Quantitative Security Evaluation with Human in the Loop

Mohammad Noureddine, Ken Keefe,
Masooda Bashir and William H. Sanders

University of Illinois at Urbana-Champaign

Outline

- Motivation
- Our approach
- HITOP
- Case study
- Challenges
- Future work

Motivation

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations.

They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations."

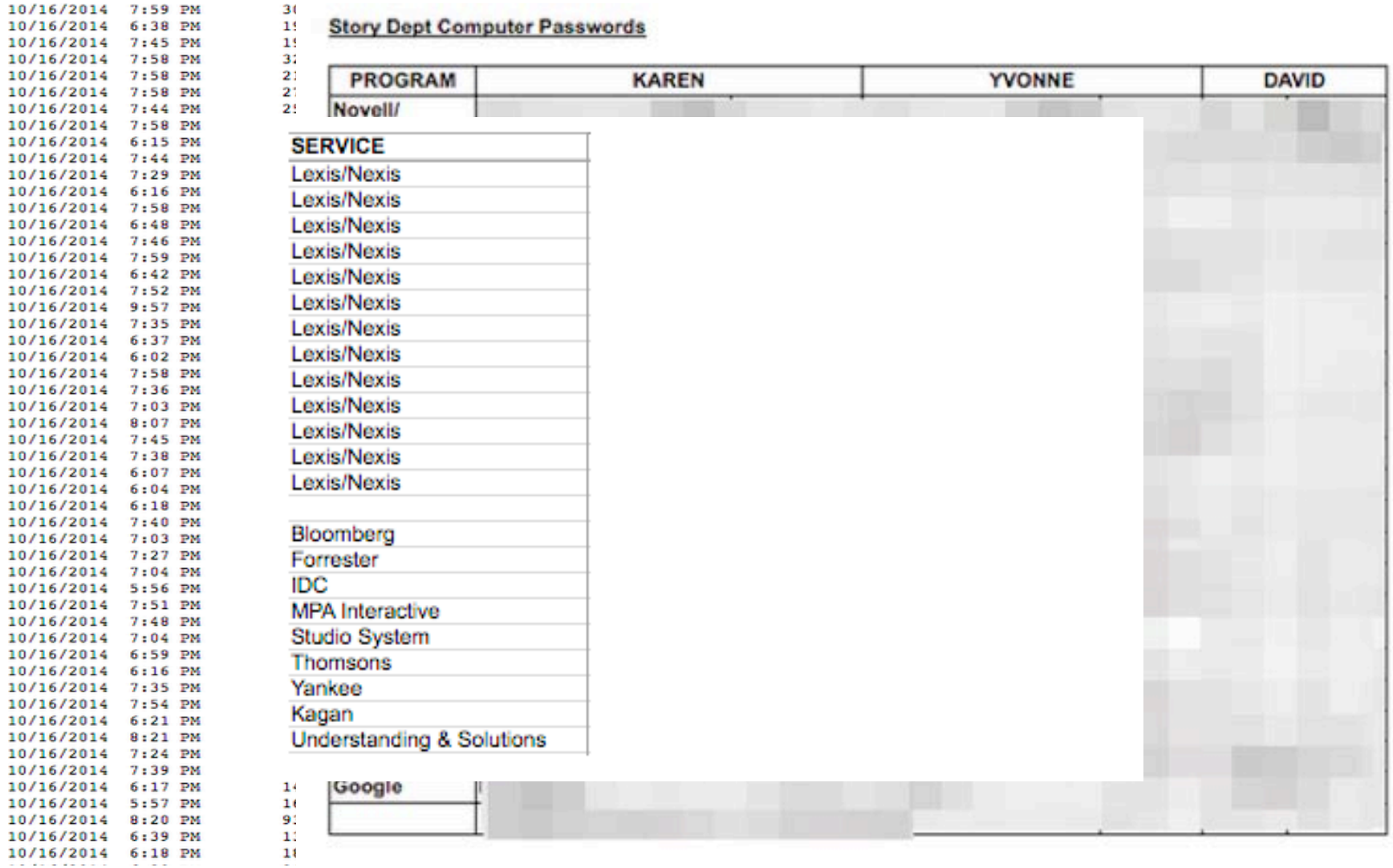
C Kaufman, R Perlman, M Speciner, "*Network Security-Private Communication in a Public World",* Prentice Hall 1995

Recent security breaches

- Public utility compromised, 2014
  - Hackers took advantage of a weak password security system at a public utility in the US
- Cook County highway department shutdown, 2013
  - It is believed that a county employee allowed a virus infection by surfing the web, or using a flash drive from home
- US Electric utility virus infection, 2012
  - A third party technician used a USB drive that was infected with a virus. The incident delays the restart of the plant for about three weeks.

