The expansion of edge computing is posing new challenges for cybersecurity: solutions need to offer robust security with low energy and low latency. To answer this challenge, the NEUROPULS project, funded by the European Union (EU), is taking a novel, neuromorphic approach, developing photonics-based hardware security primitives that draw on the properties of light for robust, yet lightweight, cybersecurity layers. HiPEAC caught up with NEUROPULS coordinator Fabio Pavanello (CNRS – Center for Radiofrequencies, Optics, and Microelectronics in the Alps – CROMA laboratory) to find out more.

Lighting the way to better security

The NEUROPULS photonics-based approach

What's wrong with the current security landscape?

The exponentially increasing number of edge devices is posing major challenges not only on the computing side, in terms of processing requirements, but also in terms of cybersecurity. The available surface for cyberattacks increases with the number of interconnected devices, as do the complexity and latency of authentication and encryption protocols. Current solutions that rely on, for example, storing cryptographic keys in non-volatile memory are not secure enough. As an example, hardware vulnerabilities can be leveraged to access specific memory sectors, and approaches based purely on electronic hardware security primitives present a series of weaknesses, such as being prone to machine-learning (ML) modelling and side-channel attacks, or reliability issues due to the ageing of key components, for example.

That doesn't sound good…

No, especially when you consider that applications in sectors such as banking, manufacturing, automotive and healthcare cannot function without robust cybersecurity.

Achieving robust cybersecurity isn't that simple, though, right?

Exactly. In addition to being robust to cyberthreats and reliable, security layers also need to be low power, lightweight, and low cost for large-volume applications. All these requirements set severe constraints on both the hardware and software layers of these devices, meaning that we need to develop unconventional cybersecurity approaches with superior robustness compared to current solutions.

So what's NEUROPULS doing about it?

Adopting a neuromorphic approach, which saves energy, avoiding the input / output bottleneck between memory and processing units, and which supports machine-learning (ML) algorithms, NEUROPULS targets the secure operation, communication, and integrity of edge devices. We're building security layers starting with hardware security primitives, using the unique technology developed in the project based on augmented silicon photonics platforms. This technology is readily available for our photonic accelerator, which is co-developed in the same photonic integrated circuit (PIC) as the security primitives. These primitives are the key ingredient of our approach and are based on photonic physical unclonable functions (PUFs), which have the potential for better performance compared to their electronic counterparts.

What gives photonics an advantage over electronics in this area?

The enhanced strength of our approach comes from the underlying physics of such complex photonic devices, which provide many degrees of freedom that can be exploited, making it more robust against ML or side-channel attacks. This is in stark contrast with electronic approaches, where essentially information propagates in a binary manner, thus leading to lower system complexity overall and thus potential vulnerabilities for various types of attacks.

In the software layer, we can then leverage key properties of photonic PUFs, such as high operation speed (Gbit/s) to enable lightweight security protocols. For example, a lightweight remote software attestation mechanism periodically ensures that the device has not been tampered with, protecting against unauthorized software, particularly malware, malicious software modifications and associated risks, by using the photonic PUF as the root of trust.

Any other cybersecurity protections?

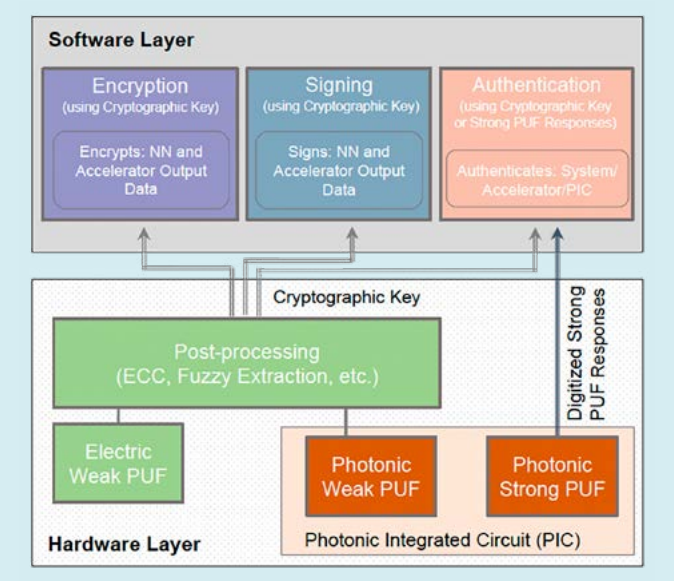
We also use encryption to protect sensitive neural-network information such as weight values and data in input / output, as well as to secure communication with third parties using the error-corrected keys generated by the photonic PUF. Finally, various lightweight authentication protocols are under investigation in the NEUROPULS project to assess the genuine identity of a given device within the network without requiring fully stable PUF responses.

