UNIVERSITÀ DEGLI STUDI DI PADOVA

UFFICIO STAMPA
VIA VIII FEBBRAIO 2, 35122 PADOVA
TEL. 049/8273041-3066-3520
FAX 049/8273050
E-MAIL: stampa@unipd.it
AREA STAMPA: http://www.unipd.it/comunicati

Padova, 26 agosto 2016

KYE ATTACCA SDN
Il Software Defined Networking è in pericolo
ma team di ricercatori scopre “scudo deflettore” contro gli attacchi

La tecnologia SDN (Software Defined Networking) promette di rendere le reti informatiche molto più flessibili ed efficienti, attraverso la separazione della cosiddetta "network logic" dalla funzionalità di semplice inoltro dei pacchetti.

SDN è già ampiamente utilizzata in ambito industriale, anche da colossi quali Google e Microsoft, e ricercatori di tutto il mondo si sono già impegnati a validarne la sicurezza, proponendo soluzioni per alle vulnerabilità individuate.

Tuttavia, come riportato da uno studio condotto dal Prof. Mauro Conti dell'Università di Padova, insieme a Fabio De Gasperi e Luigi Mancini, della Sapienza di Roma, sembra che la tecnologia SDN abbia ancora rischi di sicurezza rilevanti.

Lo studio dei ricercatori italiani mostra come sia possibile portare a termine un interessante attacco, che gli studiosi hanno chiamato Know Your Enemy (KYE). Tramite l'attacco KYE, un attaccante può venire a conoscenza dei parametri di configurazione della rete SDN, incluse anche le configurazioni di meccanismi di protezione della rete, come le soglie per la identificazione dei "network scanning", oltre a configurazioni di altri aspetti della rete (come quelli per il "quality of service" o per la virtualizzazione). Inoltre, l'attacco KYE si può portare a termine in maniera "trasparente", ovvero senza il rischio di essere individuati.

Oltre a identificare questa importante vulnerabilità, insita nelle reti SDN, i ricercatori propongono anche delle contromisure, basate sulla "offuscazione" del comportamento della rete, rendendo quindi l'attacco molto più complicato.

Mauro Conti