UNIVERSITY OF
BIRMINGHAM

CENTRE FOR
CYBER SECURITY
AND PRIVACY

User-controlled hardware security anchors: evaluation and designs

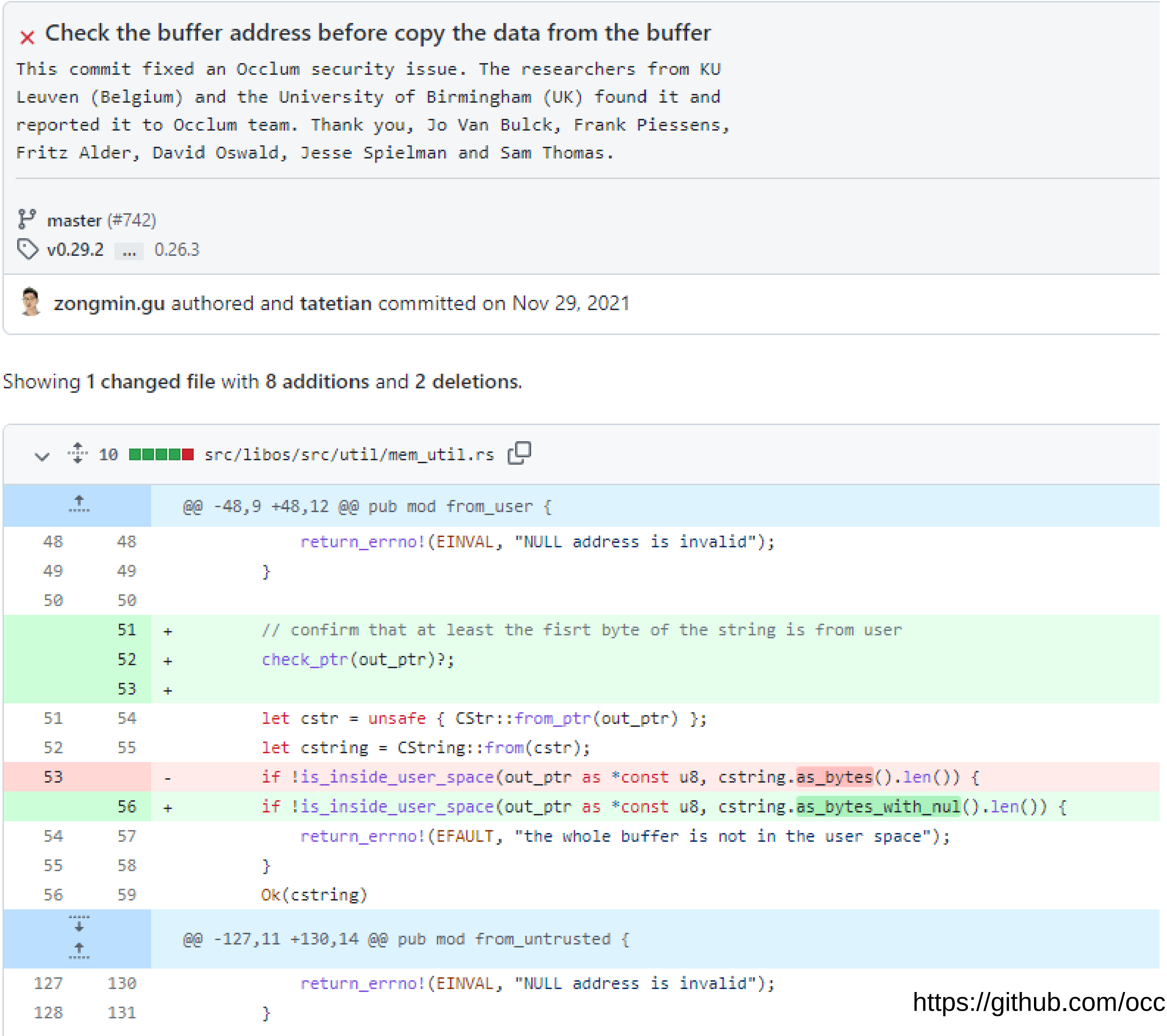
Project updates
November 2022

General updates

- Project extended until 31 July 2024
- Hiring for RF position - let us know if interested
- Organised CARDIS ’22 in Birmingham

