tpm2-software.github.io

Enabling the TPM2.0 Ecosystem in Linux

Andreas Fuchs
<andreas.fuchs@sit.fraunhofer.de>

(filling in for Peter Huewe)

Who am I ?

- **13 year on/off TPMs**
- **Fraunhofer SIT: Trustworthy Platforms**
- **TCG-member: TPM Software Stack WG**
- **Maintainer**
  - tpm2-tss: The libraries
  - tpm2-tss-engine: The OpenSSL engine
  - tpm2-totp: Computer-to-user attestation (mjg’s tpm-totp reimplemented for 2.0)

Putting TPMs into things

Agenda

- **Introducing TPMs**
- Introducing the TSS

- Existing TSS software
- What’s new ?

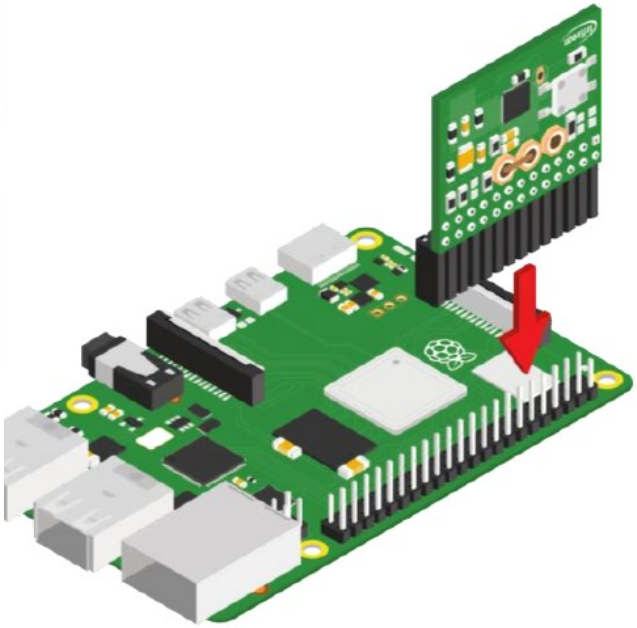
- Community

Introduction to TPMs

- **Trusted Platform Module (TPM) 2.0**
  - Smartcard-like capabilities but soldered in
  - Remote Attestation capabilities
  - As separate chip (LPC, SPI, I²C)
  - In Southbridge / Firmware
  - Via TEEs/TrustZone, etc
  - Thanks to Windows-Logos in every PC
- **CPU**
  - OS, TSS 2.0, applications

Introduction to TPMs

- **Getting started**
  - Any PC with a Windows Logo
    ACPI based discovery
  - A Raspberry-PI with a TPM daughterboard
    On Raspbian:
    /boot/config.txt:
    dtparam=spi=on
    dtoverlay=tpm-slb9670
- **tpm2-tss/INSTALL.md**



Agenda

- Introducing TPMs
- **Introducing the TSS**

- Existing TSS software
- What’s new ?

- Community

The TPM Software Stack 2.0

- **Kernel exposes /dev/tpm0 with byte buffers**
- **TCG specifications:**
  - TPM spec for functionality
  - TSS spec for software API
- **tpm2-tss is an implementation**
- **APIs for application integration**
- **Support in other modules and middle wares for seamless integration**

The TSS APIs

System API (sys)
- 1:1 to TPM2 cmds
- Cmd / Rsp serialization
- No file I/O
- No crypto
- No heap / malloc

Enhanced SYS (esys)
- Automate crypto for HMAC / encrypted sessions
- Dynamic TCTI loading
- Memory allocations
- No file I/O

Feature API (FAPI)
- Spec in draft form
- No custom typedefs
- JSON interfaces
- Provides Policy language
- Provides keystore
- Sec/func separation

