

Towards European Network Sovereignty

Nils Rodday^{1,2}, Aiko Pras², and Gabi Dreo Rodosek¹

¹ Universität der Bundeswehr München, Neubiberg, Germany
{nils.rodday, gabi.dreo}@unibw.de

² University of Twente, Enschede, Netherlands
{aiko.pras}@utwente.nl

Abstract. Almost all major remote communication in Europe today is digital and routed through the Internet. With a very limited set of enterprise networking gear vendors, Europe's dependency on foreign networking technology is shockingly high. Through the Snowden revelations we have learned that foreign manufacturers have to collude with intelligence services to install backdoors and make their hardware remotely accessible. This PhD proposal offers a way towards European Network Sovereignty, by first designing a fingerprint to detect the router manufacturer, second finding alternative routes to avoid non-trusted routers in the routing infrastructure and third investigating the potential of Open Source concepts in the enterprise networking market.

1 Introduction

Today's world is heavily relying on the Internet as a medium to communicate and exchange information. Critical infrastructures, cars, smart homes and, of course, almost every person in the modern world that is using a smartphone, tablet or PC is connected to the Internet of Things (IoT) that is estimated to consist of more than 20 billion devices by 2020 [1] [2]. The routing infrastructure of the Internet itself is built upon networking devices that are being produced by very few international companies including e.g. Cisco (U.S.), Juniper (U.S.), HPE (U.S.), and Huawei (Chinese) [3]. Since these countries follow their own national interests and some of the systematic state sponsored wiretapping and eavesdropping programs have become public [4], the security of the infrastructure has to be questioned, as not only single entities but whole countries are totally dependent on its confidentiality, integrity and availability.

We have seen in recent years, especially through the Snowden leaks, how government agencies ensure their access to information. Several backdoors being present for years in networking devices have been documented [5] [6]. Moreover, it was reported, that backdoors are actively installed by the NSA in networking devices that are shipped to clients outside of the U.S. [4] On the other hand, the U.S. government is suspecting other governments to do likewise and banned Chinese networking gear as well as Russian anti virus products from use in U.S. government facilities [7] [8] [9]. Additionally, fiber optic cables transferring data

between Internet nodes have been proven to be tapped on by government agencies [10]. Considering the huge amount of unveiled surveillance activities, it is very likely that networking hardware that is actively used these days in European data centers is compromised and can therefore be monitored or shut down by external parties, e.g. via a kill switch, to interrupt communication.

2 Research Problem and Questions

To get closer to European Network Sovereignty we first need to be able to identify the manufacturers of Internet routers between source and destination. If a manufacturer is deemed untrustworthy the second step is to establish an alternative route only containing trusted networking devices. To solve the overall problem of trust issues between a country using foreign networking equipment and the vendor under the influence of his government, the third step is to change the current model of how networking gear is manufactured and where responsibilities lie. We believe, that the concept of Open Source is a solution to this problem. We therefore define the following research questions:

1. (Detect) How should a digital fingerprint be designed that makes the detection of the manufacturer of an enterprise networking router/switch possible?
2. (Avoid) How can routing decision in the Internet be influenced to avoid untrusted networking devices?
3. (Replace) What benefit can Open Source technology provide in the reduction of dependencies and resolve of trust issues?

3 Approach

In order to answer research question number one, we will look at existing tools and techniques of detecting and fingerprinting IT hardware within networks in general, and then drill down on the specifics of enterprise networking equipment. The most important tool to mention here is Nmap, an open source network security scanning tool which is considered the swiss army knife within the network security community [11]. One challenge that can already be foreseen at the current state and has to be overcome is that enterprise providers like to keep their infrastructure details confidential and therefore try to block any scanning related activities within their networks. Another approach is to fingerprint routers by observing their normal behaviour (e.g. ICMP messages), instead of scanning the device itself (TCP/UDP ports). One study looked at initial TTL values of ICMP replies in response to certain packets to fingerprint routers [12]. Moreover, the same authors used again ICMP replies to detect middleboxes by comparing the original packet with a copy of the packet encapsulated in the ICMP reply [13]. Apart from initial TTL values, there has no other literature been found on other features that could be utilized to fingerprint a router, but the authors in [12] suggest additional research potential. Also, we plan to utilize projects such

as PlanetLab [14] with numerous vantage points to perform scans of Internet Service Provider (ISP) networks in order to build an inventory of currently used devices.

