Harnessing the potential of big data to improve the security of Internet of Things devices

May 9 2017

The power of big data is used in a strategy developed by A*STAR to improve the security of networks of internet-connected objects, known as the Internet of Things (IoT), technology which will make everything from streetlights to refrigerators 'smart'.

More than 20 billion devices are expected to be upgraded and connected to each other by 2020. However, with IoT becoming increasingly widely adopted, developers need to guarantee its security. One hacked target could be the gateway to other parts of the network, making it vulnerable to breaches of sensitive information. This was demonstrated in October 2016, when a huge attack on IoT devices across Europe and the USA, such as CCTV cameras with easy-to-guess passwords, contributed to outages for several major websites.

Currently, a number of web services, including online banking and Google, use or offer a two-step authentication process to increase the security levels. Since passwords can be leaked or cracked, these services require secondary secret information from the customer. This could be another code transmitted via SMS, email or a security token; or the user's fingerprints or facial recognition.

However, the direct application of these methods to the IoT is not practical. "We want to achieve the same level of security as bank servers offer, but the resources needed are simply an overkill to typical IoT

devices, "explains Jun Wen Wong, one of the researchers involved in the study. "We had to think about a brand new protocol."

The new strategy, devised by A*STAR researchers of the Institute for Infocomm Research, uses the conventional password as first step for authentication, but a second step uses the whole history of the data exchanged between the IoT device and the server.

The scientists proposed algorithms that generate and store in the IoT device a very small piece of secret information, which can concisely represent the whole history dataset, and can be retrieved for the authentication. Thanks to this approach, taken from the big data sector and originally applied to the IoT, this security two-step system can be compatible with IoT devices with low computation and small memory.

Using the data exchanged between the device and the server has very interesting leakage-resilience properties. As data are constantly generated by the IoT device and sent to the server, the history dataset is growing, so hackers would have to steal a considerable amount of data over an extended period of time, becoming more open to detection.

More information: Scalable Two-Factor Authentication Using Historical Data. DOI: 10.1007/978-3-319-45744-4_5

Provided by Agency for Science, Technology and Research (A*STAR), Singapore