

Weber, Arnd

Conference Paper

Protecting confidentiality: Regulation as a tool for securing computing environments

20th Biennial Conference of the International Telecommunications Society (ITS): "The Net and the Internet - Emerging Markets and Policies" , Rio de Janeiro, Brazil, 30th-03rd December, 2014

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Weber, Arnd (2014) : Protecting confidentiality: Regulation as a tool for securing computing environments, 20th Biennial Conference of the International Telecommunications Society (ITS): "The Net and the Internet - Emerging Markets and Policies" , Rio de Janeiro, Brazil, 30th-03rd December, 2014, International Telecommunications Society (ITS), Calgary

This Version is available at:

<https://hdl.handle.net/10419/106852>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

Protecting confidentiality

Regulation as a tool for securing computing environments

Arnd Weber

KIT-ITAS, Karlsruhe, Germany

arnd.weber@kit.edu

Paper to be presented at ITS conference in Rio de Janeiro, 2014

Acknowledgements

My thanks go to the research partners and experts from two European projects, namely the EU project “Open Trusted Computing” and the European Parliament-funded projects (STOA) on “Security of eGovernment Systems”. Responsibility for any errors rests, of course, with the author.

Introduction

During the last decades, various cryptographic technologies have been created to protect privacy in online communications, such as encryption, mixes, and blind signatures (cf. e.g. Chaum 1981). However, confidentiality is threatened as long as confidential information is “in the clear” on the computers, phones etc. at the end of the communication lines and if interested parties such as secret services or hackers have access to these machines. Edward Snowden’s revelations have shown that essential tools such as encryption software and operating systems have been undermined by the US government, as the NSA “(i)nsert[s] vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets” (Guardian 2013a).

On the other hand, there have been efforts within publicly funded research as well as within industry to provide more secure machines. However, these have not led to the deployment of machines that are unhackable in practice. This paper reviews some aspects of the state of the art, discusses key obstacles and explores possible government action to make the use of more secure computers mandatory.

This paper is based on my experience in a large EU research project on securing PCs (Weber, Weber 2012) and on the results of a discussion on the topic in the European Parliament (Jacobi et al. 2013).

(TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.

Fig. 1: From a Snowden document (Guardian 2013a)

Problems

Computer users store and communicate various types of confidential information such as business secrets or passwords. The debate around Snowden’s revelations has clearly shown that security agencies have the power to undermine the users’ systems (cf. Fig. 1).

It appears that the US has, for instance, spied on the Brazilian company Petrobras (cf. Guardian 2013b). Snowden has indicated in an interview on German TV that Siemens might be a victim as well: “There is no question that the U.S. is engaged in economic spying. If there is information at Siemens that they think would be beneficial to the national interests, not the national security, of the United States, they will go after that information and they’ll take it.” (Snowden 2014)

US officials claim not to conduct economic espionage, but to apply secret methods to understand “economic policy or behavior”, as James Clapper, director of the US National Intelligence, is quoted (Huffington Post 2014).

Another piece of evidence was the Stuxnet malware created by a large organization (Falliere et al. 2010). It is widely assumed that non-US secret services have similar capabilities. Among the nastiest threats are Trojan horses in hardware, inserted by the countries where the semiconductor chips are manufactured.

Cryptographic software typically is not proven as it relies on unproven mathematical problems. However, it is often quite reliable when implemented in line with the state of the art. But even well implemented crypto software can be circumvented by intruding the computers where confidential information is stored in the clear. A secure computing environment is therefore needed.

There are similar problems with integrity. A critical infrastructure may be attacked by modifying or deleting information.

Securing computers

Several approaches have been discussed to achieve a more secure, if not unhackable, computing environment. One way would be to use a “clean slate” approach and rebuild everything from scratch (cf. Univ. of Cambridge 2014). Leaving aside the fact that the existing IT tools which are likely to be used might be flawed, this approach has two disadvantages: legacy software might not be usable, and new malware could emerge. However, new malware would not emerge if code production were strongly controlled worldwide. This does not appear to be desirable, though, as companies, for example, would not be able produce and run code they have created. Still, we do not want to exclude the possibility that the world’s users might wish to see steps along this path.

Another approach would be to use some kind of containers, such as operating system compartments. Existing code could run in one container, while new code could run in full isolation in another one. A disadvantage of this approach is that the channels between the containers need to be strongly controlled. The computer industry is already moving slowly in this direction (La Grande, Trusted Computing, VMWare, etc.). In principle, the layer managing the containers might be intensively evaluated, e.g. tested and provided with open source code. A variant of this approach would be to use a proven kernel for isolation (Heiser 2013, proof published as mentioned in Heiser 2014).



Fig. 2: An “unsealed”, visible private image, which is only displayed if the hypervisor (managing the “containers” with several operating systems) has been checked to be correct.

A still unsolved problem is to make the whole system—including the hardware—unhackable. Some sort of trusted hardware might be needed as an interim, yet unproven solution.

One may need to use sealed images for mimicry protection. A tamper-resistant module could ensure that the sealed images can only be unsealed and thus made visible to the user if the relevant piece of software originates from a trustworthy source. The image should be so private to the computer user that someone else cannot guess what it is. Figure 2 shows an unsealed image in a hypervisor status bar (cf. Weber et al. 2009).

In any case, progress towards the implementation of such systems is taking place very slowly. For instance, a prototype the author participated in designing was never actually produced due to the expensive production process (see a video of the prototype at <http://www.open-hypervisor.org/index.php/HPvisor/news/31/>). However, US agency DARPA appears to be highly interested in having provable protection, e.g. for drones (ZDnet 2013). Variants of highly secure systems have been built for smartphones, for example, by NICTA using an L4 kernel and by the Fraunhofer SIT using SE Android for its “Bizztrust” smartphones (cf. Fig. 3).



