Facial Recognition based Access Revocation

Vicky Katara
vpkatara@ncsu.edu

March 24, 2016

1 Problem Statement

Several traditional and non-traditional (for example, biometric) authentication methods exist. Most contemporary secure terminal systems measure inactivity on standard I/O devices like the keyboard / mouse, so as to lock the terminal after a predefined and often default time period of inactivity [1]. No contemporary methods exist which continuously monitor the physical presence of an authorized user during the length of an open session. An authenticated user may step away from the terminal with an open session for an unpredictable length of time. This leaves the system vulnerable to malicious users who may physically hijack the session before terminal locks itself due to inactivity.

2 Solution Idea

One way to provide continuous session monitoring is to test the video signal of the frontal area of the secured terminal for the presence of a face with reasonably matching characteristics with those of the authenticated user. The session monitoring system will automatically be initiated when authentication completes. As soon as the session begins, it will capture the facial characteristics of the authenticated user and the maintain them as trusted characteristics in the memory. It will periodically capture candidate facial characteristics of the face in front of the terminal, and match them with the trusted characteristics to pass the threshold matching criteria. If the similarity between the characteristics is below a certain defined threshold, the system will revoke access from the user by locking the terminal. If the similarity is above the threshold, the system will replace the trusted characteristics with the candidate characteristics so as to account for slowly changing effects of the environment.

The system will also look for tell-tale signs of manipulation such as photography / video based masquerading exploitations of the system. It will test for expected small changes in similarity between facial characteristics. A match of characteristics above a certain 'perfect' threshold is usually a sign of exploitation, and encountering such a scenario, the system would revoke authentication. Further, the system would use facial recognition algorithms robust against changes in face yaw, skin color and facial expression, among others [2] [3] [4].

3 Threat Model

A description (at least several paragraphs) describing the security assumptions for your solution idea. A good threat model should describe: (a) who is the adversary, (b) what are the goals of the adversary, (c) what are the capabilities of the adversary, and (d) what is the trusted computing base (TCB). Note, when describing the adversary capabilities, if is often useful to describe assumptions of what the adversary cannot do (e.g., does not have physical access to a device).

4 Research Questions

A list of at least three (more desired) research questions that inquire about the problem and/or solution idea. Research questions should be specific, concrete, and unambiguous questions. For example, research questions may inquire about protection against specific threats, performance overhead, scalability, and usability.

RQ1: *What are your research questions?*

RQ2: *There should be at least three, but more would be better.*

RQ3: *Make sure the questions are specific, concrete, and unambiguous.*

5 Methodology

A high level description of how you plan to answer the research questions. For example, a project might design and implement a protection and then empirically evaluate the protection in some way.

6 Evaluation Plan

A description of how you plan to answer the research questions. The evaluation plan may mirror the research questions, or multiple research questions (e.g., **RQ1** and **RQ2**) may be answered by a single part of the evaluation. The proposed evaluation may be split into both the design and a more formal evaluation section. In system security research papers, the design section often provides a form of evaluation by describing how the solution defends against potential attacks. If possible, a security evaluation section should summarize the defense against the threat model. Systems security papers also have more formal evaluation sections that consist of several experiments. For each experiment, you should describe: (a) experimental setup (e.g., hardware, software, and datasets used), (b) specific measurements and metrics you plan to use, and (c) what constitutes success.

6.1 Name of Experiment 1

State some hypothesis for the experiment. Note which research question it is designed to address.

6.1.1 Experimental Setup

Describe the hardware, software, and datasets you intend to use. Note that you should be realistic in what you can get access to.

6.1.2 Expected Results

Describe the specific measurements and metrics you plan to use. Describe what constitutes success (i.e., what you expect to achieve).

6.2 Name of Experiment 2

State some hypothesis for the experiment. Note which research question it is designed to address.

6.2.1 Experimental Setup

Describe the hardware, software, and datasets you intend to use. Note that you should be realistic in what you can get access to.

6.2.2 Expected Results

Describe the specific measurements and metrics you plan to use. Describe what constitutes success (i.e., what you expect to achieve).

6.3 Name of Experiment 3

State some hypothesis for the experiment. Note which research question it is designed to address.

6.3.1 Experimental Setup

Describe the hardware, software, and datasets you intend to use. Note that you should be realistic in what you can get access to.

6.3.2 Expected Results

Describe the specific measurements and metrics you plan to use. Describe what constitutes success (i.e., what you expect to achieve).

References

[1] Xue Dong Yang, Peter Kort, and Richard Dosselmann. Automatically Log Off Upon Disappearance of Facial Image. In *Defense Research and Development Ottawa, Canada, Contract Report*, 2005.

[2] P. Jonathon Phillips, Patrick Grother, and Ross J. Micheals et al. Face Recognition Vendor Test 2002: Evaluation Report. In *NIST Interagency Report 6965*, 2003.

[3] Alexander M. Bronstein, Michael M. Bronstein, and Ron Kimmel. Three-Dimensional Face Recognition. In *International Journal of Computer Vision*, 2005.

[4] J. Kovac, P. Peer, and F. Solina. Human skin color clustering for face detection. In *The IEEE Region 8 EUROCON 2003. Computer as a Tool*, 2003.