WP 1: Security evaluation - Trusted execution

- “Poison” the CPU state before enclave entry, causing the TEE to mis-compute
    - Several CVEs and publications at ACSAC ‘21, DTRAP ‘22
- Timing leak in SGX Occlum runtime
    - CVE-2021-44421 - Occlum is written in Rust…



✕ Check the buffer address before copy the data from the buffer

```
This commit fixed an Occlum security issue. The researchers from KU
Leuven (Belgium) and the University of Birmingham (UK) found it and
reported it to Occlum team. Thank you, Jo Van Bulck, Frank Piessens,
Fritz Alder, David Oswald, Jesse Spielman and Sam Thomas.
```

master (#742)

v0.29.2 ... 0.26.3

zongmin.gu authored and **tatetian** committed on Nov 29, 2021

Showing **1 changed file** with **8 additions** and **2 deletions**.

10 🟩🟩🟩🟩🟥 src/libos/src/util/mem_util.rs

```
@@ -48,9 +48,12 @@ pub mod from_user {
                return_errno!(EINVAL, "NULL address is invalid");
            }

+           // confirm that at least the fisrt byte of the string is from user
+           check_ptr(out_ptr)?;
+
            let cstr = unsafe { CStr::from_ptr(out_ptr) };
            let cstring = CString::from(cstr);
-           if !is_inside_user_space(out_ptr as *const u8, cstring.as_bytes().len()) {
+           if !is_inside_user_space(out_ptr as *const u8, cstring.as_bytes_with_nul().len()) {
                return_errno!(EFAULT, "the whole buffer is not in the user space");
            }
            Ok(cstring)
@@ -127,11 +130,14 @@ pub mod from_untrusted {
                return_errno!(EINVAL, "NULL address is invalid");
            }
```

https://github.com/occlum/occlum/commit/36918e

WP 1: Security evaluation - Trusted execution

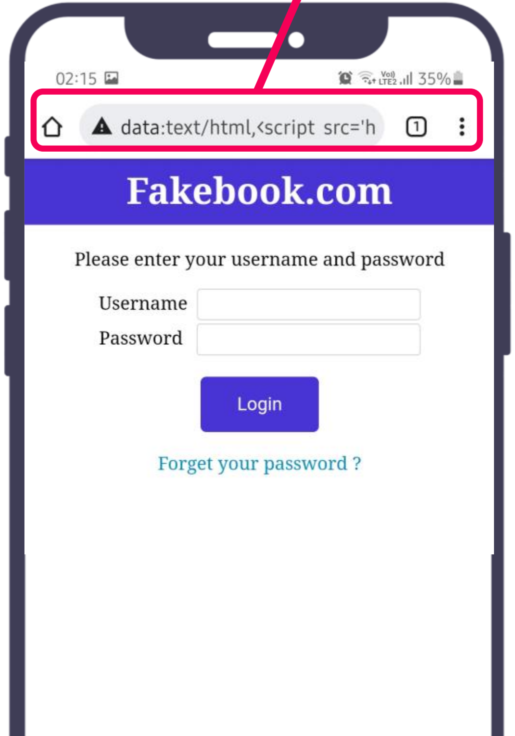
- “Poison” the CPU state outside a TEE before entry, causing the TEE to mis-compute
    - Several CVEs and ACSAC ‘21, DTRAP ‘22
- Timing leak in SGX Occlum runtime
    - CVE-2021-44421 - Occlum is written in Rust…
- “Revived" software-controlled undervolting for certain servers
    - Disclosure in progress, embargo ends 13 Jan 2023

WP 1: Security evaluation - mobile devices and more

- Attack URI parsing in mobile browsers
  - *insecure://Vulnerability Analysis of URI Scheme Handling in Android Mobile Browsers*
  - Best paper award at NDSS MadWeb ‘22

