CubeSats – A fairy tale

How academia got the chance to implement satellite (in)security and how I tried to fix it.

Marius Münch / @nSinusR

Defcamp, Bucharest

29.11.2014

WARNING

This presentation is held by an overtired speaker. Overtiredness is one of the common side effects resulting from playing CTFs.

The definition of presentation in this sense includes a collaboration of loosely tied together slides arranged in three parts. The slides will contain memes, star wars references and sometimes the opinions and insights of the speaker.

A not so long time ago in a galaxy close by ...

CUBESATS
A NEW HOPE

CubeSats

- 1999: Specification by California Polytechnic State University & Stanford University
  - Aims to bring satellites for low costs into space
  - Low Earth Orbit
  - $10cm^2$
  - Especially attractive for universities
- By now: Over 100 in space
  - Universities
  - Companies
  - Amateur Radio
- Presentation focuses on academic CubeSats

Threats / Accessibility

- Physical access: Low
  - It’s in space, dude
- Link access: High
  - Open medium
  - Easy to eavesdrop
- Network access: Medium
  - Compromised base station
  - Disregarded in this presentation

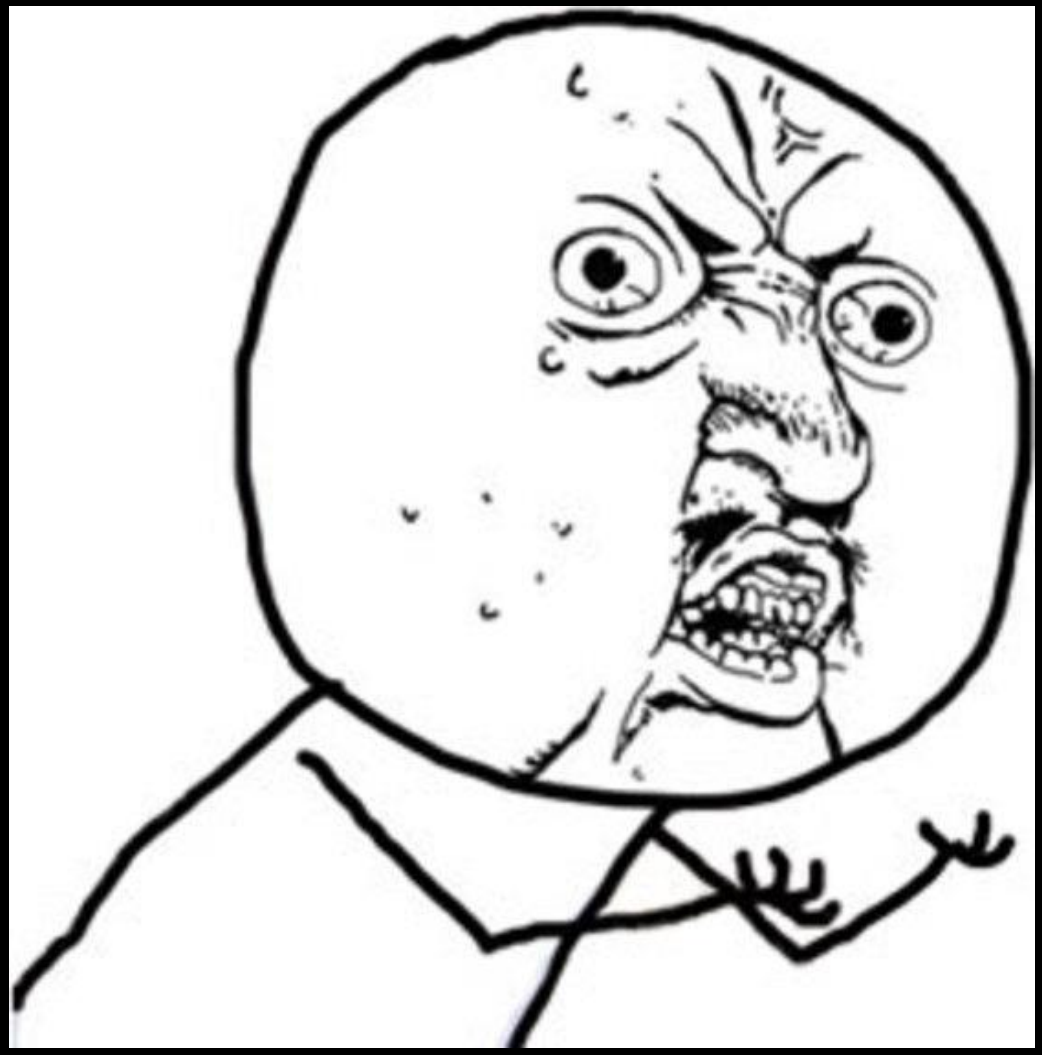
Security

- Commercial & Amateur Radio
  - Classical solutions
    - Encryption
    - propriety
    - security through obscurity
- Academia:
  - Often not present
  - Sometimes different approaches
    - Encryption
    - HMAC
    - (more later)

Security

- Commercial & Amateur Radio
  - Classical solutions
    - Encryption
    - propriety
    - security through obscurity
- Academia:
  - Often not present
  - Sometimes different approaches
    - Encryption
    - HMAC
    - (more later)

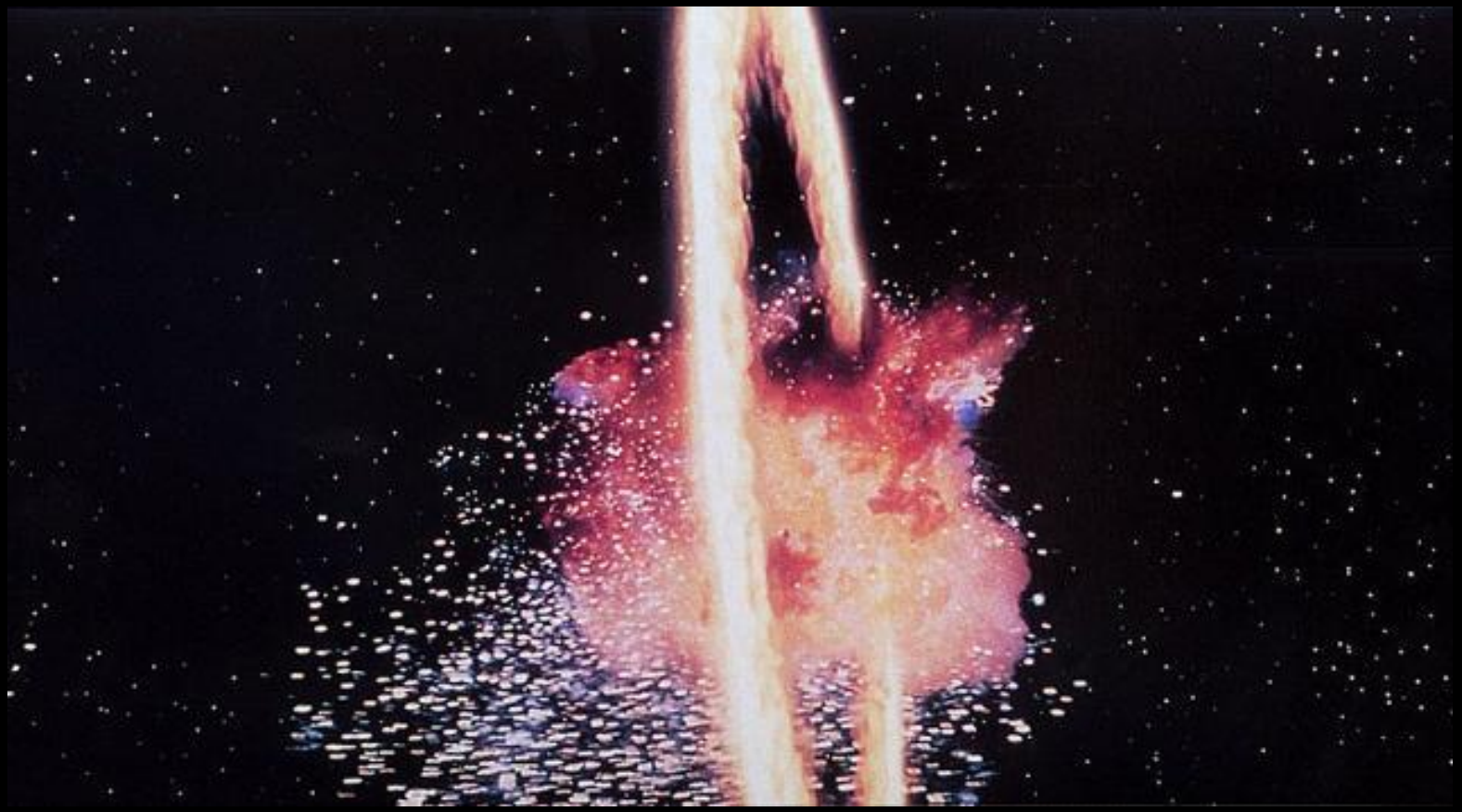
WHY U NO SECURITY?



