Tecniche di Identificazione **Anno Acc. 1997-98**
PROF. ALFREDO DE SANTIS

Tecniche di Riconoscimento

a cura di Flavio Cacace, Ermanno Auricchio e Alessandro Colonna *21 Luglio 1998*

Indice

1 Identificazione Utente

Vi sono molti motivi che rendono necessaria l'identificazione:

- **Potere Computazionale:** le persone fanno calcoli complicati. Cifratura, calcolo dell'hash, etc. tutte richiedono all'utente di eseguire computazioni difficili. Ma le persona non sanno fare computazioni, le macchine si. Come facciamo, come utenti, ad identificarci ad una macchina?
- **Controllo d'Accesso:** permette ad utenti autorizzati di utilizzare le risorse del sistema. Questo puó rifiutare o concedere il permesso ad un utente per accedere ad una risorsa e, limitando gli accessi solo ad utenti autentificati e autorizzati, protegge le risorse. Sistemi computerizzati possono richiedere controlli attraverso login o database personalizzati.
- **Autorizzazione:** permette di assegnare un privilegio di accesso ad un utente. I diritti d'accesso includono specifiche come i permessi in lettura o scrittura, oppure il permesso di modificare un file da parte di un utente. L'identificazione é usata soprattutto nei pagamenti elettronici dove per evitare transazioni "maliziose" é necessario che l'utente venga autorizzato.
- **Auditing:** E' spesso vantaggioso verificare le operazioni compiute da persone autorizzate anche se non ci sono controlli sul posto. Tali verifiche agevolano l'affidabilitá. In caso di attivitá "maliziose", l'utente puó essere ritenuto responsabile. Ció é da ritenersi molto importante soprattutto da quando gli attacchi al sistema vengono portati da persone autorizzate.

1.1 Principi

I sistemi di identificazione devono essere basati su uno dei seguenti principi:

1. ("Qualcosa che l'utente sa"). Password: Spesso compagnie di carte di credito richiedono di fornire il proprio numero di codice oppure dati personali dell'utente per verificare l'autorizzazione via telefono.
2. ("Qualcosa che l'utente possiede"). Un dispositivo serve come Token. I Token sono spesso cose, o fisiche o elettroniche. Le normali chiavi sono un esempio di Token.
3. ("Caratteristiche fisiche dell'utente"). Questo principio é conosciuto come biometrico, cioé la misurazione di alcune caratteristiche biologiche dell'utente.

Le tecniche biometriche possono essere statiche (misurazioni) o dinamiche (riconoscimento calligrafico, analisi della voce, etc.).

1.2 Considerazioni

Progettare o scegliere un sistema di identificazione richiede alcune considerazioni:

- **Resistenza alla contraffazione:** ragionevolmente determinati attacchi non dovrebbero essere in grado di raggirare il sistema di identificazione.

- **Tempo per l'Autenticazione:** l'utente non dovrebbe perdere molto tempo interagendo con il sistema. Le password richiedono solo un paio di secondi, mentre il riconoscimento della firma o la scannerizzazione della retina richiedono piú tempo; fare un'analisi del DNA é addirittura impensabile.

- **Costi dei dispositivi, di distribuzione e di protezione:** sono fattori collegati al progresso tecnologico. Attualmente le passwords sono molto convenienti, a differenza di dispositivi che analizzano il DNA di un utente. Lo sviluppo tecnologico fa diminuire i costi, quindi diventano accessibili metodi molto sofisticati.

- **Complessitá di Aggiornamento:** mantenere informazioni sulla identificazione di un utente per un certo periodo di tempo, o aggiungere una nuova autentificazione puó richiedere spreco di tempo. Questo si verifica specialmente per sistemi basati sul riconoscimento vocale, che richiede un periodo di addestramento per riconoscere la voce dell'utente.

- **Tempo Computazionale:** spesso il tempo speso dalla CPU a computare le informazioni, puó essere un problema. Una tecnica che richiederebbe un minuto per completare l'identificazione potrebbe essere fastidiosa per gli utenti. In questo caso le passwords sono efficienti a differenza del riconoscimento vocale.

- **Affidabilitá:** molte tecniche soffrono di problemi di affidabilitá. Per esempio il segno di un'impronta digitale potrebbe sporcare il lettore e divenire inutilizzabile per leggere correttamente le impronte digitali successive, rifiutando cosí l'accesso di un utente autorizzato.

- **Accettabilitá dell'utente, facilitá d'uso, fattori psicologici:** é importante che gli utenti si sentano a proprio agio con il sistema di identificazione. Sono da considerare anche fattori psicologici: per esempio lo scomodo uso delle impronte digitali, soprattutto da quando il riconoscimento delle impronte digitali é associato con attivitá criminale. Anche l'idea di lasciare entrare nei propri occhi un raggio luminoso per eseguire la scansione della retina, non provoca entusiasmo da parte degli utenti.

- **Trasferibilitá:** le passwords sono facilmente trasferibili, diversamente dalle scansioni della retina. Le proprietá di trasferibilitá dipendono fortemente dal sistema, come puó essere rischioso dare le passwords all'esterno della rete. La trasferibilitá suggerisce anche una maggiore potenzialitá contro il furto.

- **Accuratezza:** é spesso misurata con due quantitá: FAR (False Accept Rate) e FRR (False Reject Rate). Il FAR misura la percentuale di utenti non autorizzati che riescono a passare il sistema di sicurezza; mentre l'FRR misura la percentuale di utenti autorizzati che sono rifiutati dal sistema pur essendo autorizzati. L'accuratezza é usualmente misurata come il punto di incontro tra FAR e FRR. (Vedi Figura 1).

1.3 Storia

- I messaggeri del Re, in epoca medioevale, usavano portare anelli marchiati per identificarsi.
- Molto importante fu la scoperta che i cinesi, giá 2000 anni fá, usavano le impronte digitali.

Figura 1: Tradeoff tra FAR e FRR.

- Il sistema Bertillon, datato 1870, fu usato negli USA per l'identificazione criminale. Questo sistema identificava una persona da alcune caratteristiche misure come l'altezza, ampiezza del capo, altezza del torace, lunghezza dell'avambraccio, etc.. Comunque famoso fu il caso del 1903 negli USA in cui furono trovate due misure di Bertillon identiche. Il giorno dopo, le impronte digitali divennero la forma dominante di riconoscimento criminale.
- Le passwords sono state lungamente usate durante i periodi bellici.

