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 50549 (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. ?K

->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 ????????? 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 ????????????? to see if there is anything interesting : probably is something

->Subset 092 (test cases)

->P0028D004 (Eirene)

->P38T9001 or 7 (SIM card stuff)

->Subset 098-RBC-??BC Comms interface

->Index 079 9KMS-E?CS offline KMFIS)

->Subset 039 (FIS for hand????)

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

-> OST DST 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.?????? 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.?k)

->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 ????-based ???????

->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 ????systems are not standardised by EIRENE (but use it)

->11.5.5 has the ???? 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 ???????????and then GSM encryption wrapper around that (A??x)

GSM-R Class 1 Interface requirements

->from request to connection is IOS. at most

->Some good statistics and examples for error recovery

GSM-R Industry Groups-Capacity Enhancement

->19 frequency channels-very restrictive for circuit-switched ???? 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 ???????

->ERTMS Solutions.com-???? Open source software to formally model ERTMS requirements

->????.com/open etcs or open rbc

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 ?OR-see Annex E

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

Meeting with Tom no date

What is trust based on

->Connection to the key DB

->What is KMC to RBC protocol?

->Check protocol->what is Ks

->?????????????

->Is there a mapping from ???? 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 ???? 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 ????? kit

Updated Key Management diagram >diagrammed system layout

>>>>Review ?????14, 038, 037, 026, 047 (refers to ??? anyway)

Read ‘Key Management System in ETCS’ by ???Franeleova

->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 ? 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 (?????)

-> 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 ???? wishes to establish safe communications with a trackside entity the requested ??? material has to be exchanged and distributed”

“The OBU KMACS may be installed in trackside”

->Wikipedia shows each rain 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 ?? and ?? are. We just need KMAC and we derive it. KMAC in flight however is encrypt ??? 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

???? 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 ????? the model

Working on Proverif model

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 ???? ??? 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?

???? ??? a session as a whole

What happens after ??? ???What data is sent?

What do we need to do to break A5 ???? ?? ????

We are interested in replaying messages from the ???? 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 ??? can get to the end

No date

Meeting with Sam, Tom and Joeri

Ask Chris green for LM picture of engineer with laptop

Medium for transporting these keys

->how are keys distributed

High priority calls-where is the trust

->time stamps in message->where are these in the MAC?

Key Question GSM-R

What comes next in the protocol after connection set up

->How are train keys set up in the first place?

->What are application commands sent after connection set up- timestamps and opportunity to repay

How does the high priority override work?

How does the safety feature work?

-> CBC-MAC or CRC – variable value

Eurobalises

What damage can changing/adding our own balise do?

Can we make trains go faster? Is there a check at the RBC?

Can we report a train in the wrong location? What happens?

1. Any odd safety checks?

2. If so- what do the two scenarios look like?

Check Porterbrook 323 report with GPS antenna

Can we stop a train and remove preceding balises?

->Where axle counters come in

Anything about CAN-buses on trains?

2/7/2015

Requested photo from Chris

E-mailed meeting notes to everyone

Work continuing on Proverif model

Discussed with Tom inspection presentation

->We’ll focus on GSM-R for now

->Tell a story

->Get Proverif working

->Next stages would be looking at what happens before the connection and what happens after it-what messages?

->Show the questions we want to all the rail people and show how it relates into future work

Proverif model complete now-tested successfully

6/7/2015

Project inspection with Dan Ghica

->Very nice-impressive

->Proverif code counts towards the implementation part of the project-mention how I built the model and how I learnt to use Proverif

->If the model is ok, it would be worth looking at real life implantation, as they vary and might have some bug in them

7/7/2015

Focus now on the key management side

->Key operations/processes and management

->Review the KMS FIS and RSG/RSSB documentation

RSG GE/RT 8403 ‘ERTMS key management’

->A bit of contradiction e.g. when two nonces match -- protocol does not say this!

