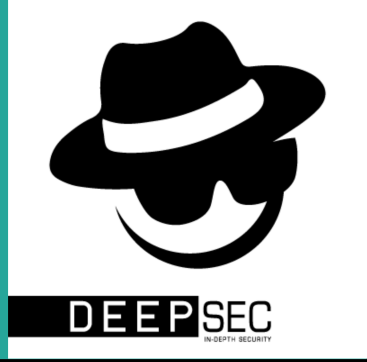



# Attacks on Mobile Operators

—

Aleksandr Kolchanov

# About me

- Now I'm an independent security researcher
- Ex russian bank security researcher
- Ex aircompany security consultant

# Interests

- Mobile operators security
- Banks security
- Uncommon attacks
- Social networks threats

# Mobile operators - keys for everything

# SMS and Calls

- Authorization in messengers
- Password reset
- 2FA authorization
- Any confirmation
- Alerts
- Remote control
- Connection for IoT

# Information and services

- Private messages
- Calls information
- Contacts
- Money balance

# Basic targets

—

# Plan for this talk:

- Networks
- Accounts
- Own services for SMS and Calls
- Abandoned services
- Paid subscriptions
- Call Centers and IVR

# Networks

—

# Why are interesting

Intercept everything
Fake SMS
Block SIM

But:

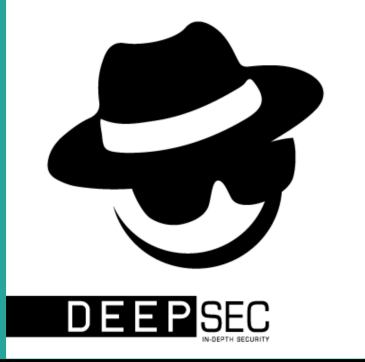
Special devices
Access to

# Typical problems

- SS7 attacks
- GSM
- Encryption
- ...

# Accounts

—



# Why interesting

Activate forwarding
Send SMS
Change tariff
Send money
Block SIM
Activate paid services

# Typical problems

- Classical web vulnerabilities
- Bruteforce
- Wi-Fi tethering

# Classical web vulnerabilities

- CSRF on mobile operator X site allows to send SMS. Victim will pay
- Insecure HTTPS implementation allows to intercept session and gain full access to account. Then hacker can activate forwarding

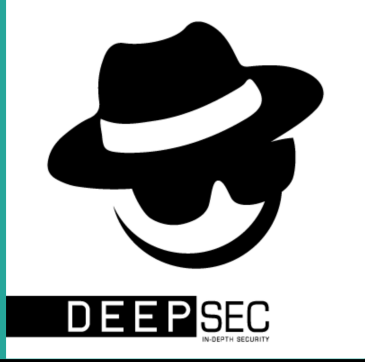
| OWASP Top 10 - 2017 |
| --- |
| A1:2017-Injection |
| A2:2017-Broken Authentication |
| A3:2017-Sensitive Data Exposure |
| A4:2017-XML External Entities (XXE) |
| A5:2017-Broken Access Control |
| A6:2017-Security Misconfiguration |
| A7:2017-Cross-Site Scripting (XSS) |
| A8:2017-Insecure Deserialization |
| A9:2017-Using Components with Known Vulnerabilities |
| A10:2017-Insufficient Logging & Monitoring |

# Bruteforce

- Bruteforce allows to send fake SMS from any mobile number in mobile operator X range
- Bruteforce with captcha bypass allows to gain access to any account of mobile operator Y
- 4 digit codes are mostly insecure

# Attacks on WiFi tethering

—



Some operators allows to sign in without password from their own network

HTTP Header Enrichment

# Methods

- Password 12345678
- Bruteforce
- Classical Wi-Fi hacking
- Just ask

# Abandoned systems and own services for SMS and Calls

—

Classical attacks and bruteforce are effective against abandoned systems

# Interesting things

- Old API
- Rate limits
- Insecure HTTPS implementation
- Fingerprinting

# Call Centers and IVR

—

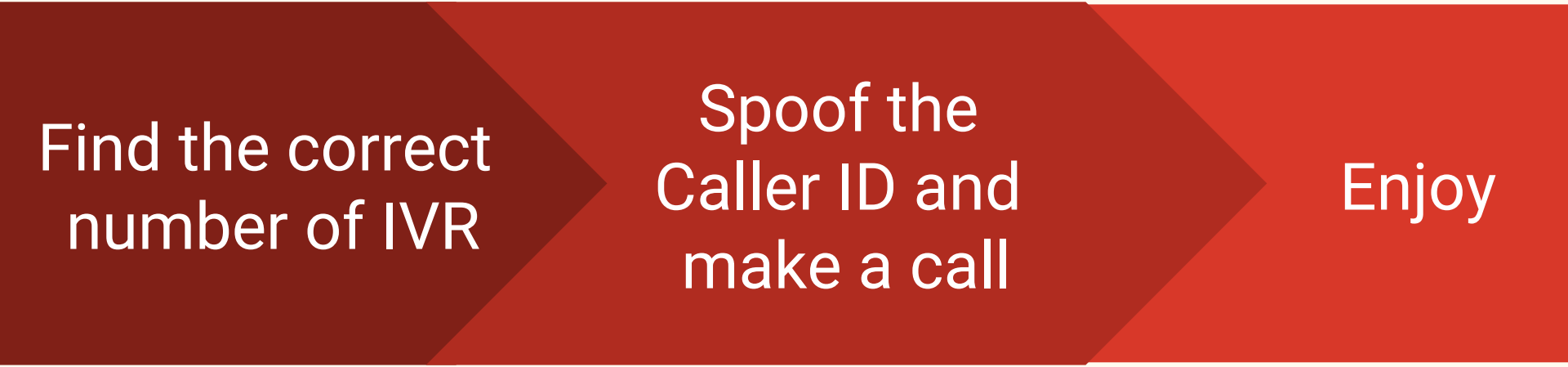
# Information

Balance
Tariff
Offers
Payments
History

# Actions

- Change tariff
- SIM blocking
- Calls forwarding
- Subscriptions
- Paid actions

# Attacks on IVR are so simple




Problems? Yes, they are

# How to make a call with spoofed Caller ID?

Target number
Caller ID

Get access
number
Get code

Call to
access
number

# Problems

Short number
Internal numbers
Protection
Only SMS
Nothing interesting in IVR

# Some solutions

- Try international number
- Use different system for spoofing
- Use forwarding
- ~~Br~~uteforce

# IVR against IoT

Call and block SIM
Change tariff
Spend all money
Call with fake command
Forward calls and messages

# Victims

- IoT devices
- Smart watch for kids
- Security alarms
- Gates
- ...

# Fake SMS from operators sites

How to send SMS online:

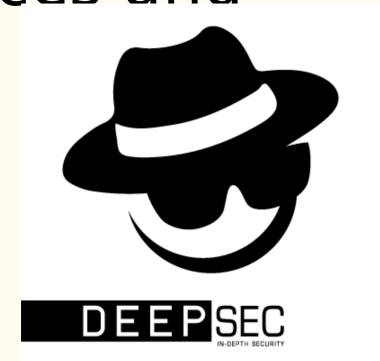
- SMS from personal account
- SMS with confirmation code to be sent

Targets:

- People
- SMS-controlled devices
- Devices for kids
- SMS commands
- SMS banks
- ...

# Results

- Too many mobile operators can be hacked with easy attacks
- Forwarding - is the most interesting feature for hackers
- Most attacks does not require special devices and knowledge
- Sometimes you can just call to hack



# Any questions?

Aleksandr Kolchanov - pyrk1@yandex.ru