User Space

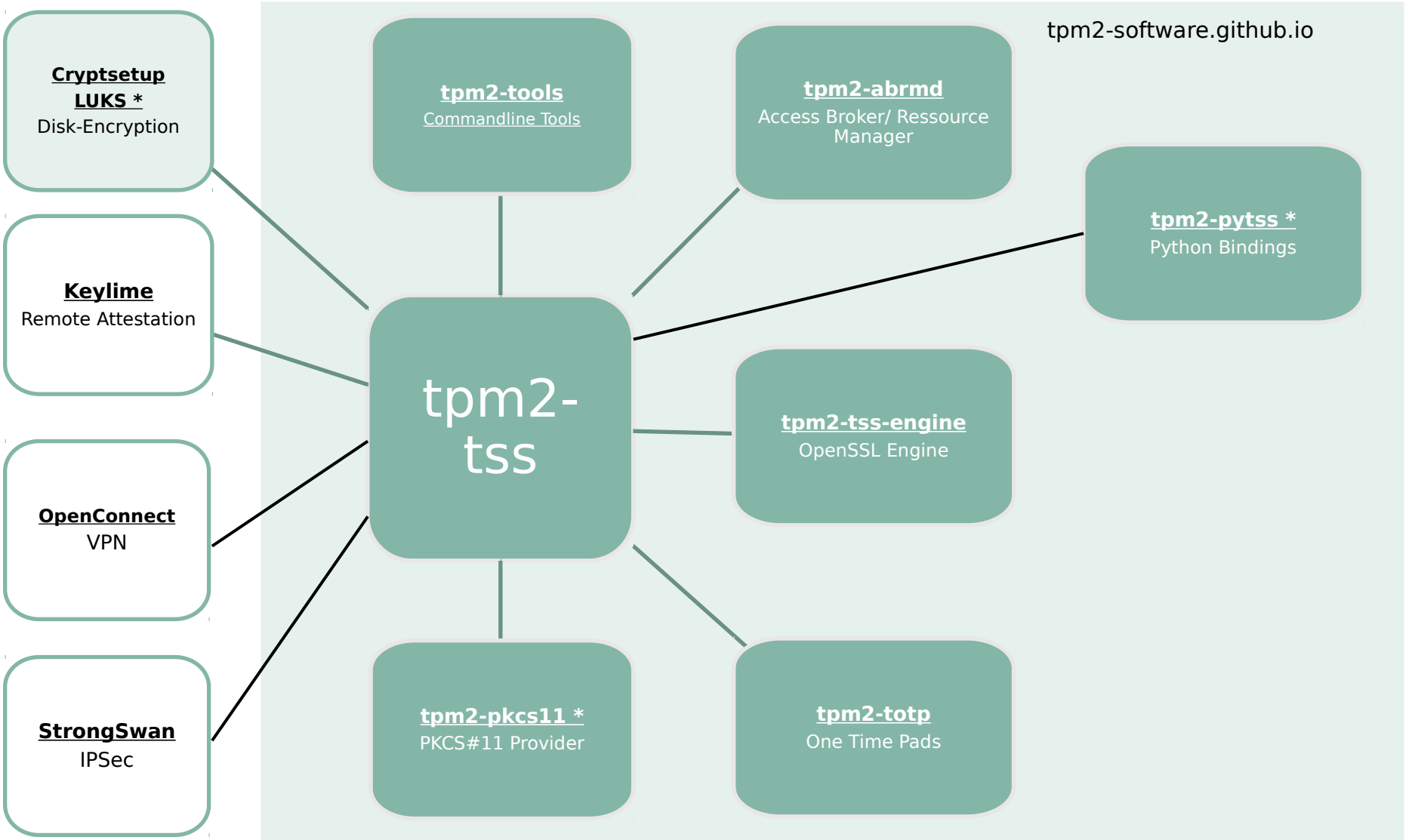
TPM Command Transmission Interface (tss2-tcti)
- Abstract command / response mechanism,
- Decouple APIs from command transport / IPC
- No crypto, heap, file I/O
- Dynamic loading / dlopen API

TPM Access Broker and Resource Manager (TAB/RM)
- Abstract Storage Limitations
- No crypto
- Power management

TPM Device Driver
- Device Interface (CRB / polling)
- Pre-boot log handoff

Kernel

Projects overview



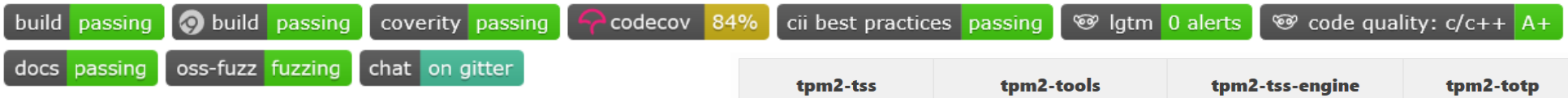
The tpm2-software core projects

- **tpm2-tss (core library)**
  - Autotools, pkg-config, deps: libcrypto OR libgcrypt
    coming deps: libcurl, libjson-c
- **tpm2-abrmd (user space RM)**
  - Autotools, pkg-config, deps: libdbus, libglib
- **tpm2-tools (CLI tools)**
  - Autotools, pkg-config, deps: libcrypto, libcurl
- **tpm2-pytss (python bindings)**
- **tpm2-tss-engine (OpenSSL-engine)**
- **tpm2-totp (PC-to-human authentication)**