Example: Origin Spoofing via Data URI

data:text/html,<script src='http://example.com/s.js'></script><script>https://facebook.com?login_page.aspx?id=1



02:15 35%

data:text/html,<script src='h

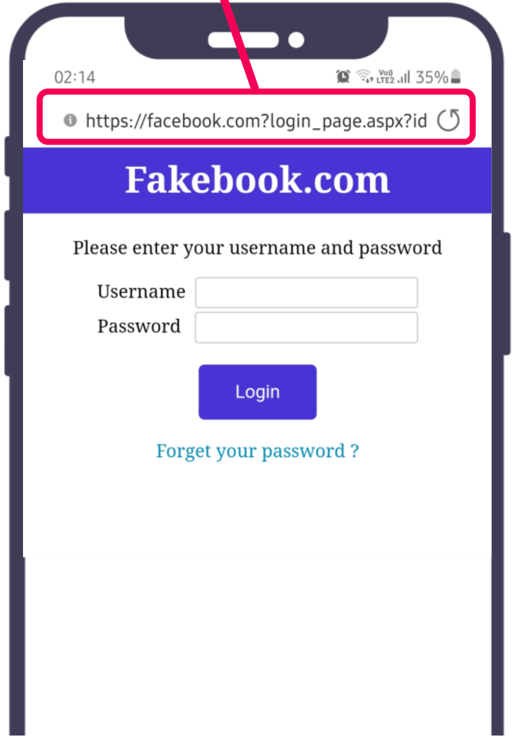
Fakebook.com

Please enter your username and password

Username

Password

Google Chrome



02:14 35%

https://facebook.com?login_page.aspx?id

Fakebook.com

Please enter your username and password

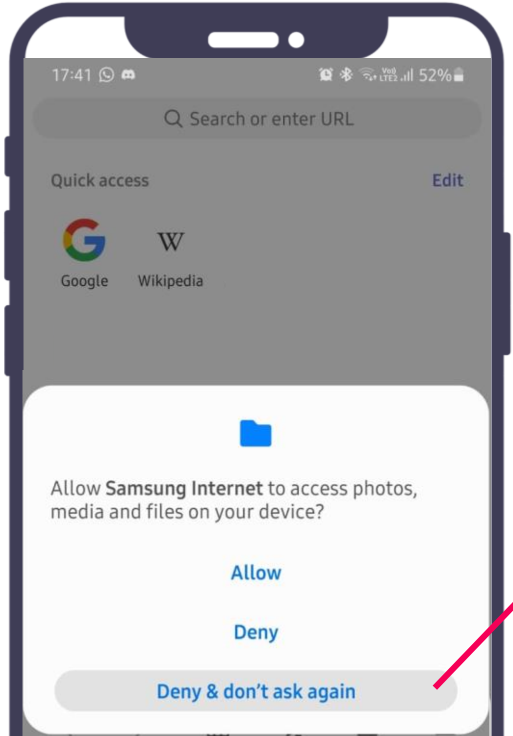
Username

Password

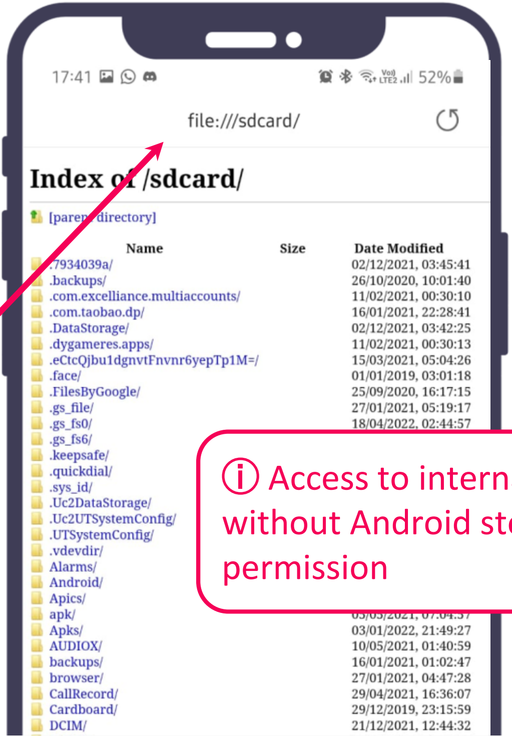
Samsung Internet

Example: Privilege Escalation via File URI

Samsung Internet



Allow **Samsung Internet** to access photos, media and files on your device?



