Chapter 1
From Sovereign Operating Systems to the Sovereign Digital Chain

Gaël Duval - Thanks to François Nemo for his lecture and his suggestions for the conclusion paragraph.

This Chapter was written for HaPop-3 Volume — Third Symposium for the History and Philosophy of Programming. History and Philosophy of Operating Systems — CNAM, 2016

Key words: Operating System, Internet, Software, Sovereignty, Security, Cryptography, Privacy, Open Source, CPU

Abstract

This chapter is a mostly non-technical reflection on the concept of "Sovereign Operating System" in the modern context of a globalized world. In a modern world, where software and data will potentially be driving anything in a near future, a nation sovereignty cannot be restricted to territory questions such as land, air, sea property and frontiers, or to general regulation of the national activity. It is either demonstrated or well admitted that many software pieces, including Operating System, include backdoors that can either be used to spy information on a system and send it to unauthorized parties, or be used by some unauthorized parties to take control of local or connected devices. Furthermore, nowadays, more and more third-party internet services (APIs) are integrated deeply in some modern OSes, and can be considered as fully part of them. Also some issues are suspected with networks and Internet, were massive amounts of data can be catched and analyzed illegally by hackers and countries, breaking confidentiality of information at corporate or government levels. Even computer hardware cannot be excluded from possible takeovers as there are some rising evidences that some modern CPUs include backdoors by design. Therefore, it appears clearly that the Operating System, even in its modern form, can not be considered alone regarding the digital sovereignty question, as all parts of the digital chain in data processing and transit has to be carefully examined and reinforced.

1.1 Introduction

Could software or computers have any impact on the security, the economy or even the sovereignty of a nation?

It seems that until this day of early 2000's years, the French State Secretary for Ministry of Economy, Finances and Industry, never ever wondered. The scene took place at MandrakeSoft headquarters in Paris, and the State Secretary was quite unbelieving when our team suggested that proprietary operating systems like Windows possibly had backdoors that could send information outside an organization without any permission. Sending unauthorized information outside his office, outside the French Army, outside a nuclear power plant. For example.

He was also doubtful when we suggested that those same proprietary operating systems, that are installed everywhere on computers in our country, could possibly be taken under control from the outside by foreign organization or hackers. Why? Because nobody else than the proprietary OS publisher can review its source code. Neither a government, nor a nation army, nor a sensitive organization like a nuclear power plant can know exactly that the software they have paid for and using can be trusted.

Another anecdote is about a former Ministry of Russian Government who had access to sensible information in the past. He once explained that during the war against Georgia in 2008[1], some Microsoft Windows operating systems that were used in some military material eventually stopped to work as expected. This has been a trigger in the quest for a sovereign operating system in Russia.

This sounds unbelievable, but this is theoretically possible, and practically certain that operating systems can be used to spy information or be taken under control remotely in case of need, especially if they are connected to a network.

And over the past years, citizens and governments all over the world have started to realize that now, having full control of their territories, land, sea and air, and being in full control of their regulatory laws and army, are not anymore sufficient to ensure their full sovereignty. Nation's security, integrity and privacy could be threatened by very quiet systems that have spread massively in the world since the 90s: computers, networks and software.

[1] Russo-Georgian war: https://en.wikipedia.org/wiki/Russo-Georgian_War

1.2 Not a fiction: these are real matters

A famous example of the capability of a group of nations to impact another nation is Stuxnet[2], a software worm suspected to have infected five Iranian organizations that were involved in Uranium-enrichment in 2010. Stuxnet is believed to be the result of a cooperation between the USA and Israel. It was using Windows operating systems to spread and finally attack Siemens industrial control systems in nuclear facilities in Iran.

