The NCP cybersecurity challenges

Olivier Zendra, Bart Coppens

The Next Computing Paradigm (NCP), with its numerous, interconnected and communicating elements, from servers and services to IoT, sensors and user interfaces, offers an immensely vast cyberattack surface. This must be addressed for the NCP to succeed.

The NCP cybersecurity challenges

by Olivier Zendra and Bart Coppens

Key insights

- NCP services are vulnerable to software supply-chain attacks, especially with the multiplication of components providers.
- The very large number of services composing the NCP creates numerous integration and communication points between these services that have not been evaluated together for security, hence potential vulnerabilities.
- The *dynamic* composition of services creates further attack opportunities.
- The NCP reaches the physical world, with significant and impactful cybersecurity issues in critical supply chains and services, like gas and electricity supply and healthcare infrastructures and hospitals.
- A tremendous number of IoT devices are unsecure, especially communication-wise.
- LLMs security is still in its infancy.

Key recommendations

- Promote research and tools for finding and removing vulnerabilities in software supply chains.
- Promote research into the cybersecurity of systems with many small components that require secure interactions, especially in cases when the interacting components are unknown.
- Promote the cybersecurity of critical physical supply chains and services, like gas and electricity supply, and healthcare infrastructures and hospitals.
- Promote IoT cybersecurity, especially with regards to radio communications.
- Promote research in LLM security, especially and urgently against prompt poisoning attacks and leakage of information.

The NCP, an extended playground for cybervillains

Digital technology is increasingly altering the interactions of EU citizens with governments and corporations. The reliance of EU citizens on the current computing continuum, and on the coming NCP, including smartphones, smart devices, large computer systems, cloud, edge, and IoT devices, is ever growing. Social media and electronic commerce streamline and individualise customer service. Today's EU citizen disregards borders when purchasing goods, services, and commodities online. Similarly, contemporary domestic appliances have been digitized and computerised. Internet-controlled HVAC systems are a feature of smart residences, and 5G/6G smart networks will accelerate this development. The Internet of people and the Internet of machines (Industry 4.0) interweave. The risks associated with the digitalization of daily life include the potential for private data exposure or harm to critical infrastructure due to security weaknesses in software systems. Such incidents have the capacity to endanger life or state sovereignty. Consequently, cybersecurity is a crucial aspect, all the more in an NCP composed of many interacting devices and services, coming from many suppliers.

In recent decades, numerous tools and solutions have been developed with the intention of finding, reducing, or eliminating vulnerabilities such as the ones that can be found in the NCP. Static analysis [15,16], fuzzy testing [17,18], compiler-based mitigations [19], verified compilation [20], symbolic execution [21] and other such techniques are among these. However, due to the difficulty and expense of recruiting a highly qualified and specialised workforce, these techniques are seldom implemented and are sometimes unattainable. Moreover, the intricacy of complex systems, such as the ones that compose the NCP, frequently renders these approaches unworkable, even when employing developers with exceptional expertise. Decades-long, unsecured code bases continue to be a significant concern throughout the NCP computing continuum.

NCP and software supply chains attacks

In an NCP composed of many interacting services, coming from many suppliers, and even more numerous software repositories and supply chains, the sheer amount of source code for components, or even binary libraries, represents a tremendous attack surface for villains.

Indeed, security vulnerabilities exist in nearly all computing software, and attackers exploit these to circumvent the host's security, which can result in dramatic consequences. Software supply chains, which include software and its dependencies, both for production and distribution, are also subject to cybersecurity concerns. It has been demonstrated that contemporary software development, which encourages the reuse of (open-source) components, fosters innovation. This is completely logical: in this manner, software developers can specialise in their own domain while simultaneously capitalising on the expertise of others. This approach streamlines and reduces the cost of software development by utilising pre-existing code bases for numerous functionalities. Many modern software projects thus do not create every line of code from scratch, but rather depend on a multitude of other projects, libraries and frameworks. Additionally, this could enhance security, e.g. by eliminating the need for an app developer to have a Ph.D in cryptography and related disciplines to establish a secure network connection for their application. However, new cybersecurity concerns have emerged due to the increased diversity and complexity of the software, its production and deployment. This is due to the fact that security weaknesses in an extensively utilised library may impact all systems that employ this library. In fact, *software supply chain* attacks further compromise security by injecting or committing malicious code into software repositories and build chains, which then unknowingly distributes the malicious code via the standard development and distribution processes.