The Repository of Industrial Security Incidents (http://www.risidata.com/)

Recent security breaches



10/16/2014 7:59 PM
10/16/2014 6:38 PM
10/16/2014 7:45 PM
10/16/2014 7:58 PM
10/16/2014 7:58 PM
10/16/2014 7:58 PM
10/16/2014 7:44 PM
10/16/2014 7:58 PM
10/16/2014 6:15 PM
10/16/2014 7:44 PM
10/16/2014 7:29 PM
10/16/2014 6:16 PM
10/16/2014 7:58 PM
10/16/2014 6:48 PM
10/16/2014 7:46 PM
10/16/2014 7:59 PM
10/16/2014 6:42 PM
10/16/2014 7:52 PM
10/16/2014 9:57 PM
10/16/2014 7:35 PM
10/16/2014 6:37 PM
10/16/2014 6:02 PM
10/16/2014 7:58 PM
10/16/2014 7:36 PM
10/16/2014 7:03 PM
10/16/2014 8:07 PM
10/16/2014 7:45 PM
10/16/2014 7:38 PM
10/16/2014 6:07 PM
10/16/2014 6:04 PM
10/16/2014 6:18 PM
10/16/2014 7:40 PM
10/16/2014 7:03 PM
10/16/2014 7:27 PM
10/16/2014 7:04 PM
10/16/2014 5:56 PM
10/16/2014 7:51 PM
10/16/2014 7:48 PM
10/16/2014 7:04 PM
10/16/2014 6:59 PM
10/16/2014 6:16 PM
10/16/2014 7:35 PM
10/16/2014 7:54 PM
10/16/2014 6:21 PM
10/16/2014 8:21 PM
10/16/2014 7:24 PM
10/16/2014 7:39 PM
10/16/2014 6:17 PM
10/16/2014 5:57 PM
10/16/2014 8:20 PM
10/16/2014 6:39 PM
10/16/2014 6:18 PM

Story Dept Computer Passwords

PROGRAM	KAREN	YVONNE	DAVID
Novell/			
Google			

SERVICE
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Lexis/Nexis
Bloomberg
Forrester
IDC
MPA Interactive
Studio System
Thomsons
Yankee
Kagan
Understanding & Solutions

http://www.buzzfeed.com/charliewarzel/it-gets-worse-the-newest-sony-data-breach-exposes-thousands#.yoqd1AoBlg

Common user mistakes

- Failing to install anti-virus and keeping its signatures up-to-date
- Opening unsolicited e-mail attachments
- Failing to install security patches, especially for Microsoft® Word, PowerPoint, etc.
- Not making regular backups