People and community

- **Maintainers:**
  - Bill, Imran, Jonas, Jürgen, John, Phil, Peter, Tadeusz, and me
- **>100 contributors**
- **CI with ~80% coverage targets, scanbuild, coverity, CII best practice, lgtm, …**
- **Building multi-distro CI using docker**

Tags tags tags



- **Tested in many ways**
- **Packaged for many distros**

tpm2-tss

Packaging status	
Alpine Linux Edge	2.3.1
ALT Sisyphus	2.3.1
Arch	2.3.1
AUR	2.0.0.r409...
CentOS 7	1.4.0
CentOS 8	2.0.0
Debian Stable	2.1.0
Debian Testing	2.1.0
Debian Unstable	2.1.0
Deepin	1.4.0
Devuan 3.0 (Beowulf)	2.1.0
Devuan Unstable	2.1.0
EPEL 7	1.0
Exherbo	2.3.1
Fedora 26	1.0
Fedora 27	1.2.0
Fedora 28	1.4.0
Fedora 29	2.1.2
Fedora 30	2.2.3
Fedora 31	2.3.1
Fedora Rawhide	2.3.1
FreeBSD Ports	2.3.1
Funtoo 1.4	2.2.3
Gentoo	2.2.3
Kali Linux Rolling	2.1.0
Mageia 7	2.2.2
Mageia Cauldron	2.3.1
Manjaro Stable	2.3.1
Manjaro Testing	2.3.1
Manjaro Unstable	2.3.1
nixpkgs stable	2.2.3
nixpkgs unstable	2.3.1
Parabola	2.3.1
Parrot	2.1.0
PureOS Amber	2.1.0
PureOS landing	2.1.0
Raspbian Stable	2.1.0
Raspbian Testing	2.1.0
Rosa Server 7.5	1.3.0
Scientific Linux 7.x	1.4.0
Trisquel 8.0	0.98
Ubuntu 16.04	0.98
Ubuntu 18.04	1.0
Ubuntu 18.10	1.4.0
Ubuntu 19.04	2.1.0
Ubuntu 19.10	2.1.0
Ubuntu 20.04	2.1.0

tpm2-tools

Packaging status	
Alpine Linux Edge	4.0
Arch	4.0
AUR	4.0.r45.af...
CentOS 7	3.0.4
CentOS 8	3.1.1
Debian Stable	3.1.3
Debian Testing	3.1.3
Debian Unstable	3.1.3
Deepin	2.1.0
Devuan 3.0 (Beowulf)	3.1.3
Devuan Unstable	3.1.3
EPEL 7	1.1.0
Fedora 26	1.1.0
Fedora 27	2.1.1
Fedora 28	3.0.5
Fedora 29	3.1.4
Fedora 30	3.2.0
Fedora 31	3.2.0
Fedora Rawhide	4.0
FreeBSD Ports	4.0
Funtoo 1.4	3.1.4
Gentoo	3.1.4
Kali Linux Rolling	3.1.3
Manjaro Stable	4.0
Manjaro Testing	4.0
Manjaro Unstable	4.0
nixpkgs stable	3.2.0
nixpkgs unstable	3.2.0
openSUSE Leap 42.3	2.0.0
openSUSE Leap 15.0	3.0.4
openSUSE Leap 15.1	3.1.2
openSUSE Leap 15.2	3.1.2
openSUSE Tumbleweed	3.1.4
openSUSE Security Tumbleweed	3.1.4
Parabola	4.0
Parrot	3.1.3
PureOS Amber	3.1.3
PureOS landing	3.1.3
Raspbian Stable	3.1.3
Raspbian Testing	3.1.3
Rosa Server 7.5	3.0.1
Scientific Linux 7.x	3.0.4
Trisquel 8.0	1.0.0
Ubuntu 16.04	1.0.0
Ubuntu 18.04	2.1.0
Ubuntu 18.10	2.1.0
Ubuntu 19.04	3.1.3
Ubuntu 19.10	3.1.3
Ubuntu 20.04	3.1.3

tpm2-tss-engine

Packaging status	
Arch	1.0.1
AUR	1.0.0.r28....
Funtoo 1.4	1.0.0
Gentoo	1.0.0
Manjaro Stable	1.0.1
Manjaro Testing	1.0.1
Manjaro Unstable	1.0.1
openSUSE Tumbleweed	0
openSUSE Security Tumbleweed	0
Parabola	1.0.1

tpm2-totp

Packaging status	
Arch	0.2.0
AUR	0.2.0rc0.r...
Funtoo 1.4	0.1.1
Gentoo	0.1.1
Manjaro Testing	0.2.0
Manjaro Unstable	0.2.0
Parabola	0.2.0

