Mobile Biometrics, Replay Attacks, and Behavior Profiling: An Empirical Analysis of Impostor Detection

ICB 2019 Poster Spotlight

Tempestt Neal, Department of Computer Science and Engineering, University of South Florida
Damon Woodard, Department of Electrical and Computer Engineering, University of Florida
Contact: tjneal@usf.edu
Simulated replay attacks using application, Bluetooth, and Wi-Fi data captured remotely and then intelligently combined with some level of noise to avoid the replay of an exact copy.

Our results also show that by contextualizing behavior in the feature representation, FPRs decrease by over 25%.
To generate attack logs, we assumed that an attacker has accessed their target’s device remotely. The attacker then generates a similar log based on the time between when real and fake events occur. Results show that our attacks lead to increased FPRs from a best case of 0.023 to a worst case of 0.420.

We found that behavior profiles generally outperformed the top-20 representation. FPRs associated with behavior profiles either improved or were not affected by the amount of data provided for authentication, while those associated with the top-20 events increased. False positive and reject rates between supervised and unsupervised learning approaches were also most similar to each other when using behavior profiles, indicating that a profiling technique may yield more reliable results during unsupervised learning.

```
Algorithm 1 Replay Attack Creation
1: procedure REPLAYATTACK(s, D)                                                  ▶ Block size in seconds and a user’s device log
2:    n ← sizeOf(uniqueEvents(D))                                              ▶ Loops through D to separate it into blocks
3:    while i < totalSeconds(D) do                                             ▶ Generate m random tags to represent fake events
4:        block ← D[i : i + s]                                                ▶ Generate new attack data
5:        m ← sizeOf(uniqueEvents(block))                                      ▶ Generate new attack data
6:        for k ← 0, m do                                                      ▶ Generate new attack data
7:            f ← random(1, n)                                              ▶ Generate new attack data
8:            tags[k] ← randomEvent(f)                                       ▶ Generate new attack data
9:        C ← [uniqueEvents(block), tags]                                     ▶ Generate new attack data
10:       for k ← 0, sizeOf(block) do                                         ▶ Generate new attack data
11:           time Stamp ← random(0, s) + firstTime Stamp(block)            ▶ Generate new attack data
12:           aD[k] ← (random(C), time Stamp)                                      ▶ Generate new attack data
13:       i = i + s + 1                                                       ▶ Generate new attack data
14:     return aD                                                             ▶ Generate new attack data
```