacks on detectors
Results

1. An attacker can disable some alarms
2. An attacker can use a microphone to listen to the environment
3. Some doors can be opened remotely
4. A lot of smartwatches for kids are in danger
5. The state of some industrial and smart-homes controllers can be changed

1. Caller ID check usually is insecure
2. 4-digit passwords can be easily bruteforced
3. Hidden passwords and commands can be found
Practical part
1. Attack on electric socket
Plan

1. You can try to call to the number of GSM electric socket from your phone to check, that socket will ignore it.
2. Make a call with SIP-account with changed Caller ID
3. The socket will change the state

- Device phone number: +79117398557
- Owner Caller ID: +79006217078 (already used in SIP-account)
2. Attack on PSTN-alarm
1. Call to the PSTN-alarm with any number
2. Wait up to 30 seconds for an answer
3. You will be asked to type a password (default password is 1234).
4. You can try to bruteforce it (there are limit of 3 attempt for every call)
5. Then you can disable alarm (press 2) or use microphone (press 3)

- Device phone number: +79967774297
- Owner Caller ID: any number
2. Attack on GSM-alarm
1. Call to the GSM-alarm with any number, you can use SIP-account.
2. You will be asked to type a password (default password is 1234, also exist interesting password for settings, try to find it in manual).
3. You can try to bruteforce it (there are limit of 3 attempt for every call)
5. Then you can disable alarm (press 2) or use microphone (press 3)

- Device phone number: +79006490511
- Owner Caller ID: any number
SIP-account: 267452
SIP-password: workshop1

Zadarma app for IOS or Android