Agenda

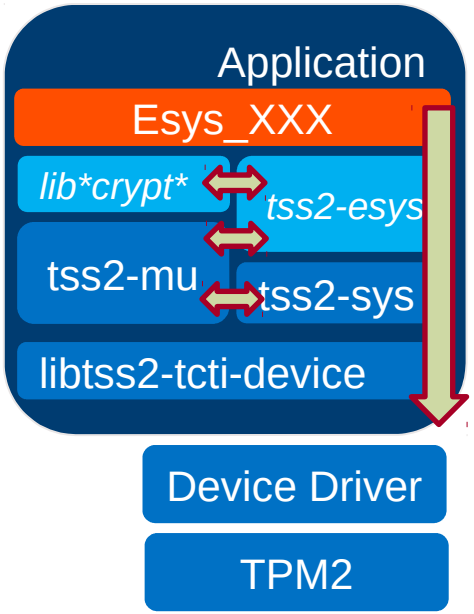
- Introducing TPMs
- Introducing the TSS

- **Existing TSS software**
- What’s new ?

- Community

Existing TSS things

- **Mostly anything runs off of Esys_*()**
- **Povides 1-to-1 mapping of TPM functionality**
- **Automates**
  - marshalling / unmarshaling
  - Object meta-data handling
  - session encryption and authentication
  - memory allocation
  - TPM detection sequence (tpm2-abrmd, /dev/tpmrm0, /dev/tpm0, simulator)
- **tpm2-tools >= 4.0 use Esys**
- **tpm2-pytss uses Esys**



UC: Shielded key storage and usage

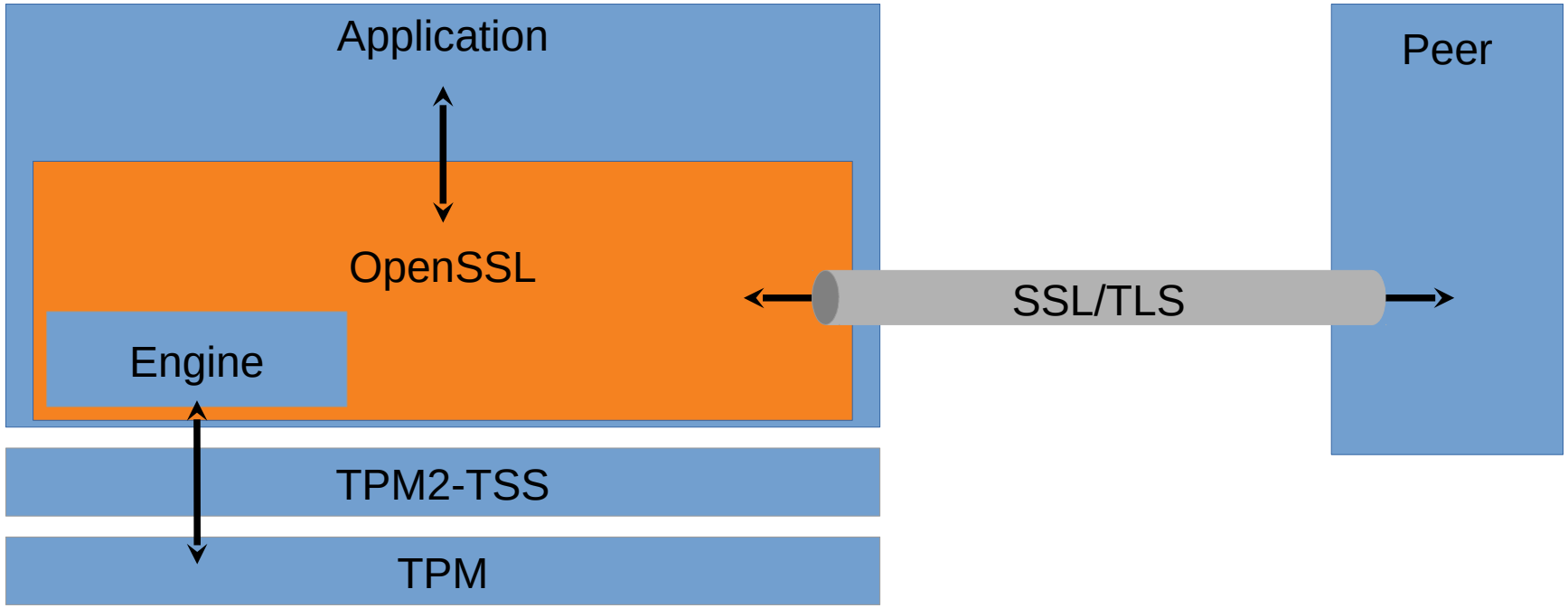
- **Keys in RAM are always dangerous**
  - “Heartbleed”
- **Keys on Disk are always dangerous**
  - You can protect them with user passwords but they can be bruteforced
  - Servers have no unlock step
  - Embedded devices have no unlock step
- **So how do you prevent ID-cloning ?**

