
IEEE ICIT 2017, Toronto

Thorsten Schulz
Frank Golatowski
Dirk Timmermann

"This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 731456."
Most Common Cryptography Mistakes

1. Don’t roll your own
2. Security shall not be negotiable
3. Passphrases do not make keys
4. Unqualified Random Number Generators
5. Encryption without authentication
6. Encrypted traffic still leaks inf. (e.g. timing)
7. Hashing concatenated strings
8. Key re-use, Nonce re-use

("1: David Wagner, UC Berkley, 2016)
("² Peter Gutmann)
Motivation

- Applications with critical safety require (e.g. EN50128: “highly recommend”)
  - formal methods for implementations
  - formal verification techniques
- Trial feasibility
- Estimate the performance deficits in implementation of dataflow-model-based versus imperative language
- Extend (own) existing models with integrated, non-bypassable cryptographic methods
Approach

- Elliptic curve cryptography based on Curve25519 are proven algorithms originating from research by Daniel J. Bernstein with many implementations
  - **Network and Cryptography Library** “salt” (reference impl.)
  - **TweetNaCl** (very concise ANSI-C)
  - **µNaCl** (8 bit-µC)
  - **libsodium** (POSIX)
    - Google QUIC, Apple iPhone encrypt, openSSH, WhatsApp … …

- **In this work**: Formalized Implementation in SCADE:
  - “SLIDE” – Safety Leveraged Implementation of Data Encryption

- **Goal**: improve development / verification process for safety-critical systems.
Modelling Tool: ANSYS® SCADE Suite

- Synchronous reactive programming language Scade for data- and control-flow modelling
- Qualified: DO-178C (avionic), EN-50128 (rail), IEC-61508 (industrial), ISO 26262 (autom.)
- Relevant, commercial toolchain:
  - Airbus, Eurostar train, many nuclear power plants, Siemens (trains), Pratt & Whitney (turbines)
Asymmetric Cryptography of NaCl

Sender side

Sender key
- public
- private

Diffie-Hellman-Precomputation

DH

secret key

Rcv. key
- public

*On channel initialization

*public

*nonce

message

secret key encryption

stream cipher

stream key

*message*

Authenticator

nonce

MAC

*message*
Scade Crypto Library “SLIDE”

- Asymmetric key generation and exchange
- Authenticated Encryption using Curve25519 algorithms (optimized)
- Signature generation and verification
- SHA2-512

- Availability: pls contact author (github planned), open-source
Exemplary Safety Microcontroller Platform

Texas Instruments Hercules RM57Lx

Features:
- IEC 61508 SIL 3 + ISO 26262 ASIL D certified µC
- LockStep CPUs – 1oo1D safety concept
- ARM-Cortex-R5F @ 330 MHz, 4 MB Flash, 0.5 MB ECC-RAM, Eth, SPI
  ...
- Automotive + Industrial control
- Digital I/O Module
- Process automation
  (train == “moving industrial plant”)

Dev-Kit:
LAUNCHXL2-RM57L
Results Key Precomputation (elliptic curve multipl.)

[ms] execution time

[kB] stack

TweetNaCl
SLIDE v0
SLIDE
libsodium

precomputation

precomputation

stream crypt.
Results Encryption + Authentication

[ms] execution time

- TweetNaCl
- SLIDE v0
- SLIDE
- libsodium

payload size:

- 0
- 1
- 20
- 120
- 160
- 320
- 1458
Reference: Model-based Safety Application

Integration with Train Safety Control (ETCS, Intervention Braking)

Degraded brake performance due to construction zone
Integration with Model-based Train Safety Control

ANSYS® SCADE System view of SDM (simplified)
Evaluation of De-/Encrypt to a Process
Results

✓ Feasible within 100ms-application-process-cycles
   Compared to optimized C-library (libsodium):
     ✓ Encrypt+Auth-Execution same magnitude
     ✓ Key calculation slower (simpler algorithm)

➢ Actual value of SLIDE will be of homogeneous integration & testing:
   ➢ Less module-interface glitches
   ➢ Verifiable application states
   ➢ But is any security assured for certification?
So, if “Crypto wont save you either”, what’s next?

- Security is much more than cryptography
- Assured security for critical systems needs wider approach:
  - Secure credential storage / boot / update
  - Proof of non-interference of resource sharing, effects of time partitioning …
  - certMILS: Compositional security certification for medium to high-assurance COTS-based systems in environments with emerging threats

http://www.certmils.eu
Conclusion & Take-Home

✓ General Proof-of-Concept:
  Crypto within the safety-verified Model-based language Scade

➢ Performance results are acceptable on a safety microcontroller

➢ Value of SLIDE is of homogeneous integration & testing

➢ More Work is required to assure Safety is Secure
Feedback, Questions, Answers

Dipl.-Ing. Thorsten Schulz

University of Rostock, Department of CS and EE
Institute of Applied Microelectronics and CE

✉ 18051 Rostock, Germany
🏠 Richard-Wagner-Str. 31 Haus 1, 18119 Rostock
📞 +49 381 498-7278
✉ thorsten.schulz@uni-rostock.de | http://www.imd.uni-rostock.de

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 731456.”

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.