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, 9 agosto 2016

SELFRANDO DIFENDE TOR BROWSER
Più sicuro l'anonimato in rete grazie a un team di ricercatori internazionale

Ricercatori dell'Università di Padova, della Technische Universität di Darmstadt (Germania), di Immunant, Inc., dell'Università di Irvine (California) e del Tor Project hanno collaborato per integrare una nuova difesa nella versione "hardened" di Tor Browser. La nuova difesa, chiamata "selfrando", protegge Tor Browser da molti attacchi volti a de-anonimizzare gli utenti di Tor.

Tor Browser, grazie a un sistema di navigazione internet di "rimbalzo" della connessione su vari computer sparsi in tutto il mondo, permette all'utente di navigare senza essere rintracciato rendendo impossibile l'identificazione del PC dal quale ci si connette.

Molte persone, come attivisti, giornalisti e whistleblower utilizzano Tor Browser per proteggere il proprio anonimato online. Naturalmente, Tor Browser è un bersaglio ambito per gli hacker, compresi quelli riconducibili a servizi di sicurezza di qualche nazione, che intendano de-anonimizzare e tracciare gli utenti di Tor. Il Tor Project sta sperimentando nuove difese nella versione "hardened" di Tor Browser per proteggere gli utenti da attacchi ai browser.

«Gli attacchi più potenti contro i browser come Tor Browser ambiscono a sfruttare remotamente una vulnerabilità sulla macchina della vittima utilizzando una tecnica avanzata conosciuta come "riutilizzo del codice" – **spiega il prof. Mauro Conti del Dipartimento di Matematica dell'Università di Padova** -. L'idea fondamentale è di raggruppare diversi frammenti del codice di un programma per formare un malware in grado di controllare la macchina della vittima; in questa maniera, l'aggressore non ha la necessità di inserire preventivamente codice estraneo nella macchina della vittima. Selfrando difende i programmi da questa classe di attacchi randomizzando i frammenti di un programma. L'aggressore, all'oscuro della nuova disposizione dei frammenti, ha notevoli difficoltà a costruire un attacco affidabile basato sul riutilizzo del codice.»

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

Selfrando migliora la sicurezza in maniera significativa senza sacrificare la velocità o la compatibilità. Non richiede cambiamenti all'ambiente di build dei programmi e causa una riduzione delle performance inferiore all'1%. In pratica, il rallentamento è impercepibile mentre la sicurezza viene rafforzata notevolmente.

I ricercatori che hanno sviluppato selfrando hanno presentato il loro progetto il 19 luglio al Privacy Enhancing Technology Symposium a Darmstadt, in Germania.

Il paper relativo alla loro ricerca è disponibile (in open access) all'indirizzo http://www.degruyter.com/view/j/popets.2016.2016.issue-4/popets-2016-0050/popets-2016-0050.xml.

Selfrando è disponibile per l'utilizzo con altri progetti open source all'indirizzo https://github.com/immunant/selfrando

Il prof. Mauro Conti è phd, head of spritz security and privacy research group, eu Marie Curie fellow - ieee senior member, associate editor for ieee tifs, ieee comst.