Once an identification of enterprise networking hardware is possible, the next step is to investigate if we are able to influence the routing infrastructure in such a way that untrusted routers on the route to our packet destination can be avoided. This answers research question number two. As the routing protocol Border Gateway Protocol (BGP) is required of most ISPs to establish routing between one another, the approach to answer this research question is to carry out a review of existing techniques and methods on BGP and investigate whether any of these can be leveraged to aid in influencing BGP in such a way that non-trusted routers can be avoided.

To answer research question number three, we will first look at the current model of how enterprise routers and switches are build. They are shipped as one device where hardware and software are produced by the same manufacturer. It is not possible for the buyer to deviate from the preinstalled Network Operating System (NOS). A thriving paradigm that separates the data plane (hardware) from the control plane (software) is Software Defined Networking (SDN) [15]. It allows the user to separately purchase hardware and software (just like in the PC/server market). A router from one manufacturer can be bought and software from another manufacturer be installed. From a security perspective SDN has many advantages, the most important one is that software is more likely to be released as Open Source and therefore can be checked and altered by everybody themselves. The concept of Open Source resolves trust issues, as it is not necessary anymore to trust the vendor. Also, more flexibility is introduced, as the buyer can make modifications to the existing NOS. The use of SDN allows innovation in both, the hardware and software segment independently from each other and smaller companies have a lower entry barrier to enter the enterprise networking market as they can only focus on one part instead of having the need to provide a complete solution. A tool that will be utilized in order to evaluate SDN architectures is Mininet [16]. We plan to evaluate the current status of SDN and its future potential. Moreover, we would like to build prototypes to answer this research question.

4 Final Considerations

The PhD research proposed is aiming at developing a fingerprint for Internet routers and exploring possibilities of finding alternative routes containing only trusted devices. Also, we will investigate the potential of Open Source concepts in the networking market. Together, the proposed approach is reducing Europe's dependency on foreign enterprise networking equipment and therefore paving the way towards European Network Sovereignty.

5 References

- [1] Mohamed Ali Feki et al. “The internet of things: the next technological revolution”. In: *Computer* 46.2 (2013), pp. 24–25.
- [2] Sam Lucero et al. “IoT platforms: enabling the Internet of Things”. In: *IHS Technology white paper* (2016).
- [3] Christian Canales, Joe Skorupa, and Naresh Singh. “Market Share Analysis: Enterprise Network Equipment, Worldwide, 2016”. In: *Gartner Database ID: G00328325* (2016).
- [4] Glenn Greenwald. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. USA: Metropolitan Books, 2014. ISBN: 162779073X, 9781627790734.
- [5] Stephen Checkoway et al. “A systematic analysis of the Juniper Dual EC incident”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2016, pp. 468–479.
- [6] Bill Hau, Tony Lee, and Josh Homan. *SYNful Knock - A Cisco router implant*. 2015. URL: https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html.
- [7] Rob LeFebvre. *New bill seeks to ban Huawei from any US government contracts*. 2018. URL: <https://www.engadget.com/2018/01/13/bill-ban-huawei-us-government-contracts/>.
- [8] *H.R.4747 - Defending U.S. Government Communications Act*. 2018. URL: <https://www.congress.gov/bill/115th-congress/house-bill/4747>.
- [9] Dustin Volz. *Trump signs into law U.S. government ban on Kaspersky Lab software*. 2017. URL: <https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4>.
- [10] Mike Wheatley. *How The NSA Taps Undersea Fiber Optic Cables*. 2013. URL: <https://siliconangle.com/blog/2013/07/19/how-the-nsa-taps-undersea-fiber-optic-cables/>.
- [11] Gordon Fyodor Lyon. *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure, 2009.
- [12] Yves Vanaubel et al. “Network fingerprinting: TTL-based router signatures”. In: *Proceedings of the 2013 conference on Internet measurement conference*. ACM. 2013, pp. 369–376.
- [13] Gregory Detal et al. “Revealing middlebox interference with tracebox”. In: *Proceedings of the 2013 conference on Internet measurement conference*. ACM. 2013, pp. 1–8.
- [14] *Planet Lab Project*. 2007. URL: <https://www.planet-lab.org/>.
- [15] Diego Kreutz et al. “Software-defined networking: A comprehensive survey”. In: *Proceedings of the IEEE* 103.1 (2015), pp. 14–76.
- [16] Mininet Team. *Mininet: An instant virtual network on your laptop (or other pc)*. 2018. URL: <http://mininet.org/>.