Ensuring security for networks of the future

January 6 2015

With their visualization software, AISEC researchers can monitor every component in software-defined networking (SDN). Credit: Fraunhofer AISEC

Company networks are inflexible – they are made up of many components that require a good deal of effort to be connected together. That's why networks of the future will be controlled by a central unit. However, this makes them a target for hackers. At CeBIT, Fraunhofer researchers will demonstrate how to protect these future networks.

Today's company networks comprise hundreds of devices: routers for

directing data packets to the right receiver, firewall components for protecting internal networks from the outside world, and network switches. Such networks are extremely inflexible because every component, every router and every switch can carry out only the task it was manufactured for. If the network has to be expanded, the company has to integrate new routers, firewalls or switches and then program them by hand. That's why experts worldwide have been working on flexible networks of the future for the last five years or so, developing what is known as software-defined networking (SDN). It presents one disadvantage, however; it is susceptible to hacker attacks.

Researchers from the Fraunhofer Institute for Applied and Integrated Security AISEC in Garching, near Munich, will be showing how to make SDN secure at the CeBIT trade fair in Hannover, March 16-20. A demonstrator at the Fraunhofer exhibition stand (Hall 9, Booth E40) will show how SDN and all related components can be monitored. One of these components is visualization software, which displays the network's individual components and depicts in real time how the various applications are communicating with the controller. "We can show how software influences the behavior of different components using the controller, or, in the case of an attack, how it disrupts them," says Christian Banse, a security expert at AISEC.

But how exactly does SDN work, and why is it so vulnerable to attack? "In the future, the plan is for a central control unit to tell the many network components what to do. To put it simply, routers, firewalls and switches lose their individual intelligence – they only follow orders from the controller," says Banse. This makes a network much more flexible, because the controller can allocate completely new tasks to a router or switch that were not intended when the component was manufactured. Plus, the tedious task of manually configuring components during installation is eliminated because components no longer need to be assigned to a specific place in the network – the controller simply uses

them as needed at the moment.

The controller is a popular target for hackers

Manufacturers have begun offering the first routers and switches that are SDN-compatible and have the necessary flexibility. "With all the hype surrounding the new adaptability made possible by a central control unit, SDN security has been neglected," warns Banse. "That's why we're developing solutions to make SDN more secure from the outset, before such systems become firmly established." In the future, networks will be controlled solely by a central controller – Banse sees this as a problem, because it might provide the perfect loophole for attackers to access the entire network. "On top of that, a whole set of new applications are being developed for SDN – for instance for firewall components or routing," says Banse. "We have make sure that these applications are reliable." It would be disastrous if, for example, outsiders were able to gain access to the company network using software installed accessing the controller.

That's why Banse and his colleagues started off by analyzing the interaction of all SDN components to identify vulnerabilities. "You have to precisely define how deep into the network a new application is allowed to go, for example. Otherwise the stability and security of the network is not guaranteed." So far, there are no sufficient security standards for communication among individual SDN components, but AISEC researchers are lobbying hard for an international standard. In addition to their visualization solution, at CeBIT Banse and his team will also present technical means for preventing unauthorized applications or malware from gaining access to SDN systems. They are developing ways to monitor if an app really carries out only the task for which it was intended. If it performs unplanned or undesirable activities, i.e. malware, it is rejected and blocked by the system.

Provided by Fraunhofer-Gesellschaft