Risk Engine for User Behavior Analytics

Samuel Marchal, Nidhi Singh, N. Asokan

Aalto University

Collaborative Research Institute for Secure Computing

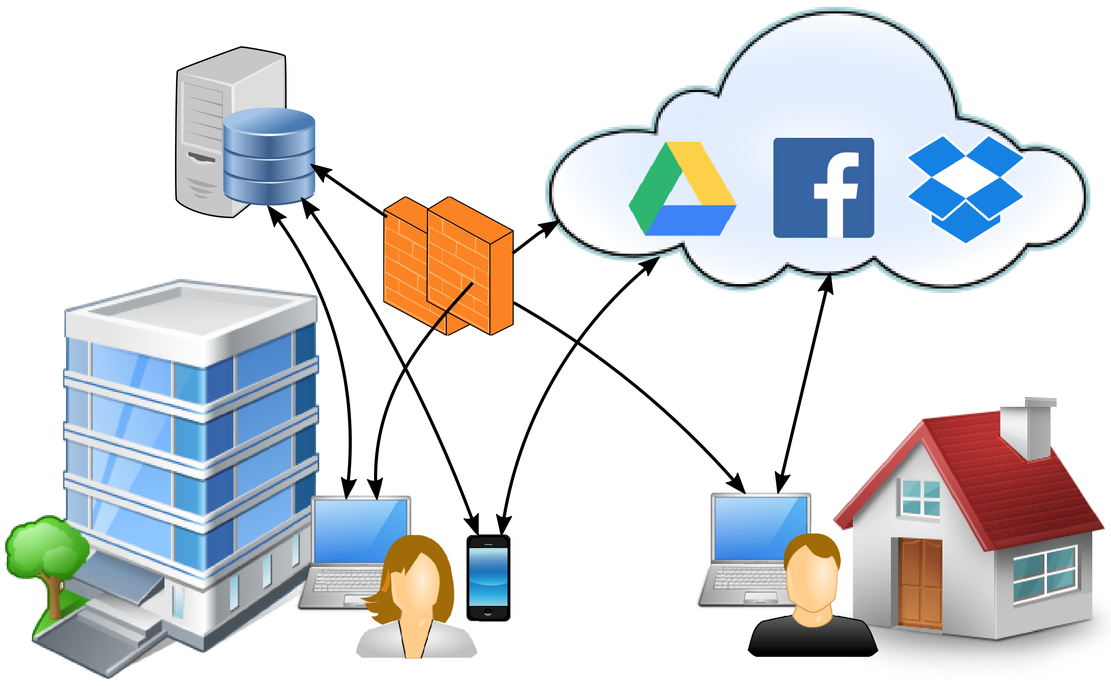
People use work devices for both personal and work purposes.

This phenomenon exposes company to new threats.

Automatic control of Internet transactions is needed to limit such threats.

Challenges in controlling Internet transactions

- Ensure ability to monitor transactions
- Protection of enterprise assets vs. personal usage freedom:
  - Authorized transactions must not expose enterprise to threats
  - Denied transactions must not impair usability in personal usage



Current transaction authorization systems implement static rules

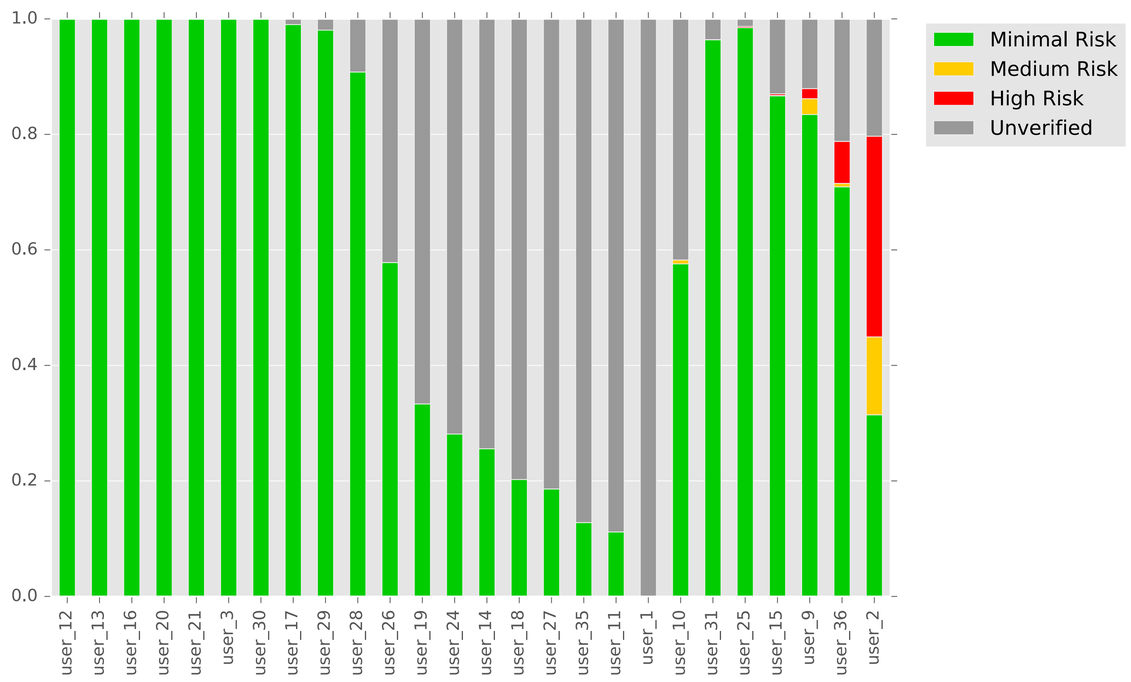
- Manually defined and fixed
- Globally applied (all employees / any use case)
- Limited to black/white lists
- Coarse grained (e.g. website categories)
- Limited to single transactions

Solution: Automated transaction authorization system

- User-specific transaction profile (abnormal transaction detection)
- Context-aware authorization (user, location, time, device, etc.)
- Consider transaction sequence e.g. downloading file from intranet + upload to cloud storage

First step: Transactions risk rating based on user behavior profiling

- Fine grained personal user profile representing normal user behavior and transactions
- Detect transactions that deviate from the profile ➡ risk score of a transaction
- Allow / deny transactions according to profile
- Identify risky behaviors / profiles for education



Ratio of websites categories visited by different users

Intel CRI for Secure Computing