Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

# How to find and hack various GSM-devices: from children's watches to industrial controllers

Aleksandr Kolchanov

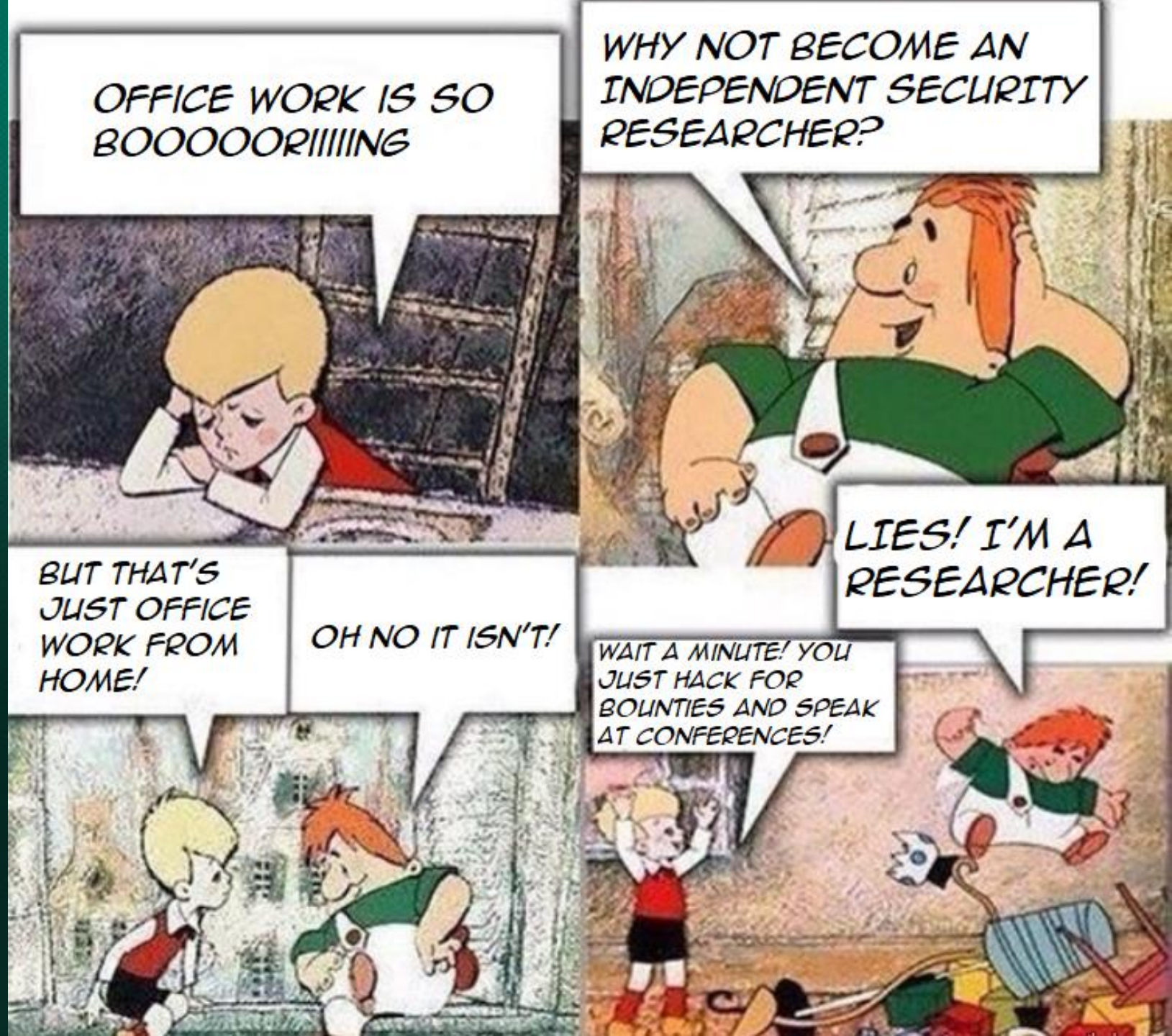
# About me

Independent researcher

GSM-devices fanboy

Telecom fanboy

I will mix it today



# Plan for this talk

Types of devices

Hacking methods

Several examples

Reasons to hack

Easy to hack, hard to find

# Types of devices

GSM-alarms

- Uses detectors
- Makes the call when someone open door or window
- Uses small microphone
- Can be configured remotely

