Weber; Arnd

Conference Paper

Europe's perspective: noncompromised terminals, free long-range communications, privacy and competition

26th European Regional Conference of the International Telecommunications Society (ITS): "What Next for European Telecommunications?", Madrid, Spain, 24th-27th June, 2015

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Weber; Arnd (2015) : Europe's perspective: noncompromised terminals, free long-range communications, privacy and competition, 26th European Regional Conference of the International Telecommunications Society (ITS): "What Next for European Telecommunications?", Madrid, Spain, 24th-27th June, 2015, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/127196

Europe's perspective:

noncompromised terminals, free long-range communications, privacy and competition

Arnd Weber

KIT-ITAS, Karlsruhe, Germany

arnd.weber@kit.edu

Paper presented at the ITS conference in San Lorenzo de El Escorial, Spain, 2015.

What next for Europe?

This paper addresses the question posed by the call for papers for the ITS conference in San Lorenzo de El Escorial (http://www.itseurope.org/): "What next for European telecommunications?" First, some problems are reviewed, such as the loss of profits and jobs in the field of information technology and security issues with current products. Subsequently, ideas for solutions are presented, such as supporting more technology competition and more unlicensed communication, legally requiring more secure computers and encouraging "privacy by design". It will be argued that regulation can play an important role in creating such markets, while products can be in competition. Future European policies could be selected from among the regulatory options presented, and but they could also be implemented in a single package.

Major problems

Loss of profits and jobs in the mobile industry

Europe has lost much of its base for producing competitive wireless communications devices and services. At the latest in 1995, with the launch of cheap PHS, as a competitor to GSM-like PDC, the level of competition in Europe fell below that in Japan, where subsequently, between 1999 and 2004, essentially all the iPhone services were discovered. The European mobile system, with Nokia at the top, was proud of technologies such as GSM and SMS, which had already become obsolete in Japan while Europe was still touting its leadership and

operators rejected the migration to IP-based services and low prices per bit (Weber et al. 2011). With its arrogant attitude, Nokia failed to copy Apple (Bouwman 2014).

Some observers may believe that Europe's digital territory was "ceded to America without a fight", as the Economist wrote (2015). But actually European industry players were fighting for their high-price, high-profit approach. For example, when GSM took off, they had actively fought to keep low-cost PHS services out of Europe (Weber 2014b). The emerging loss of competitiveness regarding services and production was already well-known by 2004, when we wrote in a report for the European Commission:

"Operators in Europe have limited experience of advanced mobile data communications … in contrast to Japan…. There is a need to favour a more user-focused perspective…. Mobile telecommunications equipment will be built cheaply in Asia, causing Europe to fall behind in the production and deployment of mobile communications systems." (Bohlin et al. 2004)

Other observers state that market fragmentation is a major cause of Europe's problems (cf. the call for papers or Oettinger 2015). While less market fragmentation would certainly reduce costs, the success of the US players covering all EU-countries shows that this fragmentation is not a major reason causing Europe's loss of leadership.

IT infrastructure compromised

Current computers and smartphones are being compromised by large organisations such as secret services. There is a long record of events; here are a few of them:

- The weakening of cryptography in implementations (Schneier 2007)
- The German "Federal Trojan" (Pfitzmann 2008)
- Stuxnet attacking SCADA systems (Falliere et al. 2010)
- The NSA's plan to "insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communication devices used by targets". (Guardian 2013)
- Implants sleeping in servers (Computer Network Exploitation, Heise 2014)
- Backdoors in hard disks (Techpowerup 2015)
- The Chinese government adopted regulation to "build so-called back doors into hardware and software" (New York Times 2015)

This list is definitely not comprehensive. One must assume that related activities compromising computer security are ongoing. European governments require that they have tools to hack into computers, as was confirmed in a European Parliament meeting (Schuster 2014). What does that mean? First, the integrity of data and the availability of systems may be compromised. Second, the confidentiality of secrets is threatened, as the attacks on products and services by Belgacom, Petrobras, Siemens and Gemalto showed (Schneier 2013, Intercept 2015). Imagine that an insider like Snowden had spied on business secrets. This

could have resulted in huge economic damage and in a significant outcry by industry, which would loudly demand change. Tools for eavesdropping on devices also become increasingly available when companies with knowledge about the backdoors sell their products to less trustworthy countries. In addition to this we must expect: “Today's secret NSA programs are tomorrow's PhD dissertations and the next day's hacker tools” (Schneier 2014). The existence of such tools and possible clones thus puts citizens’ privacy, business secrets and critical infrastructures at risk.