http://www.sans.org/security-resources/mistakes.php

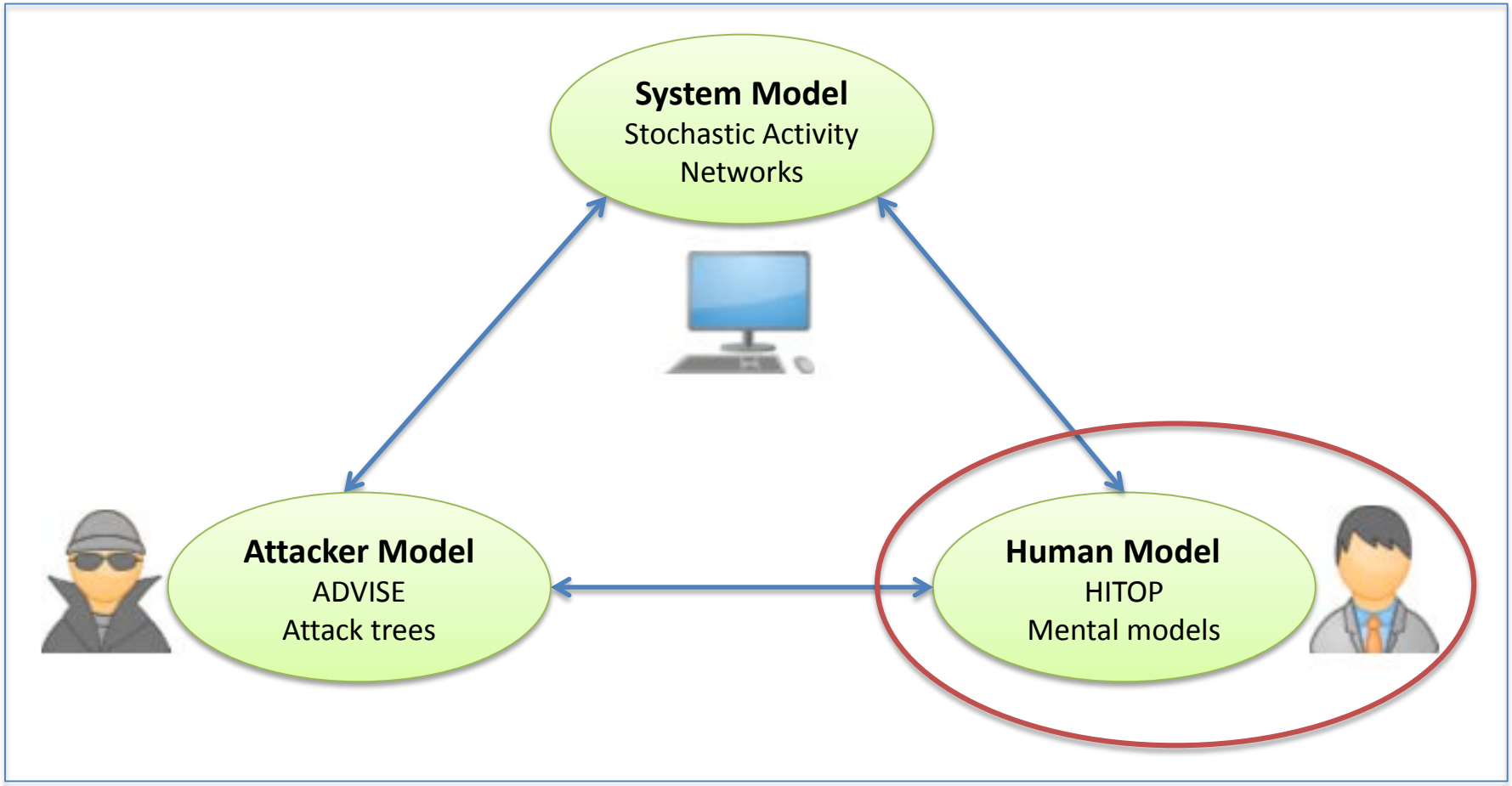
Outline

- Motivation
- Our approach
- HITOP
- Case study
- Challenges
- Future work

Problem definition

- We cannot keep humans out of the design and evaluation processes
- Usable security
  - Design systems that are usable by non-expert users
- Quantitative security metrics
  - Given a system model, quantify its degree of security
    - Are we better off with this technology or the other?
  - We need to include human behavior to have meaningful estimates