  → Use TPM

UC: Shielded key storage and usage

- **How do you use the TPM ?**

  → easy: tpm2-tss-engine

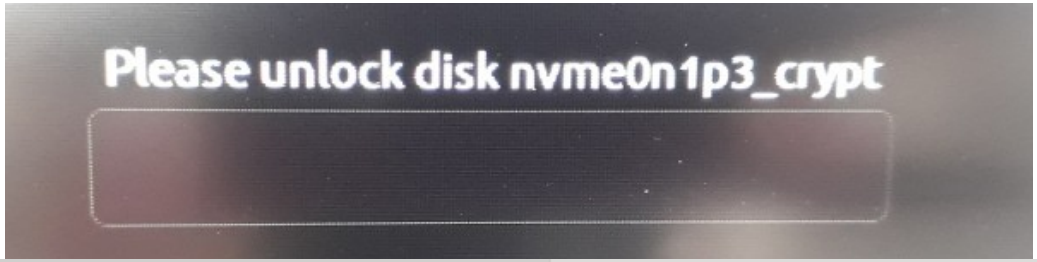


UC: Disk encryption

- **“Bitlocker for Linux”**
  - Binding the disk to the machine
  - Short PIN instead of long passwords
  - No more dictionary attacks
- **Even more utility in other areas**
  - Data Center: People stealing HDDs from the rack
  - Embedded device once more
  - Binding to BIOS integrity status (local attestation)

UC: Disk encryption

- **cryptsetup(-tpm) / LUKS2**
  - Rearchitecting with Milan
  - Making cryptsetup ”module-aware”




```
{
 "keyslots": {
  "1": {
   "type": "tpm2",
   "key_size": 32,
   "area": {
    "type": "tpm2nv",
    "nvindex": 2929459
    "pcrselection": 0,
    "pcrbanks": 1,
    "noda": true
   },
```

```
afuchs@pc-fuchslap3:~/Dokumente/oss-tss/cryptsetup-tpm-incubator$ ./cryptsetup luksFormat --type=luks2 --tpm disk.img

WARNING!
========
Hiermit werden die Daten auf »disk.img« unwiderruflich überschrieben.

Are you sure? (Type uppercase yes): YES
Geben Sie die Passphrase für »disk.img« ein:
Passphrase bestätigen:
afuchs@pc-fuchslap3:~/Dokumente/oss-tss/cryptsetup-tpm-incubator$ ./cryptsetup luksOpen disk.img --test-passphrase
Geben Sie die Passphrase für »disk.img« ein:
afuchs@pc-fuchslap3:~/Dokumente/oss-tss/cryptsetup-tpm-incubator$
```

UC: (VPN) user authentication

- **UserName + Password ?**

  → Machine + UserPassword !

  Adding security to network access
- **OpenConnect (David Woodhouse)**
  - Reuse (copy) of tpm2-tss-engine
- **Strongswan**
  - Implements Attestation and RIMs as well
- **OpenVPN via tpm2-tss-engine ?**
- **Missing WireGuard, Tinc, ...**

Agenda

- Introducing TPMs
- Introducing the TSS

- Existing TSS software
- **What’s new ?**

- Community

What’s new ? libtss2-fapi.so !

