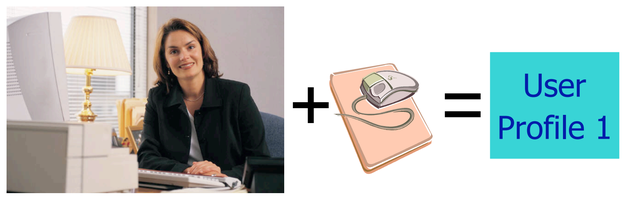
CERIAS

User Re-Authentication via Mouse Movements

Intrusion Detection

- Authentication
- Re-Authentication
- Insider Threat
  - 90% of U.S. companies were victims of malicious computer attacks in 2001
  - 80% of all attacks were engineered from within the company itself

User Re-Authentication



Classification

- Decision tree algorithm C4.5
  - –2-class decision tree classifier
  - –1 user = class (+) versus 17 users = class (-)
- Parameters:
  - –Window sizes:
    - 400, 600, 800 and 1000 points
    - Non-overlapping windows
  - –Frequencies:
    - 1, 5, 15 and 20 (1 = 100 milliseconds)
    - Overlapping frequencies

Data Sets

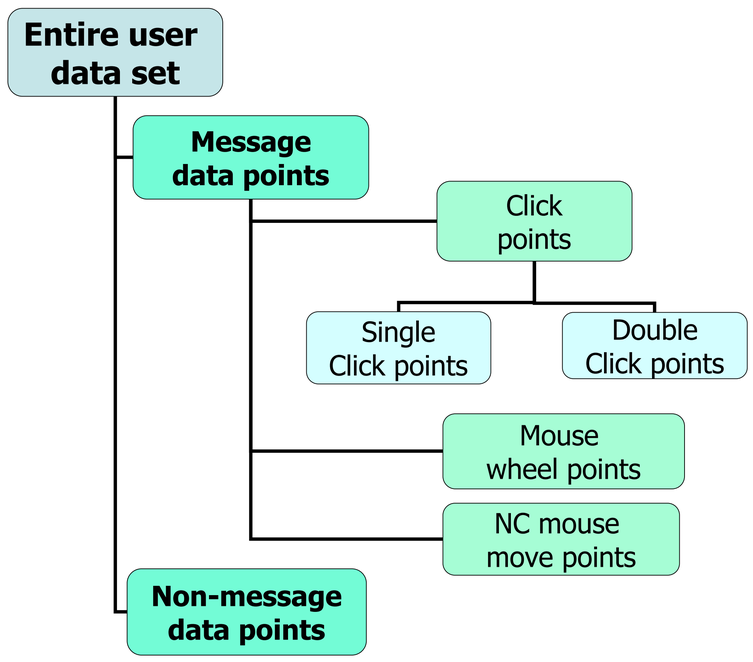
- 18 labeled user data sets
- 8,000 data points per set

Data sample:

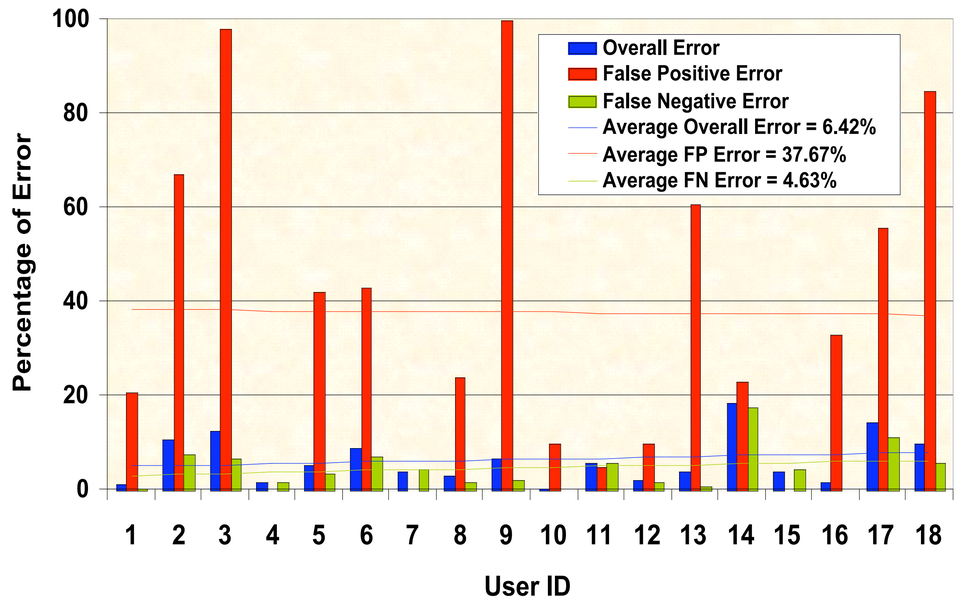
```
160 1099 1013  6.064E-1 C:\WINDOWS\Explorer.EXE
513  212  233  6.071E-1 C:\WINDOWS\mshtml.dll
514 1384   16  6.067E-1 C:\WINDOWS\BROWSEUI.dll
  0 1226  186  6.067E-1 0
  0  518  986  6.067E-1 0
  0  525 1005  6.069E-1 0
160  526 1012  6.067E-1 C:\WINDOWS\Explorer.EXE
```

ID X Y Time Application

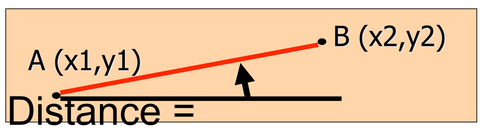
Categories of Data Points



Experimental Results



Raw Features Extraction



Distance = $\sqrt{(\Delta x)^2 + (\Delta y)^2}$

Angle = $\arccos \frac{\Delta x}{\sqrt{(\Delta x)^2 + (\Delta y)^2}}$

Time = MSecSpan (time2, time1)

Speed = Distance / Time

Statistics: Mean and Standard Deviation per window

Feature Vector

- Raw features:
  - –Distance, angle, time and speed
- Extracted features:
  - –Mean and standard deviation
- Categories of data points:
  - –Points, messages, non-messages, clicks, single clicks, double clicks, mouse wheel and NC mouse moves

Feature vector: 4 * 2 * 8 = 64 features

Results for User #7

- Window size of 800
- Frequency of 15 (15 = 1.5 seconds)
- Error = 3%

Decision tree for user #7

```
A1 <= 384 : - (106.0)
A1 > 384 :
|   A3 > 5800 : + (45.0)
|   A3 <= 5800 :
|   |   A1 <= 454 : - (2.0)
|   |   A1 > 454 : + (9.0)
```

A1: Mean of the distance

A3: Standard deviation of the distance

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center