2 Passwords

Le passwords sono economiche, facili e ragionevolmente precise, e perció di largo uso.

2.1 Proprietá

Le password hanno 2 proprietá fondamentali:

- difficili da indovinare

- facili da ricordare

2.2 Vulnerabilitá

Morris e Thompson [1] esaminarono 3289 passwords e trovarono che l' 86% (2831) di esse era vulnerabile per una delle seguenti ragioni:

- 15 erano singoli caratteri ASCII
- 72 erano stringhe di 2 caratteri ASCII

- 464 erano stringhe di 3 caratteri ASCII
- 477 erano stringhe di 4 caratteri alfanumerici
- 706 erano stringhe di 5 lettere, tutte o maiuscole o minuscole
- 605 erano stringhe di 6 lettere, tutte minuscole

Altri caratteri di vulnerabilitá sono:
- parole comuni
- nomi comuni
- informazioni facili da ottenere (data di nascita, numero di telefono ect)
- modello della tastiera (QWERTY)
- password di altri sistemi
- permutazioni della password (specialmente riscritte all'indietro)

2.3 Scelta di una Password

Diamo alcuni consigli per scegliere una password:
- misto di lettere minuscole e maiuscole
- uso di parole non pronunciabili
- includere caratteri non alfanumerici
- misto di lettere e numeri
- sistematica sostituzione, come di o con 0 (zero), oppure l con 1 (uno)
- scegliere la prima lettera delle parole costituenti una frase di senso compiuto significanti
- generazioni con il computer; queste sono combinazioni difficili da ricordare, e lo stesso programma di generazione potrebbe avere dei bug.

2.4 Memorizzare una Password

Le Passwords possono essere memorizzate ovunque. L'utente deve ricordare la parola d'ordine o memorizzandola o appuntandola. Anche il computer deve ricordare la password cosí puó provare l'identificazione di un presunto utente. Enunciamo alcune tecniche:

- **in chiaro nel file system:** questa non é un alternativa ottimale, infatti un utente che ha accesso al file system conosce le password di tutti gli utenti del sistema.
- **su un server dedicato:** questa é un alternativa migliore, sebbene un cattivo funzionamento del server rivelerebbe le passwords degli utenti.
- **in maniera cifrata:** in questo modo anche se il file delle passwords fosse compromesso, nessuna informazione si otterrebbe perché questo é crifrato.
- **hash:** l'uso di una funzione hash one-way, come MD5. Quando l'utente digita la password, ne viene fatta l'Hash, ed il suo valore viene compattato e memorizzato. Conoscere il valore Hash di una password non serve all'utente per identificarsi. Un trucco ulteriore é quello di aggiungere al valore Hash, una stringa che contiene informazioni sull'utente, tale valore é detto salt. Questo valore implica la memorizzazione della coppia di valori

(PWD,SALT). Il Salting previene la precomputazione del valore hash da parte di un nemico e fa aumentare il tempo computazionale di chi attacca.

- **con controllo d'accesso:** é spesso utilizzato da tutti gli utenti che hanno la necessitá di accedere ad alcune informazioni contenute nel file delle passwords, ma non possono accedere alle passwords recenti. Alcuni sistemi dividono in 2 "pezzi" il file contenente le parole d'ordine; in uno le informazioni degli utenti, l'altro, memorizzato in un posto segreto, contiene le password attuali.

2.5 Cambiare la Password

Cambiare frequentemente le passwords aumenta la sicurezza, anche se le rende piú difficili da ricordare. Le password dovrebbero essere cambiate almeno una volta all'anno; non é consigliabile riutilizzare vecchie password specialmente se usate di recente. Altri sistemi, invece, restringono la frequenza delle password cambiate, mentre altri ancora richiedono periodici cambi. E' opportuno cambiare la password dopo un uso che potrebbe averla compromessa (per esempio login remoti).

2.6 One-Time Passwords

L'idea che sta dietro al One-Time é di fornire l'utente di una lista di passwords, ognuna delle quali puó essere usata una ed una sola volta.

2.6.1 SKEY

E' un programma di autentificazione che basa la sua sicurezza su una funzione one-way.
Funzionamento: Alice da in input un numero casuale, R . Il computer calcola *f(R), f(f(R)), f(f(f(R)))*, ..., e cosí via, per circa cento volte. Chiama questi numeri x_1, ..., x_{100}. Il computer da in output la lista dei numeri che Alice conserva per sicurezza. Inoltre il computer memorizza il valore x_{101}, in chiaro, nel database di login.
La prima volta che Alice vuole identificarsi digita il suo nome e il valore x_{100}. Il computer calcola $f(x_{100})$ e lo confronta con x_{101}; se questi coincidono, Alice é autorizzata. Successivamente il computer sostituisce il valore x_{101} con x_{100} nel database. Alice elimina x_{100} dalla sua lista. In generale, ogni volta che Alice vuole identificarsi, digita l'ultimo numero non cancellato dalla sua lista: x_i. Il computer calcola $f(x_i)$ e lo confronta con x_{i+1} memorizzato nel suo database. Questo sistema non puó dare nessuna informazione utile poiché ogni numero é usato una sola volta, e la funzione f é one-way. Analogamente il database non é utile per chi attacca. Ovviamente quando Alice esaurisce i numeri della lista deve rieseguire l'intera procedura.

3 Token

3.1 Tipi

- **Chiavi Fisiche:** sono chiavi convenzionali. Alcuni sistemi in uso in Europa hanno una doppia chiave, dove una chiave apre e l'altra chiude.

- **Chiavi Magnetiche:** un esempio solo le carte di credito

- **Le Smart-Card:** hanno le stesse dimensioni e forma delle carte magnetiche. In una smart-card si evidenziano 3 parti fondamentali in ogni transazione (Utente, Smart Card, Sistema Esterno)

3.2 Riproduzione

- **Chiavi :** le ordinarie sono molto facili da duplicare. Le chiavi di alta sicurezza hanno forme e caratteristiche strane che aumentano la sicurezza.

- **Mag Strip Card:** piú sicure delle normali chiavi, ma riproducibili con una spesa molto limitata e in poco tempo. Infatti é possibile copiare la parte magnetica da una carta all'altra.

- **Smart Card:** molto piú difficile da riprodurre rispetto alle Strip Card.