- **TCG specifications**
  - TSS 2.0 Feature API spec
  - TSS 2.0 JSON and Policy Data spec
- **Features**
  - No TPM-specific data structures:
    Using JSON for all in-/output
  - Decouple functional design from security design:
    Using cryptographic profiles
  - Add a keystore:
    Store TPM’s blobs and meta data on disk
  - Add a policy language:
    Describe policies in JSON and automatically evaluate policies upon use
- **PRs with >25k LoC on tpm2-tss, -tools, -pkcs11**

API Code comparison (Signing)

FAPI [2 lines of code]

```
Fapi_Sign_async(fctx,
  "name/of/my/key", payload);
Fapi_Sign_finish(fctx,
  &signature);
```

ESAPI [9 lines of code]

```
Esys_TR_SetAuthValue(ectx,
  srkTR, authValue);
Esys_StartAuthSession(ectx,
  srkTR, &sessionTR);
Esys_Load_async(ectx, srkTR,
  sessionTR, keyblob);
Esys_Load_finish(ectx,
  &keyTR);
Esys_TR_SetAuthValue(ectx,
  keyTR, authValue);
Esys_RSA_Sign_async(ectx,
  srkTR, sesstionTR,
  parameters);
Esys_RSA_Sign_finish(ectx,
  &paremters)
Esys_FlushContext(ectx,
   sessionTR);
Esys_FlushContext(ectx,
   keyTR);
```

SAPI [32 lines of code]

```
Application_EncryptSalt(
  session.salt, &encryptedSalt);
Tss2_Sys_StartAuthSession(sctx,
  srkHandle, encryptedSalt,
  &sessionHandle, &tpmNonce);
Application_CalculateSessionKey(
  session.salt, &session.key);
Tss2_Sys_Load_Prepare(sctx,
  srkHandle, keyblob);
Application_GetMetadata(session.key,
  session.nonceTPM,srkName,keyName);
Tss2_Sys_GetCommandCode(sctx,&cc);
Tss2_Sys_GetCpBuffer(sctx,&buffer);
Tss2_Sys_GetDecryptParam();
Application_EncryptParamter();
Tss2_Sys_SetDecryptParam();
Application_CalculateCpHash(cc,
  srkName, keyName, buffer,&cpHash);
Application_CalculateHmac(
  session.key, session.nonceTPM,
  myNonce, cpHash, authValue,&hmac);
Tss2_Sys_SetCmdAuths(sctx,
  sessionHandle, hmac);
Tss2_Sys_Execute(sctx);
Tss2_Sys_GetRspAuths(sctx,&rspAuths)
Tss2_Sys_GetRpBuffer(sctx, &buffer);
Application_CalculateRpHash(cc,
  keyName, rpBuffer, &rpHash);
```

```
Application_VerifyHmac(session.key,
  myNonce, cc, rpHash, rspAuth,
  &tpmNonce);
Tss2_Sys_Load_Finish(sctx,
  &keyHandle);
Tss2_Sys_RSA_Sign_Prepare(sctx,
  keyHandle, parameter);
Tss2_Sys_GetCommandCode(sctx, &cc);
Tss2_Sys_GetCpBuffer(sctx, &buffer);
Application_CalculateCpHash(cc,
  keyName, buffer, &cpHash);
Application_CalculateHmac(
  session.key, session.nonceTPM,
  myNonce, cpHash, authValue,&hmac);
Tss2_Sys_SetCmdAuths(sysConext,
  sessionHandle, hmac);
Tss2_Sys_Execute(sctx);
Tss2_Sys_GetRspAuths(sctx,&rspAuths)
Tss2_Sys_GetRpBuffer(sctx, &buffer);
Application_CalculateRpHash(cc,
  keyName, rpBuffer, &rpHash);
Application_VerifyHmac(session.key,
  myNonce, cc, rpHash, rspAuth,
  &tpmNonce);
Tss2_Sys_RSA_Sign_Finish(sctx,
  &paramenter);
Tss2_Sys_FlushContext(sctx,
  sessionHandle);
Tss2_Sys_FlushContext(sctx,
  keyHandle);
```

