La serie delle norme ISO 30107 sulla Biometria

Commento

Collana: norme volontarie commentate

Sommario

di Adalberto Biasiotti

Pubblicazione n. 11

1) Premessa

Uno degli obiettivi statutari dell'AIPROS è quello di sviluppare la professionalità dei suoi soci. Oggi, nel mondo della sicurezza fisica ed informatica, il ruolo delle norme diventa sempre più importante, in quanto specifici riferimenti del codice civile italiano affermano che una prestazione professionale od un impianto di sicurezza devono essere fornita o realizzato a regola d'arte.

La conformità alla regola d'arte si documenta affermando che la prestazione o l'impianto in causa è stato realizzato in conformità a una norma italiana, europea od internazionale, con rispettive sigle UNI, CEI, EN, ISO.

Questo è il motivo per cui, ad esempio, quando sono chiamato ad operare in qualità di consulente tecnico di ufficio, per conto della magistratura inquirente o giudicante, onde valutare la qualità di una prestazione professionale oppure di un impianto, suggerisco al magistrato che il quesito debba essere articolato come segue:

La prestazione professionale o l'impianto di sicurezza, oggetto della presente consulenza, è stato realizzato in conformità ad una norma italiana, europea od internazionale?

Se la risposta è positiva, proprio in conformità a quanto previsto dal codice civile, l'impianto o la prestazione sono a regola d'arte.

Nulla ovviamente impedisce che si possa realizzare una prestazione od un impianto a regola d'arte, anche senza fare riferimento a norme vigenti, ma è evidente che in questo caso l'onere della prova resta in carico a chi la prestazione ha fornito o l'impianto ha progettato ed installato.

Per questa ragione, nei capitolati pubblici e privati, sempre più spesso, si trovano riferimenti a norme vigenti, che permettono, quindi, al committente di avere a disposizione prestazioni ed impiantistica a regola d'arte, senza che il capitolato debba dilungarsi su aspetti tecnici, certamente meglio e più correttamente illustrati nella norma, cui si fa riferimento nel capitolato.

Nella mia esperienza professionale, purtroppo, ancora rilevo come, tra i professionisti della sicurezza, la conoscenza delle norme possa essere migliorata in modo significativo ed ecco la ragione per la quale mi sono messo a disposizione per offrire una illustrazione delle principali norme, attive in specifici settori.

Negli ultimi tempi sempre più spesso si sente parlare di modalità di attacco a sistemi di riconoscimento biometrico, grazie a tecniche di varia natura. Anche i film di spionaggio sempre più spesso fanno vedere come sia possibile, almeno nel film, catturare un'impronta digitale presente su un bicchiere e trasformarla in un dispositivo biometrico di accesso.

Il problema effettivamente esiste, tanto è vero che uno specifico comitato tecnico ISO, di cui lo scrivente fa' parte, ha sviluppato una serie normativa, che probabilmente verrà ampliata

a breve, inquadrando le modalità con cui può essere correttamente impostata una valutazione dell'efficienza ed efficacia di un attacco ad un dispositivo di controllo accessi, con componente biometrica.

Ecco perché ho deciso di affrontare il tema della Serie normativa ISO/IEC 30107 - Information technology — Biometric presentation attack detection.

Questa affascinante serie normative illustra le modalità di attacco per impersonamento a sistemi biometrici. È composta di 3 norme che si vanno a illustrare.

Come noto, le norme sono protette dal diritto d'autore e, quindi, non è possibile fornire gratuitamente ai professionisti della sicurezza. Per ogni norma ho preparato un paio di pagine di illustrazione del contenuto, in modo che il professionista interessato possa valutare l'opportunità o meno di acquistare la norma in questione.

Ricordo anche ai colleghi che il comitato normativo estone, al sito https://www.evs.ee/shop, mette a disposizione, gratuitamente, le prime sei o sette pagine, in PDF, di ogni norma menzionata, che abbia già raggiunto lo stadio di pubblicazione.

Sarà così possibile, per i professionisti interessati, approfondire ulteriormente la valutazione della norma e formalizzare un'eventuale decisione di acquisto.

2) ISO/IEC 30107-1, Information technology — Biometric presentation attack detection — Part 1: Framework

Le tecniche biometriche vengono utilizzate per riconoscere degli individui, basandosi su caratteristiche biologiche o comportamentali.