WHY U NO SECURITY?

“Nobody is going to hack us”

WHY U NO SECURITY?



WHY U NO SECURITY?

WHY U NO SECURITY?

WHY U NO SECURITY?

- Lets face it: It's about the costs
  - Low budget projects
  - Frequencies are expensive!
- But:
  - Amateur radio frequencies are for free
  - Encryption not possible on this frequencies
- From the other side:
  - Low benefits for attacker
  - High equipment costs

Sometimes – One Example: The CubeSat Space Protocol

- University of Aalborg/GomSpace
  - 2011: First release
  - 2013: Launch of GomX-1
- Small protocol stack for CubeSat applications
- Features:
  - Encryption: XTEA-CTR
  - Authentication: HMAC-SHA1
- Missing:
  - Replay Protection

NUTS – My Dagobah (Part II)

The NTNU Test Satellite (NUTS)

- CubeSat program of the Norwegian University of Science and Technology
  - Originated in 2010
  - I participated 2013/14
  - Launch planned for 2016/17
- Everything from scratch
  - Starting with the hardware design
  - Including the communication stack
  - And of course, the software
- They want uplink security

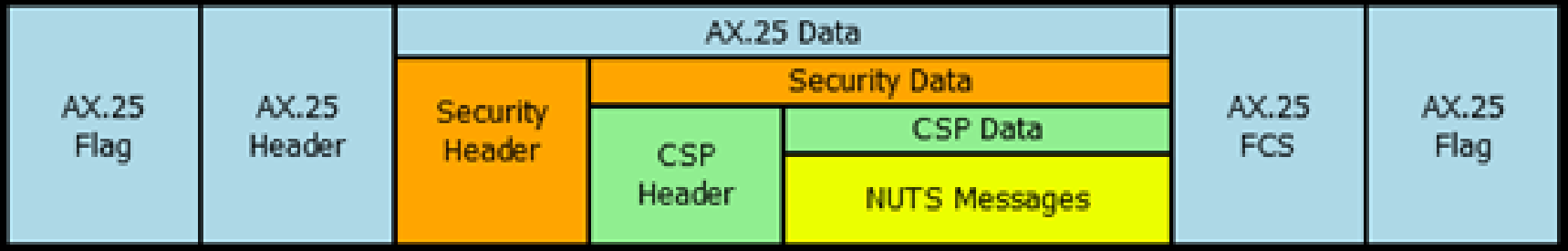
2013: What I did ...

