Project Log

14/6/2015

Look at GSM-R—standard of protocol on ERTMS site

* Formal modelling
* ‘what’s in the spec/what’s not
* All the different protocols built together-is there something that’s weak?

->Complete GSM-R focus

->Everything I can find

Next meeting Thurs 3pm

17/6/2015

GSM-R

* Product of 2 projects-MORANE and EIRENE
* Slightly antiquated standard-does not use IP-uses its own way to construct messages-reminiscent of OSS
* -> Rail Engineer issue 48 has a comprehensive description of system (October 2008)
* Train must have constant connection to the network

->requirements for ERTMS as a circuit-switched network

->Relies on TDM (time division multiplexing) at present-> not IP compatible

Core Construct

GSM-R

| ER--------------KMS

| |

| RBC ------------/

TRAIN

18/6/2015

Joeri sent some really useful documents -> need to read

Worth preparing an attack tree for GSM-R

-> Might help visualise it

Meeting with Tom, Joeri and Mark Ryan

GRM-R in Proverif

-> concerning with integrity, authentication, and other vectors e.g. relaying/ replaying

-> What level of trust is there in GSM-R? Also-how reliant is GSM-R data in the scheme of things=very?

How are trains handled-> 7 regional centres with proper handover

-> is this a possible problem with GSM-R?

22/6/2015

Further research: interests are in EURORADIO

Managed to locate CENELEC standard for BSI EN 50159 (2010 version)

* Finished reading up standards, drew attack tree and topology for GSM-R
* Reading through EN 50159 (drafts in 2006)
* Read up KPMG report (not much other than background reading due to the redactions)
* Started to read through Unisig documents Joeri suggested-EN standard is good read and others are very descriptive
* Diagrammed key management to visualise, and we might have some luck here

23/6/2015

Read over ‘Boundaries between ETCS and the GSM network on Bane.dk

->3.1 has a nicer version of my diagram

-> Shows GSM-R is only for connecting a train into their wide area network

Reading some UIC documents, they’re keen to move to an IP stack via GPRS-pipe only used when data is being sent -> currently, it’s a constant connection, so is it possible for long term keys to be found more easily?

Finished reading EORORADIO FIS and have drawn the protocol runthrough for a new connection

->FFFIS has no further info

->Read the KMS one and have some thoughts

->Read through the rest of EN 50159

-> There’s a document in subset 074 which talks about startup FFFIS tests

To do: Read more about the ETCS entity document (find out which document it is) ->still good

Read Euroradios test cases

Read EIRENE specification to see if it says anything

There’s also documentation for SIM cards FFFIS

Also look at scanned links to see if there is anything interesting : probably is something

->Subset 092 (test cases)

->P0028D004 (Eirene)

->P38T9001 (SIM card stuff)

->Subset 098-RBC-RBC Comms interface

->Index 079 9KMS-ETCS offline KMFIS)

->Subset 039 (FIS for handover)

24/6/2015

Spoke to Ian about project-he has some ERTMS stuff from Modern rail Engineer which he will dig out

->Also offered help with Proverif if needed

-> OSI is a mess->use of GSM-R is likely an old soft decision ratified at a later date

Finished reading the Test cases and KMS document

->Test cases have some ‘supplier-tested’ sections eg. timeouts Or when specific options are used.

->Read the SIM and FFFIS-there’s some stuff there but is not entirely clear how an entity gets its TRANS key-possibly baked into SIM card

Read through some more documents on EURORADIO

->Boundaries between ETCS and GSM-R (bane.dk)

->Susceptibility of GSMR-R to Railway Electro magnetic….

->Kapsch Whitepapers on ERTMS

->ERTMS-an overview: it’s from Iraqian Journal

->GSM-R traffic model for radio-based GPS

->GSM-R in support of EC Mandate-Technical Report by ETSI

Good site: railway- cables.com->has a good description of ERTMS

Read remaining documents/EIRENE and handover. (as well as GRASS PowerPoint and GSM-R interface requirements

To do: collect thoughts on possible areas to look at

-probably the connection one

-mast preference

-key management

25/6/2015

RBC to RBC handover document is not suitable for GSM-R research: it will be for ERTMS/ETCS-> review more than anything

EIRENE SRS specs are more compliance requirements e.g. Features that are mandatory/ mandatory for interoperability (MI)

->Discuss coverage requirements (3.2)

->Handover needs to be 99.5% successful under load (3.31)

->FIG 5.3 has some nice linked systems are not standardised by EIRENE (but use it)

->11.5.5 has the tags and information element format

->not much else->more manufacturer specifications for compliance-EIRENE FRS is similar: 10.6 has an access matrix which shows who can do what over the EIRENE network

Read GRASS by Senesi et al

->interesting –one handover (GSM-R) every 48 seconds at 300km/h (180mph)

->With GSM-R, Euroradio part encrypted/CBC-MACd and then GSM encryption wrapper around that (A5/x)

GSM-R Class 1 Interface requirements

->from request to connection is 10s. at most

->Some good statistics and examples for error recovery

GSM-R Industry Groups-Capacity Enhancement

->19 frequency channels-very restrictive for circuit-switched network as each train requires a dedicated ‘always on’ connection

->they are proposing changing technologies-CPRS, CSD-it’s better for the network

->issue is EURORADIO to IP/E.164 to IP

->this is the problem EURORADIO is a service, not an application-moving to IP means everything needs to move into the network layer