Not directly a case related to Operating Systems is NSA[3]'s PRISM[4] program, which was launched in 2007 and disclosed in 2013 by medias. This global Internet surveillance program launched by US government, with help from Google, Facebook, Apple, Microsoft, Yahoo!, Skype..., has organized a systematic capture and analysis of most of the Internet traffic for the purpose of anti-terrorism. PRISM put another highlight both on citizen privacy concerns, economic intelligence matters and nation-wide sovereignties questions.

Some of these digital sovereignty concerns can be addressed efficiently: in response to the USA's GPS[5] positioning system infrastructure and to Russia's GLONASS, the European Union (lately) succeeded to launch its own system Galileo[6] that should start to operate in 2016/2017. In the end, this civil alternative to GPS will guarantee that EU civil and military infrastructures would still be able to rely on an efficient positioning system in case the US Army would decide to degrade the public GPS signal for instance.

The digital era is bringing a huge sovereignty challenge to nations as everything is getting interconnected as the earth's scale and information can be processed efficiently at a low cost. How can nations keep their freedom out from any external control when they cannot be certain that they control the systems that govern the logic of their modern infrastructure and sensitive activities such as national defense?

Some solutions can be found for global infrastructures (such as with the Galileo alternative) when they can cohabit with other systems. But offering security and privacy guarantees for operating systems is more difficult: if a state was designing and building a Sovereign Operating System, it would probably not be able to ensure compatibility with existing software. This would restrict its potential usage and its acceptation. And it is also becoming more of a challenge nowadays because over the years the operating system scope of features has moved from very low-level routines — that allow

[2] About Stuxnet: https://en.wikipedia.org/wiki/Stuxnet

[3] About National Security Agency https://en.wikipedia.org/wiki/National_Security_Agency

[4] About PRISM survaillance program: https://en.wikipedia.org/wiki/PRISM_(surveillance_program)

[5] About GPS https://en.wikipedia.org/wiki/Galileo_(satellite_navigation)

[6] About Galileo positioning system: https://en.wikipedia.org/wiki/Galileo_(satellite_navigation)

software programs to interact with basic hardware functionalities — to a higher-level, sophisticated, abstraction layers that can even include graphical interface toolkits. One can even wonder whether nowadays' Operating System is not starting to move to internet services and Artificial Intelligence API[7]s, which most of the time are under control of software industry giants such as Google.

1.3 Towards an enlarged definition of "Operating System"?

Having a look at Merriam-Webster and Wikipedia definitions of an operating system, today it is still referring to the kernel[8], which allows low-level interactions with the file system, peripherals, memory and CPU processing, and also, according to Wikipedia, to a software layer that provides common services for computer programs, such as a networking software stack and a graphical interface. Understand: Linux[9], Apple's macOS[10] and iOS[11], Microsoft's Windows[12], Google's Android[13]...

But for a few years, software applications have moved to web technologies, which are commonly referring to HTML5/CSS/Javascript technologies for programs that can be run within the web browser. An exception remains on mobile devices with iOS and Android, where applications need to be installed before they can be used. But more and more, many of these applications are using external Internet-based resources: dedicated backend web-services that run on remote servers. And in many cases these web-services are using "standard APIs" and very high-level toolkits designed and offered (more or less for free) by web giants, such as Facebook, Google, Twitter authentication APIs, Google Maps APIs, Google's Firebase APIs... Even Google and Apple have integrated some basic web services as core operating services, in particular for user authentication (Apple's iCloud user id and Google ID).

It has become evident that the "low-level" operating system, formerly the kernel, recently the kernel plus some middleware and a graphical interface, and currently all of these plus a web-browser, have become a "commodity

[7] Definition of an API: https://en.wikipedia.org/wiki/Application_programming_interface

[8] OS kernel definition: https://en.wikipedia.org/wiki/Kernel_(operating_system)

[9] About Linux: https://en.wikipedia.org/wiki/Linux

[10] About macOS: https://en.wikipedia.org/wiki/MacOS

[11] About iOS: https://en.wikipedia.org/wiki/IOS

[12] About Windows: https://en.wikipedia.org/wiki/Microsoft_Windows

[13] About Android: https://en.wikipedia.org/wiki/Android_(operating_system)

software layer" in a more global infrastructure at Internet scale. Now we need to consider the Operating System as a whole: from memory, storage I/Os and processors to Google & al. APIs and any Internet service.