Index of /sdcard/

[parent directory]

Name	Size	Date Modified
.7934039a/		02/12/2021, 03:45:41
.backups/		26/10/2020, 10:01:40
.com.excelliance.multiaccounts/		11/02/2021, 00:30:10
.com.taobao.dp/		16/01/2021, 22:28:41
.DataStorage/		02/12/2021, 03:42:25
.dygameres.apps/		11/02/2021, 00:30:13
.eCtcQjbu1dgnvtFnvnr6yepTp1M=/		15/03/2021, 05:04:26
.face/		01/01/2019, 03:01:18
.FilesByGoogle/		25/09/2020, 16:17:15
.gs_file/		27/01/2021, 05:19:17
.gs_fs0/		18/04/2022, 02:44:57
.gs_fs6/		
.keepsafe/		
.quickdial/		
.sys_id/		
.Uc2DataStorage/		
.Uc2UTSystemConfig/		
.UTSystemConfig/		
.vdevdir/		
Alarms/		
Android/		
Apics/		
apk/		[illegible]
Apks/		03/01/2022, 21:49:27
AUDIOX/		10/05/2021, 01:40:59
backups/		16/01/2021, 01:02:47
browser/		27/01/2021, 04:47:28
CallRecord/		29/04/2021, 16:36:07
Cardboard/		29/12/2019, 23:15:59
DCIM/		21/12/2021, 12:44:32

ⓘ Access to internal storage without Android storage permission

WP 1: Security evaluation - mobile devices and more

- Attack URI parsing in mobile browsers
  - *insecure://Vulnerability Analysis of URI Scheme Handling in Android Mobile Browsers*
  - Best paper award at NDSS MadWeb '22

- Vulnerabilities in "secure folders" on Android phones
  - *A Tale of Four Gates*, ESORICS '22

- Side-channel attacks on PQ schemes Kyber and NTRU
  - *Magnifying Side-Channel Leakage of Lattice-Based Cryptosystems with Chosen Ciphertexts: The Case Study of Kyber*, IEEE Transactions on Computers, Oct '21
  - *Reveal the Invisible Secret: Chosen-Ciphertext Side-Channel Attacks on NTRU*, CARDIS '22

WP 2: Establishing secure channels

- Formal models for Android app/device attestation protocols
  - Revealed issues in Samsung Knox V2 and recommended use of Android key attestation
  - Under revision at AsiaCCS

