Tastiera, Schermi, Palmo touchless

Parte X

Indice

Capitolo 1

Biometria della digitazione della tastiera e schermi

1.1 *Keystroke dynamics*

I sistemi di identificazione basati sulla dinamica della battitura della tastiera (*Keystroke dynamics*) si basano sull'assunzione che **persone diverse battano la tastiera in modi diversi**.

L'analisi della digitazione e della firma online sono simili:

- tratti biometrici **comportamentali**
- **variabili** nel tempo e in base alle condizioni dell'individuo
- considerati **poco invasivi**
- acquisibili con sensori **economici**
- tecniche di matching simili, richiedono **allineamenti temporali**

Autenticazione a due fattori

La possibilità di estrarre il template direttamente intanto che viene digitato la password di fatto rende possibile una istantanea identificazione a due fattori.

1.1.1 Estrazione delle feature

Feature locali

Le feature locali che si possono estrarre sono tipicamente le seguenti:

- tempo di **latenza** fra due pressioni
- tempo di **battitura** del tasto (quanto rimane premuto)

Altre feature meno interessanti, ma che possono essere usate a corredo delle precedenti, sono:

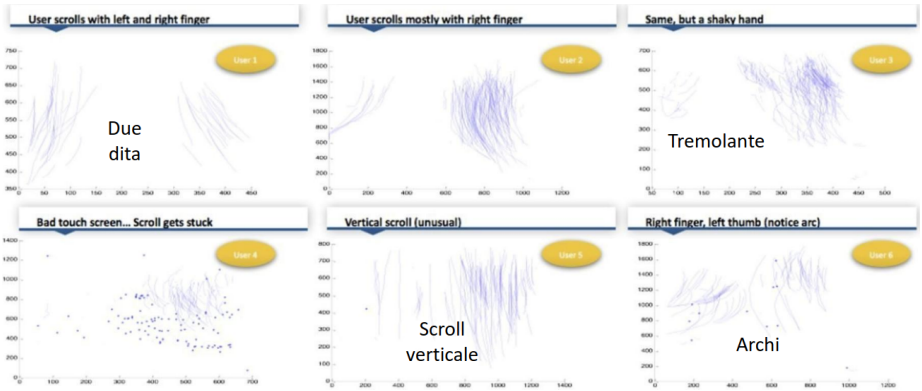
- velocità di battitura
- frequenza degli errori
- uso di *shift* o *caps lock*

Feature globali

Esistono anche delle feature globali, ovvero che si possono estrarre solo quando la sessione di battitura è finita.
Si tratta delle **associazioni di tasti** (ad esempio, quante viene usata la coppia ALT + TAB, o il tempo medio che intercorre tra la loro battitura).

1.2 Swapping su schermo

Allo stesso modo, persone diverse hanno movimenti delle dita sullo schermo diversi.



1.3 Comportamento dell'utente sul terminale

In aggiunta, esistono dei metodi che vanno ad identificare le persone in base al comportamento in:

- ambiente software
- rispetto al sistema operativo

Ad esempio, si può analizzare come viene usata la tastiera o il mouse, come si passa da un'applicazione ad un'altra, come si accede ai menu, ...

→ con il solo comportamento **non è sempre possibile, usando questi metodi, verificare l'identità di una persona** (troppa poca informazione). Tuttavia, è possibile ricavare informazioni utili (ad esempio, se durante il lavoro il terminale è usato proprio da quella persona o da un'altra).

1.4 Vantaggi e Svantaggi

- **Vantaggi**
  - Per regolare l'accesso dei terminali non è necessario un sensore, ma basta la tastiera del terminale; i sistemi sono quindi di tipo software
  - Sono considerati non invasivi (anche se lo sono per la privacy)
  - Possono essere impiegati anche senza la collaborazione dell'utente, o addirittura senza che se ne accorga
- **Svantaggi**
  - **bassa** accuratezza
  - queste informazioni possono essere usate per migliorare i tempi di **rottura delle password**
  - **cambiando tastiera**, spesso i tempi cambiano, oppure solo impugnando qualcosa con l'altra mano
  - **ferite o traumi** sulla mano possono influenzare la battitura

1.5 Attacco su canale SSH

È possibile perché esistono protocolli, come SSH, che trasmettono immediatamente un pacchetto ogni volta che viene premuto un tasto; in questo modo è possibile intercettare la password e i tempi di latenza.
I tempi di latenza non bastano per estrarre immediatamente la password, ma permettono ai motori di generazione delle password di ridurre i tempi di calcolo.

1.5.1 Contromisure

L'idea è di offuscare i dati che passano attraverso il canale SSH:

- **Randomizzazione temporale:** viene introdotto un ritardo casuale per l'invio dei pacchetti
- **Iniezioni di pacchetti *dummy***: pacchetti vuoti o non necessari, per alterare il ritmo di trasmissione
- **Aggregazione di pacchetti:** si aggregano più pacchetti in un solo, per eliminare la correlazione diretta tra i tempi di battitura e i tempi di invio

Capitolo 2

Impronta

2.1 Biometria *less-constrained* e *unconstrained*

- *Less-constrained*
  - senza contatto
  - elevata distanza
  - condizioni di luce naturale
  - in movimento
  - ...

  → serve un minimo di cooperazione
- *Unconstrained*
  - soggetti non cooperativi
  - scenari non controllati

2.2 Vantaggi e Svantaggi

- **Vantaggi**
  - less-constrained
  - assenza di distorsioni della pelle nelle immagini delle dita
  - più resistente a sporco e polvere
  - maggiore accettazione da parte degli utenti
- **Svantaggi**
  - parzialmente compatibile con i sistemi AFIS
  - sfondi complessi da gestire
  - sensibile ad illuminazione e posizione (vicino/lontano)
  - i modelli 2D possono presentare distorsioni di tipo prospettico
  - tempo di calcolo più lunghi

Capitolo 3

Palmo