->ERTMS Solutions.com – formal spec Open source software to formally model ERTMS requirements

->github.com/openetcs or openrbc

Active threats to GSM-R

->DDOS of the network. KMS has the validation keys of DDOSing. The frequencies would mean GSM-R fails, as you don’t have ‘areas’ of masts

->Key management-‘do what is right’

->There is no defined spec to say how keys should be moved (other than encrypted between KMCs

-> Connection-packet isn’t encrypted->only the MAC is-72.2 of FIS goes through the MAC process and procedure. ½ goes through the actual MAC creation->they achieve 8 bytes of MAC through CBC-MAC which uses XOR-see Annex E

->open ETCS has EURORADIO code-need to look through models

Meeting with Tom 25/6/2015

What is trust based on

->Connection to the key DB

->What is KMC to RBC protocol?

->Check protocol->what is Ks

->Kab?

->Is there a mapping from IDs to keys?

Look at formally modelling this

->Proverif-easy but we need to come up with extend it-avoid it

Who knows what key and where does it come from

Personalise notes and establish the key protocol

->What keys are in use? Where do they come from?

->Do we have a trusted 3rd party?

->What protocol drives KMC-RBC

->Check protocol for ks and have data first is transferred->does the mast have a key?

KPMG says KSMAC session key is derived from authentication KMAC. KSMAC is not managed by KMS

->Re read KPMG report

->KMC does not speak to train (fig 11)

->KPMG report probably way to go

Also look at RSG GERT 8403 ISS 1 (pdf)-this talks about RBCs

29/6/2015

Submitted Ethics self-assessment form

KPMG IT security document re read: hints connection is actually between train and RBC but RSG GE/RT 8403 (ERTMS Key Management) hints it’s between train and lineside kit

Updated Key Management diagram >diagrammed system layout

>>>>Review SUBSET014, 038, 037, 026, 047 (refers to 037 anyway)

Read ‘Key Management System in ETCS’ by Franekova

->points out the real entity open for vulnerabilities is the KMC and Key Management as a hard problem

-> Each key has a unique ID. RBC have validity set to max period

->Confirms Subset 026 and KPMG report. So base masts are not part of it! RSG defines an ERTMS Entity as OBU, RBC or the RADIO infill units

->My understanding is that the vehicle and entities all can speak to each other via GSM-R but GSM still provides transmission so we are still reliant on its structure

Read ERTMS National Identities Management (GERT072)

-> They use ‘ERTMS entities differently to say GSM-R is an entity

->Network Rail assigns the entities-engine appears to be one of them

KMAC-you’ll need to get this from KMC. It is trusted 3rd party. You get the key you are connecting to?

->You derive KSMAC from KMAC so KMC creates one for you to connect to RBC

KSMAC derived according to 7.2.3.2.4.14. The way I’m reading it from Subset 087/089

“When an OBU wishes to establish safe communications with a trackside entity the requested keying material has to be exchanged and distributed”

“The OBU KMACS may be installed in trackside”

->Wikipedia shows each train has a unique number e.g.823003

High priority data is sent without a MAC!

Direction flag is used to protect against ‘reflection attacks’

Drew up plan for Proverif model and re did protocol run through

Key validity is a problem-coded YY not YYYY (Subset 14)

30/6/2015

Looking at how to add this protocol in Proverif

Continued re reading subset 037 and subset 038

Read all the chapters in Subset 026 (systems Requirements spec)

->a lot of references to subset 037

So far: communication is in the clear-it’s text then MAC. WE know that from listening to the transmissions what Ra and Rb are. We just need KMAC and we derive it. KMAC in flight however is encrypt AND MAC not MAC then encrypt or encrypt then MAC

2 separate keys-how are these established. Must be some master key to start off with?

Chapter 8 has the actual rules for messages

Who generates keys/who can etc

Better idea is you have Train key and whenever you want that connection, you ask KMC. This is a lot cheaper

Train ID used to identify it-is there a wire to RBC

Reconnect an online option. It’s faster, cheaper and safer

Look at update protocol and mapping in Proverif and assume we have Kab1,Kab2,…,Kabn in the model

Working on Proverif model – meet after security seminar

1/7/2015

KMAC is confusing-is it only the train and the RBC pulls it from the KMC?

->something is going on->this makes it look a lot worse->anyone with procession of that key can derive Ks as the randoms are in plain text. THIS IS REALLY BAD!!!!

Meeting with Tom and Joeri

What is the key gen algorithm the KMC uses

Use Proverif to check if session key is secret->lots of

Can we replay messages?

->How much known plaintext do we need

Check from site for maps

Maybe if it sends multiple ‘okay’ messages

Attack 2: priority flag and no MAC: What are allowed messages?

Tear a session as a whole

What happens after AR is sent by the RBC? What data is sent?

What do we need to do to break A5/1 cipher in GSM?

We are interested in replaying messages from the protocol -- is this allowed by it?

Italians use CRC-different flag, but all other values are ‘reserved’

-> CRC has no protection-where does trust model come from then?

MAC always consists of length II destination address II

Message II padding

Code at MAC algorithm 3and ISO standard

Event of non-fixed data

->do session key differently

Check syntax against Tom’s

Events good to see if you can get to the end