One of the most visible sign of this recent revolution, from a user perspective, is that the "OS war" between Windows, Linux and Mac supporters — which was real by the end of the 90s and the beginning of 2000's — is now totally over. Most of the time you will use the same software and services on any of these platforms, for a simple reason: most of them are using a web-browser, such as Mozilla Firefox or Google Chrome. They are equally available on all OSes, and they offer a very high level of compatibility. Even Microsoft has started to offer Windows 10 updates for free in 2016, which means that Microsoft's business model, one of the most profitable business model of all times in the industry, has violently disrupted in a very short time and that they need to reinvent totally this model, at the Internet scale.

1.4 Concerns rise with network connectivity and Internet

Although we have moved to one dominant operating system publisher in the 80s (Microsoft) and the 90s to three now (Microsoft, Apple and Google) — which can be seen as an improvement in some way — the control of the "Operating System New-Generation[14]" by Google, Apple, Microsoft and any Android-based smartphone integrators is still problematic because many of their core components remain closed-source. They don't offer any guarantee to either individual users or organization, regarding their neutrality in term of security and absence of backdoors.

Deviances of this situation are not rare: in November 2016, two different backdoors[15] have been found by security researchers on low-cost Android devices, that would affect more than 700 millions Android devices. These back-doors continuously sending user data to servers in China...

The same month, it was also disclosed that Apple's iOS was secretly sending their user's call history to Apple iCloud servers[16].

[14] "Operating System New-Generation", used to design new forms of Operating Systems that include not only the kernel but also Interned-wide services and APIs

[15] Read about Android backdoors to China servers at: http://securityaffairs.co/wordpress/53464/hacking/android-backdoor.html and http://securityaffairs.co/wordpress/53605/mobile-2/low-cost-android-devices-backdoor.html

[16] Read about Apple sending user's call history to iCloud: https://theintercept.com/2016/11/17/iphones-secretly-send-call-history-to-apple-security-firm-says/

Worse, proprietary software publishers and software vendors are possibly cooperating with intelligence agencies to ease access to spying:

- Microsoft probably helped the NSA to allow user's interception of their communications[17]
- Encryption tools' publisher RSA is reported to have accepted 10 millions USD from the NSA in 2004 to accept using NSA-designed "Dual_EC_DRBG" random number algorithm despite many indications that this algorithm was possibly backdoored[18]

Sadly, even Open Source Operating Systems, which are known to offer better guarantees since their source code is fully opened, is not totally immune to backdoor risks: the Linux kernel security module "SELinux", which is available in many Linux distributions, has been jointly developed by Red Hat and... surprisingly the NSA[19]. It has also been alleged that Linus Torvalds was once approached by the NSA to introduce a backdoor in the Linux kernel[20].

All in all, this means that users may be concerned heavily about their privacy, and that nations can be threatened on several aspects:

- Economical impacts: unless they are disconnected from computer networks, not any single organization can now ensure that their confidential data is not escaping outside to competitors or intelligence agencies. For instance, Airbus was possibly spied by the NSA that could have abused the German intelligence infrastructure[21].

- Security impacts: as critical organization for a nation defense and army rely on computing system and software that are possibly connected to the Internet and that are possibly crippled with backdoors or trojan horse, there is no guarantee that these organizations can not be listened to or taken over by foreign organizations or hackers. Additionally, very sensible infrastructures such as nuclear power plants can be at risk because of these flaws, and expose people to major threats.