Loss of privacy

As widely discussed in the media, since the Snowden revelations, there has been a growing sense of a loss of privacy. For example, the debates in the European Parliament prior to approval of the European draft Data Regulation of 2013 show that the protection of personal data is an issue (cf. Leimbach 2014).

Concepts for solution

The above-mentioned “major problems” are related to some degree, in particular to large US players. The reader may think of other problems to be addressed in European telecommunications. The solutions to the problems mentioned here can be combined with any other policy options addressing other problems, just as the reader or the policy maker may prefer. Of course, I think the above problems are major ones, and hence review some potential solutions to them in this section.

More competition

Any government incentives should aim at creating competition between approaches. Given our analysis demonstrating that the reduction in competition contributed to the loss of leadership, we assume that stronger competition could lead to discoveries, in the sense of Hayek, using the market as a discovery procedure. Compared to the Japanese inventors of the subsequent iPhone services, apps, browsing, picture taking etc., European operators were too small. Hence Europe-wide spectrum regulation could support the emergence of large operators which could provide new services or new pricing schemes. This is in contrast to the Commission's proposals for creating European platforms competing with the US ones. For instance, government support for a single “Future Internet” platform does not create a fast, new player, as the discussion at ITS Brussels showed (Butcher 2014). Giants competing with each other – here Microsoft, Google and Apple – move much faster because they may fail if they do not identify new services quickly enough. The recent ideas for a single platform

for the manufacturing industry (Oettinger 2015) may not lead to the benefits of competition either.

The uncrippling of commons

As commons (WiFi) has been a huge success, it is straightforward to imagine that more commons with more power and on bands with better propagation characteristics will be appreciated by the users. As currently more than 50% of the wireless traffic is transmitted using unlicensed networks (Delgado 2014), such networks could contribute to transmitting future traffic which may comprise 1000 times as much data as today. Part of a solution could be to have a lower UHF band available with novel means of preventing congestion. It could be used for offloading a significant share of the traffic originating from mobile devices. If the band were in full use (i.e. would not reach beyond one's own property due to anti-congestion technology), licensed communication could be used instead, e.g. on some other digital dividend band. The novel type of unlicensed band would become cheaply available once users buy new routers. It would also be available in full, i.e. not just the fraction of bandwidth acquired by an operator. This suggestion was discussed at the ITS conference in Bangkok and has also been published in *Telecommunications Policy* (Elsner, Weber 2014).

I can now report about some feedback we have obtained meanwhile. Some media representatives have liked the idea of creating large meshes and reserving a fraction of the new band, per user, for forwarding communications across several hops. While UHF – with a limit of, for example, 2 W EIRP – would reach up to the radio horizon, communication partners such as in neighbouring valleys could establish contact over a much larger distance using such a mesh. To reduce interference, receivers in adjacent bands may need to be regulated.

In the above-mentioned paper, a band of 90 MHz was envisaged. A reason for this was that a band of this size would allow the digitisation of PMSE devices, which could then, as a primary service, have a very low latency of less than 1 ms, so as not to irritate a speaker or singer. The 90 MHz would be enough for hundreds of such devices.

The author is among those who proposed to the European Commission (cf. Lamy 2015) that such a band of about 90-100 MHz could be found in the 500 MHz band. The members of this group include Corinna "Elektra" Aichele, Simon Forge, Robert Horvitz, Alexander List, Sascha Meinrath, and Ryszard Struzak.[1] The propagation characteristics of the lower UHF bands would also make it possible to use commons for a significant share of wireless telephony if the new resident modems were opened for passers-by. The swift adoption of the proposal would make it possible for Europe to assume leadership on cost saving. If successful, "of-

[1] Our proposal is available at http://elektrad.info/download/Response-to-Lamy-Report-on-future-use-of-the-UHF-band_Elektra_Forge_Horvitz_List_Meinrath_Struzak_Weber.pdf and http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=9735 (Group of citizens.pdf).

floading" of even more capacity could be undertaken, e.g. by providing 200 MHz. Potentially, other regions of the world would regard this decline in costs with envy and follow suit.

A related trial using TVWS is already taking place in Berlin (Freifunk 2015).