- Prior work inside NUTS:
  - We need authentication, not encryption

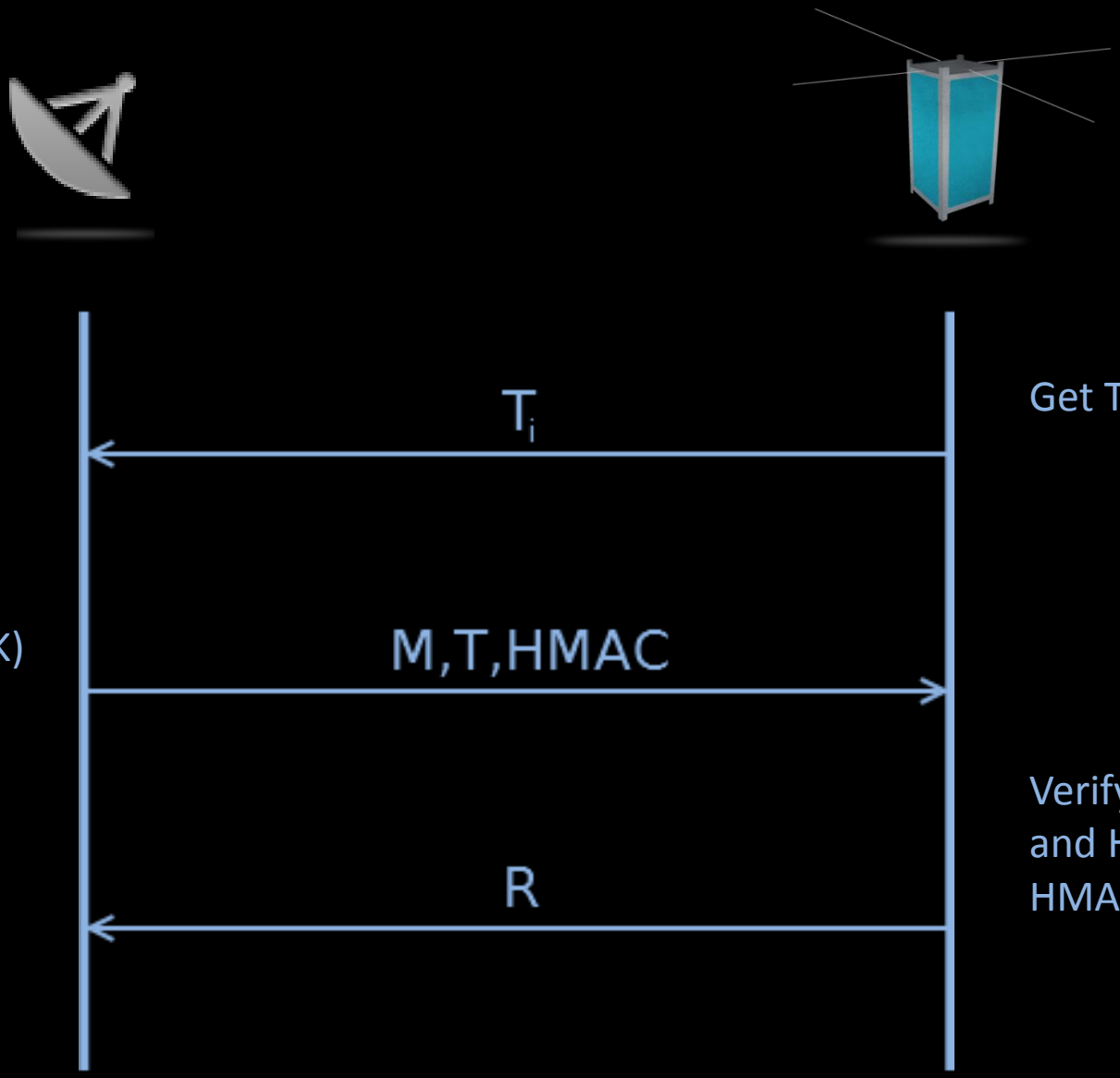
    → HMAC from CSP + sequence numbers

- My project work (in short):
  - Timestamps instead sequence numbers
  - Security as own layer in the communication stack

A packet …


AX.25 Flag
AX.25 Header
AX.25 Data
Security Header
Security Data
CSP Header
CSP Data
NUTS Messages
AX.25 FCS
AX.25 Flag