L'efficienza ed efficacia di questi sistemi, soprattutto in applicazioni di controllo accesso a locali fisici oppure a sistemi informatici, fanno sì che essi vengano utilizzati come componente privilegiata nella progettazione di sistemi di sicurezza.

Un sistema di sicurezza, basato su tecnologie biometriche, cerca di riconoscere un individuo e determinare se egli ha titolo per accedere all'area controllata. Sin dall'inizio dello sviluppo di queste tecnologie, la possibilità di neutralizzazione di questi dispositivi ha fatto sì che i criminali investissero tempo e risorse per mettere a punto tecniche di impersonamento, capaci di ingannare il sistema. Dall'altro canto, i progettisti hanno sviluppato contromisure per individuare e bloccare tentativi di impersonamento, chiamati in inglese "presentation attacks".

Il superamento di una specifica funzione di un sistema biometrico può avvenire in qualsiasi parte della catena di comando e controllo, sia da parte di un soggetto esterno, sia da parte di un interno.

La serie normativa che andiamo ad illustrare si concentra tuttavia sulle tecniche di inganno dei sistemi biometrici, che si materializzano nel momento in cui il dispositivo biometrico cattura le caratteristiche del soggetto che desidera entrare. Queste tecniche automatiche fanno riferimento alla individuazione di attacchi di impersonamento. Il potenziale per la neutralizzazione di sistemi biometrici, nel punto della raccolta dei dati, da parte di soggetti criminosi che cercano di impersonare soggetti legittimi, ha posto dei limiti all'utilizzo di sistemi biometrici laddove essi operano privi di sorveglianza, come ad esempio in punti di controllo accesso non direttamente sorvegliati.

Le linee guida per l'autenticazione informatica, per esempio, non raccomandano l'uso di apparati biometrici come fattore di autenticazione, proprio per questa ragione. In applicazioni non controllate, come ad esempio la autentica remota su reti aperte, i metodi automatici di rivelazione di un attacco per impersonamento in corso possono ridurre il rischio dell'attacco.

Per questa ragione, normative, linee guide e tecniche oggettive di valutazione possono rilevare il livello di sicurezza di qualsiasi sistema che utilizzi dati biometrici, sia sotto controllo, sia senza supervisione.

Come è del tutto normale, anche le tecniche di attacco sono soggette agli stessi problemi delle tecniche legittime di verifica ed autentica, vale a dire l'esposizione a falsi positivi ed a falsi negativi.

L'obiettivo di questa prima parte della serie normativa è quella di offrire una base per la classificazione e l'analisi degli attacchi per impersonamento, definendo un glossario e soprattutto definendo un quadro di riferimento attraverso il quale gli attacchi per impersonamento possono essere specificati e rivelati, in modo da poter essere classificati ed inoltrati al sistema decisionale, che governa l'apparato biometrico, per assumere appropriate decisioni.

Vi sono altre due parti di questa serie normativa, riferiti al formato dei dati che trasferiscono l'approccio usato nella rivelazione di attacchi per impersonamento e, rispettivamente, i principi e metodi per valutare le prestazioni degli algoritmi di meccanismi che rivelano l'attacco per impersonamento.

3) ISO/IEC 30107 -2 Information technology — Biometric presentation attack detection: Part 2 – Data formats

La serie normativa ISO/IEC 30107 è composta di tre parti. La seconda parte definisce i formati dei dati che permettono di classificare l'approccio utilizzato nel mettere a punto attacchi per impersonamento a sistemi biometrici. La stessa norma offre la possibilità di classificare i risultati dei metodi di attacco.

È bene sottolineare che gli attacchi presi in considerazione sono esclusivamente quelli che vengono perpetrati al punto di interfaccia tra l'attaccante e il dispositivo che raccoglie il dato biometrico.

Questa parte della serie normativa contiene i seguenti formati di dati:

un formato binario ed uno schema XML.

I formati per lo scambio dei dati sono generici e ciò significa che essi possono essere applicati e utilizzati in una vasta gamma di applicazioni.

La norma suggerisce caldamente che vengano utilizzate delle tecniche crittografiche per proteggere la autentica, l'integrità e la riservatezza di questi dati, anche se sono altre le norme da applicare per questa protezione.

Proviamo ad analizzare quali sono i dati che possono essere generati quando si mette a punto un attacco per impersonamento, diretto un sistema biometrico. I dati possono essere creati in qualsiasi punto del sistema. Per conseguenza i dati disponibili per un campione biometrico possono cambiare in qualsiasi stadio, nella fase di raccolta e successivo trattamento del campione biometrico.