Highly secure computers

Both US IT companies and privacy activists recently asked the US government not to subvert or undermine software (New America Foundation 2015). However, this does not solve three issues:

- Secret services may not tell the truth about their activities towards compromising computers.
- There will be weaknesses which they could exploit even if software were not compromised, such as zero-day exploits, CNE implants or hardware Trojans.
- Private IT companies do not have the incentives to improve the security of their components (e.g. software, chips) as this will increase costs without necessarily achieving a nonhackable system or significant additional revenue.

To overcome these obstacles, regulatory means could be used. It is likely that more secure computers would employ some kind of containers such as operating system compartments, which would be isolated from malware. A secured container could, however, talk to another, verified one on a remote computer. While this has already been discussed in a presentation at the ITS conference in Rio de Janeiro (Weber 2014a), two differences are noted in this paper. One is the slowly growing discussion about encrypting most Internet traffic and having European staff at European data centres. This would make widespread eavesdropping of data much more difficult (Bowden 2013, Waidner 2014, Schuster 2014). It would nonetheless still be possible for computers to be accessed to learn secrets by compromising the devices at the end. The other difference to the Rio paper is the proposal that the creation of unhackable devices could become a target of *European* policies.

Regulation of device security could be implemented in a way permitting basically two paths to be pursued:

- Proven systems: US DARPA is building unhackable drones (cf. DARPA 2014); see Heiser (2013) and Jacobi et al. (2013) for proposals for securing publicly procured computers in Europe.
- Well-tested systems, essentially testing well-specified systems until they are error-free (Kuhlmann, Weber 2009).

Regarding the potential for new systems to be compromised, a priori neither the one nor the other approach has to be given preference. Proofs could be wrong, implementers could be dishonest, and the system as a whole – including the difficult-to-verify hardware – could

have security gaps. Well-tested systems could therefore be good enough in practice. This is not to ignore clean-slate approaches (Univ. of Cambridge 2014).

Because of the difficulty in detecting Trojan horses in hardware, the production of hardware in a trustworthy fab in a trustworthy European country would be advisable, at least for sensitive processes (cf. Mitra et al. 2015). Then at least that fraction of the chips sourced locally would not be undermined. This is important, as it must be assumed that adversaries will plant Trojan horses into hardware if they cannot put them into software.

Competition among approaches would also help to solve the problem of running legacy applications. Competitors could either sell entirely new systems or have some kind of hypervisor or even a chipset to run legacy code. This is not to rule out that perhaps the same, open source components could be used in the key software kernel and hardware chips.

The plan to create regulatory incentives to make such competition emerge would have to be worked out in an effort that includes technical and legal experts (cf. https://www.itas.kit.edu/english/projects_webe12_cosiso.php). It is likely that one could learn from regulation in the sectors of health, nuclear energy or transport. For achieving economies of scale, an alliance beyond the EU would be beneficial, covering countries such as Brazil. Given its IT research and the production of security tools and car communications, Europe would be in a good position to lead along such a path. However, with the current interest of governments in hacking computers, a public push from citizens and businesses will first be needed.

Law enforcement would then have to resort to means more characteristic of James Bond, e.g. planting physical bugs and microphones, something that was the object of public discussion when the German Federal government considered using its own Trojan horse (*Bundestrojaner*) (Pfitzmann 2008). Such measures could be similar to the "load station" run by the NSA, in which a beacon was implanted in a device inside a Cisco parcel (Leaksource 2013).

Privacy by design

"Privacy by design" is a concept which has already been widely discussed, most recently when the European data protection regulation was drafted (cf. e.g. Leimbach 2014). Privacy regulation could lead organizations to avoid collecting information that can be linked back to individuals. It has been argued that such regulation could allow for new types of services to emerge. For instance, services could be pseudonymous, such as insurance services (Chaum 1981). And utilities such as electricity could be paid with untraceable eCash. A big issue is whether anonymous information can be traced back to an individual when there are entities observing all communication. While anonymous communication, untraceable networks, and other topics are important, they are of course politically "hot". After Snowden, there may be many who would like to have untraceable communications and eCommerce, and an elec-

tronic equivalent of traditional cash, as part of their free speech. Others might argue that this opens the door for libel, disinformation, spam, and terrorism. From a scientific point of view, it makes sense to spell out these options and have the public decide which to use, more precisely, how to combine the privacy-protecting tools from the toolbox. Another big issue is that anonymized data may become linkable using records from other databases. Such topics have been explored in a report produced on behalf of ENISA (Danezis et al. 2014) in the framework of the pending data regulation.