What are the particular challenges of ensuring robust security for edge computing? I assume energy is going to be at a premium, for example…

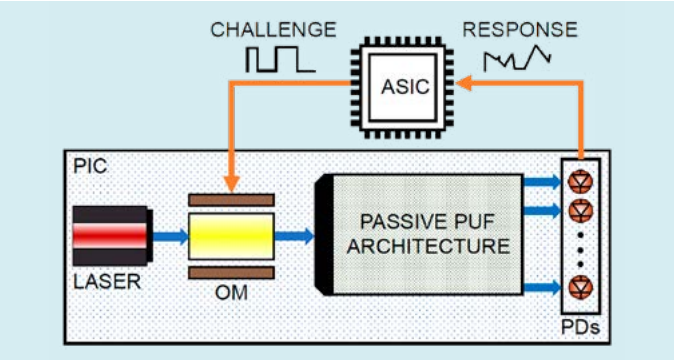
Precisely: in edge computing, the main goal is to securely process substantial amounts of data close to where these data are generated. This means that you need lightweight accelerators that can deal with massive amounts of data using little energy and with low latency, while also being protected by robust security layers. To address this problem, NEUROPULS takes advantage of the properties of light and of materials such as phase-change materials (PCMs), as well as III-V materials, to develop an ultra-low-power (sub-pJ/MAC) accelerator which at the same time presents highly robust security layers.

Sounds groundbreaking – but how would it work with existing systems?

We are co-developing processor interfaces for seamless integration in current systems. We're using RISC-V core architectures to drive our accelerator, which allow us to develop a prototype without licensing constraints. In parallel, a gem5-based simulation platform is under development to enable accelerator scaling and performance profiling, while incorporating the novel security layers.



Hardware-software communication flow for security services (Credit: 'Security layers and related services within the Horizon Europe NEUROPULS project', DATE 2024)



PUF operation considered in NEUROPULS (Credit: 'Security layers and related services within the Horizon Europe NEUROPULS project', DATE 2024)

I'm sold. What are the next steps towards commercialization, and how could this technology change the current cybersecurity landscape?

We aim to bring this technology, which is still at the proof-of-concept phase, to a much more mature technology readiness level. This would make it a realistic, scalable alternative to current insecure, power-hungry solutions for edge computing applications.

The advent of novel security primitives such as PUFs based on photonics rather than more conventional CMOS technologies, coupled with protocols which exploit their unique properties, could affect the overall supply chain and penetrate market segments that have so far been dominated by electronic solutions. This would allow us to build edge devices and sub-systems that are far more resilient to cyberthreats and fluctuations. For example, safety-critical applications such as autonomous driving could greatly benefit from security layers that outperform current solutions and that are integrated into low-power and low-latency photonic accelerators.

neuropuls.eu

NEUROPULS has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement no. 10170238. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

FURTHER READING:

F. Pavanello et al., 'Security layers and related services within the Horizon Europe NEUROPULS project', 2024 Design, Automation & Test in Europe Conference, 2024 - arxiv.org/abs/2312.09383

F. Pavanello et al., 'NEUROPULS: NEUROmorphic energy-efficient secure accelerators based on Phase change materials aUgmented siLicon photonicS', 2023 IEEE European Test Symposium (ETS), 2023 - doi.org/10.1109/ETS56758.2023.10173974

N. Marastoni and M. Ceccato, 'Remote Attestation of IoT Devices using Physically Unclonable Functions: Recent Advancements and Open Research Challenges', CPSIoTSec '23: Proceedings of the 5th Workshop on CPS&IoT Security and Privacy, 2023 doi.org/10.1145/3605758.3623502

C. Odysseas et al., 'Gem5-MARVEL: Microarchitecture-Level Resilience Analysis of Heterogeneous SoC Architectures', 2024 IEEE International Symposium on High-Performance Computer Architecture (HPCA), 2024 doi.org/10.1109/HPCA57654.2024.00047