4 Tecniche Biometriche

4.1 Introduzione

Le tecniche biometriche utilizzano le caratteristiche fisiche di un utente per l' identificazione. Sebbene tali tecniche non sono generalmente efficienti come le passwords, in quanto risulta difficile ottenere una percentuale di errore al di sotto dell' 1%, esse d'altra parte offrono un grado di sicurezza superiore. Infatti, le passwords possono essere scoperte per disattenzione e i caratteri possono essere persi o dimenticati, mentre le caratteristiche fisiche di una persona sono piú difficili da copiare. I metodi di misurazione delle caratteristiche fisiche hanno una lunga storia, in modo particolare nelle applicazioni inerenti alla detenzione criminale. Il sistema Bertillon, usato specialmente in Francia per circa 40 anni a partire dal 1870, si basava su misure corporee come la lunghezza dell' avambraccio e delle dita, l' altezza, l' ampiezza del cranio, la lunghezza dei piedi, etc.. Questo metodo, conosciuto come antropometria, serviva a conservare schedature di noti criminali e cercare di verificare l' identitá dei sospetti tramite le misurazioni fatte all' arresto. Usando questo sistema non era difficile trovare coppie di persone con le stesse misure entro i limiti di errore permessi. Il sistema Bertillon fu ampiamente rimpiazzato dalla introduzione dell' identificazione tramite le impronte digitali. Questo sistema é stato suggerito come tecnica nell metá del 1880 e fu adottato dalla polizia metropolitana londinese verso il 1900. Riconoscere individui é una esperienza comune a tutti. Lo facciamo sulla base di differenti caratteristiche fisiche: l'aspetto del volto, il colore e la lunghezza dei capelli, la statura e la stazza, il rumore dei passi, la voce e perfino l'odore. Riconosciamo anche le firme scritte quando riceviamo lettere o documenti; una firma si scrive per abitudine e non rappresenta un' azione controllata puó quindi essere considerata quasi come un attributo fisico; alcuni di questi si prestano convenientemente ad una macchina concepita per il riconoscimento, altri invece non si adattano facilmente al processo di misura e di verifica di una macchina.

4.1.1 Tecniche di Riconoscimento

E' sorprendente come molte diverse tecniche di riconoscimento siano state oggetto di sperimentazione da parte dei ricercatori. Alcuni degli schemi piú realistici includono il riconoscimento di firme, l'uso di impronte digitali e il riconoscimento vocale; considereremo ognuna di queste tecniche in alcuni aspetti. Alcuni di questi schemi meno conosciuti hanno provato ad usare impronte delle labbra, impronte prese dalla pianta del piede, ramificazioni dei vasi sanguigni della mano o del polso ed anche ricettivitá dello scheletro a stimoli fisici. Il peso dell' individuo é un altro parametro che é stato suggerito; non ci si puó aspettare una elevata discriminazione se la verifica dipende solo dalla misura del peso, sebbene ció puó essere usato come ulteriore verifica. Abbiamo giá posto l' accento sul bisogno di un sistema di riconoscimento che soddisfi determinati requisiti. Alcune delle idee appena menzionate non soddisfano tale richiesta, sebbene potrebbero comunque fornire buoni strumenti di riconoscimento. Per misurare le impronte delle labbra l' utente dovrebbe baciare l' interfaccia; ció non é facilmente accettabile dal punto di vista igienico, ed é esteticamente spiacevole. Le impronte della pianta del piede si possono ottenere se gli utenti sono disposti a togliersi le scarpe e calzini -possibilmente accettabile per l' accesso in piscina, ma difficilmente appropriato per un ufficio-. La ricettivitá dello scheletro nei confronti di uno stimolo ben calibrato puó essere misurata con un colpo controllato applicato ad alcune parti del corpo.

Un problema molto importante é il grado di rischio a cui un intrusore é esposto nel caso in cui il suo tentativo fallisca. E' molto probabile che sará acciuffato, quindi non fará alcun tentativo a meno che l'azione d' intrusione quasi sicuramente abbia successo e sia conveniente. Il fallimento nel riconoscimento puó essere reso noto tramite un allarme che desti l'attenzione di una guardia. Ció puó essere combinato con un sistema di intrappolamento in cui il soggetto é costretto ad entrare prima di qualsiasi operazione d' identificazione: ció rende l' eventuale intrusione molto piú rischiosa. Nonostante utenti autorizzati accettano tali misure poco confortevoli, rimane un problema da valutare attentamente la possibilitá di falsi allarmi occasionali. Queste forti misure fisiche non sono possibili in molti ambienti in cui é richiesto un riconoscimento personale. In una banca che utilizza il sistema ATM (Automated Teller Machines) il potenziale intrusore puó raggiungere completamente inosservato il proprio scopo. In queste circostanze é importante non permettere la ripetizione illimitata dei tentativi per ottenere il riconoscimento. Con il sistema ATM é possibile ritirare la carta dell' utente dopo tre fallimenti nella digitazione del PIN corretto. Questa misura non é ritenuta accettabile ovunque. Negli USA ed in altri luoghi il ritiro della carta rappresenta una grossa inconvenienza. In tali circostanze il sistema deve rilasciare la carta all' utente anche se ció da adito ad alcune irregolaritá. Un sistema "on line" potrebbe notificare i ripetuti tentativi falliti e creare una "lista nera" delle carte in questione per poi contattare gli utenti autorizzati.

4.1.2 Tolleranza del Sistema

Le misure delle caratteristiche fisiche di ogni individuo subiscono di tanto in tanto una sensibile variazione. Perció un sistema di verifica d' identitá realistico, ne deve tener conto e calcolare un margine di errore tra le misurazioni degli utenti. Sorge peró il problema che al crescere della tolleranza aumenta il numero di false identificazioni. Se un sistema fallisce nel riconoscimento di un individuo regolarmente autorizzato allora parleremo di "falso allarme" o "errore di Tipo 1" (FRR). D'altra parte, se un sistema accetta un individuo non autorizzato, allora questo sará chiamato "errata accettazione" o "passagio di un impostore" o "errore di Tipo 2" (FAR). Vedremo che esiste un trade-off tra l'incidenza degli errori di Tipo 1 e Tipo 2. Adesso consideriamo diversi sistemi di riconoscimento che sono stati oggetto di ricerca e sviluppo e che sono divenuti prodotti commerciabili. Tra le tecniche biometriche esamineremo:

-Riconoscimento vocale;

-Riconoscimento della firma;

-Firma dinamica;

-Impronte digitali;

-Geometria della mano;

-Scansione della retina;

-Scansione dell' iride;

-Riconoscimento del volto;

-Caratteristiche di battitura ed uso del mouse;

Nella valutazione delle tecniche biometriche dovremo tener conto dei seguenti parametri: il tempo impiegato per effettuare le misure, i costi dell' attrezzatura, il fattore psicologico, le identificazioni maliziose e i riconoscimenti falliti di utenti autorizzati.

