Ministero dello Sviluppo Economico

DIREZIONE GENERALE PER LE TECNOLOGIE DELLE COMUNICAZIONI E LA SICUREZZA INFORMATICA-ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE
DIVISIONE I

Scuola Superiore di Specializzazione in Telecomunicazioni

6 maggio 2021; ore 10.00-11.30

Cyber Sorveglianza globale: tecniche crittografiche di difesa

Relatore: Prof. Giuseppe Bianchi, docente di Sicurezza delle Reti – Dipartimento di Ingegneria elettronica, Università di Roma Tor Vergata"

Nel 2013, le rivelazioni di Edward Snowden hanno mostrato al mondo intero l'esistenza di programmi di ***cyber-sorveglianza globale***. Se un ente governativo, magari straniero, può tecnologicamente essere in grado di raccogliere capillarmente ed in modo massivo il traffico generato da milioni di utenti Internet per poi analizzarlo, come ci possiamo difendere? Il problema è estremamente importante in quanto impatta direttamente il nostro diritto alla privacy in relazione all'uso di servizi informatici e di comunicazione globali, peraltro fortemente intensificati proprio in quegli anni con la transizione verso servizi cloud. Nel seminario, illustreremo alcune tecniche che la comunità scientifica e i fornitori di servizi web e/o cloud hanno ideato e messo in campo dopo il 2013, al fine di garantire la sicurezza dei dati degli utenti e le giuste restrizioni di accesso da parte di terzi, compresi i governi. Con specifico, ma non esclusivo, riferimento a soluzioni crittografiche integrate e/o standardizzate nei protocolli per la sicurezza web (TLS/HTTPS), il seminario tratterà tre tematiche. In primo luogo, introdurremo il concetto di **Perfect Forward Secrecy (PFS), introdotto appositamente per fronteggiare attaccanti in grado di raccogliere e conservare per anni il traffico generato dai nostri dispositivi**, e mostreremo come la PFS è stata recentemente integrata nell'ultima versione del protocollo TLS (versione 1.3, agosto 2018). Parleremo poi del problema dei **falsi certificati HTTPS, e di come soluzioni basate su architetture simil-blockchain possono permettere trasparenza e verificabilità pubblica**. Mostreremo infine alcuni semplicissimi esempi di approcci cosiddetti omomorfi, estremamente promettenti per la **privacy in servizi cloud**, che permettono di fare operazioni direttamente operando su dati cifrati, ovvero senza svelare il contenuto dei dati agli stessi cloud provider.

La presentazione sarà comunque fruibile anche dai non esperti

Il seminario è **gratuito**, per prenotarsi, ed ottenere il **Link** per seguire il seminario **On Line**, inviare una email a; **scuolasuperiore.tlc@mise.gov.it**