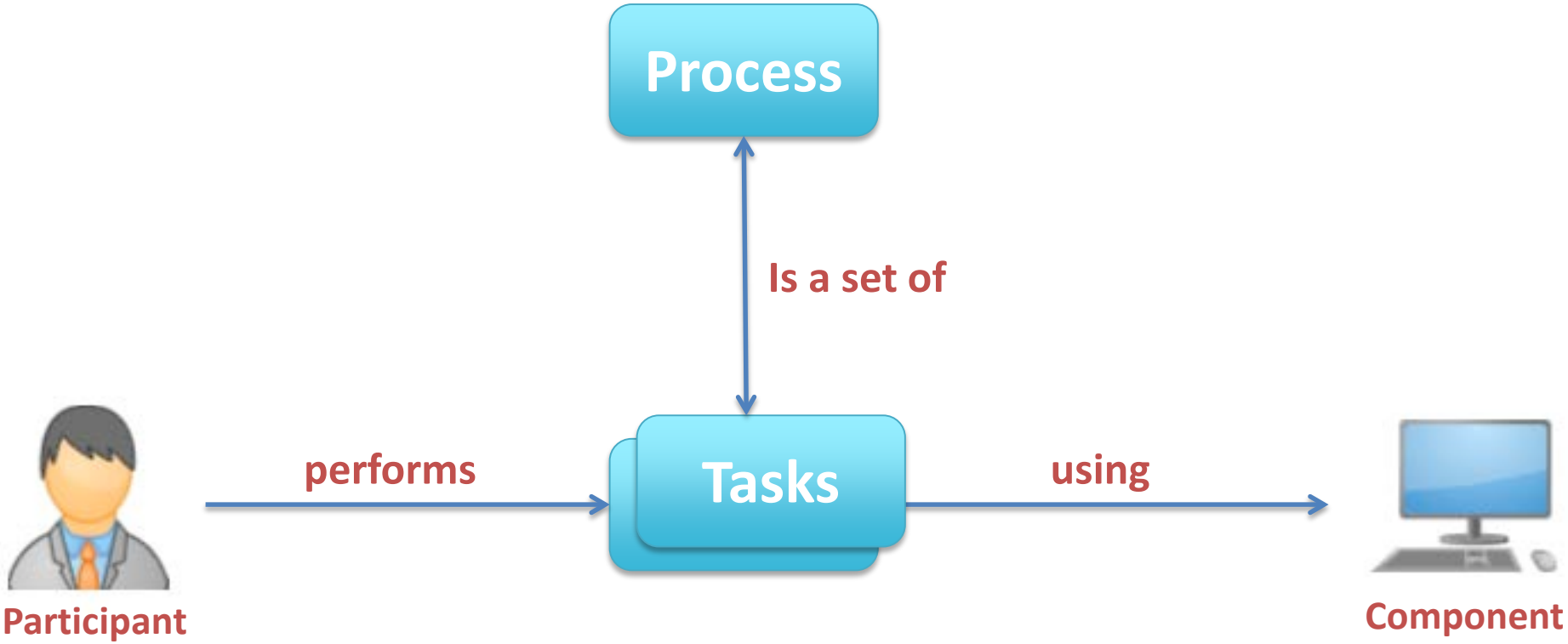
Our approach



Outline

- Motivation
- Our approach
- HITOP
- Case study
- Challenges
- Future work

Human-Influenced Task-Oriented Process (HITOP) formalism



OWC Ontology

- Proper task completion requires the presence of:
  1. *Opportunity*: Prerequisites for task performance, e.g. network access, physical workstation, …
  2. *Willingness*: Decision to perform that task, assumed to be always present for non-human participants
  3. *Capability*: The participant's ability to perform the task, e.g. knowledge, skill set, time, …

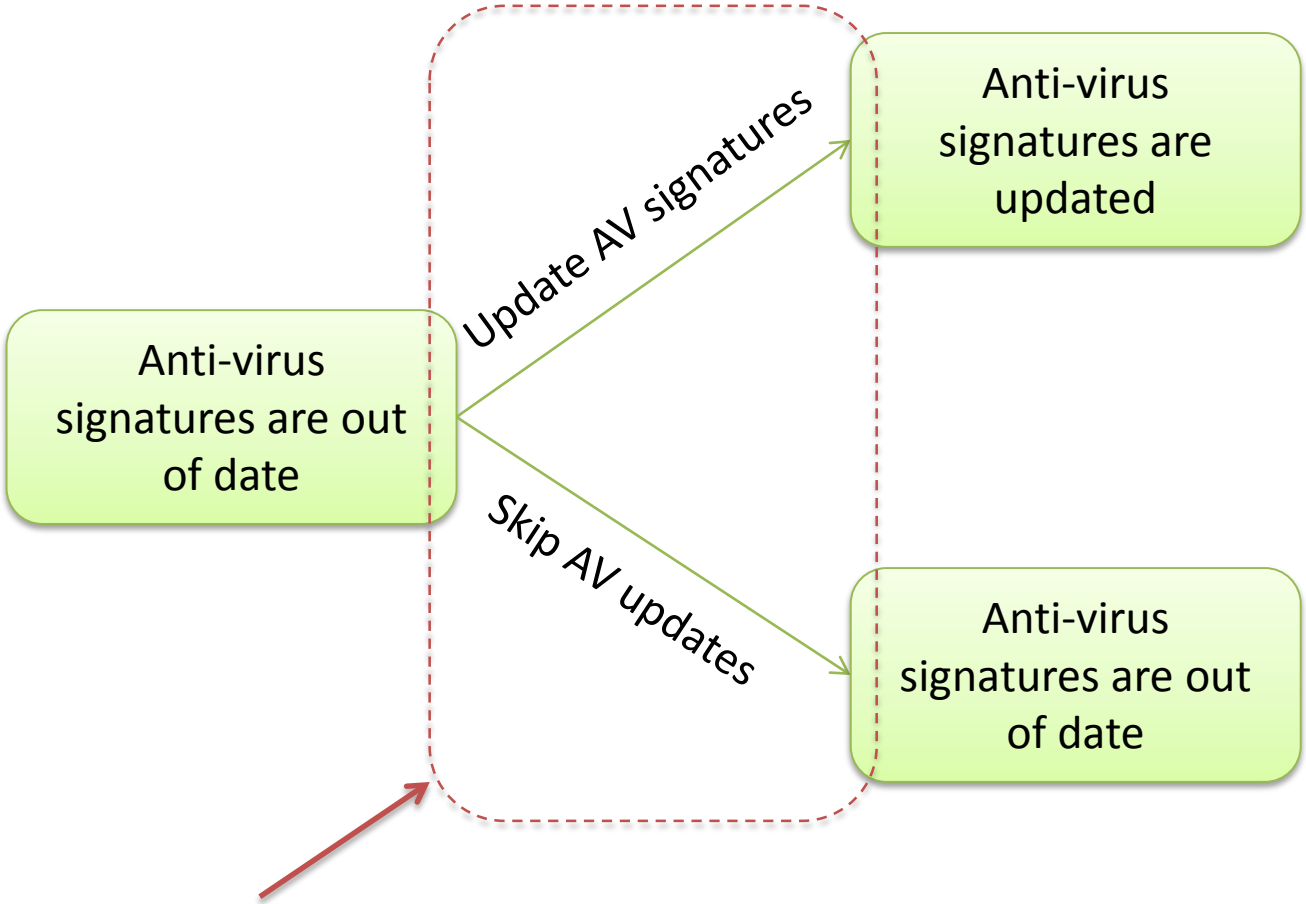
Human Decision Points (HDP)