The Log4j vulnerability [1] is one example of such a software supply chain vulnerability. Revealed in December 2021, it could provide attackers full control of a system and sent cybersecurity stakeholders rushing [2]. Log4j is a popular logging package for Java applications that is utilised in many products as a common off-the shelf tool that many use without paying too much attention to it. The potential impact was significant yet initially unknown. Mitigating factors prevented a worst-case scenario [1], such as the fact that not all versions were affected, only certain configurations allowed tampering with the affected versions, and some systems were using a non-vulnerable Log4j API despite integrating it. This can be regarded as a free warning of what could have happened when

an apparently unimportant, known, but widespread component is vulnerable.

The "2020 United States federal government data breach" [3] with the SolarWinds attack [4] is another famous example. This included a supply chain attack on Microsoft cloud services and another one on SolarWinds' widely used Orion software. Other product vulnerabilities gave attackers more access. This cyber-espionage event is the worst in U.S. history because of its duration (8-9 months) and the targets' sensitivity and relevance. At least 200 businesses may have lost data due to the attack. NATO, the UK and the US governments, European Parliament, Microsoft, and others [3] were affected.

Phishing attempts have also targeted Python Package Index contributors, a big software repository utilised by developers worldwide. Then attackers could use the phished credentials to upload malicious versions of the packages maintained by the phished users [5].

External attackers are the most typical and acknowledged source of supply chain threats. However a legitimate developer can also go rogue and inject malicious changes. A JavaScript library developer is an interesting recent example: when the war between Russia and Ukraine began, this developer changed their code to identify if it was placed on a computer with an IP address geolocated in Russia or Belarus and, if so, wipe files [11]...

As can seen, attacks through the software supply chain are varied and common. The combination of many services in the NCP makes the magnitude of secured components even greater. Without proper expertise, experience and tools, it could become exceedingly challenging, if not unattainable, for software developers to create secure applications. Thus, providing tools able to automatically find, mitigate, and correct security vulnerabilities in source code, in a scalable way, is crucial to the NCP security.

Integration and Communication of services in the NCP

The NCP is a system composed of numerous components that must communicate with one another. Due to the dynamic and modular nature of the NCP, it will be impossible to determine at the time of design or implementation which specific services will interact with one another in a given system. This has some security-related repercussions.

First, the inclusion of numerous small components in a system may potentially enhance its security by facilitating a distinct separation of concerns. Furthermore, in adherence to the principle of least privilege [6], only those privileges necessary for each component to perform its task can be granted to it. This may potentially mitigate the effects of an attack by restricting the attacker's access to that component's capabilities.

Splitting a system into numerous components is not, however, a security panacea. Privileges that an attacker desires (access to sensitive information that could be leaked, access to a cyber-physical component that could injure people, etc.), despite being restricted to specific components, will continue to exist throughout the entire system. This first implies that it continues to be critical that every component, privileged or not, be designed and developed in a secure manner, making it difficult for an attacker to compromise a component. However, regardless of how circumscribed or limited its privileges may be, a component must still engage in communication with other components. An attacker may still attempt to leverage this. Thus developers must bear in mind that interactions with other components are not reliable, as they may be susceptible to compromise by an attacker.

Unfortunately, actual attacks do occur against systems that have been designed to be secure by being divided into multiple components. Such an attack can occur when a portion of the codebase lacks trust in the operating system but still requires security guarantees. This means that a segment of the code is isolated from the operating system, that it does not trust. However, this code still needs to interact with the outside world, and requires the operating system to mediate this. The untrusted operating system thus interfaces with the protected enclave so as to provide inputs to it, thus undermining its security goals [7,8]. Similarly, when compartmentalizing a single application into smaller components with limited privileges, it does not suffice to have one component per library, with the original library's interface working as the interface between compartments. Indeed, these interfaces are typically not designed as explicit trust boundaries [9]. An attacker could thus exploit one library/compartment, and use that to force other compartments/libraries to leak data or corrupt data, which could lead to total attacker

control, loss of confidential information, or disruption of service on the targeted library/component [9].

To evaluate the security of such a system, a first step will be to evaluate the security of the individual components. One advantage of having small components is that it should be easier to evaluate the security of each of them, rather than that of a large monolithic system. But although each component is small, the system as a whole is now composed of a large number of such components, necessitating numerous evaluations. Moreover, the absence of co-development among the various components may complicate the evaluation of the *combined* system's security, since the full scope of the system is not known at development time. Thus, it is important that research continues into analysing and improving the security of systems that consist of many small components that need to securely interact with one another, especially when it is unknown upfront exactly which components will interact.