4.2 Riconoscimento Vocale

Riconoscere persone attraverso la loro voce é una capacitá dell' uomo che si é molto sviluppata ed adeguata in ogni sorta di circostanza, anche in presenza di rumore. Questa capacitá viene spesso utilizzata nelle transazioni commerciali, in cui le due parti di un affare si riconoscono l' un l' altro in una conversazione telefonica. Molti sforzi sono stati fatti nel tentativo di realizzare un sistema fidato di riconoscimento vocale come un modo per fornire prove in un tribunale; la produzione delle impronte vocali e la loro analisi da parte di esperti é un argomento che ha creato moltissimi dibattiti. Il dispositivo che esegue il riconoscimento vocale confronta le caratteristiche del suono con un insieme di dati ricevuti da ogni individuo. E' importante creare le giuste condizioni per riconoscere colui che parla, eliminando qualsiasi alterazione e disturbi ambientali. Un luogo con eco potrebbe causare problemi. Idealmente colui che parla dovrebbe trovarsi in un ambiente insonorizzato. Inoltre dovrebbero esserci ulteriori controlli dopo che la frase é stata pronunciata. Non é generalmente richiesto che l' utente pronunzi il proprio nome; alcuni nomi, ad esempio Kim King e Paddington Bear, producono suoni molto simili, quindi poche informazioni da elaborare. Idealmente il sistema dovrebbe richiedere la pronuncia di piccole frasi selezionate per massimizzare la quantitá di informazione utilizzata per poter distinguere gli utenti. Le parole scelte dovrebbero essere quelle che l' utente pronuncia piú spesso. Nella tecnica di riconoscimento vocale sviluppata da Texas Instruments inizialmente ogni utente pronunciava un insieme standard di 60 parole. Cosí il processo di riconoscimento usava principalmente i suoni delle vocali, infatti le parole erano scelte affinché contenessero differenti suoni di vocali o di dittonghi. Il sistema generava 32 frasi costruite sul vocabolario delle 60 parole. Con l' uso dell' analisi di Fourier e con intervalli di campionatura di 10ms, le frasi erano analizzate nelle parti in cui l' ampiezza di banda era considerevolmente larga e le informazioni fonetiche erano valide. Per ogni transizione identificata l' energia compresa tra i 300 e i 2500 Hz viene misurata per un periodo di 100ms fornendo cosí un modello di dati per l' utente. Nella fase di verifica l' utente pronuncia la frase presentatagli dal sistema, frase sulla quale viene applicata una trasformata di Fourier ogni 10ms. Il sistema confronta la frase con i modelli del database e cerca un' attinenza entro i limiti prestabiliti. Il sistema ha lo svantaggio di spendere molto tempo nella fase di interazione con l' utente, anche il processo di analisi richiede tempo. Quindi il troughput puó essere basso e il delay time considerevole. Inoltre la voce é condizionata dallo stato fisico delle persone, infezioni respiratorie causano cambiamenti nella qualitá della voce e addirittura stati emotivi influiscono su di essa. La richiesta di ripetere la procedura di identificazione potrebbe causare stress nell' utente e quindi allontanare la possibilitá di una corretta identificazione.

4.3 Riconoscimento della Firma

La firma é da molto tempo usata come un modo per accettare un documento, per esempio, un contratto. Piú recentemente é diventato un modo per riconoscere l' identitá di un utente, per esempio, nell'uso di carte di credito. Tradizionalmente la verifica di una firma dipendeva da un esame visivo e coinvolgeva il giudizio critico da parte di un verificatore, che tal volta non era particolarmente qualificato ne motivato nel compito assegnatogli. Laddove la validitá di una firma é in dubbio, per esempio in tribunale, testimoni competenti sono chiamati a deporre sulla paternitá di un particolare tratto di scrittura. Le firme sono scritte cosí frequentemente tanto da diventare un' azione riflessa, quasi un attributo fisico del firmatario, non soggetta ad un volontario controllo muscolare. L' imitazione di una firma é un processo molto difficile, specialmente se un tentativo viene eseguito a velocitá normale di scrittura. Molta attenzione é stata prestata nella ricerca di metodi di trattamento della scrittura attraverso macchine, sia con lo scopo di interpretare il senso di ció che é stato scritto e sia di riconoscere l'autore dallo stile della scrittura.

Nel riconoscimento di una firma non ci interessa interpretare lo scritto, bensí solo stabilire l'identitá dell' autore. La verifica puó essere compiuta o su firme scritte in precedenza (verifica statica) o su firme osservate durante il processo di scrittura (verifica dinamica). La maggior parte dei progetti di ricerca sulla verifica automatizzata si é concentrata su quest' ultimo metodo, ma anche il precedente ha una importante funzione, come nella verifica di firme su assegni. Le firme false su documenti possono essere di tre tipi: falsificazioni freehand (su carta bianca), imitate e copiate. La falsificazione freehand puó avvenire quando un libretto di assegni viene perduto dal suo proprietario e trovato da qualcuno che non ha idea di come il proprietario normalmente scrive la sua firma. Poiché i nomi dei titolari di un conto adesso sono stampati sugli assegni bianchi, il ritrovatore pone una firma che corrisponde al nome sull' assegno. Nelle falsificazioni imitate o copiate il falsificatore ha un esempio su cui lavorare. La scoperta di contraffazioni freehand puó essere basata sull' analisi della vera firma in termini di dimensioni e inclinazioni misurate sia per la firma intera sia per le singole lettere. Queste misure sono immagazzinate nel file di un computer per controllare l' identitá. Risultati molto promettenti sono stati ottenuti con un sistema progettato da Nagel e Rosenfeld. Queste tecniche non sono applicabili se le firme contraffatte sono state imitate o copiate. Un altro significativo sviluppo nel campo del riconoscimento di firme é dovuto al sistema sviluppato all' NPL(National Physical Laboratory). Il progetto NPL misura empiricamente "caratteristiche" scelte dalle firme che sono costanti ed uniche per ogni idividuo; vengono utilizzate solo misurazioni globali cioé che coinvolgono l' intera firma. Vengono valutate sette caratteristiche, ciascuna variabile su una scala da zero a nove. Il grado di discriminazione fornito con questi parametri é sufficiente per le applicazioni bancarie e quelle che utilizzano carta di credito. Nel processo di verifica si considerano anche le carartteristiche dinamiche di una firma, introducendo un set di parametri, allora ció puó rendere la fase di verifica piú semplice e il lavoro di un falsificatore piú difficile. Infatti, siamo interessati alle firme scritte in tempo reale, laddove la verifica della firma rappresenta un mezzo per il riconoscimento. Il dispositivo di verifica, é preposto a misurare il ritmo della scrittura, cioé il modo in cui la penna tocca consecutivamente la superfice e si solleva da essa. Si puó usare un determinato numero di misurazioni da applicare all' intera firma. Ad esempio si puó considerare il tempo utilizzato da un utente per scrivere la propria firma; parametro che variando di poco puó essere utilizzato come test iniziale per individuare un impostore. Un importante progetto di ricerca all' NPL produsse un sistema dinamico di verifica chiamato VERISIGN. Questo sistema utilizzó dieci misure che quantificavano diverse caratteristiche delle firme, includendo il numero di contatti, i punti di svolta, i cicli, le inclinazioni, la velocitá e l' accelerazione.

