On the way to a safe and secure smart home

September 1 2014

Building management with a tablet computer: In several modern office buildings, lights, louvers (blinds) and doors can be centrally controlled via the Internet. That brings gains in efficiency – but it holds risks, as well. Credit: Fraunhofer FKIE

A growing number of household operations can be managed via the Internet. Today's "Smart Home" promises efficient building management. But often the systems are not secure and can only be retrofitted at great expense. Scientists are working on a software product

that defends against hacker attacks before they reach the building.

Botnet. A term from the world of computers is gradually tiptoeing its way into the world of building automation. You have to anticipate this kind of attack scenario, according to Dr. Steffen Wendzel of the Fraunhofer Institute for Communications, Information Processing and Ergonomics FKIE in Bonn. The researcher from the "Cyber Defense" department is the expert in hacker methods and, working jointly with Viviane Zwanger and Dr. Michael Meier, meticulously examines them. Attackers infiltrate multiple computers – "bots" (from the word "robots") – without their owners' knowledge, weave the computers together into nets, and misuse them for computer attacks. The researchers studied something that does not yet exist at all today: attacks by Botnets on "Smart Homes" using Internet-linked buildings or building operations. The finding: The threat is absolutely real: Internet-controlled electric roller shutters, HVAC and locking systems could all be used for these kinds of attacks."Our experiments in the laboratory revealed that the typical IT building is not adequately protected against Internet-based attacks. Their network components could be highjacked for use in botnets," Wendzel continues. In the process, the hackers do not have to seek out the PCs as in the past; instead, they look for the components in building automation that link the buildings with the Internet. These are small boxes installed in the buildings that look and work like routers for home computers."However, they are configured quite simply, can only be upgraded with some difficulty, and are loaded with security gaps. The communications protocol that they use is obsolete," explains Wendzel.

Sentinel software switches between Internet and building IT

To ensure that the heating, lighting, and ventilation of buildings can be controlled via the Internet, it is necessary to install special equipment:

This involves mini-computers that measure temperature, light or humidity and are incorporated into networks. "Keeping them up to the latest standards is expensive," Wendzel says. At FKIE, the team has developed security software that can easily switch between Internet and building IT. The technology filters out potential attacks from communications protocols even before they reach the four walls of the actual brick-and-mortar home or office building. No matter what technologies are being used within the building: With this approach, they do not have to be replaced.

The researchers additionally examined the conventional communications standards of building automation, and building upon these, they have developed rules for data traffic. If arriving data do not adhere to these rules, then the communications flow is modified. "The software operates like a firewall with normalization components," explains Wendzel. All the results that are sent on their way to the systems are tested for plausibility by an "analyzer". If the alarm goes off, then the incident is immediately dispatched to the "normalizer." This either blocks the incident in its entirety or modifies it accordingly. The basic research has been concluded successfully. "In the next stage, we want to make the technology production-ready with an industrial firm. In no later than two years, there should be a product on the market," states Wendzel.

In their analysis of Botnet attacks, the researchers sketched out definitive threat scenarios for smart homes."From my perspective, the most compelling issue is 'monitoring,'" the cyber defense researcher says. When the attacker hacks into the building operations IT, he or she will learn where the residents or tenants are located and what they are doing, in a worst case scenario. That includes everything, right down to going to the toilet. Intruders, for example, could use this data in order to prepare for a burglary or raid. In this case, the hacker is acting in a passive capacity, simply tapping data. However, he or she could be equally capable of actively invading the systems. Take a contractor from

the energy industry, for example. He could profit from more oil or gas sold if the consumption of multiple heating systems is artificially elevated. A recent example demonstrates how real this scenario is: Last year, there was a gap in the security system of a heating system connected to the Internet. Attackers had the ability to shut down or damage heaters. Therefore, security expert Wendzel is currently advising against carelessly linking all building functions in private homes to the Internet.

Provided by Fraunhofer-Gesellschaft