[17] Read: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

[18] Read https://en.wikipedia.org/wiki/RSA_Security#Relationship_with_NSA

[19] Read https://en.wikipedia.org/wiki/Security-Enhanced_Linux

[20] Read https://falkvinge.net/2013/11/17/nsa-asked-linus-torvalds-to-install-backdoors-into-gnulinux/

[21] Read: https://www.theguardian.com/business/2015/apr/30/airbus-could-sue-following-allegations-germany-spied-on-them-for-the-us

At this point, it's important to notice that all these aspects can probably only be considered if some people can understand them and wonder about them. This means that the digital sovereignty concerns and the way they can be addressed can only be handled by people who have enough education to understand both all technical aspects and their impact on security and users' privacy.

1.5 Would a Sovereign Operating System be a solution?

Over the past decade many nations have started to understand the stakes of a situation where a few nations have taken a huge advance and have been massively using all possible techniques to ensure that they could both listen to private and sensible information from any place in the planet such as with the PRISM program, and take control or attack others' sovereign infrastructures, such as with the Stuxnet worm.

One of the key component of modern infrastructures is the computer operating system which is the bottom layer that is supporting all data processing and transit. Proprietary operating systems such as Microsoft Windows, Apple macOS and iOS… are massively used nationwide both by individuals for their personal life and professional life, and by civil, governmental and military organizations. And they are like black boxes that do not offer any guarantee about the privacy of all the information processed and possible interactions with other organizations: competitors or foreign nations. Each of this black box, such as a computer or a smartphone can be seen as a potential trojan horse at someone else's service.

As a result, some countries have decided to build "national Operating Systems" that they could control from A to Z. These operating systems are often forked from the Linux Open Source operating system.

Red Flag[22] started in China in 1999 as a fork of the Red Hat Linux distribution, initiated by the Institute of Software Research at the Chinese Academy of Sciences. The Chinese government eventually asked Chinese Ministries to replace Windows 2000 with Red Flag, but Red Flag was terminated in 2014. The same year, China launched COS[23] "China's Operating System", a Linux-based alternative to iOS and Android.

In Russia, several initiatives tried to build a viable alternative to proprietary OSes, such as ROSA Linux[24] that started as a fork of Mandriva Linux,

[22] About Red Flag: https://en.wikipedia.org/wiki/Red_Flag_Linux

[23] About COS: https://en.wikipedia.org/wiki/COS_(operating_system)

[24] About ROSA: https://en.wikipedia.org/wiki/ROSA_Linux

and in 2015, "Open Mobile Platform" was announced as a fork of Linux-based Sailfish OS.

In Cuba, Nova[25] is a state-sponsored Linux distribution launched in 2009, possibly discontinued in 2016.

Linux-based Canaima[26] in Venezuela can also be seen as an attempt to have a Sovereign OS as it was required by a change in the Venezuelan law.

Red Star OS[27] is probably one of the most used "Sovereign operating system", as the official North-Korea OS. It is also a Linux-based operating system.

CLIP[28] is an initiative that was started in 2005 by French Government agency ANSSI[29] to build a secure operating system. It is built around a patched Linux kernel and is only available for government use and private partners[30] (despite the fact that it is based on Open Source software...). It seems to be targeted only at office workers.

Early in 2016 the French Parliament decided by law to explore possible actions to better understand and improve French Digital Sovereignty. An Institute for Digital Sovereignty[31] was created to federate actions in this field.

But it has become clear that a Sovereign Operating System, in the traditional meaning of an Operating System, wouldn't be enough to guarantee digital sovereignty for a nation: software applications, networks, the nature of digital contents, and even hardware should be considered. Additionally, considering a nationwide perspective in non-democratic countries, a Sovereign Operating System wouldn't prevent any dictator to embed software mechanisms into the OS, that would be meant to control freedom of speech and contribute to mass surveillance.

