Project proposing to move security applications from device to network nodes

June 28 2016

The rapid rise of mobile devices has left many security gaps in its wake—with sources of concern including operating systems with flaws, configuration issues, vulnerable apps and public networks. All in all, it is estimated that 75 % or more mobile apps would fail basic security tests. OS vulnerabilities, on the other hand, are more than doubling each year.

In the face of these alarming statistics, consumers are left to resort to protection tools that may not exist on all systems, have capabilities that vary greatly across devices, and often consume too many resources. These problems could all be solved in a single technological shift: offloading execution of security applications into a programmable device at the edge of the network—such as a home gateway or an enterprise router.

The SECURED (SECURity at the network EDge) project has been designing such solution since October 2013. A few months before the end of the project, its coordinator Prof Antonio Lioy, of the Polytechnic University of Turin, details its results so far, how they fit in today's technological landscape and their potential fields of applications.

What are the main problems with current mobile device security systems?

Current mobile device security is mostly device-based: users need to locally install the appropriate solution on each of their own devices, for example an anti-virus to protect them against malware or a firewall to block unwanted connections. This is both complex—as the average user tends to have several devices—and difficult—as some security applications are not available for all kind of devices or do not have the same performance or features.

Large companies tend to address this problem by restricting the type of mobile devices used by their employees and by adopting a MDM (Mobile Device Management) system. However, this is not feasible for general users who are therefore increasingly exposed to risks. In a nutshell, security of mobile devices is variable and mostly insufficient, as it depends on the products available and the device used.

How does the SECURED architecture help overcome these problems?

SECURED proposes to delegate protection—totally or in part—to a trusted and secure network node, specifically crafted to run security applications selected by the user and configured according a protection policy specified by himself.

We name this device a NED (Network Edge Device), as to ensure best performance it is preferable to place it in the network as close as possible to the mobile device—although the use of a remote or cloud-based NED is also possible.

When the user connects his mobile device to the NED, a proof of the identity and integrity status of the NED is provided so that the user can trust the NED to work on his behalf, and a dedicated virtual execution domain is created for the user. The NED will then download the selected security controls from user-specified repositories and will configure them according to his/her protection profile retrieved from a policy repository.

Can it be used on existing networks? How?

Yes it can be done, by inserting NEDs into the network and asking the users to connect via a VPN to their selected NED. Of course if the network access point of the user—the home gateway, the Wi-Fi access point or the 3G/4G access node is already a NED, then a VPN would not be needed and performance would be improved.

In any case, the option to have the NED directly available as first hop in the network or as a remote entity provides a lot of flexibility in the deployment scheme. This in turn permits a gradual adoption of the solution and makes it available also in those environments that do not directly adopt the SECURED technology. In other words, the user is in control of his own security and the only variable parameter is network performance which is maximized with a local NED and decreases with a remote one. Trust and security are guaranteed in both cases.

How about future Internet, more specifically the Internet of Things?

The paradigm developed by SECURED is suitable also for the Internet of Things. Typically the nodes of these environments have limited power and capabilities and hence have low or no protection because they cannot execute complex security controls. We can achieve a good degree of protection for IoT nodes by connecting them to the external network via a NED, which takes care of their protection.

Cross-network security policies can also be enforced thanks to your system. How did you achieve that?

The NED is actually a component that has many stakeholders, depending on who is the owner. For example, NEDs offered by an ISP (Internet Service Provider) or a MNO (Mobile Network Operator) will apply not only the user security policy but also the operator's. SECURED has developed algorithms to combine these different policies and apply the resultant one. Of course in cases where the operator policy is more restrictive than the user's, the NED informs the user of the additional restrictions and provides the option to disconnect.

Since security controls and policies are downloaded onto the NED on demand when a user connects to a network, and this automatically works across different networks. Additionally, the solution also provides seamless support for mobility: if a user moves from one access point to a different one then his virtual execution domain is automatically connected to the new access point.

Can you tell us more about the marketplace you created?

Our target are normal users who are not necessarily technical security experts. We have therefore tried to simplify the usage of SECURED as much as possible. First we created a high level interface to specify the security policy in a nearly-natural language—actually a restricted language, for example only the verbs related to protection are available, such as 'permit', 'deny', or 'record'.

Then the user can access a marketplace where various security applications are available, quite similar to the typical marketplace you would find on your smartphone. Technically-savvy users can directly select the desired applications while neophytes will benefit from automatic selection based on their specified policy.

For example, if the user asked to block access to websites with inappropriate content for children and to be protected from malware, then the system will suggest acquiring a parental control app and an anti-virus one. If more than one app of a certain kind is available, the user is presented with the features that distinguish them such as price, performance and recommendations from other users.

The project will be completed soon. How well do you think it will be received on the market?

When we started the project back in 2013, our main target were network/service providers and Wi-Fi hotspots. We still think that these are reasonable adopters but, at the same time, we have discovered that new interesting fields of applications have emerged.

Besides the Iot paradigm which we already discussed, modern software-based networks are a big target: the SDN (Software-Defined Networking) and NFV (Network Function Virtualization) paradigms are rapidly changing the networking scenario from an hardware- to a software-based one. This means that the network itself is a possible adopter of the SECURED technology as it offers on-demand security functions configured according to specific policies and executed in a trusted environment. We had a presentation and a demo on February 2016 at a meeting of the ETSI NFV working group and the SECURED technology raised a lot of interest. So there are various markets where I think SECURED will play a role in the near future.

More information: Project website: www.secured-fp7.eu/

Provided by CORDIS

Citation: Project proposing to move security applications from device to network nodes (2016, June 28) retrieved 13 May 2024 from https://phys.org/news/2016-06-applications-device-network-nodes.html