Policy Comparison

- **ESYS:**

```
TPML_PCR_SELECTION pcrSelection = {
        .count = 1, .pcrSelections = {
        { .hash = TPM2_ALG_SHA1,
          .sizeofSelect = 3,
          .pcrSelect = {00, 00, 01} } } };

TPM2B_DIGEST pcr_digest_zero = {
    .size = 20, .buffer = {0x67, 0x68, 0x03,
0x3e, 0x21, 0x64, 0x68, 0x24, 0x7b, 0xd0,
0x31, 0xa0, 0xa2, 0xd9, 0x87, 0x6d, 0x79,
0x81, 0x8f, 0x8f}};

r = Esys_StartAuthSession(esys_context,
            ESYS_TR_NONE, ESYS_TR_NONE,
            ESYS_TR_NONE, ESYS_TR_NONE,
            ESYS_TR_NONE, &nonceCallerTrial,
            TPM2_SE_POLICY, &symmetric,
            TPM2_ALG_SHA1, &session);

r = Esys_PolicyPCR(esys_context, session,
            ESYS_TR_NONE, ESYS_TR_NONE,
            ESYS_TR_NONE, &pcr_digest_zero,
            &pcrSelection);
```

- **FAPI:**

```
{
   "description":"PCR 16 value",
   "policy":[
      {
         "type":"POLICYPCR",
         "pcrs":[
            {
               "pcr":16,
               "hashAlg":"SHA1",
               " digest":"00...00"
            }
         ]
      }
   ]
}
```

UC: (General) user authentication

- **Typical SmartCard workflow (PKCS11)**
  - Proof of possession (of smartcard)
  - Proof of knowledge (of PIN not password)
  - More secure and convenient than passwords

  → tpm2-pkcs11 (Virtual SmartCard)
  - Proof of possession (of TPM-holding device)
  - Proof of knowledge
  - Fully compatible
- **Heavy rework to run off of FAPI**

