absorptions

random hacks & assorted infodumps

May 4, 2013

A determined 'hacker' decrypts RDS-TMC

As told in a previous post, I like to watch the RDS-TMC traffic messages every now and then, just for fun. Even though I've never had a car. Actually I haven't done it for years now, but thought I'd share with you the joy of solving the enigma.[disclaimer 1]

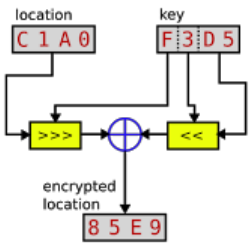
RDS-TMC is used in car navigators to inform the driver about traffic jams, roadworks and urgent stuff like that. It's being broadcast on a subcarrier of a public radio FM transmission. It's encrypted in many countries, including mine, so that it could be monetized by selling the encryption keys.

A draft of the encryption standard, namely ISO/DIS 14819-6, is freely available online. Here's an excerpt[disclaimer 2] that reads blatantly like a challenge:

> ability for terminals to be activated to receive an encrypted service on an individual basis.
>
> After calling for candidate proposals, the submission from Deutsche Telekom was judged by an expert panel to have best met the pre-determined criteria the task force had established. The method encrypts the sixteen bits that form the Location element in each RDS-TMC message to render the message virtually useless without decryption. The encryption is only 'light' but was adjudged to be adequate to deter other than the most determined 'hacker'. More secure systems were rejected because of the RDS capacity overhead that was required.
>
> After ratification by the TMC Forum Business Group and Management Group of the decision to adopt the

TMC messages consist mostly of references to a static database of preset sentences and locations. The database is not a secret and is freely available. The location information is encrypted with a key that changes daily. Every night, a random key is picked from 31 pregenerated alternatives. The key is never transferred over the air, only its numeric ID (1-31). The keys are preprogrammed into all licensed TMC receivers, and they can decrypt the locations knowing the key ID.

The size of the key space is 2^16 and the encryption algorithm consists of three permutation operations:



The algorithm is simple enough to be run using pen-and-paper hardware, and that's just what I did while creating the above crypto diagram:

The tricky part is that I don't know the keys. But there's a catch. To save bandwidth, only regional messages are transmitted. This limits the space of possible locations, giving us a lot of information about the encrypted data. Assuming all messages are from this limited region, we can limit the number of keys to a very small number, in the dozens.

The next day, we have an all new encryption key again. But there's another catch. Many messages persist over several days, if not weeks. These would be messages about long-lasting roadworks and such. We just need to wait for messages that we heard yesterday that only have their location code changed, and we can continue limiting the keyspace by collecting more data.

About the Author

Oona Räisänen

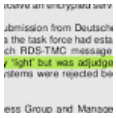
Self-taught signals & electronics geek from Finland.

View my complete profile

Popular Posts

The sound of the dialup, pictured

If you ever connected to the Internet before the 2000s, you probably remember that it made a peculiar sound. But despite becoming so familia...

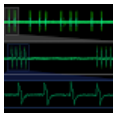


A determined 'hacker' decrypts RDS-TMC

As told in a previous post , I like to watch the RDS-TMC traffic messages every now and then, just for fun. Even though I've never had a...

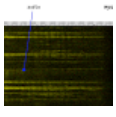
Eavesdropping on a wireless keyboard

Some time ago, I needed to find a new wireless keyboard. With the level of digital paranoia that I have, my main priority was security. But ...



The GSM buzz

You probably recognize the loud buzz a ringing mobile phone often causes in nearby speakers. But where does it come from? Let's dissect ...



How I discovered RDS

One stormy night in 2007, I was listening to local FM stations while viewing a live spectrogram of the audio on the computer, through the ra...

How I made my Ubuntu usable again

Many fellow Ubuntu users have been protesting the recent developments in user interface design, call it Unity/Gnome 3/whatever. But what can...

Subscribe To

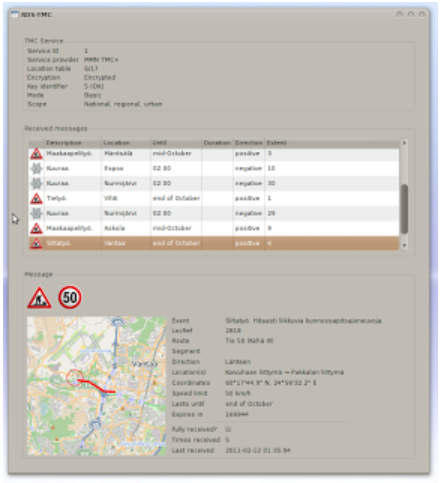
Posts

Comments

Once we've limited the keyspace to a single key, we can decrypt all of today's messages. When the key changes again, it is trivial to find today's key by knowing yesterday's key and comparing the locations of persistent messages; this is known as a known-plaintext attack or KPA.

Here's some encrypted data straight from the radio.

A little Perl script then decodes everything and even plots the affected segment on a little map. The screenshot is from a few years back.



Now I just need a car. Well, actually I prefer motorcycles. But I guess it would work, too.