The Authentication Scheme



2014: My Masterthesis

”Integration and verification of a keyed-hash message authentication scheme based on broadcast timestamps for NUTS”

Formal Verification

- Goal: Assure correctness of cryptographic protocols
- Formal methods based on logic on mathematics to proof satisfaction of security properties
- Automated Tools, e.g. Scyther

- Further Reading: Needham-Schroeder Protocol

Authentication

- Remember: It's the goal
- Authentication != Authentication
- Different kinds of authentication are verifiable
- E.g. Lowe 1997*:
  - Aliveness
  - Weak agreement
  - Non-injective agreement

*G. Lowe. A hierarchy of authentication specifications. In Computer Security Foundations Workshop, 1997. Proceedings., 10th , pages 31–43. IEEE, 1997.

Scyther

- Automated tool for formal verification
- Developed by Cas Cremers
  - http://www.cs.ox.ac.uk/people/cas.cremers/scyther/
- Easy and intuitive description language for protocols
- Easy to use
- Efficient

File Verify Help

Protocol description | Settings

```
 8 usertype Timestamp;
 9
10 // Protocol description
11
12 protocol NAP(B,S)
13 {
14       const m: Msg;
15       const r: Msg;
16
17       role B
18       {
19             var t: Timestamp;
20
21             recv_1(S,B,{t}sk(S));
22             send_2(B,S,m,t,hash(m,t,k(B,S)));
23             recv_3(S,B,{r}sk(S));
24
25             claim_b1(B,Alive);
26             claim_b2(B,Weakagree);
27             claim_b3(B,Niagree);
28             claim_b4(B,Nisynch);
29             claim_b5(B,Secret,k(B,S));
30       }
31
32       role S
33       {
34             fresh t: Timestamp;
35
36             send_!T1(S, S, t);
37             send_1(S,B,{t}sk(S));
38             recv_2(B,S,m,t,hash(m,t,k(B,S)));
39             send_3(S,B,{r}sk(S));
40
41             claim_s1(S,Alive);
42             claim_s2(S,Weakagree);
43             claim_s3(S,Niagree);
44             claim_s4(S,Nisynch);
45             claim_s5(S,Secret,k(B,S));
46       }
47 }
```