GSM-electric sockets

- Uses SMS or calls to switch on/off
- Can be configured remotely


GSM-smarthomes controllers

- Can control different devices
- Uses SMS, calls or apps to be managed
- Can be configured remotely

# Types of devices


Industrial controllers

- Are close to a home controller, but have more features
- Different control methods

Access control systems

- Uses SMS or calls to open or close door or gate
- Can be configured remotely

GSM-trackers

- Collects information about location, etc
- Some models can be configured remotely


Smartwatches for kids

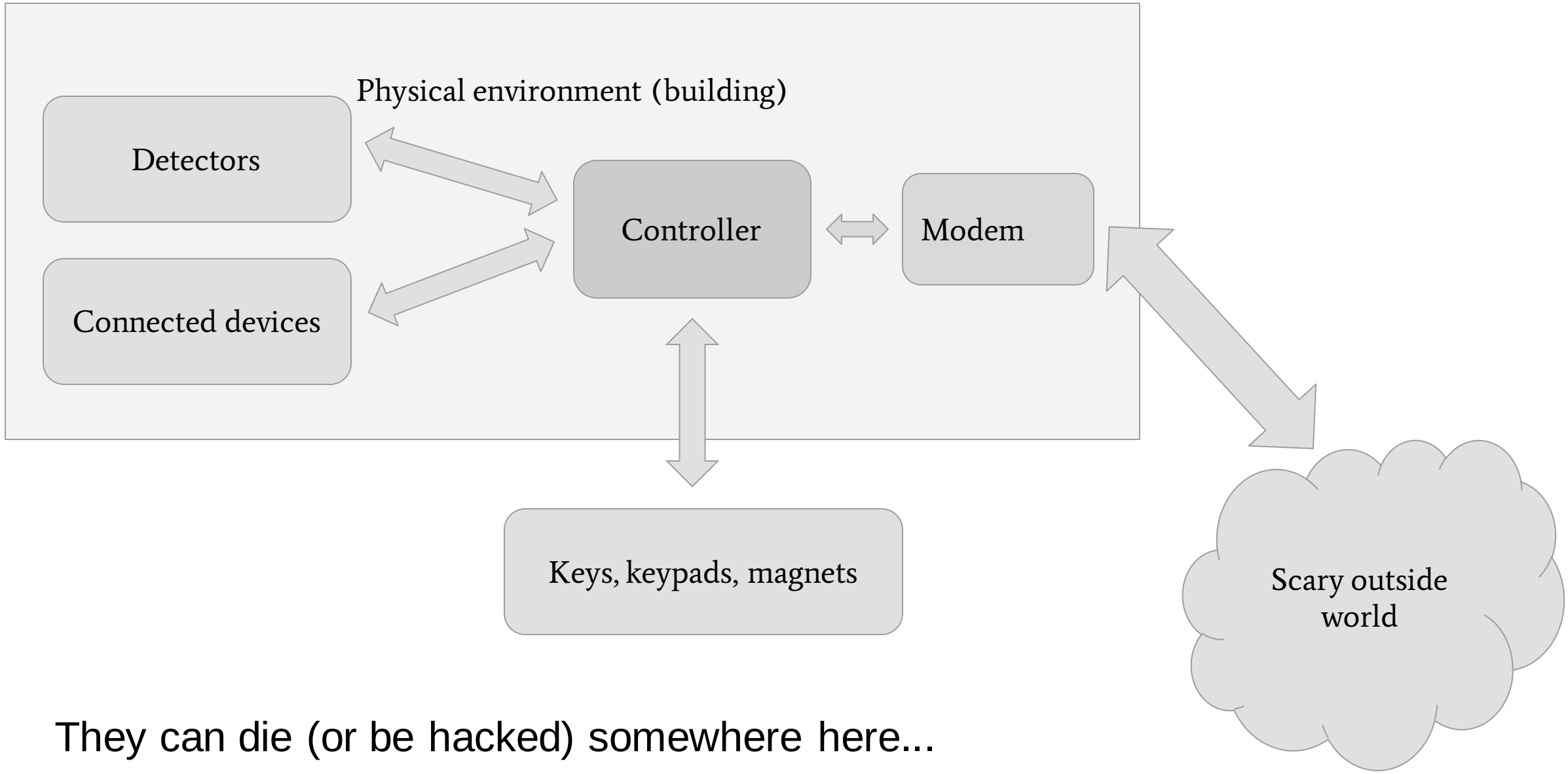
- Like mobile phone, but with addition control
- Can use microphone
- Can be configured remotely

