The race for NCP cybersecurity

Olivier Zendra, Bart Coppens

The Next computing Paradigm (NCP), with its massively interconnected components, faces compounded cybersecurity and privacy issues, at all levels of its continuum. These must be addressed for the concept to succeed.

The race for NCP cybersecurity

by Olivier Zendra and Bart Coppens

The Next Computing Paradigm (NCP), characterized by its massive interconnectivity between numerous services and systems, faces significant cybersecurity and privacy challenges across its entire spectrum.

The vast number of interconnected systems and services offer a very large attack surface. Given the pervasiveness of the NCP, reaching the cyber-physical world, the potential consequences of attacks include not only the risk of leaking sensitive data and potentially leading to large economic losses, but attackers could also gain the capability to yield tangible and, in some cases, life-threatening impacts.

Implementing the NCP thus extends way beyond facilitating harmonious interactions among its myriad services, which is a challenge in itself. It fundamentally hinges on ensuring the cybersecurity of this intricate network. The acceptance of the NCP is contingent on trust, and to garner trust, effective security must be guaranteed. Significant challenges persist in establishing the necessary levels of security for the NCP, and these challenges are of critical importance to pave the way for the paradigm's acceptance and success.

This chapter contains six contributions related to cybersecurity for the NCP, four of them more related to software security and two to hardware security:

- **"The NCP cybersecurity challenges".** This article provides an overview of some of the cybersecurity challenges the NCP faces, including classical software supply chain issues, as well as challenges in this context of massively interconnected elements. The case is also made for the vulnerability of two specific domains of interconnected elements belonging to the NCP, namely critical supply chains and services (like gas and electricity supply) and healthcare infrastructures and hospitals. If the EU wants to be strong, it needs strong cybersecurity on these aspects, now.
- **"More data for the NCP implies more privacy risks"**. This article addresses the privacy issues induced by the multitude of data and communication in the NCP. Indeed, the latter includes numerous home sensors that will communicate with servers and services, and that could very easily leak private information if not properly taken care of, impairing the NCP acceptance by people.
- **"The browser: the key to your privacy on the Web"**. This article addresses browser tracking issues. Currently, and in the Next Computing Paradigm (NCP) as well, one of the major ways of interacting with the Web is through the browser. But tracking users through their browser is commonplace, and often underestimated, with the user not being aware of them. The browser is thus a keystone to user privacy in the NCP.
- **"DLT and IPFS Technologies are Paving the Way for the NCP"**. This article explains how distributed ledgers and file systems can provide the trustability and resilience to the NCP through decentralization, immutability,

and transparency of interactions and transactions, removing single points of failures. However, significant challenges remain, such as scalability, interoperability, and user adoption.

- **"Integrity at Every Link: A Roadmap to Trustworthy Hardware Supply Chains"**. This article makes the case that hardware constitutes the foundation of any computer system, and thus its integrity is crucial for cybersecurity. However, ensuring this integrity throughout the entirety of the hardware supply chain poses a significant challenge in establishing a secure computer system.
- **"Microarchitectures as Root-of-Trust in Computing Systems – Research Needs in Formal Security Analysis"**. This article explores using formal methods for verifying hardware security, a shift from the traditional software-centric approach. While computing systems rely on hardware as a "root-of-trust" for security, new vulnerabilities exist that cannot be patched in software alone. Thus, security verification and the development of defense mechanisms must be pursued at the microarchitectural hardware level, utilizing formal methods specifically tailored for security verification.

Key insights

- The NCP comprises many small components that are discovered and integrated at run time. This leads to cybersecurity risks, in software supply-chain and in inter-components interactions.
- A tremendous number of IoT devices are unsecure, especially communication-wise.
- LLM security is in its infancy.
- Many innocuous data sources like IoT-based sensors can be used alone or in combination to infer personal and private information. The NCP will merge multiple data sources, which may present privacy risks if not properly designed and implemented.
- User tracking through the browser is extremely widespread. Users are tracked almost all the time, on most websites. But browser fingerprinting has security uses that websites actively use.
- Vendors add new functionalities to browsers at a fast pace, but not enough effort is put into minimizing privacy risks.
- DLTs and IPFS are key enablers to an overall decentralized secured platform on the Internet.
- Mass adoption of this new computing paradigm will require thorough transformation of European laws and policies, including on the legal value of smart contracts.
- Design-dependent hardware Trojans are a fundamental security issue. Standard detection systems only identify known hardware Trojans.
- Hardware microarchitecture security flaws expose a very large attack surface. Vulnerabilities often arise from integrating multiple components and specific hardware-software interactions.
- Ad hoc processes that require design changes and software developer collaboration are used to mitigate hardware security issues. Security methods to address timing side channels increase manual design workload and hardware overhead.

Key recommendations

- Promote privacy-enhancing technology research to prevent data breaches or lower their impact.
- To enhance privacy, systems should be designed to not leak any data without explicit and meaningful user consent. No backdoor should be allowed.
- Invest in methods and tools to have security/privacy as a first-class citizen during the development of NCP hardware and software elements, including quantitative security metrics/properties.
- Invest in methods and tools to find vulnerabilities in existing IT systems (e.g., with static analyses on source code and behavioural analyses at runtime), and automatically prevent or mitigate them (e.g., with automated refactoring tools and blocking systems),
- Invest in automated methods and tools, possibly based on AI, for runtime detection of intrusions, attacks and privacy breaches, and active cyber defense.

- Base the critical parts of the NCP on understood open-source software and hardware, or on EU-made, trustable because audited software and hardware.
- Invest in authentication/identification of people and NCP software and hardware elements, both for end-to-end trust and tracing of suppliers
- Evaluate and improve blockchains/DLTs security and performance/scalability, both at algorithmic level and implementation level.
- Investigate the security of LLMs, with a particular focus on LLM prompt security.
- Mandate securing the radio communications of IoT systems.
- Expand mandatory EU-based, multi-level NCP elements security certification, holding IT systems providers and resellers liable for poor security, while taking the specifics of open-source projects into account.
- Invest in methods and tools that break the uniqueness of people when browsing and allow users to control fingerprinting techniques.
- Encourage browsers to block third-party cookies.
- Enforce GDPR wrt. user tracking, ensuring collected data is strictly necessary to the usages accepted by users.
- DLTs and IPFS allow combining security and controlled openness. EU companies and public authorities (including regulators) should thus rethink their models, moving from "paper-based policies" to "code-base policies" relying more on mission-oriented consortiums than competition.
- Investigate and monitor possible ways, especially security issues, to circumvent European policies using DLTs and IPFS technologies, whether by European or foreign actors
- Invest in long-term research to secure the hardware supply chain and in short-term, best-effort security to protect against malicious hardware Trojans:
    - automatic, zero-fault, non-destructive reverse engineering methods enabling end-to-end equivalency validation, and complete equivalence checking methods from design specifications to physical devices.
    - active measures to prevent malicious design modifications in hardware supply chains.
- Invest in methods and tools for SoC microarchitecture security analysis, formalising micro-architectural threat models for new non-functional formal verification approaches.
- Invest in verification-driven, secure-by-construction design providing system-wide threat coverage.
- Promote open-source and public-domain initiatives, such as the RISC-V ecosystem.

Olivier Zendra is a Tenured Computer Science Researcher at Inria, Rennes, France.

Bart Coppens is a part-time assistant professor and a post-doctoral researcher in the Electronics department of Ghent University, Ghent, Belgium.