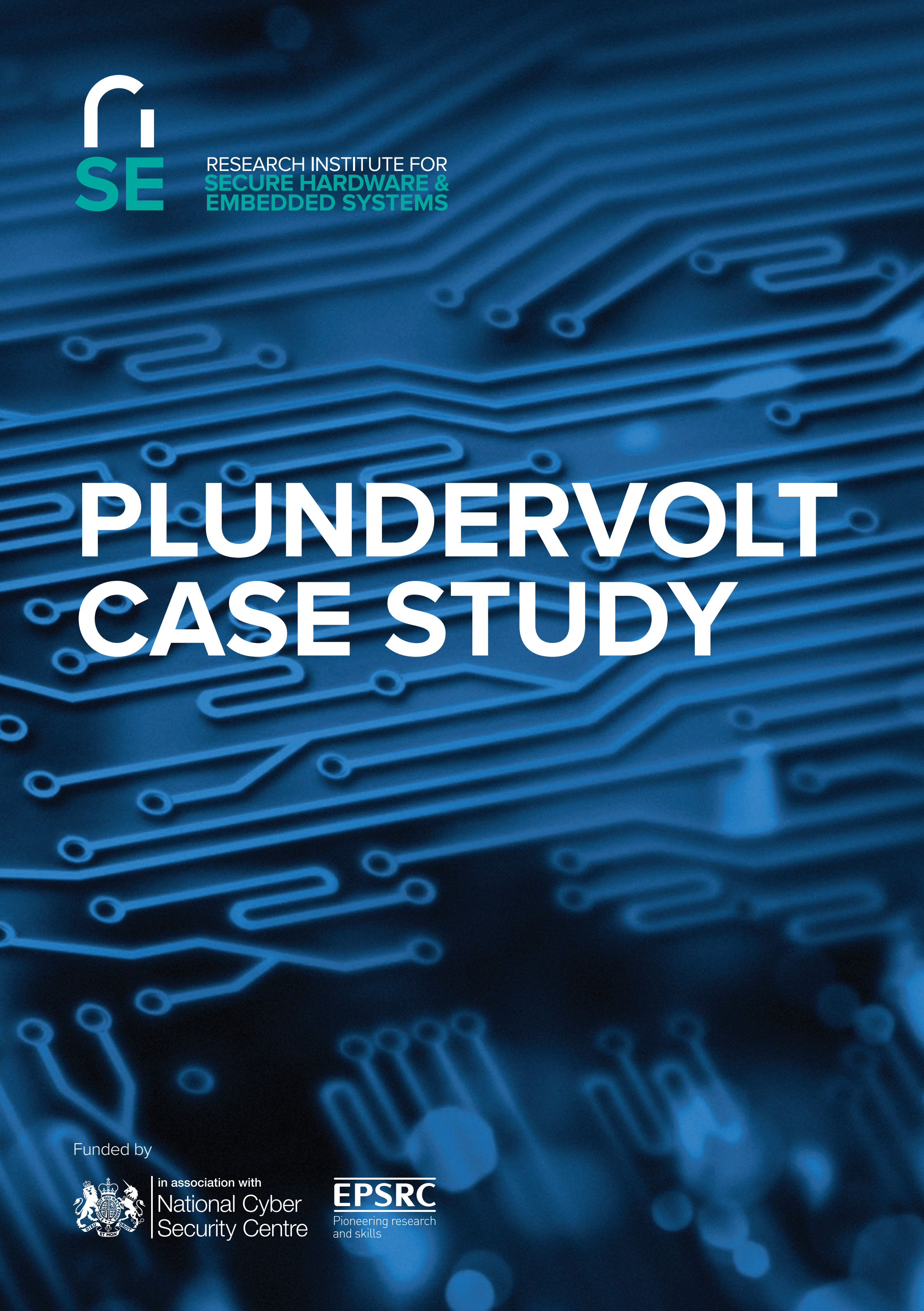

RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

PLUNDERVOLT CASE STUDY

Funded by

in association with
National Cyber
Security Centre

EPSRC
Pioneering research
and skills

UK RESEARCHERS COMPROMISE INTEL SGX SECURITY – LEADING TO FIX

Security researchers at the University of Birmingham, members of the UK Research Institute for Secure Hardware & Embedded Systems (RISE), have identified vulnerabilities with Intel's Software Guard Extensions (SGX), a technology designed to shield sensitive computations inside secured processor "enclaves".

The attack, named Plundervolt, exploits the processor's in-built voltage control features, to dynamically undervolt the processor during enclave execution, leading to errors that can leak secret information such as encryption keys.

Vulnerability

Dynamic frequency and voltage scaling are capabilities present in modern processors that enable processing speed, power consumption and heat generation to be controlled.

The researchers discovered that an undocumented Intel core voltage scaling interface was accessible, enabling SGX computations to be corrupted. Since the interface is accessible from software, any remote attacker who can become the root user can also mount the attack.

The researchers were able to demonstrate the retrieval of encryption keys, perform out-of-bounds memory accesses, and break the processor's integrity guarantees, even for securely written code.

Industry Engagement and Response

Prior to publication of results, a responsible disclosure process was undertaken, with Intel subsequently releasing a microcode update that, together with a BIOS update, allows disabling of the undervolting interface.

Impact

- Researchers identified a serious weakness in systems using Intel's SGX technology, resulting in published Common Vulnerability CVE-2019-11157.
- Intel released new microcode, to be used in conjunction with a BIOS update, to provide a fix for the attacks.
- Research gained widespread prominence in the hardware security community, with dissemination via academic papers, website www.plundervolt.com and numerous industry publications.

About RISE

The UK Research Institute in Secure Hardware and Embedded Systems (RISE), funded by the Engineering and Physical Science Research Council (EPSRC) and the National Cyber Security Centre (NSCS) seeks to identify and address key issues that underpin hardware security.

A key focus is to accelerate the industrial uptake of the Institute's research output and its translation into new products, services and business opportunities for the wider benefit of the UK economy.

ukrise.org