# Reasons to hack

- Direct attack (silently open door)
- Using microphones to overhear someone
- Destroy property (explosions)
- Terrorism
- Political events
- Financial attacks
- Botnets for spam
- Reverse attack on accounts
- Penetration in a system
- Some funny ideas

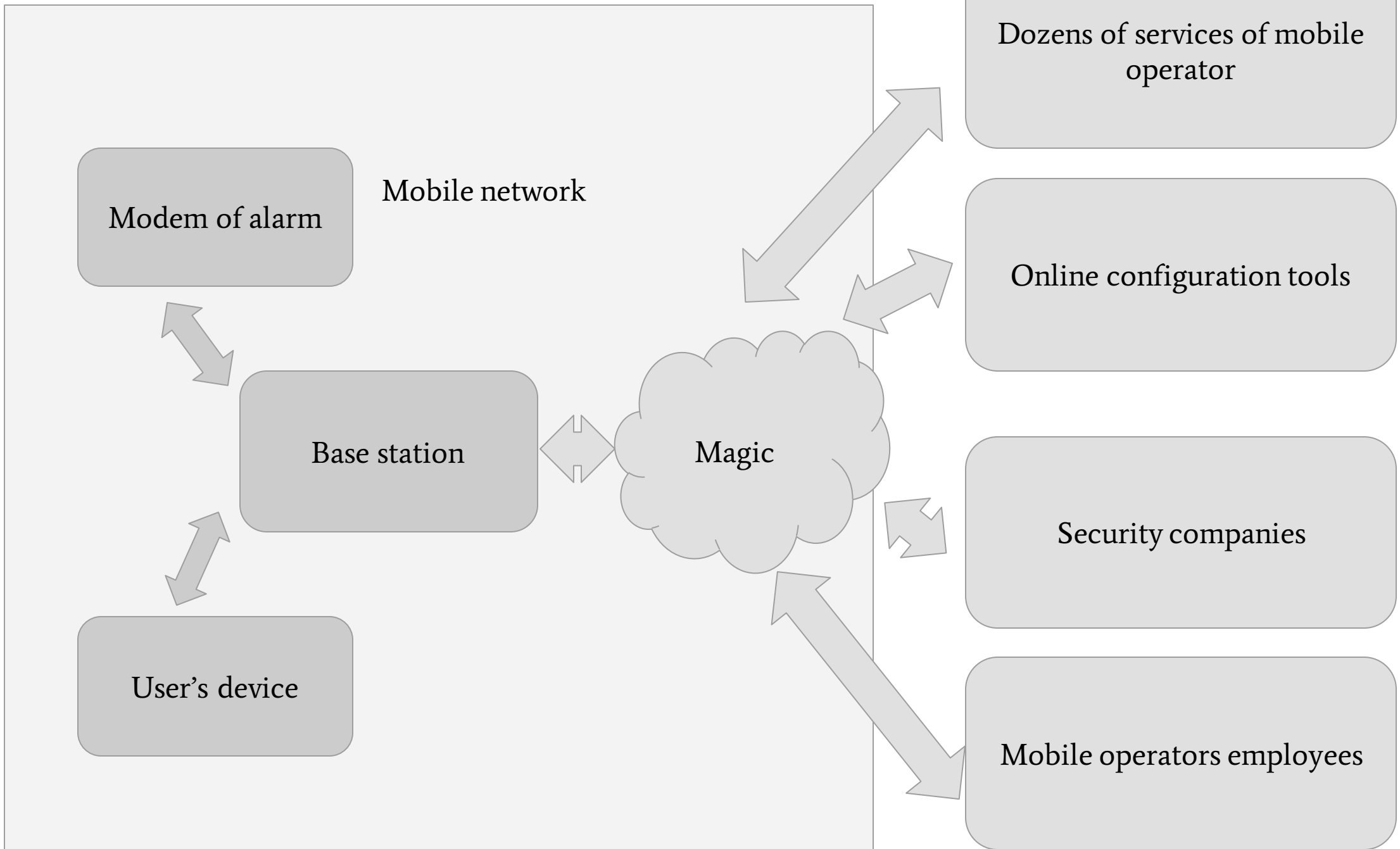
Big problem:

# Thousands of devices have dozens of points of failure




They can die (or be hacked) somewhere here...

… or there...


Modem of alarm
Mobile network
Base station
Magic
User’s device
Dozens of services of mobile operator
Online configuration tools
Security companies
Mobile operators employees

# Attack on environment

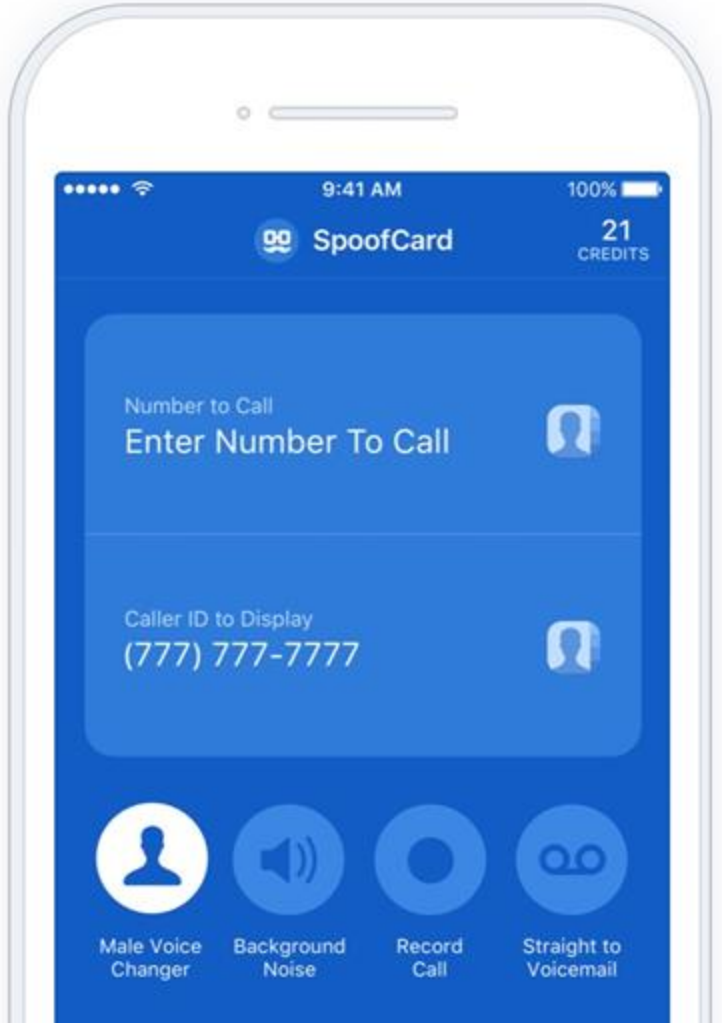
- Break the wall
- Break the window or door without opening
- Smash main unit fastly
- Bypass detectors (magnets, Faraday cage)
- Jamming

# Attack on connection

- Jamming connection modem - base station
- Attacks on mobile networks
- Spend all money in account or change tariff
- Block SIM-card
- Flood with calls

# Attacks on device

- Caller ID check
- SMS sender check
- Bruteforce
- Default passwords, stolen passwords
- Lack of authorization
- Online configurators
- Hidden commands and passwords



# Attack on other systems

- Insecure security agency
- Old protocols
- Attacks on family/employees
- Phishing
- Spoofed reverse call from device
- Reverse-attacks on mobile operator

# Home devices

- Thousands (or millions) of devices
- Easy to research
- Easy to hack
- A bit hard to find
- Can be used to steal private information