Fig. 3: Insecure and secure containers on a smartphone (Bizztrust of Fraunhofer SIT and Sirrix).

Such systems can also be used to protect the integrity of data. Note of course that they, as such, do not provide for the availability of the computer, as in the case of a power failure or a denial of service attack.

Conclusions

If governments made it mandatory that more secure computing environments were used, industry would have to comply with it. A process just like that in the automotive industry (Ralph Nader), in the aeronautics industry or in the pharmaceutical industry can be imagined. Mallery (2013) produced a fairly comprehensive list of governmental actions: "international tariffs, regulations, taxes, insurance, legal liability, reputation damage and criminalization are among the means commonly used to shape markets and to compensate for negative externalities".

On the other hand, there will be government institutions that try to keep their power to produce Trojan horses (Pfitzmann 2008) or to produce attacks in cyber warfare (Heise, 2014, is referring to statements made by the German politicians Elmar Brok and Karl-Theodor von Guttenberg). The results of such a process will depend strongly on the relative power of the actors. The fight against short encryption keys has been won by an alliance of business and computer activists, which is encouraging. A country or a supplier leading the transition towards a computer that is unhackable in practice could possibly earn the benefits of having found a disruptive innovation (in the sense of the paper "Disruptive Competition vs. Single Standard", also to be presented at this conference, Weber 2014).

The Karlsruhe Institute of Technology, Germany, has started a project to create a global discussion and put forward concrete legislative suggestions, which can be found at https://www.its.kit.edu/english/projects_webe12_cosiso.php. KIT is active in fields such as smart electricity grids in the framework of the German energy transformation. In this field it is essential for systems to remain free of Trojan horses and malware. Concrete steps and future events could be discussed at this conference.

References

Chaum, David: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: Communications of the ACM 1981, 84-88

Falliere, Nicolas; O Murchu, Liam; Chien, Eric: W32.Stuxnet Dossier. 2010.

<http://www.symantec.com/connect/blogs/w32stuxnet-dossier>

Guardian (2013a): (Snowden documents).

<http://s3.documentcloud.org/documents/784159/sigintenabling-clean-1.pdf>

Guardian (2013b): Brazilian president: US surveillance a “breach of international law”.

<http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance>

Heise online: Cyber Security Summit: Der Krieg ist nach Europa zurückgekehrt. 03.11.2014.

<http://www.heise.de/security/meldung/Cyber-Security-Summit-Der-Krieg-ist-nach-Europa-zurueckgekehrt-2441236.html>

Heiser, Gernot (2013): White Paper: Protecting e-Government Against Attacks.

https://www.itas.kit.edu/downloads/projekt/projekt_webe12_cosiso_heiser_paper.pdf

Heiser (2014): seL4 is free! Posted on 29 July 2014, <http://l4hq.org/>

Huffington Post: China Mocks U.S. 'Hypocrisy' On Hacking Charges. 20.5.2014.

http://www.huffingtonpost.com/2014/05/20/china-cyber-spying_n_5356072.html

Jacobi, Anders; Jensen, Mikkel; Kool, Linda; Munnichs, Geert; Weber, Arnd: Security of eGovernment Systems. Conference Report. September 2013.

http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Sec%20of%20eGovernment%20-%20Conference%20Report.pdf

Mallery, John: Rebalancing Cyber Defense and Offense: Can incremental technical evolution achieve sufficient work factor impacts or are clean-slate transformational architectures required? Presentation at the Expert Workshop on “Advanced Strategies in Cybersecurity,” Federal Foreign Office, Berlin, February 13, 2013. Quoted after Gaycken, Sandro: Resetting the System, New York 2014.

<http://www.ewi.info/sites/default/files/Resetting%20the%20System.pdf>

Pfitzmann, Andreas: Contra Online-Durchsuchung. [Informatik Spektrum 31](#)(1): 65-69 (2008)

Snowden, Edward: Interview Transcript. 26.01.2014.

http://www.ndr.de/nachrichten/netzwelt/snowden277_page-1.html

University of Cambridge Computer Laboratory: CTSRD – Rethinking the hardware-software interface for security. <https://www.cl.cam.ac.uk/research/security/ctsr/>

Weber, Arnd: Disruptive Competition vs. Single Standard. The Role of Risk-averse Investors in the Decline of the European Computer and Handset Industries. Paper to be presented at ITS conference in Rio de Janeiro, 2015

Weber, Arnd; Weber, Dirk: Verifizierte Virtualisierung für mehr Sicherheit und Komfort. Datenschutz und Datensicherheit 1/2012, 43-47. English: Verified Virtualisation for more Security and Convenience. <http://www.itas.kit.edu/pub/v/2013/wewe13b.pdf>

Weber, Dirk; Weber, Arnd; Lo Presti, Stéphane: Requirements and Design Guidelines for a Trusted Hypervisor User Interface. Paper presented at: Future of Trust in Computing. Berlin, Germany, 30 June – 2 July, 2008. In: Grawrock, David; Reimer, Helmut; Sadeghi, Ahmad-Reza; Vishik, Claire (eds.): Future of Trust in Computing. Vieweg & Teubner, Wiesbaden 2009. Available at: <http://www.springerlink.com/content/v308v4228m107365/fulltext.pdf>

ZDnet: Research for unhackable UAVs could be used for BYOD: NICTA. May 28, 2013. <http://www.zdnet.com/au/research-for-unhackable-uavs-could-be-used-for-byod-nicta-7000015937/>