Abstract— **The material released by Edward Snowden has raised serious concerns about pervasive surveillance. People worry that their privacy is not properly protected when they are using the Internet. Network product vendors also encounter the doubts on the security of their products (e.g., routers, switches, firewalls). Such doubts are seriously damaging the Internet ecosystem. In this paper we try to analyze the affects brought by the Snowden scandal on our ability to trust products at the core of the Internet and discuss what the standard organization can do to help vendors address these security concerns.**

Thoughts of Strengthening Network Devices in the Face of Pervasive Surveillance

Dacheng Zhang, Fuyou Miao

Huawei

{zhangdacheng, fuyou.miao}@huawei.com

I. Introduction

There are lots of discussions in dealing with the risks of pervasive surveillance since the National Security Agency scandal exposed by Edward Snowden [1]. In IETF, pervasive surveillance has been regarded as an attack. In addition, IETF founded a mailing list, perpass, to lead the discussion of strengthening the Internet protocols for better privacy protection. This paper tries to discuss the negative effects introduced by pervasive surveillance on the Internet industry from the perspective of network product vendors and discuss whether there is anything we can do to mitigate the problems imposed by this new type of attack.

The released NSA ANT catalog [2] shows that NSA has developed a set of tools used to compromise the network devices (e.g., routers and firewalls) of multiple vendors and install backdoors on them. The compromised devices then becomes unwitting collaborators and can be taken advantage of by attackers performing pervasive surveillance to get their interesting information or smuggling other malware for further attacks. Currently, the security of the network devices is being challenged by the customers. In addition to security drawbacks caused by defective implementations, people suspect that a vendor may join the attack and embed backdoors or particular security features in to their devices to meet government demands. As a result, the government or organizations can easily spy. The issue of lacking trust is seriously damaging the Internet ecosystem. Operators depend on a diversity of products in order to meet security and other objectives. Vendors are facing difficulty in markets where governments they work with closely are not trusted, reducing operator and user choice.

In this paper, we try to classify the pervasive surveillance attacks into approved pervasive surveillance attacks and un-approved pervasive surveillance attacks. The approved pervasive surveillance is normally performed by the governments with the name of national security and under the assistance of owners of the equipments (e.g., operators). We do not try to discuss how to protect network devices in the legal pervasive surveillance attacks because in this case the network devices are not compromised actually. Instead, in this paper, we focus on unproved pervasive surveillance where attackers attempt to manipulate certain network devices for surveillance purposes without getting permissions from the owners of the equipments.

The remainder of this paper is organized as follows. In Section 2, we briefly introduce the background of pervasive surveillance. In Section 3, we discuss how this problem affects network product vendors and what we should do to help vendors to mitigate such negative influences. Then, in Section 4, we discuss what the standard organizations like IETF and W3C can contribute in this work. Section5 is the conclusion.

II. Attacks on Network Devices

Compromising network devices has been regarded as an important method in performing pervasive surveillance. Through the backdoors or malware installed on network device, attackers may be able to re-direct the traffics that they are interested to the specified targets. The key material and other statistic information can be also valuable to the attackers.

In existing attacking scenarios, the network devices various from ISP routers for home using to the firewalls of enterprises could become the potential targets in pervasive surveillance. For instance, in [3], it is disclosed that some IPS routers provided in UK are deployed with costumed firmware. A second IP address is assigned to such a router, which is used by the device to join a spy network automatically. After that, attackers can direct the interested traffic to the spy network and wiretap the communications of home/ office networks. All the operations are unaware to users. In addition, the NSA ANT catalog lists 50 pages of costumed hardware or software spy tools. If an attacker can physically access the network device, the attacker may be able to compromise the devices by physical attacks. Some hardware tools can be installed on the network devices and secretly collect information and sent them to the requested places. Some software tools (e.g., HEADWATER and FEEDTROUGH) can help an attacker employ the drawbacks in the software or operation systems deployed on certain devices to inject backdoors and manipulate the device to perform further attack operations. Although the released material of NSA does not disclose any novel methodology in attacking network devices, the scales of the attacks and the number of affected victims is surprisingly large. In order to deal with the pervasive surveillance issue, we need to consider the countermeasures at each critical step in achieving a pervasive attack, and enhancing the attack tolerating capability of network devices is one of them.