4.3.1 Tecniche per registrare il movimento della penna

Le tecniche per misurare il movimento della penna si sono sviluppate rapidamente durante questo secolo. La tecnica piú recente é stata quella del Teleautograph che usava un sistema di leve per registrare i movimenti dello stilo; i movimenti furono quindi digitalizzati per una trasmissione su una linea di comunicazione. Da allora la Teleatograph Corporation ha sviluppato tecniche piú sofisticate di acquisizione dei movimenti della penna e progetti con lo stesso scopo. Piú recentemente le penne sono state inserite in accellerometri ortogonali che registrano l' accellerazione in due direzioni; altri progetti hanno misurato il valore della pressione esercitata durante la scrittura. Tutti i progetti che misurano un qualche parametro e lo trasmettono all'apparecchiatura preposta all' analisi hanno il problema di come collegare (tramite filo o cavo) la penna per inviare i dati. Un collegamento del genere puó risultare inconveniente allo scrittore in quanto questi puó cambiare lo stile della sua firma o addirittura sbagliarla. Tuttavia é auspicabile trovare un metodo che registri il movimento della penna senza ostacolare l' utente. Le tecniche esaminate usano un tampone che é in grado di tracciare il movimento della penna in termini di spazio bidimensionale ed anche di misurare la presenza o assenza di contatto con la superfice. Un tampone di questo tipo fu ideato all' NPL con il nome di CHIT. Esso consisteva in due membrane conduttrici che normalmente non erano in contatto, cosa che invece avveniva quando si usava lo stilo. Fu quindi possibile misurare le coordinate X ed Y del punto di contatto trattando ciascuna membrana come un dispositivo che converte un segnale di natura fisica in un segnale elettrico. Il tampone fu utilizzato per campionare le coordinate cinquanta volte al secondo. Il CHIT fu utilizzato nel sistema VERISIGN dell' NPL. Altri sistemi che usavano tamponi speciali per registrare firme utilizzarono solo il tempo di contatto con la superfice; ció fornisce meno informazioni sulla firma e risulta difficile distinguere le firme vere da quelle false.

4.3.2 Utilizzo del sistema

Per farsi conoscere da un sistema di verifica di firma ciascun utente deve prima fornire un numero di firme campione. Il sistema di verifica le analizza e registra le loro caratteristiche; ad ogni soggetto richiede piú firme finché é soddisfatto della coerenza dei parametri. Per utenti che normalmente firmano in modo incoerente il sistema prevede misure speciali. Queste possono includere un aumento della tolleranza o la richiesta di utilizzare un altro mezzo di accesso. D' altra parte, se la tolleranza aumenta é piú semplice per un impostore assumere un' altra identitá. Quando gli utenti si presentano per la verifica, é loro permesso un numero limitato di tentativi. Un fallimento nel riconoscimento porta l' utente a tentare l' accesso in un altro modo oppure l' accesso é negato. Poiché il modo di scrivere degli utenti puó variare lentamente col tempo, il sistema puó avere un grado di adattabilitá; questo deve essere scelto accuratamente poiché ció puó aumentare il numero di impostori che riescono a superare la fase di accesso.

4.4 Verifica delle Impronte Digitali

E' stato da molto tempo riconosciuto che gli individui si differiscono per il tipo di impronta digitale e per altre caratteristiche del corpo. Inoltre la differenza tra impronte digitali é cosí evidente che é generalmente impossibile trovarene uguali a due persone. Anche se le dimensioni delle dita cambiano al crescere dell 'individuo la geometria delle sue impronte digitali non subisce alcuna variazione; a meno di interventi di chirurgia plastica conserviamo per tutta la vita il nostro modello di impronta digitale. Poiché le impronte digitali sono facilmente recuperabili da una superfice, ció le ha rese molto utilizzate nell' ambito della investigazione criminale. Diverse tecniche sono state usate per la rilevazione delle impronte nascoste rendendole visibili per fotografie e memorizzazioni temporanee. Al fine di riconoscere individui sospetti é necessario essere in grado di classificare le impronte digitali secondo i loro aspetti caratteristici. Il sistema usato da gran parte delle forze di polizia si basa su quello ideato da Edward Henry, Metropolitan Police Commissioner, 1897. I tratti fondamentali sono archi, anelli e vortici. Ogni impronta digitale ha una o piú di queste caratteristiche sebbene le piú piccole sfumature o minuzie giocano un ruolo importante nella loro classificazione. Queste piccole caratteristiche sono simili a linee troncate e biforcazioni come possiamo vedere in Figura 2:

Figura 2: Tratti salienti delle impronte digitali

Tipicamente ve ne sono da 50 a 200 su un dito e una corretta identificazione dipende concretamente dalla loro posizione e direzione. Basta rilevare 20 aspetti particolari per rendere corretta l' identificazione. I sistemi sono stati progettati per automatizzare il processo di acquisizione e verifica dei dati sulle impronte digitali. In realtá sono stati fatti tentativi per analizzare impronte digitali con l'ausilio di dispositivi meccanici, automatizzando l' intero processo, ma ció non é facile se le impronte risultano poco chiare e incomplete.