While one might believe that personalised data and its exploitation (big data mining) is the future, two facts shall be referred to in order to show how things can change:

- There is interest in using pseudonyms, as the case of the social network service Mixi in Japan shows (Japan Society 2013). Would a regulation make sense which makes it mandatory to allow pseudonyms?
- It is only 20 years ago that the Commission considered the introduction of an untraceable, electronic form of the Euro, then called ECU (electronic currency unit), for use offline (cf. Weber et al. 1995, Next 1999, Schmidt et al. 1999). This project failed because of then insurmountable patent problems. Could the approach get another chance in the future?

Of course, as long as end-user devices remain hackable, there will be no assurance of confidentiality.

A European Policy Strategy

The author envisages a European policy implementing all of the above. Without knowing what disruptions might emerge in the global IT market because of its competition, such a policy package could give markets a very different direction and thus allow for creative destruction. More neutrally argued, policies makers and the population not only have the options for fine-tuning the above proposals, but of course also for selecting among them. The author, however, retains some optimism regarding the transposition of the whole package, as similar things have proven beneficial in the past, such as WiFi on ISM bands and strong encryption in Internet communications.

Acknowledgements

The author expresses his thanks to Chris Dalton, Robert Horvitz, Armand Puccetti, Michael Wilson and to the reviewers who provided valuable comments and suggestions.

References

Bohlin, Erik; Lindmark, Sven; Björkdahl, Joakim; Weber, Arnd; Wingert, Bernd; Ballon, Pieter (Rodriguez Casal, Carlos; Burgelman, Jean Claude; Carat, Gérard, eds.): The Future of Mobile Communications in the EU: Assessing the Potential of 4G. IPTS Technical Report prepared for the European Commission – Joint Research Centre. Seville 2004. http://ftp.jrc.es/EURdoc/eur21192en.pdf

Bouwman, Harry: Why Nokia failed to nail the Smartphone market. Presentation given at ITS Brussels, 2014

Bowden, Caspar: Cloud computing, mass-surveillance and Data Protection, Presentation at the Workshop "The potentials of Cloud Computing for Europe", Brussels, available at http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/2_events/workshops/2013/20131002am/Caspar%20Bowden.pdf, accessed 11 October 2013.

Butcher, Mike: (comments on the Future Internet Public-Private Partnership). 2014 ITS Brussels

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

Danezis, George et al.: Privacy and Data Protection by Design. 2014. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

DARPA (2014): High-Assurance Cyber Military Systems (HACMS), available at http://www.darpa.mil/opencatalog/HACMS.html, accessed 14 October 2014.

Delgado, Juan: Reallocating the 700 MHz band: Should we do it? Univ. of Navarra, 2014. http://www.iese.edu/Aplicaciones/upload/OP0259E_1.pdf

Economist: Europe v Google. Nothing to stand on. Apr 18th 2015. http://www.economist.com/news/business-and-finance/21648606-google

Elsner, Jens; Weber, Arnd: Beachfront commons. Telecommunications Policy 2014, Volume 38, Issues 8–9, September 2014, Pages 709–714

Falliere, N.; O Murchu, L.; Chien, E.: W32.Stuxnet Dossier. 2010. http://www.symantec.com/connect/blogs/w32stuxnet-dossier

Freifunk: MABB:TVWS. 17.5.2015. wiki.freifunk.net/MABB:TVWS

Guardian (2013): (Snowden documents). http://s3.documentcloud.org/documents/784159/sigintenabling-clean-1.pdf

Heise online: NSA-Skandal: US-Geheimdienst hat inzwischen 100.000 Computer infiziert. 15.1.2014. http://www.heise.de/newsticker/meldung/NSA-Skandal-US-Geheimdienst-hat-inzwischen-100-000-Computer-infiziert-2085968.html?view=zoom;zoom=1

Heiser, Gernot (2013): White Paper: Protecting e-Government Against Attacks. https://www.itas.kit.edu/downloads/projekt/projekt_webe12_cosiso_heiser_paper.pdf

Intercept (2015): The Great SIM Heist. https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

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

Japan Society: A Brief History of Social Media in Japan. Oct. 16, 2013. http://japansocietyny.blogspot.de/2013/10/a-brief-history-of-social-media-in-japan.html

Kuhlmann, Dirk; Weber, Arnd: OpenTC Final Report. The Evolution of the OpenTC Architecture illustrated via its Proof-of-Concept-Prototypes. Bristol, Karlsruhe 2009, www.opentc.net, http://www.itas.kit.edu/pub/m/2009/kuua09a_contents.htm.