III. Dilemmas of Vendors

The disclosed documents have raised the concerns of people on the vulnerability of the network devices to the passive attacks performed by NSA or other organizations. The ecosystem of vendors is becoming harder. Some vendors have met problems in the abroad markets because their products are suspected to have backdoors for adversaries to perform attacks. In order to re-construct the confidence of people on the security of their products, there are two problems that product vendors have to address.

The first problem is how to improve the capability of protecting network devices against illegally manipulations on the hardware and software. The second problem is how to prove to the customers that they are innocent in pervasive surveillance attacks. That is, vendors need to convince customers that there is no backdoor or malware injected in their network devices to benefit the attacks before they are provided to customers.

To address the first problem, vendors need to consider the potential security risks more carefully in the design of network devices. Integrity verifying capability on the hardware and software is desired. For instance, if the CF card containing the operation system of a router is replaced by an adversary, the owner of the equipment should be able to notice that. However, this function is missed in quite many network products. In addition, it is desired for vendors to publish the design details of the products and provide sufficient functions for clients to check whether certain hardware or software of a device has been improperly modified. There are various techniques that could be used for this purpose. For instance, a vendor may sign its firmware and publish the signature so that customers can ensure the vendor is releasing the same firmware to everyone. In addition, if the firmware is used by many customers, back doors or drawbacks may be easier to detect. Actually, the authors of [3] detect there are backdoors in the firmware of ISP routers by comparing the firmware with the firmware published over the network.

The second problem is very hard to be addressed by a single vendor or even by vendors themselves. Any third party hardware (e.g., chips) or software (e.g., compile tools, applications) used in network devices may potentially contain backdoors. Vendors lack sufficient resources and technical capabilities to detect all of them. It is reasonable to predict in future there will be some trusted third parties (e.g., neutral testing labs) which can be more professional to evaluate the security conditions of hardware and software and publish the evaluating results.

IV. What Standard Organizations Can DO

At least the following work can be done by Standard organizations such as IETF to help vendors in addressing the first problems mentioned above:

- Discuss the best current practice that can protect network devices from being taken advantage of to perform pervasive surveillance attacks in different scenarios and find gaps. Such instructions are valuable for both vendors and customers. In practice, some security solutions defined by IETF protocols are not widely used because customers do not realize they are necessary or important. The encryption function provided in SNMP is a good example.
- Design the solutions to enhance the capability of protecting network devices against illegally manipulations.

The owners of network devices should be able to detect any integrity breaches on the software or hardware of their network devices. For instance, if it is a good idea to sign the firmware of network devices, it may be worthwhile to discuss how the device owners can verify such signatures remotely in IETF.

- Provide the standards describing how to design secure network devices. There is already some similar work such as the US standard FIPS 140. But this work could focus more on the practices for handling privacy.

V.CONCLUSIONS

Attacks on network devices have been an active research area for a long period. However, after the NSA scandal, it has been realized that the network devices are more vulnerable than people have imagined. Using the tools developed by NSA, an attacker can effectively hack into the network devices (including routers and firewalls) of different vendors. In pervasive surveillance, the compromise of network devices is normally regarded as a preparation for further attacks. Therefore, enhancing the security strength of network devices is also an important countermeasure to the pervasive attacks. In addition, in this paper we clarify that the doubts of the security strength of network devices have caused lots of problems to the vendors. They lack methods to prove their innocence, and this problem will eventually affect the healthy development of global Internet industry. Re-building people’s confidence on the network security needs the efforts of the whole industry and could take a long period. However, for a better Internet in future, this work must be done. We that believe standard organizations such as IETF can play an important role in this work since they provide a platform for security experts to discuss how to push work into a correct direction.

VI. REFERENCES

[1] The Guardian, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", 2013, <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>.

[2] Applebaum, Jacob and Stöcker, Christian, 2013 <Shopping for Spy Gear: Catalog Advertises NSA Toolbox>.

[3] “Full Disclosure”, 2013,<http://cryptome.org/2013/12/Full-Disclosure.pdf>.