4.4.1 Dispositivi per il riconoscimento delle impronte digitali

Da non trascurare é il grado di disponibiltá con cui l' utente accetta di identificarsi attraverso la lettura delle proprie impronte digitali. In un tale sistema non é richiesto l' uso di un tampone ichiostrato per leggere una impronta; infatti l' utente pone il suo dito su una su un' apposita superfice dove la lettura implica la riflessione dell' impronta digitale su uno specchio. Poiché la posizione dell' impronta puó variare di volta in volta é necessario che il dispositivo di input permetta all' immagine acquisita di effettuare piccoli angoli di rotazione. Il dispositivo cerca i tratti particolari e ne riconosce posizione e direzione. Questi dati vengono confrontati con quelli presenti nell' archivio del sistema. Possono insorgere problemi in fase di verifica con utenti che si procurano ferite alle dita. Per quanto riguarda l'accettazione di un sistema di riconoscimento basato su impronte digitali c'é, sfortunatamente, da parte degli utenti un ostacolo psicologico in quanto le impronte digitali sono associate alle procedure di schedatura dei criminali. Molti cittadini onesti sono molto restii a memorizzare le loro impronte in un computer. L' accettazione si basa sull' affidabilitá del sistema nell' identificare gli utenti e sulla sua convenienza. Un sistema di impronte digitali é costoso perché il dispositivo di input é complesso e il processo di verifica difficile. In queso aspetto i sistemi dinamici di verifica della firma sono migliori.

4.5 Geometria della Mano

Si basa sulle misurazioni delle caratteristiche fisiche delle mani degli utenti per determinare l'identitá. Tipiche misure sono la lunghezza delle dita, ampiezza della mano e spessore delle dita. Questo é uno dei migliori metodi biometrici in termini di precisione e accettabilitá da parte degli utenti. La sicurezza offerta da questo metodo é fonte di discussione.

4.6 Analisi dell'Iride

Simile al concetto di impronta digitale, ma ha come modello l'iride. Questo metodo riceve potenzialmente 6 volte piú informazioni del metodo di impronta digitale.

4.7 Riconoscimento del Volto

Il lavoro sullo sviluppo delle tecniche di riconoscimento del volto sono state fatte da Tommy Poggio's group e Ai Lab. Il computer prende una immagine della faccia di un utente e la confronta con quella memorizzta su un disco. La tecnologia per questo metodo é tuttavia in fase di sviluppo, e probabilmente sará pronta per l'uso fra 10 a 20 anni.

4.8 Scansione della Retina

Il modello dei vasi sanguigni di una retina dell'occhio umano, rappresenta una caratteristica discriminante per ogni individuo. Un sistema di identificazione che usa questa proprietá, é stato sviluppato da Eydentify Inc. of Portland, Oregon (versione di un disposistivo che usa un sistema monoculare). La macchina permette di localizzare la fovea del soggetto ed inizia l'analisi con un movimento a spirale utilizzando un raggio infrarosso di bassa intensitá. Quindi essendo il punto di riferimento del dispositivo, questo scoprirá tutto il modello retinale che cade all'interno dell'area scannerizzata. La Figura 3 seguente mostra la geometria della retina:

Figura 3: Retina

Il modello retinale acquisito, puó quindi essere confrontato con il modello memorizzato usando una tecnica che utilizza trasformate di Fourier (Cross Correlation). Questa tecnica non é accettata dagli utenti poiché richiede che un raggio di luce di penetri nell'occhio. Un'altro problema di questo metodo é l'allineamento della testa in relazione allo scanner.

4.9 Caratteristiche di battitura e uso del Mouse

Una ulteriore tecnica é quella di riconoscere un utente dal suo stile di battitura o dall' uso del mouse. Questo metodo veniva comunemente usato durante la prima guerra mondiale con lo scopo di determinare quale operatore stava battendo il codice Moorse tedesco. Possibili problemi sorgevano se l'utente variava il suo stile.

4.10 Il Processo di Verifica

Tutti i metodi di verifica dell'identitá che usano discriminanti caratteristiche dell'uomo hanno molti punti in comune. Analizzeremo in modo generale il Tradeoff di questi sistemi. In primo luogo consideriamo 2 fasi, introduzione di un nuovo utente e la sua successiva verifica d'identitá.

4.10.1 Introduzione Utente

L'utente procede alla fase di introduzione (di solito sotto la supervisione di un operatore) fornendo elementi identificativi come il nome o altre caratteristiche, e poi esegue le operazioni richieste come: scrivere la propria firma, presentare l'impronta digitale del dito per la scannerizzazione o pronunciare un insieme di parole. Questa operazione é ripetuta il numero di volte necessario a creare un affidabile "reference set", cioé un insieme di misure di riferimento caratteristiche di ogni utente. Il sistema memorizza il profilo dell'utente o in un file o in un Token, come ad esempio una carta magnetica.

4.10.2 Fase di Verifica

Prima di iniziare la procedura di verifica, l'utente rivendica la propria identitá tramite documenti identificativi. L'identificativo deve essere unico - ogni utente ne ha uno diverso. il sistema cerca il profilo identificativo presentato dall'utente. Successivamente l'utente é invitato ad eseguire le azioni su cui il sistema di verifica si basa. Il sistema costruisce il profilo dell'utente con le misure fornite e confronta tale profilo con il corrispondente profilo di riferimento. Sia il profilo misurato che quello di riferimento sono composti una serie di parametri, che rappresentano il risultato di calcoli fatti dopo le misurazioni iniziali. Ad esempio, la misurazione della firma dinamica potrebbe avere come parametri un insieme di coordinate calcolate ad intervalli di 20ms, la velocitá di movimento o i cambi di direzione della penna. I parametri sono progettati in modo che sia difficile che un impostore riesca a controllarli.