- A Human Decision Point is a special task that
  - Is performed by a *human* participant
  - Involves the human making a *decision*
  - Typically has an effect on the overall security utility of the system
- This is where the *willingness* to perform a task comes into play

The Willingness probability (P_w)

- It reflects a human participant's willingness to perform a task
- We assume that humans are "bounded rational" decision makers
  - They process their current state in order to maximize their own utility
  - It resembles solving an optimization problem

Example



- This is the actual HDP task in HITOP
- P_w is used to determine which decision the human participant is willing to take
- The state of the system changes based on the decision that the human considers

Outline

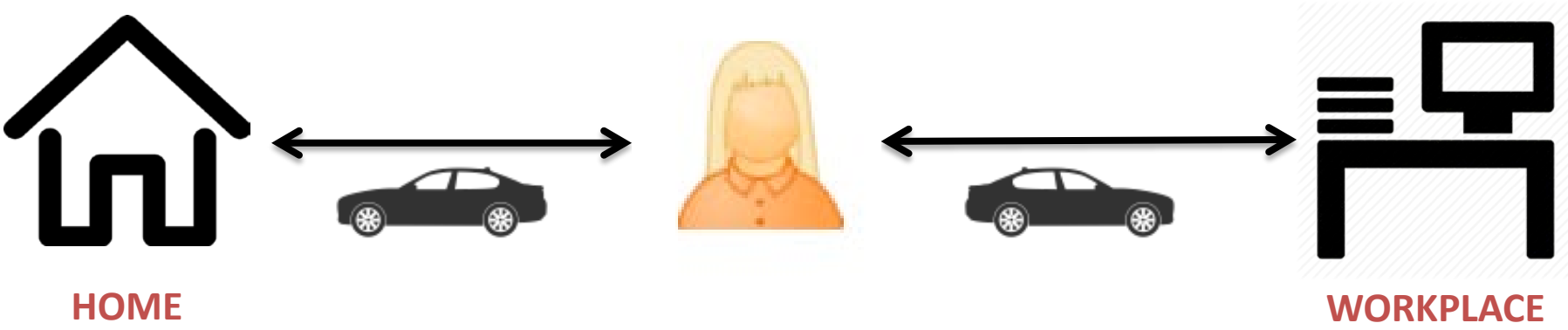
- Motivation
- Our approach
- HITOP
- Case study
- Challenges
- Future work

