### Work in Progress: Usable Security vs Workflow Realities

#### THE WORKFLOW VIEWPOINT

**An Important Type of Context**

Usability and success of security in-the-wild depends on many factors. Contact that is critical for usability includes cognitive bias, environmental factors, mental models, mismorphism and workflow.

Workflow is complementary to other viewpoints, such as mental models, bounded rationality.

We advocate attention to workflow as one of a set of viewpoints to help predict issues with security apparatus in its setting and to help avoid or mitigate issues. We are of course not the only ones to do this [Adams & Sasse 96; Herley; Kirlappos et al. ...], but seek to build a classification that exploits the unique viewpoint of coordinated, repeated tasks and shared responsibility in organizational workflow.

Regularities in workflow effects lead to complementary generalizations and predictions

In some cases the structure of shared work can be generalized between settings, while in others human features or environmental factors can lead to useful predictions.

**Complementary observability**

Sometimes a time-and-motion study can elucidate stress points in a workflow, or physical measurements can predict them. This complements what can be learned from, e.g., behavioral analysis of security users.

#### B. Alternative paths through a workflow

Security developers may not be aware of every path to an authentication point. In many cases, alternative paths are needed when security is not usable.

**Bypassing biometrics**

Pen-testers found they could bypass hand-geometry biometrics with a bandaged hand.

**Hotel room keys**

Hotel policy may be to ask for ID from someone who has lost their key. Often the requester has come from the pool or sauna and has no ID on their person. Receptionists may not feel they have time to escort the requester to check ID in the room.

**D. Bypassing barriers in information flow**

Policies may forbid information of a certain type being shared or leaving a site, when the informal workflow requires it, e.g. for second opinions.

**Wrapping information**

If a medical record may not be shared by policy, physicians have embedded screenshots in powerpoint files, or shared passwords. We have heard of tech-savvy physicians sniffing packets of unencrypted data on their local network.

The result is far less control of private data than a more forgiving policy might allow.

#### WHAT ARE WE DOING NEXT?

This is work in progress with an initial demonstration of the potential of a complementary workflow-centric analysis. Here are some next steps.

- Build a more comprehensive catalog and categorization of cases, both using existing cases and those predicted by workflow analyses outside of the security community.
- Use what we learn in our existing agent-based models to predict larger-scale effects of organizational workflow stresses on security.
- More fieldwork

*Ethnography, surveys and focus groups, some by our team, should (and will) include workflow considerations.*

#### LOOSELY CLASSIFIED EXAMPLES

**A. Cost to individual workflow tasks**

The simplest cases focus on cost of important or frequent tasks regardless of workflow topology.

**Alternative network access for temporary workers**

In some organizations, it takes a long time to obtain an account with approved network access. Summer interns, needing to perform tasks but without accounts, used wifi from local companies.

Result: all safeguards and protection on communication by-passed.

**Alternative access to critical function**

A tractor company forbids repairs and upgrades outside of an authorized dealership, with firmware. The dealerships are far from many farms leading to days of lost productivity at critical times. Farmers download cracked software from a Ukrainian site to make unauthorized repairs.

Result: open to ransomware or even control of heavy equipment.

**C. Time-stressed mobile environments & auto-logout**

Workflows sometimes lead to high time stress. Frequent tasks requiring authentication may appear more costly to the worker than the security developer.

**Proximity sensors in mobile environments**

In an example communicated to us, workers used styrofoam cups to defeat proximity sensors since repeated logins were seen as too costly.

A time-and-motion study might have predicted the stress that would be caused.

**E. Positive workflow interaction**

Just as workflow makes a policy surprisingly unusable, it can also make one surprisingly usable. Organizations adapt to the serendipity, but may not realize the barriers to exporting the policy.

**Everyone logged off by 5**

The New York Stock Exchange (at the time communicated to us) automatically logs all users out and sweeps the system shortly after 5pm. The greatly reduced attack surface could not be duplicated by most organizations but works because, once trading is over, nobody seeks to remain online.


---

**http://shucs.org**