Le misure utilizzate per la verifica di ogni individuo subiscono di tanto in tanto una sensibile variazione. Perció l'esatta corrispondenza tra i parametri misurati e quelli di riferimento é poco utilizzata. La decisione di rifiutare o di accettare l'identificazione di un utente perció richiede un intervallo di tolleranza dell'errore. Ogni parametro puó avere una propria tolleranza e le tolleranze possono essere decise utilizzando misurazione ripetute, fatte nella fase in cui l'utente viene introdotto nel sistema. Entrambe le tolleranze e i valori di riferimento sono suscettibili a variazioni. Questa fase d'apprendimento é meno significativa in sistemi come la verifica delle impronte digitali o la scansione della retina. Adattare i valore misurati puó essere fatto solo quando l'identificazione é verificata; questo lavoro di adattamento viene fatto soprattutto tenendo conto della possibilitá di impostori. Per questa ragione l'adattamento dei valori deve essere molto graduale e il grado di tolleranza deve essere limitato alla possibilitá che impostori non ottengano il permesso dal sistema.

4.10.3 TradeOffs

Stabilire il margine d'errore é una fase critica per la pefomance del sistema. Se l'indice di tolleranza é alto, allora la discriminazione tra gli utenti si riduce e l'indice di accesso degli impostori (Errore Tipo II) é alto. D'altra parte, se la tolleranza é bassa, utenti autorizzati potrebbero incontrare difficoltá in fase di verifica, e quindi aumenterebbe l'indice di allarmi falsi (Errore Tipo I). Generalmente il livello del grado di tolleranza é adattabile e si puó calcolare un tradeoff tra i due tipi d'errore. La Figura 4 mostra una tipica caratteristica dei sistemi di verifica, evidenziando come l'indice di identificazioni corrette varia al variare della tolleranza.

Figura 4: Rapporto tra identificazioni corrette e tolleranza

Il modo in cui sono determinati l'errore e la tolleranza fanno parte del sistema e ci sono diversi modi per calcolarli. Infatti vedremo come la fase di testing serve per adattare il valore della tolleranza.

Dopo le misurazioni iniziali, (come la posizione della penna o l'energia di un spettro vocale) vengono computati una serie di parametri. Spesso questi sono elaborati facendo la media dei valori misurati, ció per ridurre la loro variabilitá. Nel lavoro di ricerca fatto da Versign, dozzine di parametri furono inventati e testati su un grosso insieme di firme e, di questi, 10 furono selezionati perché soddisfacevano le richieste prima menzionate. Per ogni parametro, l'insieme delle misure di riferimento é usato per trovare i valori medii e la varianza. Usando la deviazione standard come unitá di misura, l'errore di ogni parametro puó essere normalizzato. Si potrebbe ottenere una singola misura dell'errore, per esempio sommando i quadrati dei parametri normalizzati. Ció permette di sbagliare al piú un parametro. Il sistema di Verisign non lavorava in questo modo, infatti richiedeva che ogni parametro venisse ridotto entro certi limiti. Per raggiungere una tolleranza accettabile un singolo valore t é usato per indicare la tolleranza. Per esempio sia x un parametro, e sia m il valore medio ottenuti dai valori di riferimento, allora l'errore é $\mid x - m \mid$, e $\mid x - m \mid /s$ é l'errore normalizzato dove s é la derivazione standard dell'insieme di riferimento. La condizione di accettabilitá potrebbe essere scelta se $\mid x - m \mid < t$.

Infatti, se t=0, nessun test riesce a passare la verifica, ma per t molto alto tutti i tests passerebbero la fase di identificazione. La Figura 5 mostra l'indice di permesso per 2 classi di utenti; un insieme di utenti autorizzati che fanno del loro meglio per essere identificati rispettando a criteri di verifica con le proprie caratteristiche di riferimento, e un insieme di impostori che cercano di accedere al sistema.

Figura 5: Indice di permesso

I valori di riferimento sono calcolati facendo la media dei tentativi. Un valore di riferimento ideale dovrebbe avere un valore t che separi le due classi di utenti, tale da accettare gli utenti autorizzati e rifiutare l'accesso agli impostori, ma ció raramente accede in pratica. Un compromesso accettabile é il valore t', che implica 2 tipi di errore:

Tipo I - utenti autorizzati che falliscono la verifica. L'indice di passaggi per utenti autorizzati é 100-FAR, dove FAR é "l'indice di falso allarme", misurato in percentuale.

Tipo II - impostori. L'indice di passaggio per gli impostori é IPR (Impostor Pass Rate).

Una altro modo di vedere il tradeoff é di disegnare l'indice FAR in relazione all'indice IPR(FRR), come mostra la Figura 6, dove sulla curva sono marcati i valori medi di t.

Figura 6: Relazione tra FAR e FRR

4.11 Sperimentazione delle tecniche per la verifica dell'identitá

Alcuni articoli specializzati hanno presentato la descrizione dello sviluppo dei sistemi di verifica e hanno preteso le performance ottenute da ogni sistema. Purtroppo é estremamente difficile fare una comparazione obiettiva di tali richieste, perché non esistono condizioni standard con cui i sistemi sono stati testati. Uno dei piú importanti studi di questo tipo fu portato a termine da Mitre Coorporation, quando, sotto contratto con l'aviazione americana, furono valutati mediante studi comparati alcuni sistemi per la verifica dell'identitá.

4.11.1 Gli Studi di Mitre

I termini di riferimento della sperimentazione di Mitre si basavano sul fatto che i sistemi Elettronici della divisione aerea degli U.S.A richiedevano sistemi di verifica d'identitá che ragiungessero un range di errore di tipo I non piú grande del 1%, e un range di errore di tipo II non piú grande del 2%; un ulteriore richiesta era che il sistema doveva essere in grado di eseguire quattro riconoscimenti al minuto. Negli studi di Mitre furono valutai 3 sistemi di verifica dell'identitá: verifica della voce, verifica della firma e verifica delle impronte digitali. Ad ogni stage almeno 200 persone prendevano parte agli esperimenti. Ad ogni esperimento, ogni persona tentava il riconoscimento con ognuno dei tre sistemi. Furono misurati non solo gli indici d'errore ma anche il tempo speso in ogni parte del processo di verifica. L'indice d'errore I non richiede commenti, essendo semplicemente relativo a guasti che si verificavano durante la verifica. La filosofia della sperimentazione era diretta a creare accoppiamenti falsi tra profili di diversi utenti ed a deliberati tentativi per mascherarsi con altri soggetti. Si vide che deliberati tentativi con firme false davano un errore di tipo II piú grande rispetto ad accoppiamenti casuali. Gli indici d'errore di tipo II riscontrati da Mitre si basano sulla comparazione del profilo misurato da ogni soggetto con tutti quelli memorizzati.