Goal

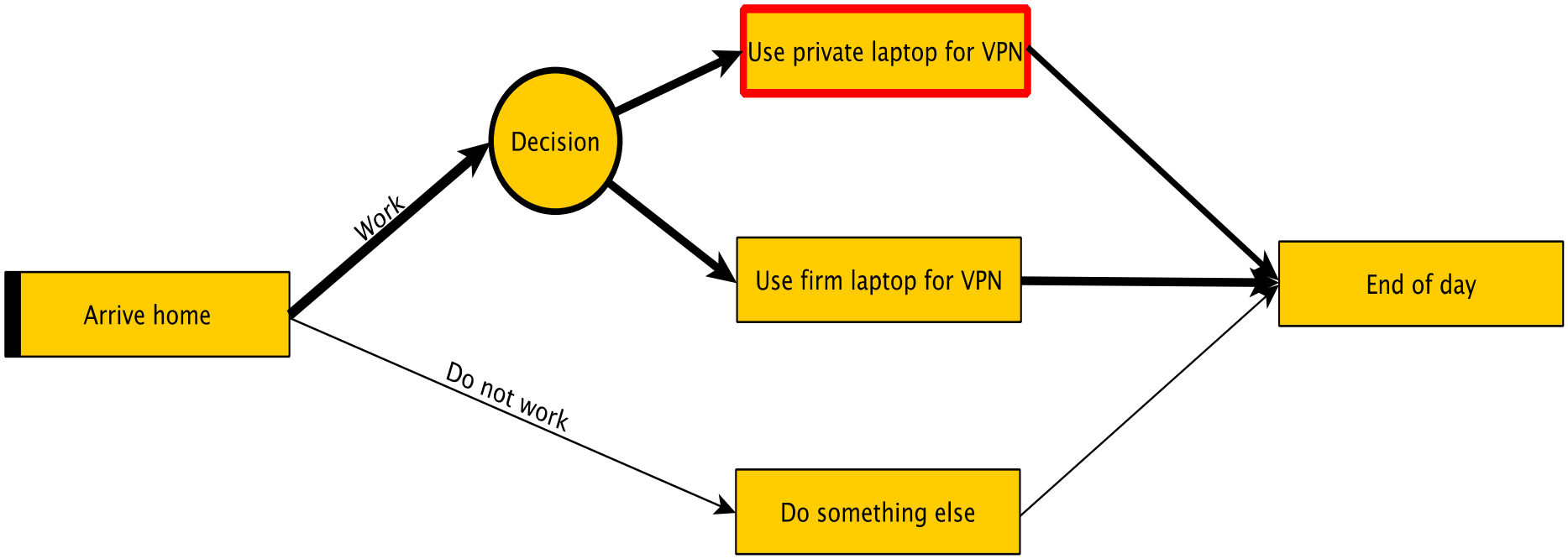
- We are designing a sample case study to
  - Evaluate how well HITOP is suited to achieved our goal
  - How accurate HITOP is in modeling human decision making
- We are considering the daily tasks that an engineer performs at a sample engineering firm, given an employed security policy

Case study

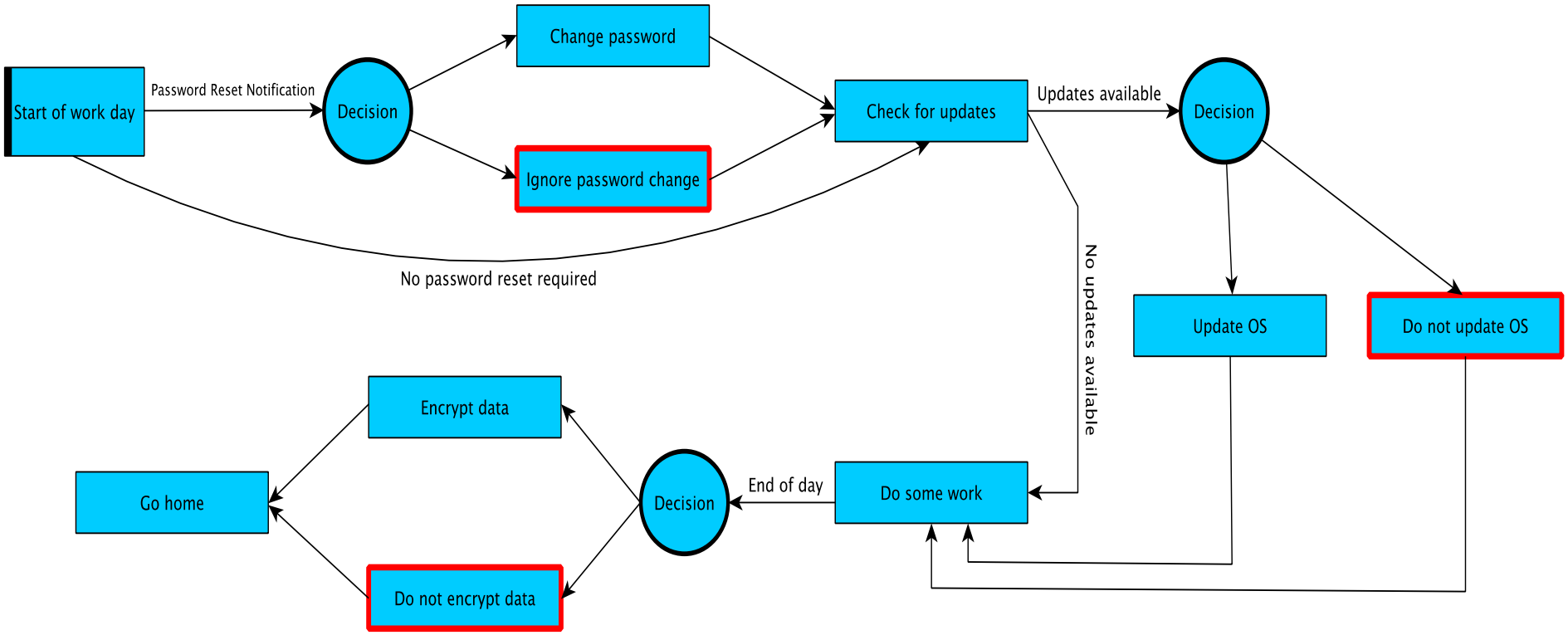
- An engineer travels between Home and the Workplace
- She performs daily tasks at the Workplace
- She is allowed to also work from Home by establishing a VPN connection