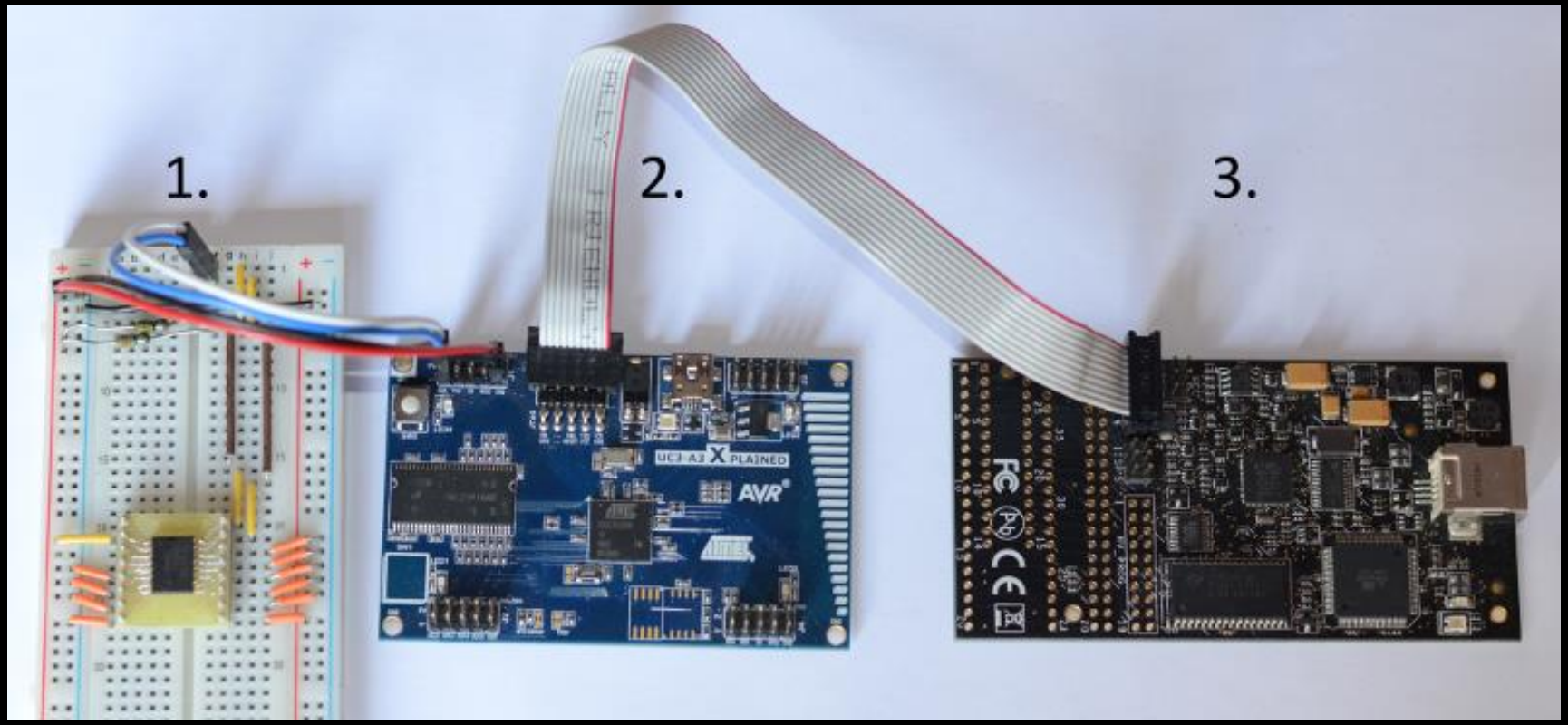
Claim				Status		Comments	Patterns
NAP	B	NAP,b1	Alive	Ok	Verified	No attacks.	
		NAP,b2	Weakagree	Fail	Falsified	At least 1 attack.	1 attack
		NAP,b3	Niagree	Fail	Falsified	At least 1 attack.	1 attack
		NAP,b4	Nisynch	Fail	Falsified	At least 1 attack.	1 attack
		NAP,b5	Secret k(B,S)	Ok	Verified	No attacks.	
	S	NAP,s1	Alive	Ok	Verified	No attacks.	
		NAP,s2	Weakagree	Ok	Verified	No attacks.	
		NAP,s3	Niagree	Ok	Verified	No attacks.	
		NAP,s4	Nisynch	Ok	Verified	No attacks.	
		NAP,s5	Secret k(B,S)	Ok	Verified	No attacks.	

Done.

Err … wait!?

