**Source: Joop Verbeek**
**CEPIS LSI SIN**

**Version: v.1.2 JV/23.12.2018**

**Document for:**

| | |
|---|---|
| Decision | |
| Discussion | |
| Information | |
| Publication | **x** |

# CEPIS calls for really secure ICT hardware and software in Europe

## CEPIS

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote a high standard among Informatics Professionals in recognition of the impact that Informatics has on employment, business and society. CEPIS – which represents 32 Member Societies in 31 countries across greater Europe – has agreed on the following statement:

## 1. Background

With reference to the research of its German Member Society *Gesellschaft für Informatik eV* (GI) [1] CEPIS calls for finally ending the decades-long insecurity of marketable PC and server processors and software.

Even in 2018, there are still basic information security deficits in Europe: confidentiality, integrity and also availability of data from authorities, companies and private individuals are still not guaranteed. Moreover, countless security holes are the gateway to successful attacks on data and digital infrastructures.

We shouldn't ignore the experiences of the past. Already the findings of only the last 18 years show the effort and success of espionage and sabotage in industry and politics internationally.

These findings include the European Parliament's Echelon report (2001) [2], Edward Snowden's (2013) revelations [3] and many more.

They show that intrusions into Information and Communication Technology (ICT) systems are not only exploited inadvertently, but also specifically installed security holes: backdoors in software, firmware and microcode [4]. Vulnerabilities in software and firmware security are often not published by the manufacturers. Other vulnerabilities are not known yet by the manufacturers themselves. Hence, the European citizens and companies do not know about these inherent software and firmware vulnerabilities in ICT security.

At least since 2009, most commonly used processors have built-in microcontrollers ('engines') whose firmware is inadequately documented or unpublished. This firmware is compressed and signed and, while bypassing the main processor, can be activated by third parties, even when the computer is turned off, without the user noticing. The firmware has full access to all connected devices and components and can exchange undocumented and encrypted data with the Internet. In addition, common operating systems permanently exchange data with their manufacturer, without this being completely suppressible. The content of this data can only be partially checked.

## 2. Concerns

As a result of the previous findings, we almost always have to deal with systems which (1) contain numerous - known and unknown - vulnerabilities and (2) which functionality is therefore unclear and in principle not completely controllable by the user.
The possible consequences of these security ‘failures´ or - in other words - the current damage potential ranges from the manipulation of democratic elections to political destabilization by the spying on corporate secrets to the manipulation of industrial processes.

Improving ICT security requires far more than publishing security holes that have become known to government agencies, businesses or individuals. It is also not enough to penalize the concealment of security holes. Such reactive measures are indispensable. However, secure IT infrastructures can only be achieved through a proactive approach: hardware, firmware, system software, applications and network components, security software, et cetera should be developed free of security vulnerabilities, especially free of backdoors.

The importance of ICT security is generally known to the national and European legislator. National ICT Security Acts together with the demands of the European General Data Protection Regulation (GDPR) are the first real safeguarding steps. However, devices and programs are internationally (among others) fundamentally (inherently) equipped with security gaps for espionage and sabotage purposes by the manufacturers, rendering the security measures ineffective. This has been used by the intelligence services of most countries and the worldwide organized crime for years to launch successful attacks.

Although CEPIS understands that State Security is necessary within the legal boundaries, the ICT security for innocent European citizens might be seriously compromised by the inherent insecurity of the hardware and software those citizens use on a daily basis

The prospects for effective international agreements for a political-legal solution for the mentioned inherent ICT insecurity currently appear low given the geostrategic interests of powerful actors that are massively pursued at the international level. Only a massive build-up and expansion of own hardware and software production in the EU and its Member States, driven by appropriate industrial policy and economic-strategic measures, will enable really secure systems.