I meccanismi di perpetrazione hanno dei dati in ingresso, come ad esempio il campione biometrico, e generano dati in uscita.

La norma è assai articolata e prevede l'acquisizione di tutt'una serie di dati, relativi alla tecnica di attacco, che permettono di classificare in vario modo i criteri legati alla tipologia di attacco.

La norma si chiude con degli annessi, che offrono alcune semplificazioni, assai accurate, sia dei dati di tipo ordinario, sia dei dati raccolti secondo il formato XML.

4) ISO/IEC DIS 30107-3 Information technology — Biometric presentation attack detection — Part 3:Testing and reporting

I sistemi biometrici attirano l'attenzione dei professionisti della security, ma anche dei criminali! Di Adalberto Biasiotti

La crescente diffusione dei sistemi di controllo accesso e riconoscimento biometrico ha fatto sì che anche i criminali cominciassero a dedicare a questi sistemi le loro poco gradite attenzioni: sono ormai note alcune tecniche di violazione di sistemi biometrici, e per questa ragione uno specifico comitato tecnico ha già sviluppato una proposta di norma per studiare queste nuove tecnologie di attacco.

Si chiama ISO/IEC DIS 30107-3 una proposta di norma, sottoposta a votazione internazionale per il quattro gennaio 2017, che illustra alcune modalità con le quali è possibile attaccare sistemi biometrici, mettendo a punto una metodologia, che individua non solo le modalità di rivelazione dell'attacco per impersonamento, ma anche classifica gli strumenti che vengono adoperati.

Le due sigle fondamentali di questa norma sono rispettivamente PAD -presentation attacks detection e PAI - presentation attack instruments.

L'oggetto della norma è lo studio delle modalità con cui le caratteristiche umane vengono presentate a un sistema di cattura biometrica, con modalità tali da ingannare il sistema. La serie normativa 30107, composta di tre norme, mira proprio a classificare in modo strutturato le tecniche di rivelazione dell'attacco e di perpetrazione dell'attacco stesso.

Com'è noto, i sistemi biometrici sono soggetti a falsi positivi, quando non viene accettato un soggetto, che è quello autorizzato, e falsi negativi, quando viene accettato un soggetto, che invece non è autorizzato. In tutti i sistemi di riconoscimento biometrico si cerca di trovare una ragionevole equilibrio fra le due caratteristiche, per garantire un uso efficiente ed efficace del dispositivo.

L'obiettivo di questa parte della serie normativa illustrata è il seguente:

definire i termini collegati alla individuazione di attacchi per impersonamento, con la illustrazione delle modalità con cui è possibile condurre un test e di analizzare i risultati,

specificare i principi e i metodi per condurre una valutazione delle prestazioni dei dispositivi biometrici.

Questa norma in particolare è dedicata ai produttori di apparati biometrici e ai laboratori di prova, che sono incaricati di condurre delle valutazioni sulle modalità di comportamento del dispositivo a fronte di attacchi per impersonamento.

a) Il rilievo statistico

Le modalità di prova degli apparati biometrici utilizzano per solito una serie statisticamente significativa di esperimenti, in modo da avere a disposizione una banca dati che possa permettere di classificare in modo credibile sia i falsi positivi, sia i falsi negativi. L'esperienza dimostra che l'aumento del numero delle prove accresce il valore statistico dei rilievi.

Negli attacchi per impersonamento, molti dispositivi biometrici possono essere attaccati utilizzando un gran numero di strumenti di attacco. In questi casi è molto difficile o perfino impossibile riuscir avere a disposizione un quadro sufficientemente articolato di tutti gli strumenti che possono essere utilizzati. Questa considerazione è importante perché i ratei che vengono calcolati, utilizzando particolari strumenti di attacco, potrebbero non essere applicabili a diversi strumenti di attacco.

Ad esempio, nella biometrica dell'impronta digitale, sono già conosciuti numerosi strumenti che possono permettere di simulare la presenza di un'impronta digitale, in grado di ingannare un sensore biometrico. Poiché tutti i dispositivi biometrici devono incorporare un certo grado di tolleranza, nella valutazione dell'impronta digitale sottoposta a controllo, in funzione della variazione di età, dell'umidità, della temperatura e di altre tecniche, può essere estremamente difficile riuscire a classificare oggettivamente i ratei di falsi positivi e falsi negativi connessi all'utilizzo di uno specifico strumento di impersonamento.

b) È possibile confrontare i risultati delle prove effettuate su vari sistemi?