Lamy, Pascal: Results of the work of the High Level Group on the future use of the UHF band (470-790 MHz). (2015). https://ec.europa.eu/digital-agenda/en/news/report-results-work-high-level-group-future-use-uhf-band

Leaksource (2013): https://leaksource.files.wordpress.com/2013/12/nsa-tao-supply-chain-interdiction.jpg

T. Leimbach, D. Hallinan, D. Bachlechner, A. Weber, M. Jaglo, R. Nielsen, M. Nentwich, St. Strauß, T. Lynn, G. Hunt (2014a): Potential and Impacts of Cloud Computing Services and Social Network Websites. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf

Mitra, Subhasish; Wong, H.-S. Philip; Wong, Simon: Stopping Hardware Trojans in Their Tracks. IEEE Spectrum 2015.

New America Foundation: (Letter to Obama). May 19, 2015. https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf

New York Times: New Rules in China Upset Western Tech Companies. Jan 28, 2015. http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html?ref=business

Next Magazine: Hoe DigiCash alles verknalde. 1999. http://www.nextmagazine.nl/ecash.htm

Oettinger, Günther: Speech at Hannover Messe: Europe's future is digital. 14 April 2015. https://ec.europa.eu/commission/2014-2019/oettinger/announcements/speech-hannover-messe-europes-future-digital_en

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

Schmidt, Jan; Schunter, Matthias, Weber, Arnd: Can Cash be Digitalised? In: Günter Müller, Kai Rannenberg (Hrsg.): Multilateral Security for Global Communication. Addison-Wesley, München u.a. 1999, 301-320

Schneier, Bruce: Did NSA Put a Secret Backdoor in New Encryption Standard? 2007. https://www.schneier.com/essays/archives/2007/11/did_nsa_put_a_secret.html

Schneier, Bruce (2013): More about the NSA's Tailored Access Operations Unit. https://www.schneier.com/blog/archives/2013/12/more_about_the.html

Schneier, Bruce: QUANTUM Technology Sold by Cyberweapons Arms Manufacturers. Aug 18, 2014. https://www.schneier.com/blog/archives/2014/08/quantum_technol.html

Schuster, Stefan (ed.): Mass Surveillance. European Parliament, STOA, draft 2014

Techpowerup: NSA Hides Spying Backdoors into Hard Drive Firmware. February 17th 2015. http://www.techpowerup.com/209925/nsa-hides-spying-backdoors-into-hard-drive-firmware.html

University of Cambridge Computer Laboratory (2014): CTSRD – Rethinking the hardware-software interface for security. https://www.cl.cam.ac.uk/research/security/ctsrd/

Waidner, Michael: Stellungnahme zur Anhörung des NSA-Untersuchungssauschusses am 26. Juni 2014. http://www.bundestag.de/blob/285122/2f815a7598a9a7e9b4162d70173ecedb/mat_a_sv-1-2-pdf-data.pdf

Weber, Arnd: Protecting confidentiality. Regulation as a tool for securing computing environments. Paper presented at ITS conference Rio de Janeiro, 2014 (a). http://itsrio2014.com/public/download/Arnd%20Weber%20-%20Protecting%20confidentiality.%20Regulation%20as%20a%20tool%20for%20securing%20computing%20environments.pdf

Weber, Arnd: Disruptive Competition vs. Single Standard. The Role of Risk-averse Investors in the Decline of the European Computer and Handset Industries. Paper presented at ITS conference in Rio de Janeiro, 2014 (b). http://itsrio2014.com/public/download/Arnd%20Weber%20-%20Disruptive%20competition%20vs.%20single%20standard.%20The%20role%20of%20risk-aver-se%20investors%20in%20the%20decline%20of%20the%20European%20computer%20and%20handset%20industries.pdf

Weber, Arnd; Carter, Bob; Pfitzmann, Birgit; Schunter, Matthias; Stanford, Chris; Waidner, Michael: Secure International Payment and Information Transfer. Towards a Multi-Currency Electronic Wallet. Frankfurt 1995 (Project CAFE)

Weber, Arnd; Haas, Michael; Scuka, Daniel: Mobile Service Innovation: A European Failure. Tele-communications Policy, Volume 35, Issue 5, June 2011, 469-480.