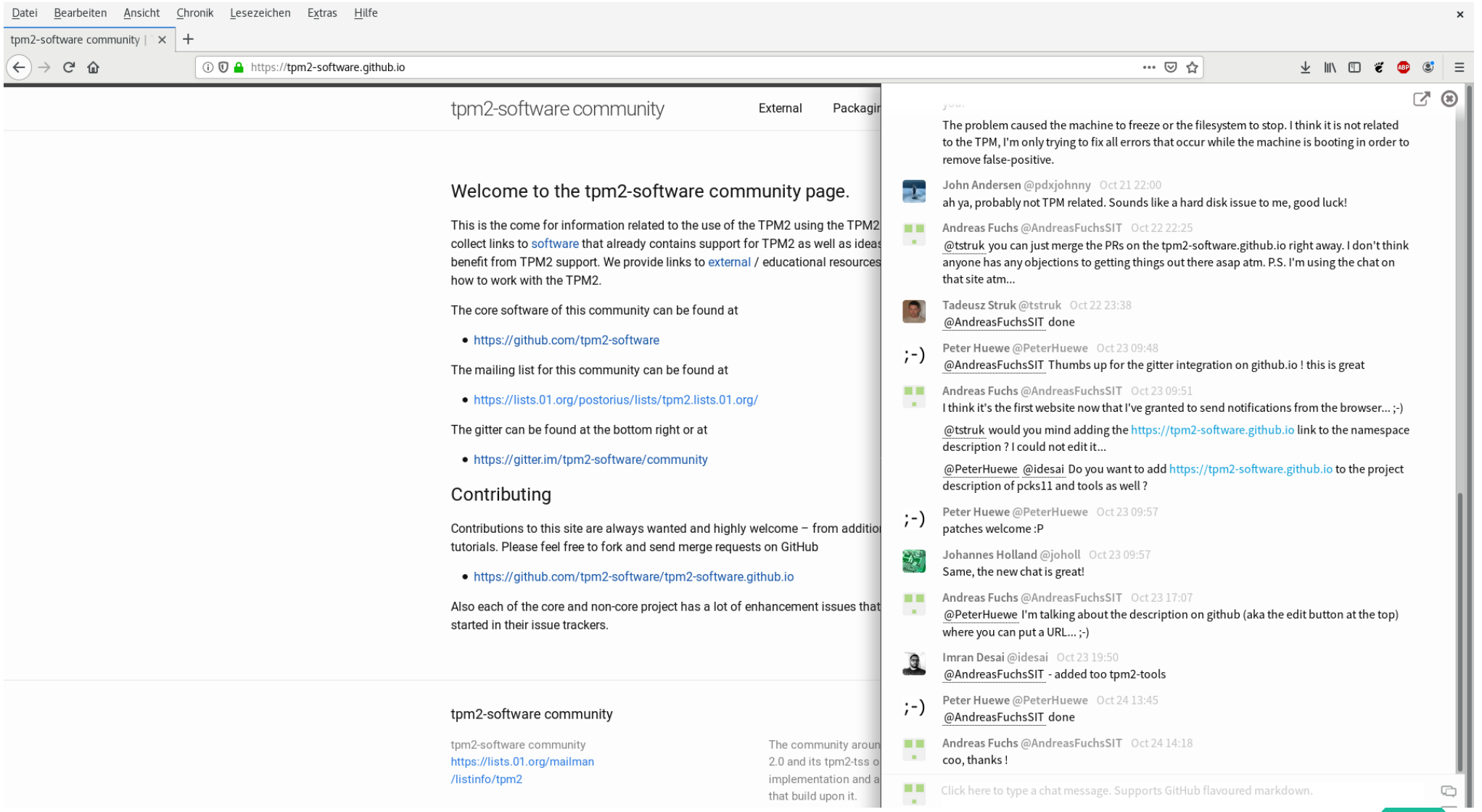
Agenda

- Introducing TPMs
- Introducing the TSS

- Existing TSS software
- What’s new ?

- **Community**

Community


Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
tpm2-software community
https://tpm2-software.github.io
tpm2-software community
External
Welcome to the tpm2-software community page.
This is the come for information related to the use of the TPM2 using the TPM2
collect links to software that already contains support for TPM2 as well as ideas
benefit from TPM2 support. We provide links to external / educational resources
how to work with the TPM2.
The core software of this community can be found at
https://github.com/tpm2-software
The mailing list for this community can be found at
https://lists.01.org/postorius/lists/tpm2.lists.01.org/
The gitter can be found at the bottom right or at
https://gitter.im/tpm2-software/community
Contributing
Contributions to this site are always wanted and highly welcome – from additio
tutorials. Please feel free to fork and send merge requests on GitHub
https://github.com/tpm2-software/tpm2-software.github.io
Also each of the core and non-core project has a lot of enhancement issues that
started in their issue trackers.
tpm2-software community
tpm2-software community
https://lists.01.org/mailman
/listinfo/tpm2
The community aroun
2.0 and its tpm2-tss o
implementation and a
that build upon it.
The problem caused the machine to freeze or the filesystem to stop. I think it is not related to the TPM, I'm only trying to fix all errors that occur while the machine is booting in order to remove false-positive.
John Andersen @pdxjohnny Oct 21 22:00
ah ya, probably not TPM related. Sounds like a hard disk issue to me, good luck!
Andreas Fuchs @AndreasFuchsSIT Oct 22 22:25
@tstruk you can just merge the PRs on the tpm2-software.github.io right away. I don't think anyone has any objections to getting things out there asap atm. P.S. I'm using the chat on that site atm...
Tadeusz Struk @tstruk Oct 22 23:38
@AndreasFuchsSIT done
;-)
Peter Huewe @PeterHuewe Oct 23 09:48
@AndreasFuchsSIT Thumbs up for the gitter integration on github.io ! this is great
Andreas Fuchs @AndreasFuchsSIT Oct 23 09:51
I think it's the first website now that I've granted to send notifications from the browser... ;-)
@tstruk would you mind adding the https://tpm2-software.github.io link to the namespace description ? I could not edit it...
@PeterHuewe @idesai Do you want to add https://tpm2-software.github.io to the project description of pcks11 and tools as well ?
;-)
Peter Huewe @PeterHuewe Oct 23 09:57
patches welcome :P
Johannes Holland @joholl Oct 23 09:57
Same, the new chat is great!
Andreas Fuchs @AndreasFuchsSIT Oct 23 17:07
@PeterHuewe I'm talking about the description on github (aka the edit button at the top) where you can put a URL... ;-)
Imran Desai @idesai Oct 23 19:50
@AndreasFuchsSIT - added too tpm2-tools
;-)
Peter Huewe @PeterHuewe Oct 24 13:45
@AndreasFuchsSIT done
Andreas Fuchs @AndreasFuchsSIT Oct 24 14:18
coo, thanks !
Click here to type a chat message. Supports GitHub flavoured markdown.

What’s missing ?

- **Attestation**
  - Some support by FAPI; protocol bindings
  - Reference value descriptions
- **More core system integration**
  - 802.1X: NetworkManager, systemd-networkd
  - User keyrings: gnome-keyring, kwallet
  - VPNs: Wireguard, Tinc, ...
  - Signing: GnuPG
  - WebCrypto / WebAuthn (Firefox, Chrome, ...)
  - ……
- **2nd maintainer for tpm2-tss-engine :-)**

Questions ?

https://tpm2-software.github.io