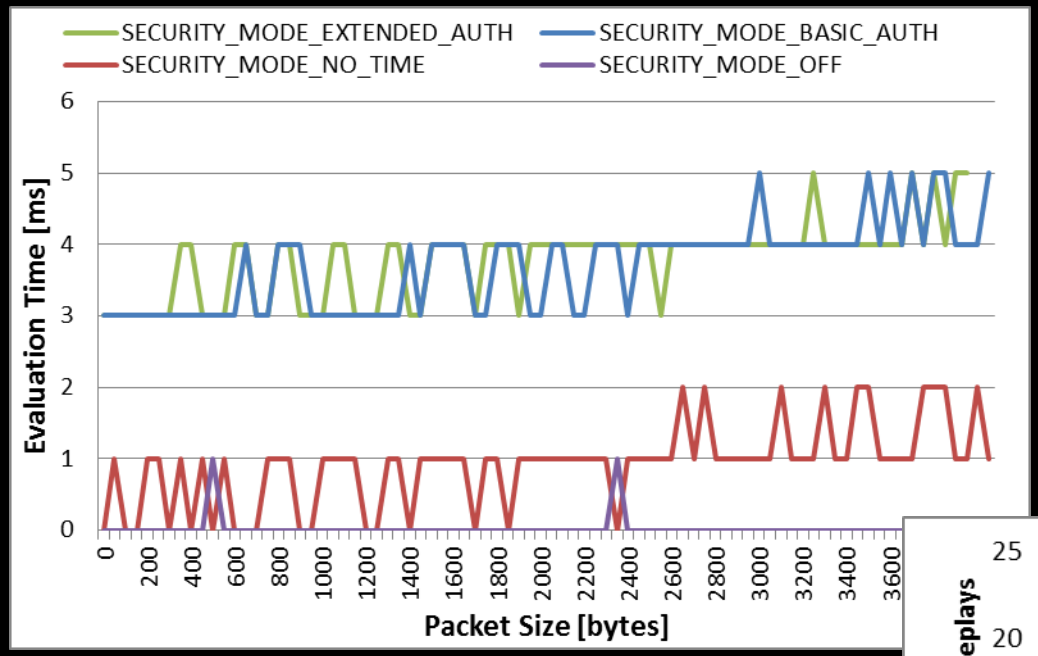
- The cryptographic protocol is obviously flawed
- I implemented it and recommended its usage nevertheless
  - Flaws can be neglected
  - Why: Outside scope ;)
  - Better answer: We assume satellite as a completely trusted entity
    - Doppler shift
    - Low probability of fake satellite

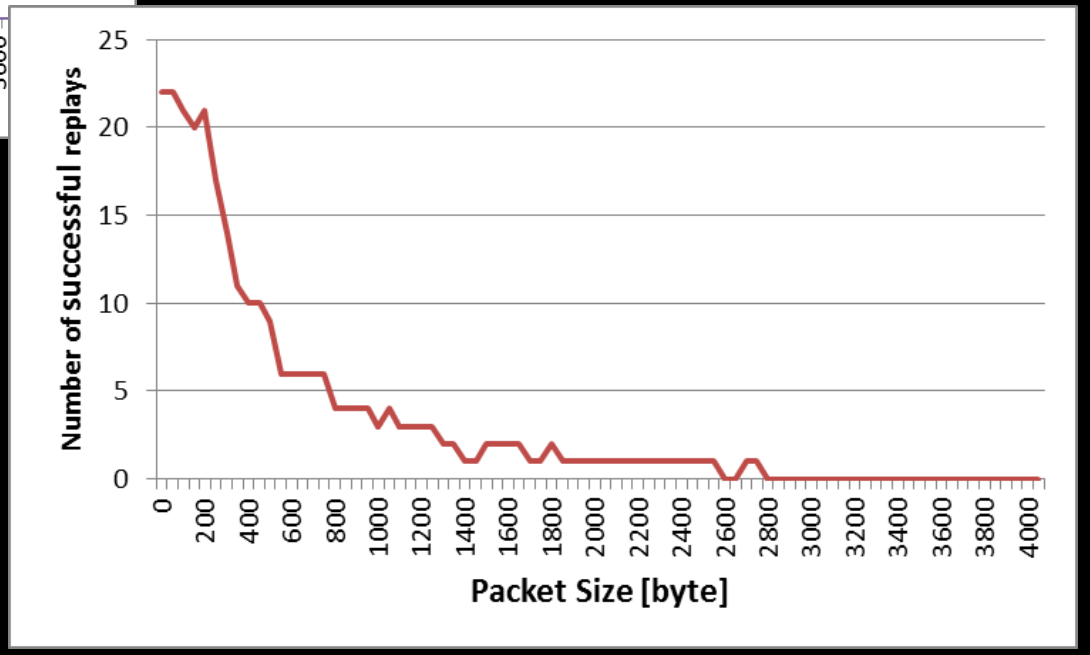
Implementation



1) RTC
2) AVR UC3-A3 Xplained
3) AVR Dragon

Some charts


SECURITY_MODE_EXTENDED_AUTH
SECURITY_MODE_BASIC_AUTH
SECURITY_MODE_NO_TIME
SECURITY_MODE_OFF
Evaluation Time [ms]
0
1
2
3
4
5
6
0
200
400
600
800
1000
1200
1400
1600
1800
2000
2200
2400
2600
2800
3000
3200
3400
3600
Packet Size [bytes]