The NCP and physical world cyberattacks

The NCP is not only all the code and software components that form it. The NCP does extend its reach to the physical world, through CPS (cyber physical systems), that are computing systems intertwined with physical systems. As such, attacks against the NCP do reach or specifically the physical world too, especially physical critical infrastructures.

Physical supply chain attacks have become (in)famous. The Aurora Generator Test [10] by the Idaho National Laboratory in 2007 first publicly demonstrated how a cyberattack could damage a 2.5MW diesel generator on the electric grid. But the first publicly widely recognised successful cyberattack on a power grid outside of a lab was the 23 December 2015 hack on Ukraine's power infrastructure [12], which left 230,000 people without power for several hours. Critical supply chain cyberattacks like this stand out. This sophisticated operation was planned and executed for months, meticulously gaining access and placing triggers in the Ukrainian electrical grid. It used many techniques, including trojans, viruses, and 1990s Microsoft Word macro-based malware. The latter proves that even dated attack vectors may cause harm. It was a full attack on both customer-delivery systems and distribution centre backup systems to blind power technicians. It also included a DDoS attack on the operators' call centres to prevent customers from reporting the problem's breadth and getting informed. Several factors suggested a Russian strike, while attribution is still unclear [12].

The "NotPetya" malware is considered the "most devastating cyberattack in history" [14]. It targeted "complete energy companies, the power grid, bus stations, petrol stations, the airport and banks" [13], critical infrastructures and mostly supply chains. World leaders including Merck, TNT Express (European division of FedEx), Maersk, DHL, India's largest container port JNPT, food firms, and others are among them. Restoration of minimum operations took days and full operations months for affected companies.

In addition to these very widespread attacks in physical supply chains, scores of more localized, yet devastating attacks have taken place in other vulnerable areas inside the NCP, especially on the *healthcare infrastructures and hospitals*.

Much evidence exists of major attacks on healthcare infrastructures throughout Europe [23]. For example, the National Health Service (NHS) of the United Kingdom was significantly impacted by the 'WannaCry' ransomware attack in 2017. The Health Service Executive (HSE) of Ireland was compromised in May 2021 by the 'Conti' ransomware. Compared to 2019, the number of successful cyber attacks targeting critical infrastructure health service providers in Germany more than doubled in 2020. In 2020, 27 significant cyberattacks were directed at French health institutions. Throughout the entire year of 2020, Spain's health sector was subject to frequent attacks, with reports of as many as 50,000 harmful incidents, of which 375 were successful [23].

The following are some tangible, specific incidents that have occurred in recent years (this list is in no way exhaustive). The hospitals in Villefranche-sur-Saône and Dax, France, were targeted by ransomware attacks in February 2021 [29]. Critical departments, including radiotherapy, radiology, the laboratory, pharmacy, automated washing cycles, and room catering, were significantly impacted by these incidents. As a consequence, operational activities were significantly disrupted, leading to treatment delays and patient rerouting. Surgical procedures were cancelled at Dusseldorf University Hospital in Germany due to a ransomware at-

tack that occurred in September 2020 [23]. In September 2022, an additional ransomware incident unfolded in Corbeil-Essonnes, which had an impact on the blood work laboratory and imaging services [30]. The University Medical Centre in Maastricht (MUMC+) was the target of a Distributed Denial of Service (DDoS) attack in January 2023 [27]. Sites affiliated with nine hospitals in Denmark were rendered inaccessible in February of that year due to DDoS attacks [27]. Early in March, Hospital Clínic de Barcelona in Spain declared a ransomware attack that rendered clinical records inaccessible, necessitating the cancellation of thousands of appointments, including non-urgent procedures and patient exams [27]. In March 2023, a ransomware attack targeted the Centre Hospitalier Universitaire Saint-Pierre in Brussels, necessitating the reliance of staff on paper records. As a precautionary measure, ambulances and medical vehicles were redirected to adjacent establishments [27]. A cyberattack was also disclosed in March 2023 by Walsall Healthcare NHS Trust, a public sector healthcare provider in the United Kingdom that serves approximately 260,000 individuals [27]. The list goes on, clearly showing the magnitude of this issue.

Indeed, these healthcare infrastructure and hospitals are typical examples of the NCP continuum, comprising highly computerized, highly interconnected services and devices, both for the purely medical technical aspects and for the management of daily operations, staff and patients. Yet, these have historically been very poorly secured against cyberattacks, making them tempting targets for cybercriminals.

