In the Know About Nodes? Exploring a New Patching System for Securing the IoT

December 20, 2017 | Devices & Systems

Fixing individual IoT devices infected by malware may not be the best solution to a widespread cyberattack.

IoT devices are prime targets for hackers. They are connected to multiple devices and often have weak security measures. To address this problem, researchers created a system to strengthen the cyber security in wireless networks connected to IoT devices.

The key is a new traffic-aware patching scheme <http://ieeexplore.ieee.org/document/7981520/> that focuses on fixing critical intermediate nodes before an infected device has time to transmit its virus to a wireless network.

An intermediate node is a general term for an upper-level device in a wireless network infrastructure that is responsible for communicating with individual IoT devices. It can be an access point (AP), a gateway, or even a laptop. Figure 1 depicts how intermediate nodes interact with IoT devices in a network.

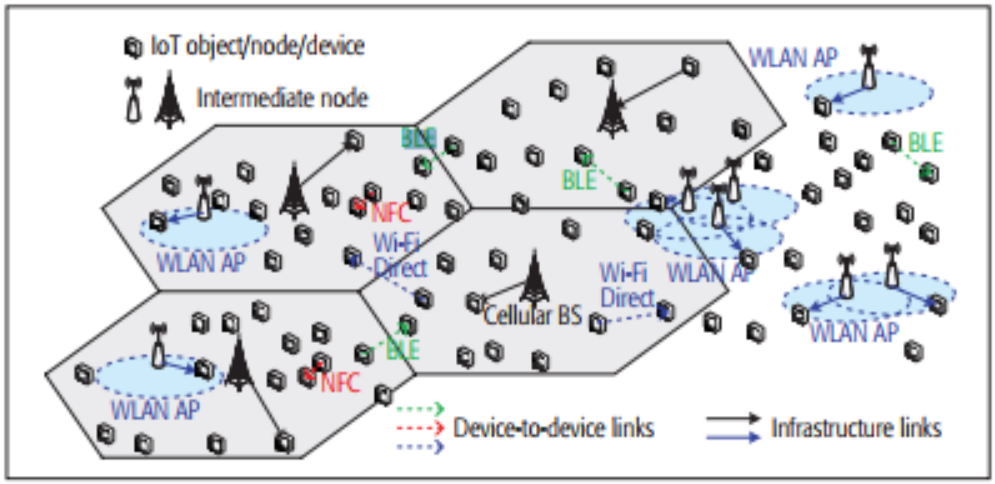

Figure 1: IoT platform with infrastructure and device-to-device links.

Today, most approaches involve a traditional random patching scheme, which immediately patches nodes randomly when malware is detected. By contrast, a traffic-aware patching scheme identifies the most critical nodes that are most likely to spread a virus rapidly, due to the higher number of devices to which they connect.

Compared to wireless devices like smartphones, IoT devices are much more difficult to patch. Because these devices have various features that differ in complexity and usability, they tend to be harder to configure. Since the researchers' scheme deals specifically with patching nodes, not each individual device, the solution works on both old and new IoT systems.

"Our patching scheme solves the practical difficulty of directly patching IoT devices," said Pin-Yu Chen, a researcher at IBM. "Instead of trying to fix an infected IoT device, we patch intermediate nodes in the wireless network infrastructure the infected device is connected to. This is like the strategy of avoiding catastrophic outbreak of an infectious disease by quarantining high-risk objects."

The system involves two phases:

- Detection, which uses a traditional intrusion detection system (IDS) or firewall to identify the existence of infected nodes or malicious software in a device.
- Patching, where the scheme patches nodes the system determines are most critical for limiting the malware spread.

To determine which nodes are most critical, the scheme analyzes readily available traffic information in IoT systems. This efficient approach allows the traffic-aware scheme to be much more cost-effective than patching individual IoT devices or randomly patching a number of nodes all at once.

The researchers simulated a mobile social network to test the scheme. The results (as shown in Figure 2) showed the system was more effective than a random patching scheme, whether it only had time for a few patched APs (under 30 percent patched) or time to patch most APs in a system (over 90 percent patched).

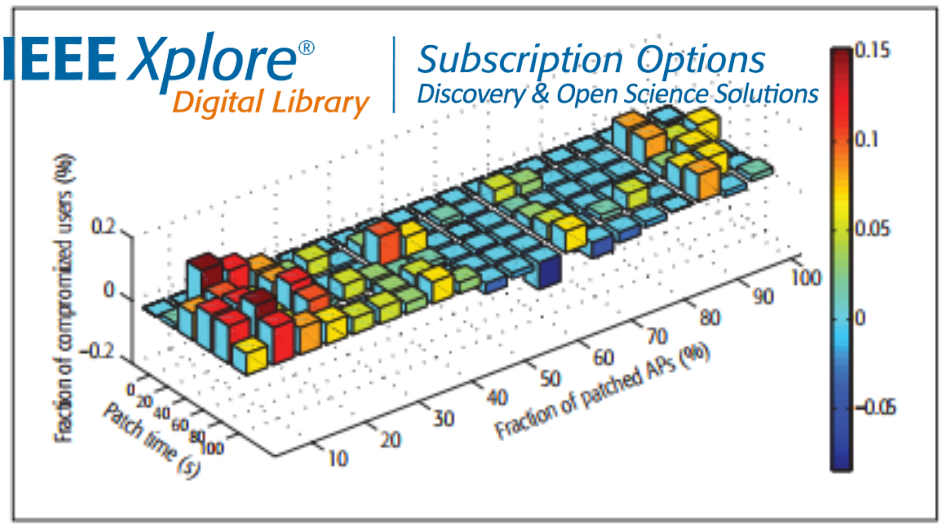

Figure 2: Performance comparison between random patching and traffic-aware patching in terms of the difference between the fraction of compromised users under each scheme.

The researchers are currently working to fine tune their system in a number of ways. They are developing a model to predict the spread of malware in their scheme and a method for virtually patching IoT devices. Additionally, they are also looking to eliminate human error from their scheme. The traffic-aware patching scheme patches infrastructure links, but a virus can still be spread from device-to-device links, which means people can download viruses to their device if they don't follow proper cyber security measures.

Considering that the number of IoT devices in the world is expected to reach 31 billion by 2020[1], it's plain to see that securing each and every single device is not a realistic expectation. For this reason, the team's new research could very well have a major impact on how widespread IoT systems actually become.

For more information on IoT cyber security <http://ieeexplore.ieee.org/search/searchresult.jsp?queryText=IoT%20cyber%20security&newsearch=true>, visit the IEEE Xplore Digital Library.

1) https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#48fdfca81480 <https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#48fdfca81480>