->Review HS/CR CCS TSI. There are a set of requirements listed in 1.2.2.2

->The model gets very nasty with all the operations e.g. update far better to be dynamic? Online KMS

->But what if a train has to be directed e.g. West coast on to East coast for part of its journey with little advance warning. Again a call for online KMS

Balises receive ‘3 copies of the telegram’ at 500km/h

ERTMS allows staff to be responsible for movement if RBC cannot establish position (RAIB report 2011). What Tom wants is ‘on sight’ which allows you to move into a block occupied by another train

Subsets to review: 037/038/091

Read RSSB’s GE/GN 8603 (Guidance for GE/RT 8405

->There are a few gaps that need to be addressed

Meeting with Tom

Good work on Proverif model-make fixes to the typos and look at how names are bound->may be able to define train ETCS id into the train process, but how do we get it to the RBC?

Look at the train model we have

Future reading Subset 058 App. Layer – Reread SIM FIS

8/7/2015

Finished working on Proverif model-query with Tom about the name bounding for RBC visibility

Confirmed that the protocols do establish trust in each entity but not that one key generation must give the generation of another, as the nonces could be broken

Side research-there is a Doppler radar on each unit for reading speeds accurately

From RSG (RSSB-ERTMS-OC-Dec 2014) page 119 ‘management of keys-no staff interaction is required’-remote management can take place

->Backup system must be provided

Chatted with Tom

->nice for full run of protocol e.g. start, middle and end tested

->How do RBC’s do the handover?-do they give keys over or is the session torn down?

->Is it possible to replay messages?

->Look at having an event on the MAC themselves as they might be able to be replayed

Franekova has CBC-MAC wrong

Started to write up key management notes

Need to start looking at the app layer-what comes immediately after connecting?

Reviewed Franekova crypto paper-appears to be single DES up to the last block Why? Is this a performance hack?

Spoke to Tom-appears to be a performance hack

->This modified CBC-MAC uses DES using K, up to the last one

->It is vulnerable to a length extension attack.

Show Tom an updated Proverif model tomorrow

9/7/2015

Still reading FIS for EURORADIO keys and key management specs

Some background research-‘Secure your MACs’ and presentation from Westinghouse

->CrossRail will be ERTMS L3

->FT report about CrossRailand Thames link

->We’re involved with Nomad - people who may behind a CAN bus (nomandtech.pt) – Met & Mat might apparently were involved with them?

From Subset 037, all the header of a data SaPDU contains is Message type & direction flag with some user data and MAC

MAC is length, destination address and message

We have to trust SA is the person with the key->should be explicit?

->In CBC-MAC only the final block is output as the tag.-Jonathan Katz, Maryland Cyber Centre-crypto/f12/chap4.pdf

Try to find EEIG document for key assignment rules

Ask Tom-is it possible to get the final block ‘looking the same as another’-only issue is 3DES . Would make it not possible

MAC =length || dest address|| message || padding

->Is it possible for an attacker to replay the MAC for a carefully constructed message he knows----YES COLLISION ATTACK

Can we add 56 bits of random data at end of a message?

Experiment: What we want to do was the generate session key but we can use secret

-> Check secrecy of train KS

Forwarding RBC message to train causes it to fail 2nd envinj

Save and put on SVN as a different filename

->Use Proverif to show no injective 1:1 between train and RBC with replaying

Need train to send event, RBC accept event, explicit 1:1 needed

15/7/2015

Defence against length extension attack HMAC

Randoms are 64 bits each

Cleaned up Proverif code and started looking at events for injective property for replay attacks

->Length extension attack-is it possible as you would have an explicit length sent as part of the MAC, which will mismatch the format of the message, so may be rejected

Definition of the data SaPDU read-trust is based on the ability to produce MACs-there is no msg ack as part of the protocol

It won’t be possible to append 56 bits of random text due to the length used in the MAC-it would be rejected because the lengths don’t match

->Does the model suggest it’s possible as it’s written-might need to move MAC generation into a let statement? then can have length/1?

The length function concerns itself with (DA||M) and does not include padding

Added notes about application layer and read FT/Westinghouse articles and presentation

There is a lot of reliance on the ATP application where things should be at a protocol lead?