4.11.2 Verifica della Voce

Questo sistema si sviluppa in tre fasi. Nella prima fase (Registrazione) il soggetto dichiarata la sua identitá, doveva pronunciare una serie di frasi formate da 4 parole, non ripetitive, in risposta ai suggerimenti ascoltati dal sistema, cosí che ogni parola fosse registrata nel vocabolario del sistema ogni 5 secondi. Le frasi venivano poi elaborate dal sistema al fine di creare un file di dipendenze. La seconda fase richiedeva che il soggetto pronunziasse 4 frasi scelte dal sistema (frasi precedentemente inserite). Nella terza fase, detta anche “fase normale di riconoscimento”, il sistema richiedeva al soggetto di pronunziare tante frasi quante erano necessarie per ottenere la verifica, fino ad un massimo di 8 tentativi. Al fine di migliorare il sistema contro possibili impostori, questo fu programmato per esigere progressivamente la migliore correlazione tra i profili memorizzati e quelli misurati. Dopo periodi di prova, seguirono cambiamenti nelle caratteristiche di riferimento della voce, che migliorarono le peformance del sistema.

	Fase 1	Fase 2	Test
Errore I	0.92	0.20	1.06
Errore II	0.99	4.40	3.26
Tempo Verifica(secs)	6.54	5.85	6.21

Tabella 1: I risulatati ottenuti da Mitre per la verifica della Voce

Molte difficoltá si presentarono in soggetti sofferenti da raffreddore o da laringiti. Dagli esperimenti si notó che circa 11% delle persone presentavano un indice di errore I superiore al 5%, e che circa il 9% dei soggetti presentavano un indice di errore II superiore al 10%. Tali persone erano incapaci di produrre una pronuncia accettabile. Fu anche notato che le donne erano maggiormente soggette a percentuali di errore piú elevate. D’altra parte fu notato che uno dei piú rilevanti indici di performance dipendeva dal luogo in cui si era cresciuti, dall’educazione e dall’etá.

4.11.3 Sistema di Riconoscimento Scrittura

Il metodo usato nella sperimentazione di tale sistema per riconoscere la firma durante i tests di laboratori, fu la misurazione della pressione esercitata dalla sfera della penna. La penna fu equipaggiata con un dispositivo che misurava la pressione durante lo scorrimento della sfera sul foglio. Nella prima fase ad ogni utente veniva chiesto di apporre un totale di sei firme (successivamente incrementate a nove), 5 delle quali servivano al sistema per creare “file di reference”, cioé il file dove vengono registrate tutte le caratteristiche della scrittura di un utente. Come per il sistema di verifica della voce, seguiva una seconda fase durante la quale erano richieste 3 firme per ogni utente, e tutte e tre venivano usate per aggiornare l’insieme delle caratteristiche degli utenti. Nell’ultima fase, quella di verifica, era chiesto all’utente di firmare per essere identificato dal sistema, con un limite di tre tentativi altrimenti la verifica falliva. In questa fase il “file di reference” era aggiornato solo con le firme esatte. Nella fase di sperimentazione l’algoritmo di verifica fu cambiato incrementando la performance del sistema. Si trovó che l’indice d’errore I era vicino al 1.9% e quello di tipo II é un pó superiore al 5.6%. Gli sperimenti il laboratorio hanno anche evidenziato che le donne e i mancini hanno un lato indice d’errore I rispetto agli altri soggetti. Il tempo speso dal sistema di riconoscimento era

13.5 secondi, per un totale di 25,8 secondi ottenuti aggiungendo ulteriori 12.3 secondi per operazioni secondarie.

4.11.4 Sistema di riconoscimento della Impronte Digitali

I dispositivi usati nella sperimentazione era disegnati ad acquisire l'impronta e registrare la posizione e l'orientamento dei tratti finali del dito. Questi parametri erano immagazzinati e fornivano le caratteristiche e il profilo dell'utente. Nella prima fase, tutte le impronte venivano scannerizzate dal sistema, che in un secondo momento sceglieva quale di queste fosse l'impronta di riferimento. Nella fase di verifica l'utente veniva invitato ad apporre l'impronta di un dito per la fase di scan; se l'impronta acquisita non combaciava con quella memorizzata nel file, allora veniva richiesto all'utente di ripetere l'operazione. Se si verificavano 3 fallimenti nel riconoscimento di un'impronta, allora veniva chiesto di cambiare dito. Sei tentativi producevano il fallimento della verifica. A differenza dei sistemi basati sulla voce e sulla scrittura, qui non veniva fatto nessun aggiornamento al "file reference". Le fasi erano due e i risultati della sperimentazione di Mitre sono riportati qui sotto:

	Fase 1	Fase 2	Test
Errore I	6.25	3.20	1.88
Errore II	2.97	1.71	5.63
Tempo Verifica(secs)	14.42	13.03	13.49

Tabella 2: In tabella i dati ottenuti dalla sperimentazione di Mitre

Per molti utenti l'indice di rifiuto per l'impronta scelta dal sistema per il riconoscimento era del 14%. L'alto indice di errore I fu reputato alla scarsa pulizia delle mani da parte degli utenti, sebbene é difficile pensare che l'utente lavi le mani prima di ogni riconoscimento. Il tempo totale per la verifica era 8.9 secondi, che diventava 21.2 secondi per operazioni addizionali della durata di 12.3 secondi.

4.11.5 Conclusioni

Sebbene sia possibile fare un'approssimazione dei range d'errore di tipo I e tipo II, é molto difficile fare un preciso confronto fra i 3 sistemi di verifica dell'identitá. In generali si ha un errore totale del 4.4% per il sistema vocale, 7.5% per il sistema di scrittura e 8.8% per il sistema di impronte digitali. Peró nessuno dei tre sistemi soddisfaceva le richieste fatte dall'Aviazione Americana, che richiedeva un errore di tipo I non piú grande del 1% e di tipo II non piú grande del 2%. Successivamente maggiore attenzione fu posta nel migliorare lo sviluppo dei sistemi tale da ridurre il tempo speso nella verifica. Gli studi di Mitre conclusero che il sistema di verifica della voce garantiva un sufficiente sviluppo della sua performance.

Riferimenti

[1] Morrison R. and Thompson K., *Password security: a case history*, Comm. ACM, 22, 11, 594, November 1979.

[2] Bruce Schneier, *Applied Cryptography*, John Wiley and Sons, Second Edition.

[3] D. W. Davies, W. L. Price, *Security For Computer Networks*, John Wiley and Sons, 1989.