[25] About Nova https://en.wikipedia.org/wiki/Nova_(operating_system)

[26] About Canaima : https://en.wikipedia.org/wiki/Canaima_(operating_system)

[27] About Red Star OS : https://en.wikipedia.org/wiki/Red_Star_OS

[28] About CLIP: http://www.numerama.com/tech/138683-los-souverain-made-in-france-existe-deja-decouvrez-clip.html

[29] About ANSSI : http://www.ssi.gouv.fr/en/

[30] About OIV https://fr.wikipedia.org/wiki/Op%C3%A9rateur_d'importance_vitale

[31] About "Institut pour la Souveraineté Numérique" http://www.souverainetenumerique.fr/

1.6 The "digital chain sovereignty"

In fact, the whole computing chain has to be considered when some digital information is processed:

- Computer Hardware (CPU): on early 2016 it was revealed[32] that new Intel x86s CPUs were incorporating an independant small CPU that served a dedicated TCP/IP server that could be used to manage the computer. As it is totally encrypted, only Intel engineers could manage it, and possible some US government security agencies such as the NSA. In fact, according to some technical studies[33], the whole x86 architecture is likely to have security and privacy concerns.
- Operating System and applications: kernel and various OS services and software applications that run on the top of the operating system. They can possibly relay some information to non-authorized systems or be infected by a virus that can act as a Trojan Horse and perform actions within the operating system or hardware.
- External APIs used by applications: when using an external API to get or process some information, the application is sending some non-sensitive or sensitive information to the API publisher, for instance: the user location. The API publisher can also restrict access to the API to some users or countries.
- Network hardware: WAN and LAN switches and routers, firewalls. Backdoors have been found on consumer and professional hardware, and the PRISM surveillance program is collecting and analysing a big part of the Internet traffic.
- Data contents: information is processed and is moving from place to place within the computer and outside the computer, using networks. Unencrypted or low-encrypted electronic documents are easy to spy.

In order to regain sovereignty on the whole digital chain, each piece of this chain has to be examined on their technical aspects and understood. Then, actions have to be taken to ensure that this digital chain won't be taken over at some point by non-authorized parties:

- Computer hardware is maybe one of the most problematic issue because in some cases, it may be impossible to avoid some non-encrypted data to

[32] About Intel processors backdoor "Intel x86s hide another CPU that can take over your machine (you can't audit it)": https://boingboing.net/2016/06/15/intel-x86-processors-ship-with.html

[33] A technical and comprehensive study of Intel x86 plateform security and privacy "Intel x86 considered harmful", by Joanna Rutkowska, october 2015 : https://blog.invisiblethings.org/papers/2015/x86_harmful.pdf

transit through the processor and eventually be catched by some independent processor parts like they exist in new Intel processors. Routine evaluation tests are needed to detect such cases. Regulation and laws are probably a way to explore to prevent these drifts. Open-sourced hardware designs can also be an option and could be encouraged by governments and regulation.

- Operating systems: kernel security patches and isolation techniques can provide efficient ACLs to many parts of the system: memory, file system... Encryption and signature can also be introduced to guarantee software integrity and some level of privacy in data exchanges. Of course, having access to the operating system source code is a huge advantage to guarantee its integrity, security and privacy through certification programs[34]. Open Source operating systems such as Linux or BSD should be used when it's possible but suspect security features such as NSA's sponsored SELinux should be avoided. When highest confidentiality and security are needed, the use of a highly secured Open Source Operating System such as Qubes OS[35] should be considered.
- External APIs concerns are also difficult to address since they are external black boxes that can not be trusted unless you can deal with its publisher to access their source-code. Regulation and laws are probably a way to explore to prevent possible drifts. An option would be to provide alternate, independently and transparently operated APIs that would offer all guarantees.
- Network hardware: routine evaluation is needed to detect issues. Impact on data privacy can be lowered a lot if data is heavily encrypted since collected data would normally[36] be impossible to unveil its useful content. Anyhow, a real concern remains specifically with Internet routers that need to be upgraded very carefully with latest security patches to avoid possible large-scale takeovers[37] or other abuses.
- Data content: it is a key aspect of the "digital sovereignty". If all the data was heavily encrypted from its source to its destination, all the surrounding infrastructure could be open to any wind with low risk of being hijacked, although useful information about "who is talking with who" could still be catched by a third-party. This is reasonably easy to achieve for data transit by using modern encryption algorithms with long keys. It's more of a challenge to perform the same with the operating system or the processor when it comes to process the data. Difficult to compute 2+2 when operands and operator are encrypted.