Meeting with Tom and Joeri

Length extension is still possible

Review key management 11SO 9797/EN50159

ISO 9797 proposes 2-key encryption in the last stage->we use 3

->why not 3DES 1st block as well-this would make a lot of problems go away

Read papers on attacks on ISO 9797 and RBC-RBC handover FIS

Why does there exist an error condition for replays in Auth protocol?-it’s a state machine?

14/7/2015

Read RBC/RBC handover FIS and RAIB to summarise

->need to read Subset 093-has some good diagrams about app layer

Reading attacks against ISO 9797

15/7/2015

Finished reading papers

->Agree that MAC Algo 3 is weak, but it’s modified to use 3DES at end-would 3DES in first block work?

Subset 026 might be relevant to us

->GSM-R voice may-go via EURORADIO- need more evidence

Possible conferences-ESSOS

Moving one layer out into SFM-this is where the protocol continues, feeding into EURORADIO

Meeting with Tom:

->Need to look at SAI-how does it work?

->How are timestamps and seg no’s checked

->What are formats of messages like?

->Keep working on Proverif model->model shows a replay of a connection message

16/7/2015

Proverif model shows that you can just replay a MAC’d message eg one at the start of the connection, because it has the plaintext- ciphertext pair which is valid

->Issue comes when we look at the application layer-this won’t allow replays (unless it’s the HP PDU)

Reviewing SAI specs (not in a single document)

->Replay is possible in Subset 098 as EURORADIO will accept it but SAI won’t

->Making notes as appropriate

Found packet structure for SAI, so we can now see the structure of data from application layer to SAI to SFM to EURORADIO and to GSM

->Emergency messages are the only ones that are allowed to go via HP SaPDU

->Does application layer do anything?

Outside of EURORADIO?

->Need a proper procedure for post TTT/EC

Check Proverif model as whilst it is able to replay and get an accept, the data is not really valid as part of the state machine

20/7/2015

Looking at Proverif model, as according to the state machine, we’ve gone out of state

->Add a DATA DT flag and use the direction flag the property holds

->Need to prove we can replay the messages between train and RBC

Mark wants to see a practical element (or hinted) e.g. listening to traffic (experiments)

Read more specs (Triple Time Stamp) and message formats

Tom thinks that the TTT would give us 46 bits to work with or something depending on resolution

21/7/2015

Continued working on Proverif model-seems to be the event that isn’t correctly firing

Rail Meeting

Few pages on what we’ve done so far-protocols

What is adaption of comms layer?

Read more on SAI

Layer between GSM and session key setup

Choose Chris Green for picture

22/7/2015

Writing up notes for Tom and Joeri

23/7/2015

Looking at the application layer

->Subset 058 has a number of messages but a number of layers within that

CFM has a spec for the Adaption Layer Entity (ALE)

Spoke to Tom to reaffirm what we’ve found so far

27/7/2015

SCEPTICS Meeting

Work with Joeri on TTT and EC

Message format and actual messages

3/8/2015

SCEPTICS meeting

E-mail Sam and Joeri our document

Check heartbeat stuff-is there a heartbeat?

Research API security work (as a tangent)

Graham steel has tools to check API’s

->get a feel for it, as we have train API

LRBG-is it the RBC confirming location, or with respect to the actual message

->Is there a sequence of API commands which could lead to Emergency steps being rejected?

->Can we verify this to see if train locks up or does something dumb?

->Checking API correctness-would it be right e.g. ES, revoke, MA, Conditional ES

->Could 2nd ES be revoked by the existing revoke and then emergency stop? Can we delay the ES?

250 messages needed

How far are messages broadcast?

How many messages do we need for a collision?

Rough estimate how long it would take to do this

Tom-our contributions are good

Experiments show negligible difference between use of DESEDE and no MAC. Thus, there is no reason why the MAC should not be used.

Meetings with SCEPTICS and writing dissertation

17/8/2015 Demonstration with Dan and Neil-Good feedback

18/8/2015 – writeup period with update meetings with the Rail Group throughout to update progress.