SMS parking ticket hacking

Pavol Lupták, Lead IT security consultant

$whoami

- Pavol Lupták
- Active in many different organizations (Slovak hackerspace Progressbar, SOIT, Slovak OWASP chapter, Nethemba IT security company, ...)
- Proposed and published the **SMS public transport ticket hacking** paper in 2008 (and had the presentation about it at HAR2009)

Abstract

- We have revealed **critical vulnerabilities in Slovak Mobile Parking (all big Slovak cities including Bratislava) are vulnerable**
- We are able to **force any registered Mobile Parking user to pay for parking of an arbitrary car**
- We are able to **dump mobile numbers of all registered users in Mobile Parking**

How does Mobile Parking work?

- **Registered users** – they need to register to the Mobile parking system with their mobile number and car plate number, after the registration they need to charge their credit (and transfer their money to their Mobile Parking account) – **billing is done by the Mobile parking company**
- **Unregistered users – billing is done by the mobile operator** – no registration is necessary

Syntax of SMS parking request

- **ParkingTime_CarPlateNumber**
- Parking Time – in hours (Bratislava) or in minutes (Vienna)
- Car Plate number – you can pay for parking of an arbitrary car (not only yours!)

- The SMS message is sent to the specific number, e.g +421902020202

Payments for Mobile Parking

- **The payer of the Mobile parking is identified according to the SMS sender of the SMS parking request!**
- And of course it can be easily spoofed!
- We use the SMS spoofing service http://www.armsms.com - 1 SMS costs 0.17 €
- And yes, the attacker can be completely anonymous and use TOR and Bitcoin payments using https://smsz.net

How to force the existing registered users to pay for the parking without their notice

- OK, we are able to send any SMS parking ticket with an arbitrary spoofed sender number
- But, if we want to park for free, **we need to send it from the sender number that is already registered in the Mobile Parking system**
- How it is possible to reveal existing registered numbers?

Using registration forms to dump all mobile numbers

- Slovak M-Parking system www.m-parking.sk and Austrian M-Parking system www.handyparken.at are vulnerable to the trivial enumeration attacks!
- During the registration process the Mobile Parking system informs you if the given mobile number exists or not → this behavior can be exploited to dump all mobile numbers of all Mobile parking registered users!!!

Mobile Parking anarchy

- The victim receives the SMS notification that he pays for parking of XYZ car plate
- The owner of XYZ car doesn't need to know necessarily anything about the victim and the attacker
- The attacker can be still anonymous and cause a maximum chaos because it will be difficult to distinguish between justified and unjustified complaints
- This chaos can be used for a mobile parking anarchy and parking for free :-) (or shutting down the Mobile Parking service very soon :-(

CAPTCHA protection I.

- Registration form of www.m-parking.sk is protected against enumeration attacks by CAPTCHA
- We were able to crack 100% of all CAPTCHAs using commercial CAPTCHA cracking services http://decaptcher.com and http://www.deathbycaptcha.com, 1000 CAPTCHAs cost 0.97 €, cracking one mobile subnet (0905XXXXXX) cost 978 €
- If the open-source CAPTCHA cracking is used, this can be done completely for free!

CAPTCHA protection II.

- Registration form of www.handyparken.at DOES NOT USE CAPTCHA at all!
- All mobile numbers of all registered users can be dumped just in few hours / days!

Proposed solution I: SMS center verification

- The Mobile Parking system SHOULD VERIFY if the number of SMS center of the SMS request has the given country prefix (Slovakia +421*, Austria, +43*) - if not, the SMS parking request should be throw away
- **Advantages:** probably very efficient solution, because SMS spoofing services are prohibited in Slovakia / Austria
- **Disadvantages:** you can not pay for parking your car in Slovakia, when you are outside of Slovakia

Proposed solution II: Shortened numbers

- Disallow using the international number (e.g. +42190202020202) for the Mobile parking that can be easily reached from the SMS spoofing service
- In case of the shortened numbers, spoofing will be much more complicated, because the SMS spoofing service has to exist in the given country

Proposed solution III: Protect against enumeration attacks

- If the user put his mobile number to the registration form, a random authentication token is sent to his number
- He enters this authentication token to the second form and if it is valid, he is successfully registered to the system
- If anyone with this number is registered to the system – he receives the SMS message with text "*This mobile number has been already used. Please ask for your forgotten credentials*".
- No CAPTCHA is used at all
- Be aware of SMS DDoS attacks (use SMS rate limiting per IP address)

I would be happy to answer to all your questions!

Thanks for your attention!