Jens Kaessner
Switzerland

Canadian Multistakeholder project draft report IoT security recommendations

April 4, 2019

Dear Sirs

With the following, I want to comment to the IoT draft report Canada.
I learned about the IoT draft report as a member of ISOC Switzerland. I have two decades of experience in the development of telecoms and internet regulation.

I'd like to inform you about a functioning solution to the problem of IoT security.
In my opinion, the NRWG's IoT draft report is on the right track with its abstract wish for network control of IoT device security. But there exists a functioning solution is simpler and more robust than all the propositions otherwise heard concerning IoT security. In particular, it can be locally implemented, without trying to educate IoT device producers worldwide.

The functioning solution is SCION, an internet architecture.
SCION is being developed at the Institute of Information Security at ETHZ, one of the world's top universities in the field.
It has recently been presented at the ENISA (European Network and Information Security Agency) Art 13a-(ensuring the security and integrity of electronic communication networks) meeting in Stockholm.
It is already being commercially deployed by ISPs Deutsche Telekom, Swisscom, Switch, and Init7. It is used by several banks and the Swiss Foreign Department already.

All information on the technical functioning of SCION is available on the homepage of the project under www.scion-architecture.net . On the website, which is maintained by the SCION project at ETHZ, you can find all the information you need.
You'll also find a two-page article on the subject of IoT defence via SCION: https://www.scion-architecture.net/pdf/2017-IoTdefense.pdf . Since the article, SCION has been further developed.

SCION allows hosts to choose where their traffic goes and via what ASes. It allows for trustworthy and lightweight routing hat the same time.

In a nutshell,

1. IoT devices can be allocated network paths that are hidden from attackers. That protects the IoT device from being taken over by these attackers. Under this regime, there is no particular need for device manufacturers to secure the devices they manufacture.
2. Servers attacked by IoT botnets (like the mirage botnet that was in the news in 2016) can be maintained under DDoS-attacks. So, the owner can manage these servers even while the servers are under attack. That minimizes the effects of IoT security holes.
3. These attacked servers can use several different paths at the same time, which complicates DDoS-attacks.
4. DDoS-attacks can not easily be hidden through packet reflection.
5. BGP-hijacking is avoided.

Best regards,

Jens Kaessner