CHEATING AT POKER
JAMES BOND STYLE

Elie Bursztein
Celine Bursztein
Jean Michel Picod
This busted up poker in east texas a few years ago. Maybe 5 years ago now. A group of guys got away with it for almost a year before one of them spilled the beans to someone and everyone found out. Poker was everywhere here before that, but the cheating turned all the recreational players off and they won’t play anymore. Really sucked. Some estimate the guys made 70k before they were caught. No one really knows. Dealers and 1 or 2 hosts were in on it. Some hosts had no idea what the dealers were doing. These were 1-2 NLHE games, maybe some 2-5 games. People were already suspicious before it came out. Someone calls an all in preflop with 9-2o vs KK because they knew they’d be best in the end. Something was up. From how I understand the cheating players had an ear piece and it told them, seat 4-1st place, seat 8-2nd, seat 1-3rd and so on. Really a crap move. Ruined the game for everyone.
Electronic voice: Heart 2, Diamond 5
Visible differences

Galaxy Core

Poker cheating device
Security measures

Activation code sent separately
Prevent activation of a “lost” device

ADB / debug mode gone
No “easy” way to get the APK / analyze what is happening

Screenshot shortcut disabled & framebuffer owned by root
Prevent to do screenshot / screencap either via SSH or UI
Fun facts

Custom rom with custom kernel
Chinese 4.2.2 Jelly Bean ROM AOSP

Cheating hardware hidden from the UI/system
No way to trigger the system without the correct application / setup

Backdoor? No need for network or SIM
Lots of phone home code in the APK and lot of weird APK in the phone
App walkthrough
Game hall

- Trio Identical
- Trio Identical [3005]
- Trio Identical [9651]
- Trio Identical [9652]
- French Game with 40 cards in total [9653]
- Bullfight
- Golden Fraud
- Treasure
- Small Nine Pairs
- Big Nine Pairs
- Big Ace
Can buy the game number: 3 Has purchased the game number: 2

1. 7-card Texas Hold’em poker [7003]
2. Read the card directly [1016]
Number of players: 2
Result: H6, D8,
Game type in use: 1016
Feedback device: P4 disconnect
Cards as seen by camera: face down
Fun facts

App(s) not obfuscated
Easy to read as 123 if you know Java :)

Super user password hard coded in string file...
The app has a super user password that allows access on any devices

Most of the interesting features are in a kernel module
Remote devices control and cards recognition handled by a kernel module
Basic principle

How does this thing work anyway?

Underlying principle
B&W camera

IR LEDs

IR passband
plastic housing

Phone

IR illumination
Cards marking

Casino Royale
Marked cards vs regular cards

Device camera view
Card encoding

6H

6C

6D

5D

5H
public static String GetSpeakCardStr(int number) {
    String str = "";
    int type = number / 1000;
    int idx = number % 1000;
    int sType = idx / 100;
    int sidx = idx % 100;
    if (type == m_SpeakNoneType) {
        if (sType >= 1 && sType <= 4) {
            str = (str + GetCardTypeStrEn(sType)) + GetCardNameStr(sidx);
        } else if (sType == 5) {
            str = str + GetCardNameStr(sidx);
        }
        return str;
    } else if (type == m_SpeakCardType) {
        return "" + idx;
    } else {
        if (type == m_SpecialCardType) {
            return str;
        }
        if (IsSpecialSound(number)) {
            return str + GetSpecialSoundText(number);
        }
        if (type >= 1 && type <= 6) {
            str = str + GetCardTypeStrEn(type);
        }
        if (idx >= 0 && idx <= 19) {
            str = str + GetCardNameStr(idx);
        }
        return str;
    }
}
Feedback devices
Intercepting radio-command

Center frequency: 868.289 MHz
Data rate: 2400bps
Measured $\Delta f = 19$kHz

2-FSK modulation
“Mini vibrators”

Bluetooth P4 receiver
Sneaky time display
Wireless camera
Transmission module VM152T

传输频道频率（transmission frequency group）：
CH1: 2370MHz CH2: 2470MHz

1.3 调制类型（Modulation type）：FM

2 结构规格书（Mechanical Specification）

VM152T Please refer to Figure 1.

3 环境条件（Environmental Specification）
3.1 工作温度（Temperature）：-10°C ~ 60°C

4 测试条件（Test Condition）
4.1 周边环境温度（Ambient temperature）：25°C
4.2 视频输入电压（Video input voltage）：1.0Vp-p, 150 (IRE)

电源电压（Supply Voltage）：3.3V, 5.5V DC

2 电流(Current Consumption)：95 105 mA

5.2 视频特性（Video Characteristics）
1 输入阻抗（Input Impedance）：75 Ω
2 峰值频偏（Peak Deviation）：1.2 MHz

载波源(MOD):
正弦波(sine wave)
400KHz 1Vp-p

5.4 RF输出特性（Output Characteristic）
1 发射功率(Tx Power)：18 17 18 dBm

CH1：2370GHz 0 1
CH2：2460GHz 1 0
CH3：2570GHz 1 1
CH4：2670GHz 0 0

体积：15*8.3
Transmission analysis

metadata?

image
Transmission analysis
Open questions

Who created such device? Casinos?
Level of sophistication means either stolen tech or large underground market

Who is ripping who?
Where is this thing actively used? Need detection means and field study!

Where is the ink is coming from?
You can't buy it easily - only for secure marking of docs
James Bond devices exist!
They are hard to find but reality match fiction

Crimeware can be super sophisticated
While NSA have cool tools, the crime mob does too!

A very diverse skillset is required to tackle this type of device infiltration, hardware analysis, software analysis, RF analysis, Vision Alg.
Co-conspirators

**Pixel:** Hardware specialist

**Vivi:** Chinese blackmarket infiltration expert
Thanks!