

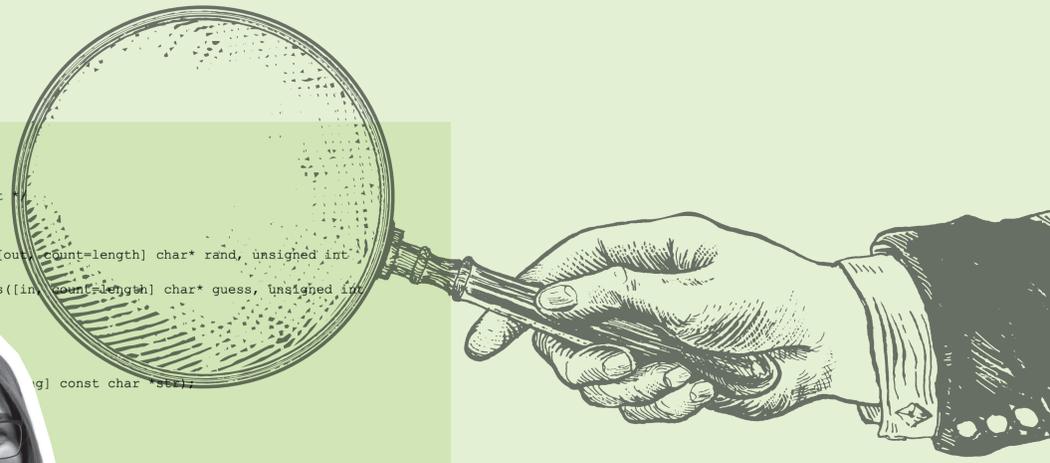
TRUSTED
EXECUTION
ENVIRONMENTS

```
enclave.edl
enclave {
    include "user_types.h" /* buffer_t */

    trusted {
        public void ecall_get_random([out, count=length] char* rand, unsigned int
            length);
        public void ecall_verify_guess([in, count=length] char* guess, unsigned int
            length);
    };

    untrusted {
        void ocall_([in, count=length] const char *str);
    };
};

enclave.cpp
#include <sgx_trts>
char* rand = null;
void ecall_get_ra([out, count=length] char* rand, unsigned int length) {
    sgx_read_rand(rand, length);
}
...
```



ANNIKA WILDE.

HARDWARE
ISOLATION

SIDE-CHANNEL
RESISTANCE

PLATFORM SECURITY



WOMEN IN IT SECURITY

Annika Wilde is a PhD student at the Chair for Information Security at Ruhr-Universität Bochum (RUB).

Within the scope of her research, she is engaged in the investigation of vulnerabilities in hardware-supported Trusted Execution Environments in order to gain insights for the development of more secure versions using open-source platforms such as RISC-V. She studied IT security in her Bachelor's degree at RUB and was able to start her PhD during her Master's degree via fast track.



casa.rub.de | hgi.rub.de

Concept and Design: HGI Annika Gödde & Conny Robrahn
Bildnachweise: CASA, Michael Schwettmann; stock.adobe.com: cherezoff, amorroz, cgterminal, channarongsds; Annika Wilde

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

HGI
HORST
GÖRTZ
INSTITUTE

RUB