The growing dependency on cyberspace has greatly increased the need for situation awareness involving three key areas: computing and network components, threat information and mission dependencies. Resilience is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. In comparison to cybersecurity, cyber resilience requires different pragmatic oriented perceptions and paradigms on handling cyberattacks. Although traditional defenses remain essential, organizations need additional technology so they can complete their missions despite successful attacks. Resilience to cyberattacks requires technical, procedural and policy changes to the infrastructure, architecture and enterprise operations. [5]

## 3. Recommendations

1. From the background of the current situation, CEPIS calls for massive efforts to achieve the digital sovereignty of the European Member States. There is a clear demand for higher ICT security proved by European and Member States' legislation and an independent and trusted control body. This applies to public authorities, companies and private users alike.
2. In order to achieve this goal, proactively an independent European development and production of really secure systems for computer hardware and software are indispensable, which don´t contain monitoring possibilities and this fact should be completely documented and understandable by all users. Such proactive strategy would also put Europe in a very competitive position. This new endeavor and even task could create a new sense of community in the light of the current ICT security challenges of the EU and the whole of Europe.

Both recommendations keep good pace with the recent Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. [6] They might be considered as an attempt to provide a particular idea for the Proposal's framework.

## References

[1] Especially its presidium working group "data protection and IT security", with Prof. Dr. Hartmut Pohl as spokesman. See: www.gi.de and the Berlin press release of August 29, 2018: see https://gi.de/meldung/gi-fordert-sicherere-it-hardware-und-software-in-europa/

[2] See Schmid, Gerhard (11 July 2001). "On the existence of a global system for the interception of private and commercial communications (ECHELON interception system), (2001/2098(INI))" (pdf – 194 pages). European Parliament: Temporary Committee on the ECHELON Interception System. Retrieved January 5, 2013.

[3] See e.g. "European parliament invites Edward Snowden to testify via video". *The Guardian.* Associated Press (Brussels). January 9, 2014. Retrieved April 11, 2015. See also: Peter, Gregor (December 12, 2013). "Edward Snowden to Make Video Appearance to European Parliament". *Der Spiegel.*

[4] Microcode is a computer hardware technique that imposes an interpreter between the Central Processor Unit (CPU) hardware and the programmer-visible instruction set architecture of the computer. See: Kent, Allen; Williams, James G. (April 5, 1993). Encyclopedia of Computer Science and Technology: Volume 28 - Supplement 13. New York: Marcel Dekker, Inc. ISBN 0-8247-2281-7. Retrieved January 17, 2016. It involves especially the so-called Intel Management Engine and the AMD Secure Technology. The Intel Management Engine (ME), also known as the Manageability Engine, is an autonomous subsystem that has been incorporated in virtually all of Intel's processor chipsets since 2008. The subsystem primarily consists of proprietary firmware running on a separate microprocessor that performs tasks during boot-up, while the computer is running, and while it is asleep. As long as the chipset or SoC is connected to current (via battery or power supply), it continues to run even when the system is turned off. Intel claims the ME is required to provide full performance. Its exact workings are largely undocumented and its code is obfuscated using confidential Huffman tables stored directly in hardware, so the firmware does not contain the information necessary to decode its contents. Intel's main competitor AMD has incorporated the equivalent AMD Secure Technology (formally called Platform Security Processor) in virtually all of its post-2013 CPUs.

See https://en.wikipedia.org/wiki/Intel_Management_Engine.

In our view, these technologies might be necessary in some professional environments, but definitely not in the private space of European citizens and the greater part of European SME´s. They are in other words not necessary for the normal processing of data by these citizens and SME´s and as such are a serious threat to ICT security.

[5] Many thanks to Prof. Radoslav Yoshinov PhD of the Bulgarian CEPIS Member Society who pointed us to the importance of the stated resilience aspect. See also the Cyber Resilience Review (CRR) by the Department of Homeland Security of the USA as Cyber Security Framework (https://www.us-cert.gov/ccubedvp/assessments) and intersect it with the five pillars of cybersecurity proposed by Symantec: Prepare/Identify, Protect, Detect, Respond and Recover; see: https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf .

[6] See https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research.