Alcuni esperimenti hanno dimostrato come un diverso strumento di attacco può avere ottimi risultati con un particolare sistema e pessimi risultati in un altro sistema. Ad esempio, il fatto che il lettore di impronta digitale possa analizzare l'immagine presentata in profondità, superando l'epidermide, migliora in maniera drammatica l'affidabilità della rivelazione.

c) La cooperazione del soggetto coinvolto

Un altro aspetto meritevole di massima attenzione riguarda il fatto che spesso i dispositivi biometrici non funzionano correttamente per il semplice fatto che chi si presenta per l'uso non si attiene strettamente alle indicazioni, che sono state fornite dal fabbricante. Questo comportamento non cooperativo, che può essere deliberato od accidentale, può alterare in modo significativo le prestazioni del sistema e rendere quindi poco utili i rilievi dei ratei di errore che vengono rilevati durante le prove. Tra le modalità di attacco occorre quindi prevedere anche quelle in cui il soggetto non è cooperativo, perché gli attaccanti cercheranno di sfruttare delle debolezze del sistema, che sono state inserite proprio per rendere il sistema stesso più accessibile a soggetti non cooperativi.

d) Le procedure automatizzate di prova

Per valutare le prestazioni di sistemi biometrici, si cerca talvolta di effettuare dei confronti utilizzando degli algoritmi specifici. L'utilizzo di data base biometrici, con impronte digitali già memorizzate, potrebbe non essere significativo per valutare le prestazioni di un sistema, in quanto il dispositivo di captazione del sistema sotto esame potrebbe catturare parametri che superano l'analisi ottica dell'impronta digitale presentata, andando ad esempio a rilevare parametri che non sono visibili ad occhio nudo, ma solo a speciali apparati, come rivelatori ad infrarosso. Ecco il motivo per cui sistemi automatizzati di prova dei dispositivi biometrici non rappresentano un'opzione accettabile.

e) Qualità e prestazione

Nell'effettuare prove di sistemi biometrici, la prestazione è collegata direttamente alla qualità del dato biometrico. Un dato biometrico di bassa qualità può dare un più elevato livello di errore; ecco perché è indispensabile definire con chiarezza la qualità del campione che viene sottoposto a prova. Ad esempio, l'esperienza ha dimostrato che la realizzazione di una falsa impronta digitale certe volte dà risultati migliori rispetto all'utilizzo dell'impronta digitale originale, perché il simulacro ricostruito ha caratteristiche, che vengono più facilmente accettate e riconosciute dal dispositivo biometrico.

Tutte queste considerazioni giungono alla conclusione, ben illustrata nella norma, che le modalità di test di un sistema biometrico sono decisamente critiche e sono legate a tutt'una serie di parametri, a loro volta legati alle tecniche di attacco ed agli strumenti utilizzati, che possono modificare in modo estremamente ampio i risultati finali delle prove.

La norma è completata da un annesso, che classifica i tipi di attacco, e soprattutto da un annesso, che mette in evidenza alcuni tipi di strumenti di attacco che vengono utilizzati nei confronti di dispositivi biometrici, basati sul riconoscimento dell'impronta digitale.

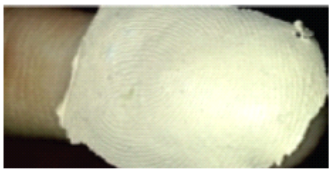
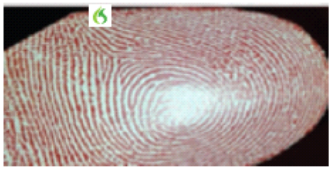
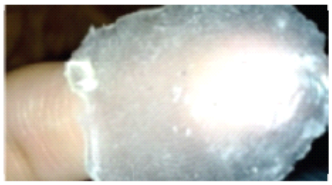
Artefact species	Description	Illustration
Silicon finger artefact	Matte or glossy	
Laser print finger artefact	Ordinary 2D print out	
Gelatin finger artefact	Half-transparent gelatin with glycerin	

Figura 1: Tipologie di attacco

L'Autore: l'ing. Adalberto Biasiotti, è socio A.I.PRO.S. e consulente professionale