



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, 7 novembre 2016

PRIVACY A RISCHIO QUANDO SCRIVIAMO MENTRE PARLIAMO ON LINE

La privacy di chi digita sulla tastiera del proprio computer durante una chiamata via Skype potrebbe essere a rischio. Questi i risultati di una ricerca condotta da un team internazionale che coinvolge l'Università degli Studi di Padova (Prof. Mauro Conti, che guida il gruppo **SPRITZ - Security And Privacy Research Group**, e Daniele Lain), la Sapienza Università di Roma (Alberto Compagno), e l'University of California, Irvine (Prof. Gene Tsudik). In uno studio pubblicato recentemente su «arXiv», i ricercatori hanno mostrato che i suoni prodotti dalla digitazione sulle tastiere di computer fissi e portatili, se registrati durante una telefonata online, permettono ad un attaccante di ricostruire il testo digitato da una vittima ignara.

I software VoIP (Voice-over-IP, ovvero di telefonia attraverso la rete Internet), come Skype, Google Hangouts, e Viber, sono tra i programmi più utilizzati ogni giorno. Tra questi, Skype è sicuramente tra i più popolari nel mondo, con 300 milioni di utenti attivi ogni mese nel 2016. **A questi utenti, che passano più di 3 miliardi di minuti ogni giorno in audio o videoconferenza, può succedere spesso di digitare informazioni sensibili, come ad esempio password, e-mail private, o altro testo che vorrebbero comunque tenere confidenziale. Lo studio mostra che la persona con cui stiamo effettuando la chiamata, se malintenzionata, può registrare il suono prodotto dalla pressione dei tasti e, tramite tecniche di *machine learning*, capire cosa abbiamo digitato sulla nostra tastiera.**

Nella comunità di ricerca in *cyber-security*, era già noto che tra i diversi tasti delle tradizionali tastiere meccaniche ci fossero leggere differenze di suono, che permettono di capire quale tasto sia stato premuto da un utente. Finora, però, l'attaccante necessitava, oltre che di una buona conoscenza dello stile di digitazione della vittima, anche di posizionare un dispositivo di registrazione vicino alla tastiera della vittima.

«Il nostro lavoro mostra che tale registrazione è possibile anche da remoto, grazie ai software VoIP che, non alterando il suono dei tasti, ci consentono di effettuare l'attacco con successo», dice lo studente **Daniele Lain**, co-autore dello studio, recentemente laureatosi con il massimo dei voti presso la Laurea Magistrale in Informatica dell'Università di Padova.

Il team di ricerca ha mostrato, inoltre, che è possibile colpire anche vittime per le quali non si disponga di informazioni riguardo il loro stile di digitazione: tramite il suono dei tasti, è possibile determinare quale modello di tastiera stia utilizzando la vittima. Successivamente, utilizzando dati di addestramento presi da altre persone (ad esempio, complici dell'attaccante) su tastiere della stessa marca, si può ricostruire quanto la vittima ha digitato durante la chiamata con precisione allarmante.

«Non sempre le persone che parlano su Skype si conoscono, o godono di fiducia reciproca - spiega il **Prof. Mauro Conti** -. Si pensi ad esempio a chiamate tra avvocati di parti contrapposte, oppure a politici, diplomatici, o aziende concorrenti. La capacità dello studio di attaccare vittime potenzialmente sconosciute all'attaccante invita a non digitare informazioni



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>

sensibili durante chiamate VoIP, o ad utilizzare tastiere diverse dalle tradizionali tastiere meccaniche, come ad esempio tastiere olografiche e superfici *touch-screen*.»

Lo studente Daniele Lain (a sinistra) e il Prof. Mauro Conti (a destra)