# Industrial devices

- Are not so widespread, as home devices
- Not so easy, not so hard to hack
- Harder to hack
- Hard to find
- Can be more profitable

# Targets

## Individual person

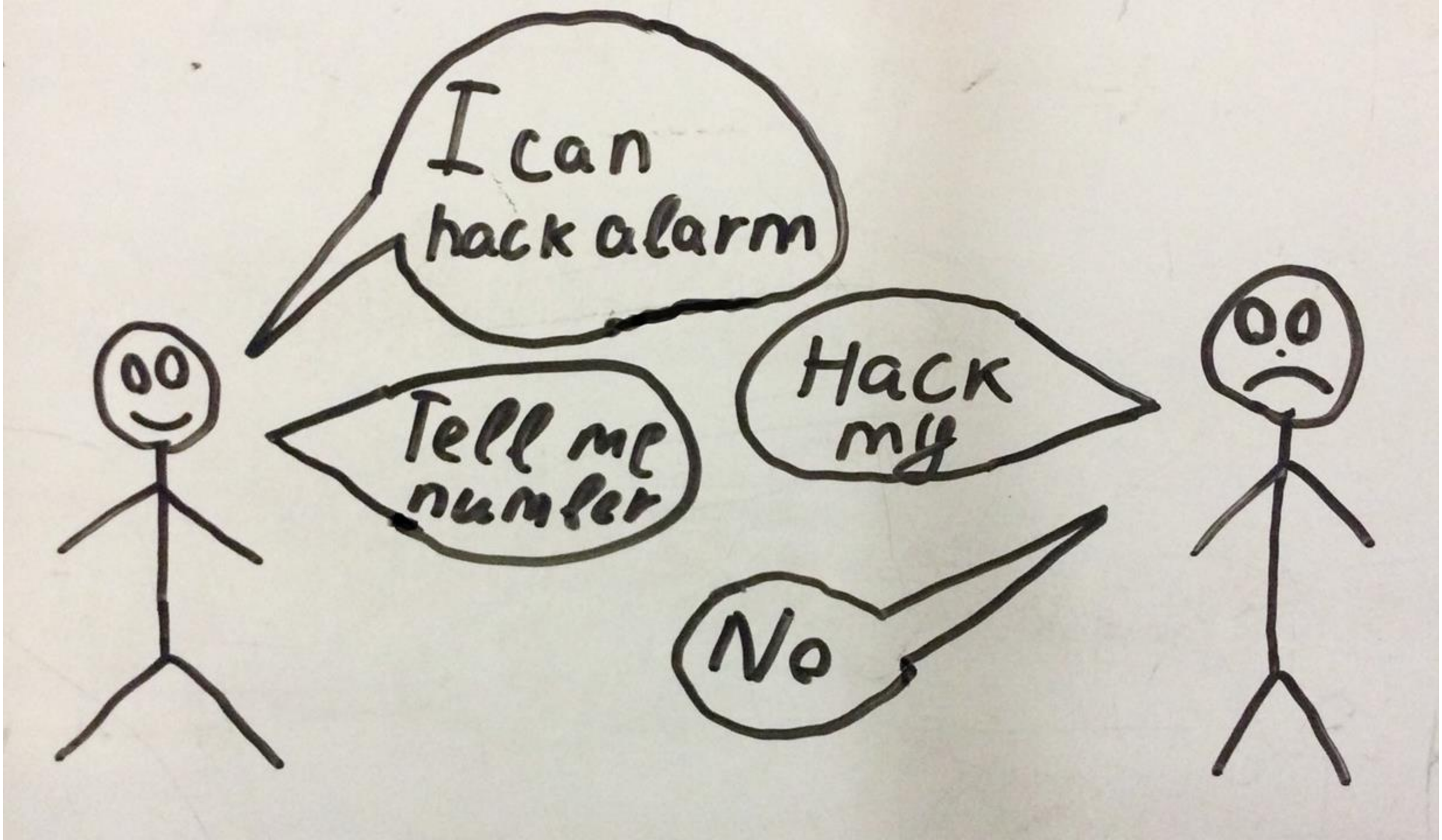
- Target is an individual person
- Several facts are available usually
- Devices are common
- Several people can manage device