Tools used: Ordinary FM radio, sound card, computer. All data is from public sources. RDS was decoded from intermodulation distortion in the radio's Line Out audio caused by the stereo demuxer circuitry.

Disclaimer 1: I will take this post down on the first appearance of any complaint from any party, of course. My intent is not malicious and I'm not even publishing any keys or code.

Disclaimer 2: This use of the above excerpt of the ISO standard is not an infringement of copyright as it is being used here under the doctrine of "Fair Use" of the United States Copyright Law (17 U.S.C. § 107), seeing as this blog is hosted on US soil.

Posted by Oona Räisänen at 19:36

+11 Recommend this on Google

Labels: bad stuff, infodump, RDS

47 comments:

Barry Kelly 05 May, 2013 02:27

That is some very fine work!

Reply

Anonymous 05 May, 2013 02:36

Love it! This would be a great project for engineering students.

Reply

Anonymous 05 May, 2013 03:34

Bad ass dude.

Reply

Replies

Oona Räisänen 05 May, 2013 08:23

I'm not a dude.

Anonymous 05 May, 2013 10:49

Still, take it as a compliment :)

Anonymous 05 May, 2013 12:58

Bad ass chick! :)

Anonymous 05 May, 2013 20:19

Where I come from, "dude" doesn't necessarily mean "male". "Ungrateful bitch" does generally mean "female" though.

Eduardo A. Bustamante López 06 May, 2013 00:32

Anonymous, it seems like your naming system is flawed, because the "Ungrateful bitch" tag applies just perfectly to you. Also, the correct term would be dudette, which clearly expresses that the subject is a female.

To Oona, what a wonderful piece of work. Do you have any recommendations on reference material for this area? Also, recommendations on signals in general are appreciated :)

Anonymous 06 May, 2013 00:46

^Fuck off, Anon.

Oona Räisänen 06 May, 2013 07:26

I've studied cryptanalysis from books but also through a lot of practice. :) As for signals, The Scientist and Engineer's Guide to Digital Signal Processing is a good start. RDS and TMC internals are well described in the standards and they're often a fascinating read.

Reply

Anonymous 05 May, 2013 04:50

Can you put this up on github?

Reply

Replies

Oona Räisänen 05 May, 2013 08:23

No, see Disclaimer 1 :)

Anonymous 05 May, 2013 19:17

Put anonymously? Information wants to be free

Oona Räisänen 05 May, 2013 19:28

There's no way I can anonymously publish the code any more, ever. Also, there is no "proof of concept" that's all in code and ready to be executed. The process involved, for example, handwritten notes about persistent messages and recovered keys. But it should be very simple to implement based on this post. Anyone can do it, I believe.

hack2root 06 May, 2013 09:56

Respect your efforts, hope we can get working online RDS decriptor with usage of simple LCD on Arduino or raspberr

Oona Räisänen 06 May, 2013 09:58

I've done it already.

Reply

Adam Baxter 05 May, 2013 05:28

To find my local RDS-TMC frequency, what am I looking for?

As far as I know, Australia doesn't use RDS for anything other than an encrypted TMC broadcast provided by http://www.intelematics.com.au/products-services/motoring-content/traffic-services/suna-rds-tmc

Reply

Replies

Oona Räisänen 05 May, 2013 19:57

You can scan through the stations, decode the RDS and find a frequency that has TMC in its application list.

Reply

Anonymous 05 May, 2013 08:36

Nice one! You might enjoy reading Bamford's Puzzle Palace if you haven't already.

Reply

Replies

Oona Räisänen 05 May, 2013 10:21

Thank you! It looks very fascinating indeed!

Oona Räisänen 05 May, 2013 20:39

Amazon'd

Reply

Anonymous 05 May, 2013 11:15

so, are you coming to defcon somday soon?

Reply

Replies

Oona Räisänen 05 May, 2013 11:39

I was invited to 44CON to talk about something else, and I'm still kind of pondering whether I can write a talk that long. But who knows.

Anonymous 05 May, 2013 12:26

I know they do workshops at 44CON. What if you offered to do a shorter talk and a workshop?

Oona Räisänen 05 May, 2013 19:29

That kind of sounds doable.

Reply

Anonymous 05 May, 2013 11:19

Very impressive!

Reply

Anonymous 05 May, 2013 12:13

I love it :D

The thrill of solving these kinds of things is one of the main parts why I love my field of work.

Thanks for writing it down so we can take part.

Reply

Replies

Oona Räisänen 05 May, 2013 12:14

Do share your field of work! For me, it's just a hobby.

Reply

John Jones 05 May, 2013 18:11

This reminds me of the type of code breaking they did at Bletchley Park during the Second World War. At Bletchley they had to guess the messages but particularly loved the weather forecast because once they cracked that they had the days cipher (there where lots of differences but you get the general similarity between weather and roadworks). I find it particularly amusing you used PERL which is perfect for this and whose origins are also in security field. I only ever saw this system working in Germany. Great work deciphering and documenting it.
Regards
John Jones

Reply

Loic 05 May, 2013 20:11

Huge ! Now it is possible to fuzz RDS data and find bugs within GPS or car radios !
Could be nice/evil to get remote code execution on cars as I assume GPS and other equipments using RDS are connected to other sensitives parts of the car, and the security isolation must be pretty low...

