Profiling Users by Modelling Web Transactions

Radek Tomšů, Samuel Marchal, N. Asokan

• Same device (and even same user account) can be used by several people, some possibly unauthorized.
• Automatically detecting account impersonation mitigates the threat.
• Web transaction patterns are characteristic for a user and can be used for identification.

Challenges in detecting account impersonation
• Discriminative user behavior modeling
• Scalable solution
• Real-time decision making

Current solutions
• Mostly rely on biometrics: keystroke, touchscreen, face, cloth color analysis
• Need local software
• Need additional hardware
• Do not prevent malicious behavior of authorized users

Solution: Profiling users by modeling web transactions
• User-specific behavior profile (built from historical web transaction logs) → applied to new web transactions
• Consider sequences of transactions (60s window)
• Context-aware modelling: Web transaction logs enhanced by URI categories, applications, ...
• Centralized monitoring (gateway)

Implementation and performance
• One-Class SVMs, SVDD (one model per user)
• Expected time for detecting impersonation: ≈5mins: 10 windows (60s) with 30s overlap
• Average accuracy ≈90 % (≈7 % FP)

Intel CRI for Secure Computing

Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
*Other names and brands may be claimed as the property of others.