[34] Read for instance about the EAL levels: https://en.wikipedia.org/wiki/Evaluation_Assurance_Level

[35] About Qubes OS, "A reasonably secure operating system": https://www.qubes-os.org/

[36] Read about the potential of Quantum Computing for cryptanalysis: https://en.wikipedia.org/wiki/Cryptanalysis#Quantum_computing_applications_for_cryptanalysis

[37] Read about German-wide routers attack: http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack/

1.7 Conclusion

In the modern world, where software and data will potentially be driving anything in a near future, a nation sovereignty cannot be restricted to territory questions such as land, air, sea property and frontiers, or to general regulation of the national activity. It has been demonstrated or is well admitted that many software pieces, including operating systems, include backdoors that can either be used to spy information on a system and send it to unauthorized parties, or be used by some unauthorized parties to take control of local or connected devices. Furthermore, nowadays, more and more third-party internet services (APIs) are integrated deeply in some modern OSes, and can be considered as fully part of them. Also some issues are suspected with networks and Internet, where massive amounts of data can be catched and analysed illegally by hackers and countries, breaking confidentiality of information at corporate or government levels. Even the computer hardware cannot be excluded from possible takeovers as there are some rising evidences that some modern CPUs include backdoors by design.

Therefore, it appears clearly that the operating system, even in its modern form, can not be considered alone regarding the digital sovereignty question, as all parts of the digital chain in data processing and transit have to be carefully examined and reinforced, technically speaking. A key aspect regarding operating system is the capability for their users to access and review all their source code. As a result, Open Source software, even if it does not offer a full guarantee for digital sovereignty, should be highly encouraged by governments, as well as open-sourced hardware designs for CPUs.

Another key aspect of data privacy and integrity is encryption. Robust and proven encryption techniques and algorithms should be used and encouraged to ensure data integrity when transiting over networks. In a modern democratic country, just like for regular mail service, it can be accepted that governments can intentionally break into some data in specific situations, when they have good reasons to fear some illegal activities. But a massive interception and analysis of all users, corporate and government data that is going through networks, just in case of a possible future benefits, should not be tolerated.

It should also be highlighted that digital sovereignty concerns and security questions can only be understood and addressed by educated people with sufficient knowledge and expertise to understand them, in particular in case of cyberattacks, that need to by analyzed in depth very quickly to be defeated. This means that the quest to Digital Sovereignty could hardly go without a strong educational system.

A strict regulation on these questions, at a world level, should also be brought to the negotiation table between nations in the future, as losing the digital sovereignty is a threat for all, comparable to nuclear weapons and climate change threats. As a particular case, EU nations should probably reinforce their links and work together as a single voice if they want to be heard and impose their views: it appears clearly that small nations have not enough power to negotiate against big blocks such as the USA, China or Russia, or even against the giant "GAFAM"[38] corporates. If EU nations could join forces and speak as only one voice, it would be easier to negotiate and suggest new models to ensure nation's sovereignty, by emphasizing on Open Source software and hardware designs, strict Internet regulation, public and/or own standards on cryptography, and a balanced policy on privacy versus security. Proposing a civil-oriented approach, just like it was done with Galileo positioning system and doing a lot of pedagogy on these questions, would also probably help to gain support from the majority of Citizens and therefore make possible a move to an ambitious and new strategy regarding the data chain sovereignty.

[38] "GAFAM" is an acronym for "Google, Apple, Facebook, Amazon, Microsoft"