Reply

Replies

Sean Harlow 06 May, 2013 01:15

"I assume GPS and other equipments using RDS are connected to other sensitives parts of the car, and the security isolation must be pretty low..."

You'd be assuming wrong, in general. I won't say it doesn't happen at all, but I am very knowledgeable about the BMW systems from the late '90s on up (IBus and beyond, seen in parts on the E36 but fully utilized in E38/E39/E46) and can say that there the passenger-facing systems are on one data bus while the important systems like the engine, transmission, gauge cluster, etc. are on others. If you somehow got code execution on the radio in my E46 the most you'd have access to is the door locks. Sure, not the best, but if the radio is on the key's already in it, so if I'm not also in it the car is unlocked and running, so it's a moot point.

From what I've seen when messing with other modern vehicles (VW, Kia, Ford) it's pretty similar across the board. Some parts are on both buses and will proxy specific requests, but they're things like queries for information or selection of performance / economy modes.

Also, these are a few small, fixed length messages. Not impossible to screw up, but less likely to be exploitable than a variable length freeform text field, such as the RDS RT field, which is entirely unencrypted and publicly documented. That is to say if you want to fuzz RDS, this doesn't really add much of use, the interesting bits were already out there.

A more "interesting" use of figuring out the keys, aside from accessing a subscription service for free of course, is for pirate broadcasters to add their own traffic events to the system. Obviously that's a fast way to get your local radio authorities interested in your operations though, so experimenting with such in to anything but a dummy load is probably not a good idea.

Eric 06 May, 2013 01:15

That makes about as much sense as people saying they can hijack your locks to make the car accelerate since the locks lock automatically when you actually

accelerate the car. Cause -> Effect does not always go backward.

Svante 06 May, 2013 22:55

That would be close to what is described in *Comprehensive Experimental Analyses of Automotive Attack Surfaces* from http://www.autosec.org/publications.html, which is an interesting read.

The level of protection between critical and non-critical buses apparently was not high enough for their target vehicle(s), as they write that "Consequently, the result is that compromising any ECU with access to some CAN bus on our vehicle (e.g., the media player) is sufficient to compromise the entire vehicle."

Reply

Anonymous 05 May, 2013 23:04

Did you use some kind of third party lib to get Perl to plot on a map or is it just a image with scaled coordinates?

Reply

Replies

Oona Räisänen 06 May, 2013 07:22

Just an image that I know the corner coordinates of, and that I can then draw on using PerlMagick and crop to fit.

Reply

Julius Friedman 06 May, 2013 03:59

Flawlessly elegant! Kudos!

Reply

kdc 06 May, 2013 06:00

Nice work!

Reply

Kristofer Jarl 06 May, 2013 09:34

Ciao Feds? Hah! Intentional, I guess? :)
Great work!

Reply

Replies

Oona Räisänen 06 May, 2013 09:37

You're the first one to notice :D

Reply

Leszek Jakubowski 06 May, 2013 17:03

Where did you find the locator databases? I guess they have to be maintained so they're not in the standard (or are they?).

Reply

Unknown 06 May, 2013 17:15

What do the yellow boxes with >>> and << in the diagram mean?
I'm trying to understand what you did on the piece of paper, but can't figure out where the two middle lines used for "xoring" came from.

Reply

Replies

Oona Räisänen 06 May, 2013 17:29

Bitwise rotate right, bitwise shift left

Unknown 06 May, 2013 21:02

Kiitos! :)

Reply

Tuomo Eloranta 06 May, 2013 17:16

Sad to request, but can you take thisoffline. It is kind of our service you hacked :)

Tuomo Eloranta,
Technology Director
Mediamobile Nordic

Reply

Replies

Oona Räisänen 06 May, 2013 19:08

"Kind of"? Sure, if that's what you deem appropriate.

Please send me a cryptographically signed email (windyoona@gmail.com) with the complaint, i.e. some explanation as to how I'm infringing your IP rights, and which parts of the post are infringing and should be removed. I will replace them with [deleted as requested by Mediamobile Nordic].

Also, please provide me with a means of verifying the signature and sender, preferably a public key at a URL under your company domain.

Reply

Gus 06 May, 2013 19:16

Please ignore Eloranta's request. His company sells this service. He does not provide sufficient justification for censorship.

Reply

Replies

Mikko Rauhala 06 May, 2013 19:43

Well, he might have a legal angle anyways, so heeding a complaint is an understandably prudent thing to do. But indeed it is also wise to ask for specifics, and to ascertain that he's actually representing the company (after all, one wouldn't want to aid some pretender in smearing the company name).

I'm guessing this post is getting a fair number of persistent copies made at this time.

Reply

Enter your comment...

Comment as: Google Account

Publish Preview

Links to this post

Create a Link

Home Older Post

Subscribe to: Post Comments (Atom)