PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5684 di Mercoledì 04 settembre 2024

La sicurezza dei dispositivi biometrici di riconoscimento sta diminuendo

I deepfakes stanno diventando sempre più sofisticati e possono minacciare la sicurezza dei sistemi biometrici, come quelli per il controllo degli accessi. Tuttavia, con le giuste precauzioni, è possibile mantenere un livello di sicurezza adeguato.

Oggi gli applicativi, chiamati deepfakes, vale a dire sofisticati simulatori, possono creare immagini video e generare audio che possono ingannare gli attuali sistemi biometrici di riconoscimento.

Questa situazione può avere dei riflessi significativi sugli attuali sistemi di riconoscimento biometrico, che sono stati per anni ritenuti i più sofisticati disponibili per il mondo della sicurezza.

Questi applicativi presentano delle immagini, dei file video o degli audio che sono in grado di riprodurre, in modo artificiale, un mondo che praticamente non è distinguibile dal mondo reale. L'applicazioni di questi software sono numerose: ad esempio, vi sono persone che li utilizzano per realizzare un video nel quale queste persone possono ballare con un famoso ballerino, oppure cantare insieme ad un famoso cantante.

Altri invece possono utilizzare questi applicativi per commettere delle frodi, che hanno un'elevata probabilità di andare a buon fine.

Tutti gli esperti di sicurezza sanno che uno dei grandi vantaggi degli applicativi biometrici è legato al fatto che l'utente non deve temere di dimenticare una parola chiave, oppure non deve temere che questa parola chiave venga in qualche modo catturata.

La crescente diffusione di sistemi di controllo accesso biometrici, sia nel mondo industriale, del commercio, della finanza, ha fatto sì che la disponibilità di sistemi, in grado di violare questi controlli accessi, possa costituire un rischio gravissimo per l'organizzazione coinvolta. Ecco la ragione per la quale è indispensabile mettere a punto sistemi di contrasto di queste tecniche avanzate di violazione dei controlli accessi, alcune delle quali vengono di seguito illustrate. La soluzione corretta non è quella di eliminare i sistemi biometrici, ma di renderli sempre più intelligenti ed in grado di individuare alcuni segni caratteristici dei prodotti contraffatti, sviluppati degli applicativi truffaldini.

Ecco alcuni accorgimenti che è possibile utilizzare, con relativa rapidità e semplicità.

Autentica a più fattori

Aggiungendo alla identificazione biometrica anche un ulteriore parametro, per esempio una OTP ? one time password, oppure abbinando l'accesso al sistema con una geolocalizzazione, compatibile con la posizione in cui si trova il terminale di accesso, è possibile aumentare in maniera significativa il livello di sicurezza dell'accesso.

"Vivezza" dell'immagine

Con questa espressione si f' riferimento ad applicativi che sono in grado di esaminare una immagine e verificare se la stessa corrisponde a una persona viva ed attiva, o non piuttosto ad una contraffazione. Il sistema può essere ulteriormente migliorato se l'applicativo chiede al soggetto, che desidera effettuare l'accesso, di fare una operazione specifica, come ad esempio sbattere le ciglia. La falsificazione di queste attività risulta per ora estremamente difficile per gli applicativi fraudolenti.

Anche una più attenta analisi dell'immagine proposta, ad esempio un volto, può permettere individuare segni caratteristici di una contraffazione. Ad esempio, spesso la dilatazione delle pupille non è coerente con il battito delle ciglia, oppure possono esservi delle anomalie nelle pieghe della pelle, che sono caratteristiche del collo.

L'educazione degli utenti

Ancora una volta, una educazione appropriata degli utenti rappresenta un prezioso strumento di aumento della sicurezza del sistema. Può essere caldamente raccomandato ad un responsabile del sistema informativo di educare tutti i soggetti, che a tale sistema accedono, a rilevare possibili anomalie, anche simili a quelle appena illustrate.

L'adozione di stringenti protocolli di cattura e custodia di dati biometrici

In Italia, è bene ricordare che la nostra autorità garante ha sempre avuto un atteggiamento estremamente prudenziale nei confronti dei sistemi biometrici, imponendo regole prudenziali ed addirittura proibendo l'utilizzo di questi sistemi in particolari contesti.

In questo contesto, può essere oltremodo utile l'introduzione di regole che obblighino tutti coloro, che utilizzano applicativi di intelligenza artificiale generativa ad introdurre dei contrassegni nelle immagini generate, in modo da mettere in evidenza la origine artificiosa.

Ci si augura che gli organi legislativi, a livello nazionale, europeo e mondiale si attivino al più presto per introdurre strategie di protezione e garanzia, che possano aiutare i responsabili della sicurezza informatica nel gestire sistemi tanto sicuri, quanto facilmente accessibili per i soggetti debitamente autorizzati.

Adalberto Biasiotti

www.puntosicuro.it