## Individual company

- Target is a company or a part of company
- Can be very hard to find devices phones and control phones
- May use uncommon and expensive devices

## Unspecified (massive attack)

- Find as many as possible
- Hack all devices
- Expenses/profit balance
- Automatization and “big data”


I can hack alarm
Tell me number
Hack my
No

Big problem for hackers:

# It is easy* to hack devices, but how to find targets?

## IP-addresses

- We can have 4 294 967 296 IPv4 addresses at all
- We can scan fast
- We can do it cheap
- We have actual databases

VS

## Phone numbers

- We can have more than 999 999 999 numbers only in Russia
- No public database
- Scanning is expensive
- Scanning is slow

# Mass “Scanning”

1) Making a calls to all phone numbers (yes, it sounds terrible)
2) Record answers
3) Try to get some information form answers
4) …
5) Hack and get profit (or go broke)

# Results:

- More, than million of roubles spent
- Collected information about thousands of active* devices
- Maybe, some organisations will try to understand, what happening
- Money burned in small regions

Idea:

# Using different methods to get information about phone numbers of devices and reduce time for an attack

# Groups of phone numbers

## Confirmed

- Used for required type of device
- Ready to be hacked, yeah

## Unconfirmed

- Can be used for device
- Can be used for anything
- ...

## Removed

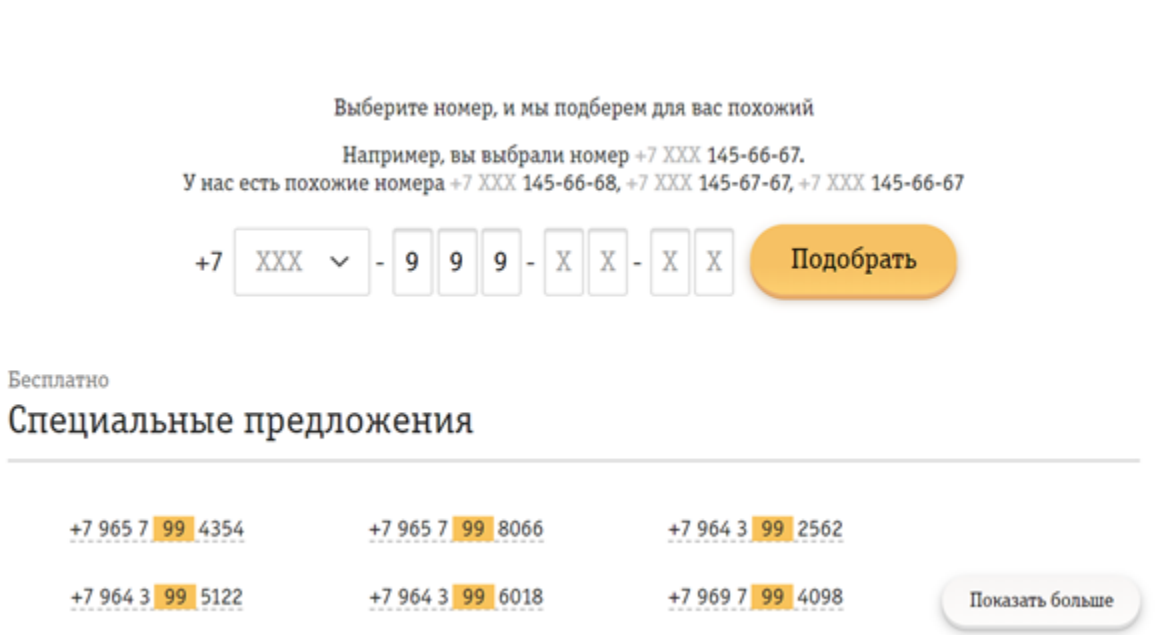
- Used in mobile phones
- Used in IVR systems
- Abandoned
- Are not sold