In 2020, 60% of the total ransomware attacks reported in the USA were specifically directed at the healthcare sector [24]. Cybercriminals frequently targeted medical suppliers, utilizing third-party organizations to gain unauthorized access to healthcare systems and bypass internal protections. In 2021, 60% of healthcare data breaches were attributed to third-party vendors [24]. The year 2021 witnessed several significant healthcare-related data breaches, with over 40 million patient records compromised in the USA [24]. Shockingly, the prevalence of ransomware attacks on healthcare organizations soared to 66%, a substantial increase from the previous year's 34% [27]. The situation worsened in 2022, as over 50 million patient records were compromised, and a staggering total of 905 incidents were reported [24].

The situation is as bad in Europe. A comprehensive overview of the cybersecurity threats between 2019 and 2023 in the EU health sector, as well as more examples of attacks, can be found in ENISA's detailed report [31].

However, in spite of all these attacks, an August 2021 survey revealed that cybersecurity ranked as a high-priority investment for less than 11% of hospital IT executives [22]. Paradoxically, during the same period, 48% of these executives reported instances of either forced or proactive shutdowns of their systems in the preceding six months, attributable to ransomware attacks or queries. A recent report by ENISA [31] highlighted that surveys found that merely 27% of organizations surveyed within the health sector had established a dedicated ransomware defense program. Furthermore, a concerning 40% of these organizations lacked a security awareness program for non-IT staff. The shortfall in cybersecurity preparedness is further underscored by the fact that 95% of health organizations faced challenges during risk assessments, with a striking 46% having never conducted a risk analysis.

Yet, in addition to the disruption of services and risk of harm to humans, the financial costs are staggering. The average cost of a healthcare data breach reached $9.42 million in 2021 [25]. In 2023, while the average cost of a data breach across all industries was $4.45 million, the healthcare sector incurred the highest average cost among them, at $10.93 million [26]. This signifies a substantial 53.3% increase in healthcare data breach costs over the past three years.

The magnitude of the issue calls for immediate and strong action. Solutions exist, and are effective. Notably, the healthcare industry demonstrated a noteworthy average cost savings of $2 million when equipped with incident response (IR) and testing teams, in stark contrast to those without such provisions [26]. Moreover, health organizations leveraging artificial intelligence (AI) and automation in their cyber responses achieved substantial average cost savings of $850,000. The EU is also funding research projects to protect hospitals from cyber attacks, and co-funding cybersecurity procurement for hospitals, meeting 50% of the cost of new measures [28]. These efforts must be expanded until a proper level of cybersecurity is reached in healthcare infrastructure and hospitals.

Conclusion

For the NCP to succeed, it has to elicit trust from the users. The latter hinges on a proper level of cybersecurity.

This article highlighted technical areas in which the NCP could be prone to security issues and vulnerabilities, e.g. its extended code base and communications between services, as well as NCP application domains that concretely reach the physical world, namely critical supply chains and healthcare systems and infrastructures, where cyberattacks are common and known to have dramatic effects. Cybersecurity efforts are crucial in these areas and must be intensified.

Other technical areas exist nonetheless that could not be addressed in this article, but present weaknesses and contribute to the attack surface of the NCP. For example, the IoT (Internet of Things) segment of the NCP often relies on objects that radio communicate (using wifi, Bluetooth, ZigBee and many other kinds of protocols), yet most of these devices' communications are very poorly secured and easy to hack. Another area is the human interface the NCP offers to humans, such as the browser (see the relevant article in this HiPEAC Vision 2024), or LLMs (Large Language Models) prompts. The latter offer scores of new kinds of security issues that will have to be taken into account for the LLMs segment of the NCP to succeed as well.

The NCP thus presents formidable opportunities, but these opportunities could be wasted because of cybersecurity issues if they are not properly taken care of.

References

[1] Java Logging Package RCE Vulnerability. https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-067.pdf

[2] Log4j vulnerability - update from the CSIRTs Network. https://www.enisa.europa.eu/news/enisa-news/log4j-vulnerability-update-from-the-csirts-network

[3] 2020 United States federal government data breach. https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

[4] The SolarWinds Cyber-Attack: What You Need to Know. Center for Internet Security. March 2021. https://www.cisecurity.org/solarwinds

[5] Actors behind PyPI supply chain attack have been active since late 2021. Dan Goodin. Ars Technica. September 1, 2022. https://arstechnica.com/information-technology/2022/09/actors-behind-pypi-supply-chain-attack-have-been-active-since-late-2021/

[6] Saltzer, Jerome H.; Schroeder, Michael D. (1975). "The protection of information in computer systems". Proceedings of the IEEE. Institute of Electrical and Electronics Engineers (IEEE). 63 (9): 1278–1308.