Number of successful replays
0
5
10
15
20
25
0
200
400
600
800
1000
1200
1400
1600
1800
2000
2200
2400
2600
2800
3000
3200
3400
3600
3800
4000
Packet Size [byte]

… AND THE MORAL OF THIS STORY

(Part III)

CRYPTO
IS HARD

(No shit, Sherlock)

CRYPTO IN SPACE
IS HARDER

Random Bit Flips

Low Computational Power

CRYPTO IN SPACE IS HARDER

Link Budget

Integration & Paranoia
(„Failsafeness“)

FORMAL VERIFICATION
IS AWESOME

Finds flaws hidden to the human eye

Not limited to academia

FORMAL VERIFICATION
IS AWESOME

It‘s not that hard to use

Already enough ways to screw the implementation – let‘s have a sound design

SOMETIMES …

MD5 IS STILL OKAY

Security of HMAC does not rely on the security of the underlying hash function

2^{64} vs 2^{16}

SOMETIMES …
MD5 IS STILL OKAY

Small Digest Size

Fast to compute

Know your constrains and limits!

ACADEMIC PROJECTS
- DRIVEN BY STUDENTS -
ARE HARD TO COORDINATE

Everyone wants to change the World™

Rush for deadlines

ACADEMIC PROJECTS
- DRIVEN BY STUDENTS -
ARE HARD TO COORDINATE

Continuity is lacking

The procrastination might be strong with this one

BUT THAT‘S TOTALLY FINE!

EPILOGUE

Ongoing & Future Work

- Integration to the actual NUTS hardware
- Radiation hardness testing
- Test operation in space
- Key management

- … CubeSat Space Protocol?

Acknowledgements

- Roger Birkeland – The head of NUTS
- Stig Frode Mjølsnes – Supervising professor
- Timo Stein – Fellow Jedi & part of the council

- The NUTS Team.
- Tasteless.

Sources

- Y U NO Guy: http://i2.kym-cdn.com/entries/icons/facebook/000/004/006/y-u-no-guy.jpg
- Exploding Deathstar: http://img1.wikia.nocookie.net/__cb20060724101310/jedipedia/de/images/thumb/3/35/Todesstern_explodiert.jpg/640px-Todesstern_explodiert.jpg - taken from http://www.jedipedia.de - Copyright holder: Lucasfilm Ltd. - Original Source: Star Wars Episode IV: A New Hope
- Evil Hacker: http://blog.hosterpk.com/wp-content/uploads/2014/05/hacker.jpg
- Amatuer Radio Operator (DJ1YFK): http://upload.wikimedia.org/wikipedia/commons/b/bb/Dj1yfk_in_sweden.jpg - CC BY 2.5 - Photo by Henryk Kotowski Kotoviski
- Dagobah: http://img3.wikia.nocookie.net/__cb20090616143649/jedipedia/de/images/7/72/DagobahSumpf.jpg - taken from http://www.jedipedia.de - Copyright holder: Lucasfilm Ltd. - Original Source: StarWars Episode V - The Empire Strikes Back
- Little Red Riding Hood: http://upload.wikimedia.org/wikipedia/commons/thumb/8/84/Offterdinger_Rotkappchen_%282%29.jpg/640px-Offterdinger_Rotkappchen_%282%29.jpg – Illustration by Carl Offterdinger
- Star Jedi Hollow font: http://www.dafont.com/star-jedi.font - by Davide Canavero
- All NUTS Artworks are created by the ‘’NUTS - NTNU Test Satellite‘‘ research group
- Tasteless Logo by Marius Münch