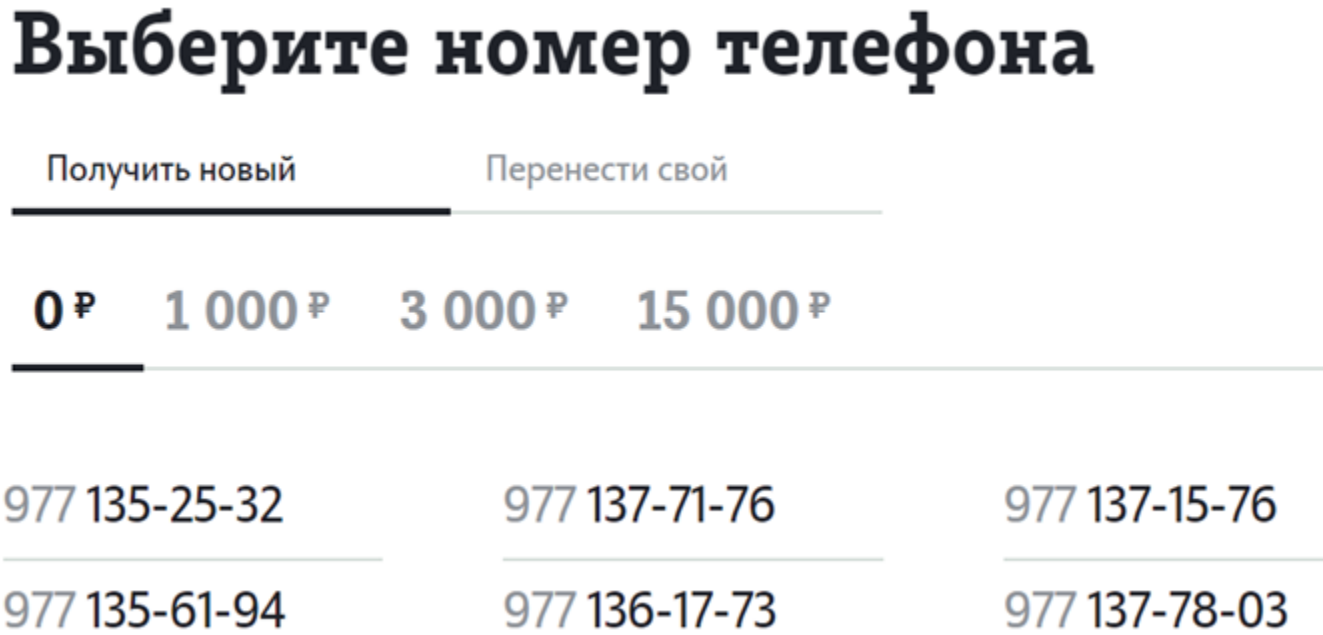
# Numbers recycling problem

- Mobile operators deactivate numbers abandoned for 2-3-6 months
- We can’t blindly beleave to old information, owner can be changed

# Select new number service

- Get information about definitely unused numbers
- Remove previous information



# Mobile operators API answers

- Mobile operators systems can have special API, which can be used to check, if this number is in use or no
- Errors, different answers
- Unused numbers can be removed from list

# Companies databases and anti-spam databases

- Several apps (like 2GIS on right) allows to get information about phone numbers
- Attackers can download this databases and remove companies phone numbers from list
- Also, an anti-spam database can contain information about numbers, that can be released soon

# Spam databases

- Spam databases contain information about thousands active phone numbers
- Attackers can buy/steal/get this databases and remove all active numbers from list

# Leaked databases

- Sometimes it is possible to get database with information about millions users
- Attackers can try to select active numbers and remove these numbers from list