[7] Stephen Checkoway, et al. Iago attacks: why the system call API is a bad untrusted RPC interface. Architectural Support for Programming Languages and Operating Systems (ASPLOS) 2013: 253-264

[8] Jo Van Bulck, et al. A Tale of Two Worlds: Assessing the Vulnerability of Enclave Shielding Runtimes. CCS 2019: 1741-1758

[9] Hugo Lefeuvre, et al. Assessing the Impact of Interface Vulnerabilities in Compartmentalized Software. Network and Distributed System Security Symposium (NDSS) 2023.

[10] Aurora Generator Test. Wikipedia. (accessed 2023-12-04). https://en.wikipedia.org/wiki/Aurora_Generator_Test

[11] Sabotage: Code added to popular NPM package wiped files in Russia and Belarus. Dan Goodin. Ars Technica. March 18, 2022. (accessed 2023-12-04). https://arstechnica.com/information-technology/2022/03/sabotage-code-added-to-popular-npm-package-wiped-files-in-russia-and-belarus/

[12] Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired. 3 March 2016. (accessed 2023-12-04). https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[13] Petya ransomware attacks. (accessed 2023-12-04). https://en.wikipedia.org/wiki/Petya_(malware)

[14] The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Andy Greenberg. September 2018, Wired. (accessed 2023-12-04). https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[15] Infer Static Analyzer (accessed 2023-12-04) https://fbinfer.com/

[16] CodeQL (accessed 2023-12-04) https://codeql.github.com/

[17] American Fuzzy Lop plus plus (AFL++) (accessed 2023-12-04) https://github.com/AFLplusplus/AFLplusplus

[18] libFuzzer – a library for coverage-guided fuzz testing (accessed 2023-12-04) https://llvm.org/docs/LibFuzzer.html

[19] Open Source Security Foundation (OpenSSF) Best Practices Working Group. Compiler Options Hardening Guide for C and C++. 2023-11-29 (accessed 2023-12-04) https://best.openssf.org/Compiler-Hardening-Guides/Compiler-Options-Hardening-Guide-for-C-and-C++.html

[20] CompCert (accessed 2023-12-04) https://compcert.org/

[21] Lacombe, G., Feliot, D., Boespflug, E. et al. Combining static analysis and dynamic symbolic execution in a toolchain to detect fault injection vulnerabilities. J Cryptogr Eng (2023). https://doi.org/10.1007/s13389-023-00310-8

[22] Cyberattacks top list of 2022 health tech hazards alongside supply chain problems, damaged infusion pumps. https://www.fiercehealthcare.com/tech/cyberattacks-top-list-2022-health-tech-hazards-ecri-report-alongside-supply-chain-problems

[23] Cyber attacks in healthcare: the position across Europe. Dorian Rees. 2021-06-18 (accessed 2023-12-04). https://www.pinsentmasons.com/out-law/analysis/cyber-attacks-healthcare-europe

[24] Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know. Joel Witts. 2023-03-28 (accessed 2023-12-04). https://expertinsights.com/insights/healthcare-cyber-attack-statistics/

[25] The Average Cost of a Healthcare Data Breach is Now $9.42 Million. Steve Alder. 2021-07-19. (accessed 2023-12-04) https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-9-42-million-2021/

[26] Cost of a data breach 2023: Healthcare industry impacts. Michelle Greenlee. 2023-08-16. (accessed 2023-12-04) https://admin05.dev.blogs.cis.ibm.net/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts/

[27] Ransomware Is a Growing Threat for European Healthcare Organisations. Jason O'Connor. 2023-04-21. (accessed 2023-12-04) https://www.keepersecurity.com/blog/2023/04/21/cyberattacks-soar-across-the-european-healthcare-sector/

[28] The race to make hospitals cybersecure. Tom Cassauwers. 2023-05-24. (accessed 2023-12-04) https://ec.europa.eu/research-and-innovation/en/horizon-magazine/race-make-hospitals-cybersecure

[29] Cyber attacks hit two French hospitals in one week. 2021-02-16. (accessed 2023-12-04) https://www.france24.com/en/europe/20210216-cyber-attacks-hit-two-french-hospitals-in-one-week

[30] Paralysed French hospital fights cyber attack as hackers lower ransom. 2022-09-22. (accessed 2023-12-04) https://www.rfi.fr/en/france/20220902-paralysed-french-hospital-fights-cyber-attack-as-hackers-lower-ransom-demand

[31] Health Threat Landscape. ENISA. 2023-07-05. (accessed 2023-12-04) https://www.enisa.europa.eu/publications/health-threat-landscape?v2=1

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

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