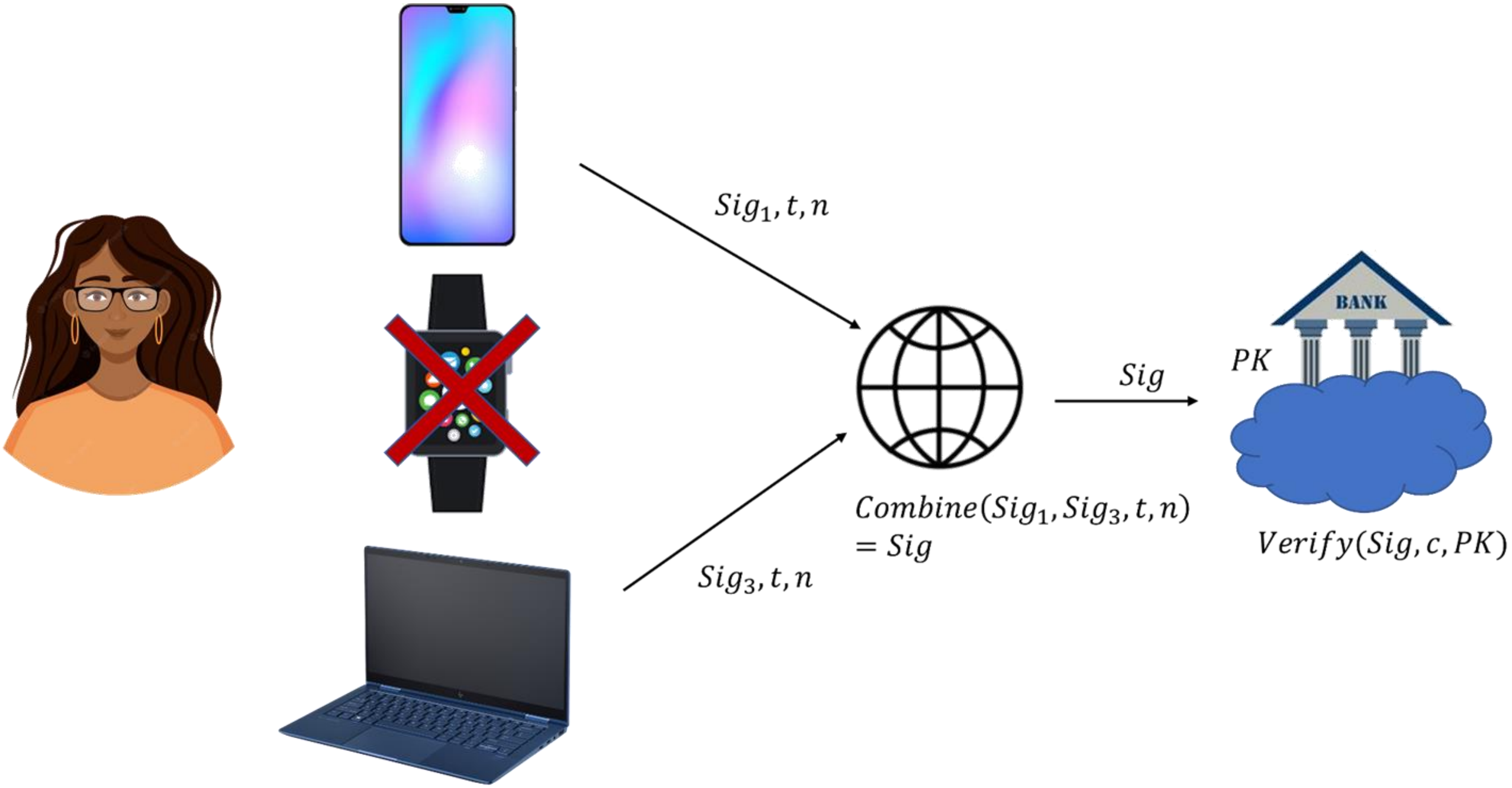
- Out-of-band channels for key exchange on medical devices
  - Establish a private channel between reader and implanted device using vibration and other channels
  - IACR eprint

- Comparing fuzzy cryptographic primitives on resource-constrained devices
  - Use “fuzzy” schemes to derive keys based on shared entropy sources in an energy-efficient way
  - Published at CARDIS ’21

WP 3: Enhancing user authentication

- Use multiple wearable devices (glasses, jewelry, … - PICO style) and threshold-based signatures for user authentication
  - *Symbolon: Enabling Flexible Multi-device-based User Authentication*, IEEE DCS 2022.
  - Birmingham/HP Labs

Symbolon authentication



WP 3: Enhancing user authentication

- Use multiple wearable devices (glasses, jewelry, … - PICO style) and threshold-based signatures for user authentication
    - *Symbolon: Enabling Flexible Multi-device-based User Authentication*, IEEE DCS 2022.
    - Birmingham/HP Labs

- Use ring signatures to generalise FIDO2 to allow one authenticator to register another
    - Allows backup tokens to be cold-stored securely, yet still registered when needed
    - Paper under review