Automated Deauthentication using Web Transaction Analysis

Radek Tomšů, Samuel Marchal, N. Asokan

Aalto University

Collaborative Research Institute for Secure Computing

Same device or user account can be used by several people, some possibly unauthorized.

Detecting account impersonation and applying automated deauthentication mitigates the threat.

Web transactions are characteristic for a user and their analysis can be used for deauthentication.

Challenges in detecting account impersonation

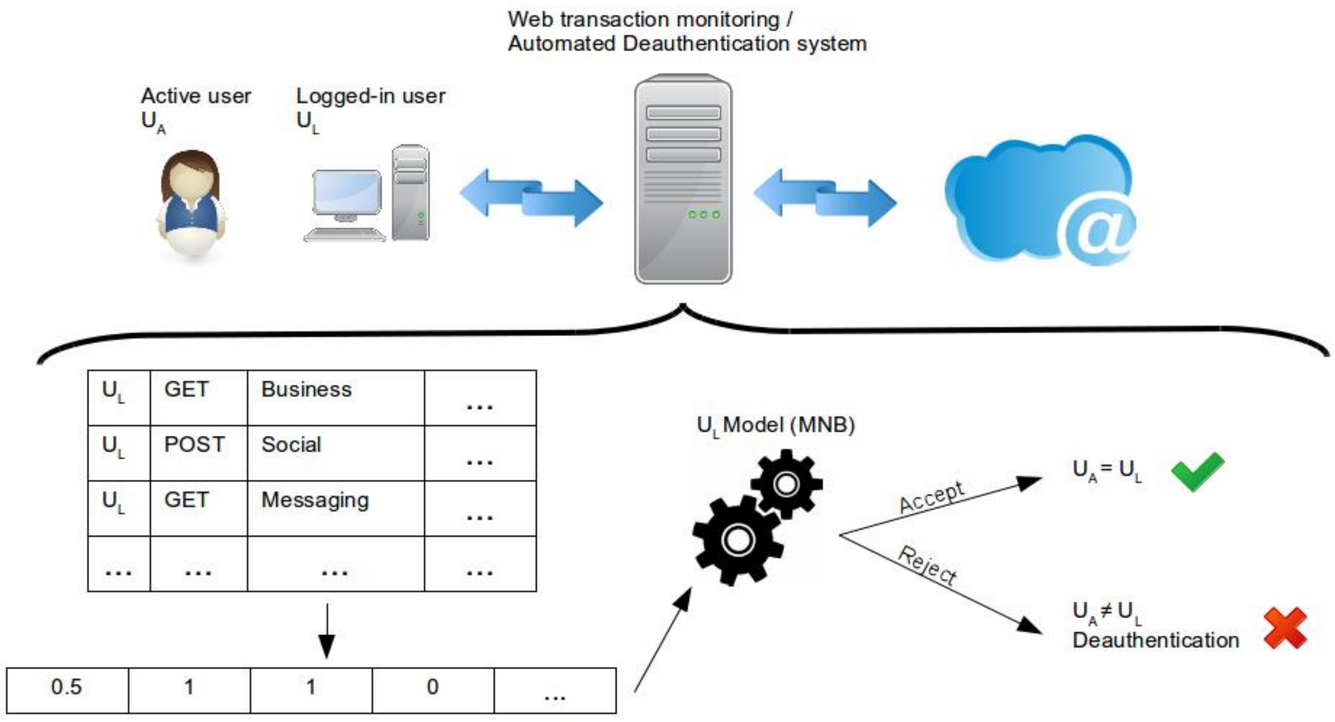
- Discriminative user behavior modeling
- Scalable solution (100s of users)
- Fast decision making
- Low overhead in deployment

Current solutions:

- Automated deauthentication:
  - Mostly relies on biometrics: keystroke, touchscreen, face, cloth color analysis
  - Needs local software / additional hardware
  - Does not prevent malicious behavior of authorized users

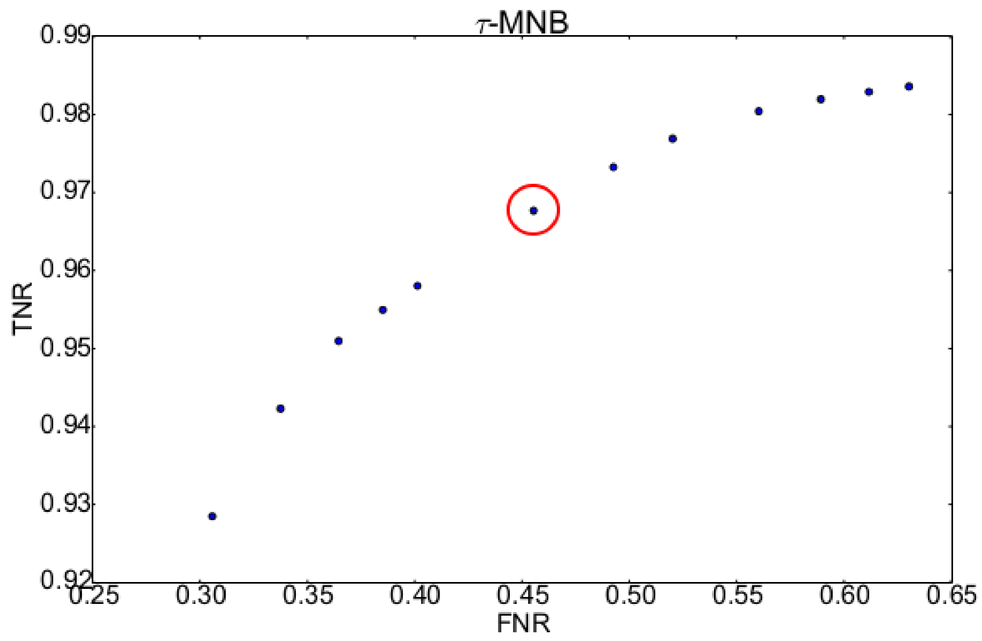
Solution: Profiling users by modeling web transactions

- User-specific profile (built from historical web transaction logs) using Multinomial Naïve Bayes
  - Applied to new web transactions — Scalability
- Consider sequences of transactions (60s window = 1 transaction window)
- Context-aware modelling: URI, URI categories, applications, media types, …
- Centralized monitoring (gateway) — Low overhead
- Works on top of an existing Authentication system



Performance

- Speed: 5.5 minutes (10 consecutive transaction windows) for deauthentication — Fast
- Accuracy (tested on real-world dataset containing 40 users):
  - Deauthenticates an illegitimate user with the probability: Recall = 54.5% — Discriminative
  - Deauthenticates a legitimate user with the probability: False positive rate = 3.3%



Intel CRI for Secure Computing