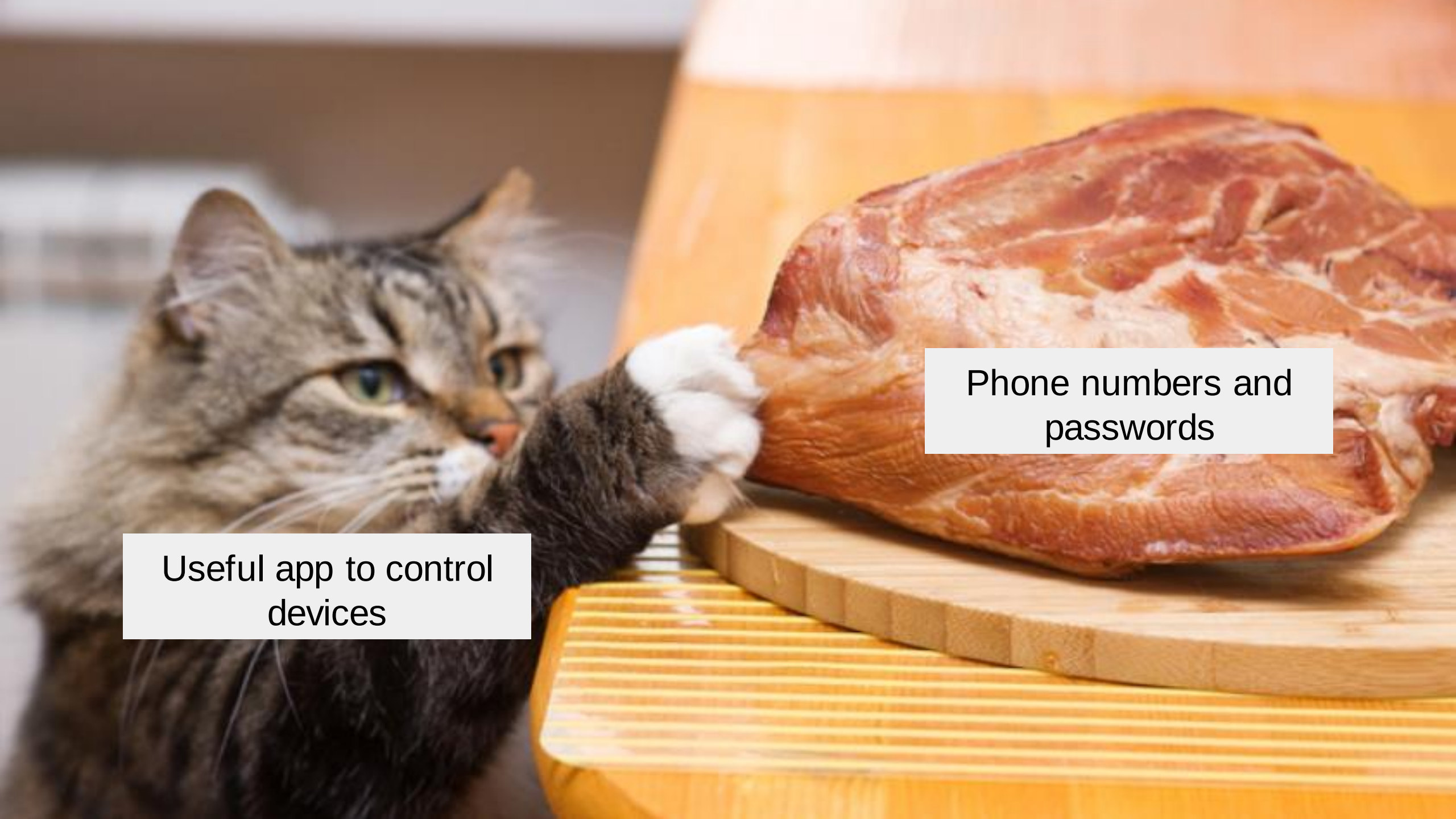
# Unauthorized access to mobile operators databases

By information from several public sources, it is possible to pay a small bribe and get access to info from mobile operators database:

- It is possible to get info about subscribers phone numbers
- Information about regular calls can be used to find device and phone numbers of family

# GetContact and similar apps

- Several applications can show phone number with related name from list
- Attackers can try to select active numbers and remove these numbers from their database
- Also, it can be interesting to find phones with names like “Alarm”, “Home”, “Car’, “Datcha”, etc


Phone numbers and passwords
Useful app to control devices

# Direct search

Usually, we know something: address, names, phone numbers

- Bribes are still useful (it is not a suggestion)
- Antennas
- Fake base stations
- Social engineering
- Phishing
- Insecure security agency

# Security companies

- Promotion is important
- Vendors can show information about clients
- Security agencies can show examples of projects
- Some companies show full list of clients

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

# Conclusion

- It is not so hard to find devices
- Several models are totally insecure
- Industrial devices are not widespread, but you can find some
- The security level of mobile operators is questionable

Thank you,
Aleksandr Kolchanov, pyrk1@yandex.ru