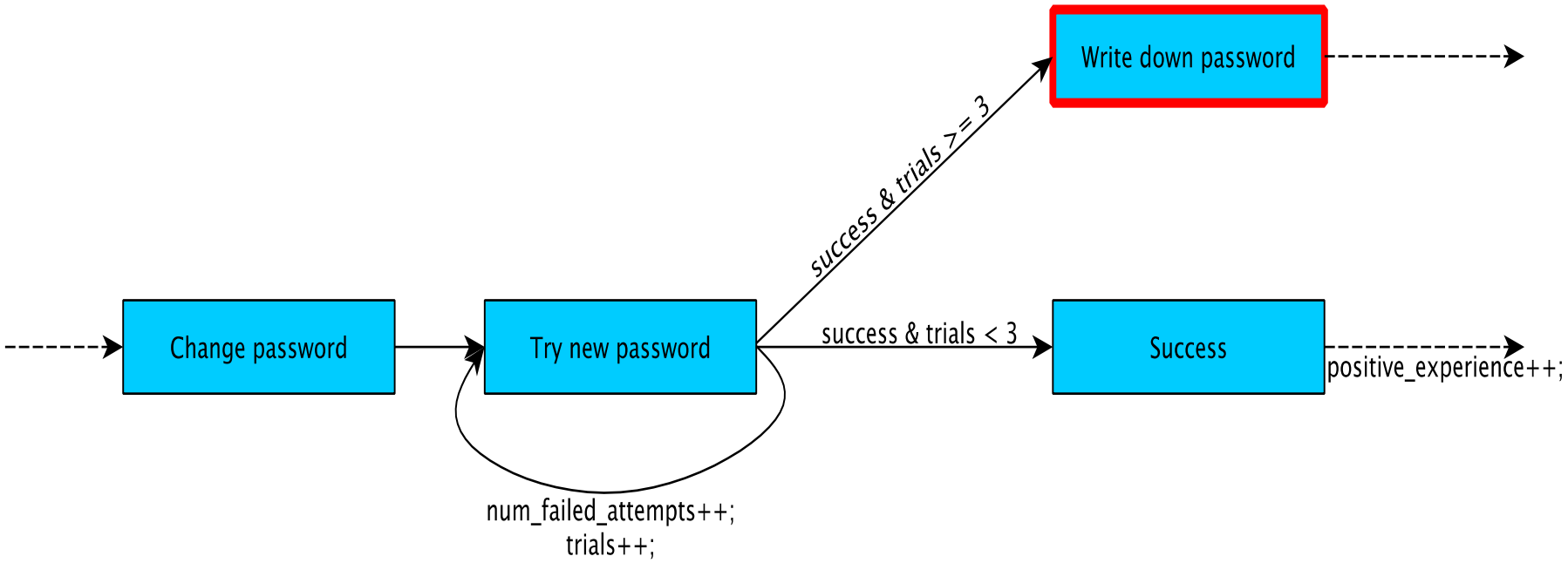
Engineer at Home



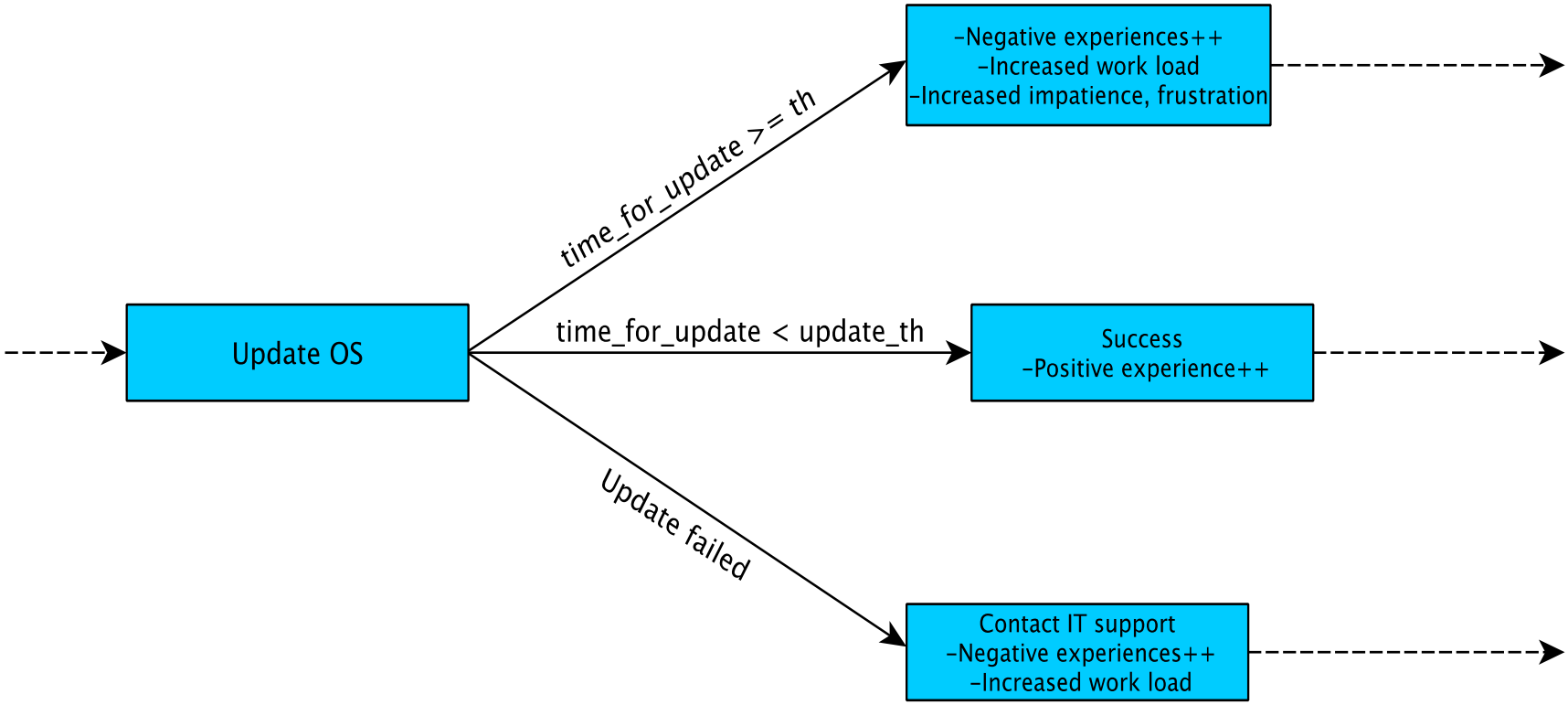
Engineer at Workplace



Changing a password



Update OS


Update OS
time_for_update >= th
-Negative experiences++
-Increased work load
-Increased impatience, frustration
time_for_update < update_th
Success
-Positive experience++
Update failed
Contact IT support
-Negative experiences++
-Increased work load

Variables affecting decisions

- The following factors affect the engineer's decision (i.e they determine P_w)
  - Workload
  - Frustration with security policy
  - Presence of sanctions
  - Satisfaction with security policy
  - Cognitive load

Outline

- Motivation
- Our approach
- HITOP
- Case study
- Challenges
- Future work

Challenges

- How do we quantify and determine how the variables change? How do we determine the utility functions?
  - We are looking at previous surveys in the literature
- How do we obtain quantitative inputs?
  - Work done by colleagues in Newcastle University
- How do we validate our model?

More on validation

- Recall the questions we seeks to answer
  - Are we better off with this technology or the other?
  - Which policy or technology is riskier?
- Quantitative security metrics provide us with insights needed to answer the questions
  - The actual numbers are not the goal
  - They help in providing insights on answering these questions

Outline

- Motivation
- Our approach
- HITOP
- Case study
- Challenges
- Future work

Future work

- We are seeking more understanding about the behavior of human users
  - Specifically we are interested in how users make risk assessment when it comes to cyber-security
- We want to consider different models of human behavior
- We are seeking to obtain data from CITES or NCSA to characterize our case study

THANK YOU!