CS6282: Statement of Work

Spring 2019 Teammates: Stephanie Lew, Zhang Ji Yi

Prof. Jun Han Date: 04/03/19

Executive Summary

To be completed.

Introduction

/ Need for privacy

(Rewrite) Mobile devices (e.g. smartphone and Mobile devices are now infused into various aspects of our daily lives including work, social activity and entertainment. A wide variety of smartphone and tablet apps enrich the personal lives of millions of users in a variety of ways. As a consequence of the extensive usage, ample private data is stored on or is accessible through mobile devices.

/ Need for continuous and passive authentication To protect such private data against threats imposed by unauthorized access, mobile devices and their operating systems employ traditional access control mechanisms using passcode, lock pattern and fingerprint. Previous work has shown drawbacks of these methods with regards to security, usability and cost [2][3][4][26]. To tackle the challenges, researchers propose continuous and passive authentication as a supplement to existing schemes [9][24][32]. The proposed system constantly senses a user's interactions with the device and authenticates the user in runtime through behavioral data. The behaviors typically include touchscreen gestures, frequent physical locations, poises holding or picking up the device and so forth. They can collectively contribute to all-round protection against unauthorized users. Embedded sensors on devices, such as touchscreen, accelerometer and gyroscope, facilitate the collection of behavior-related measurements.

/ Need for Cross-device user authentication Though extensive efforts have been devoted into continuous authentication, the rapid and massive development in the mobile industry brings new opportunities and corresponding challenges. Many customers now own multiple devices. According to mar- ket research, about 31% of US adults have both smartphones and tablets [1], while UK households typically own on average three types of internet-enabled devices [20]. Mobile users switch between their devices in daily usage. It raises the problem of user authentication across multiple mobile devices in a seamless manner.

/ Need for Context awareness

/ Need for good security and usability tradeoff. Caveats of face and voice recognition in general - Physiological biometrics

/ Our approach:

We propose a multi-modal biometric approach to authenticate users continuously in smarthome environments. Time sampling method. Don't require all information. Only a good biometric sample.

Problem statement Multifactor authentication is considered more secure than single factor authentication [14].

Put your Problem statement here! Example of a Citation[**?**]. See [**?**] for more info.

Objectives

Succinctly describe the problem that this research will address (1 or 2 paragraphs is fine). Describe the scientific and technological baseline, that is, the current state-of-the-art or developmental status of the field to be advanced

Detailed project description and goals Project tasks, milestones, deliverables Task timeline / schedule (Fine-grained as possible) Summary of related Potential risks and backup plan (s) Team member responsibilities / effort Project budget Risks Backup Plan References

Presentation Clear motivation Important details of project Time limit 10 min. A novel mechanism takes in

Scope of Work

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Administration

If there are meetings, calls, conferences, or other "soft" deliverables, they should be outlined in the administration portion of the SOW. Any requirement that is not an end product of a specific task, but is required of the performing party, needs to be described in the administration section of the SOW.

Timeline

This section lays out all dates for the project. It states dates for the tasks and deliverables. It also covers the dates for the administration portion of the SOW.

Attachments

Lab Notes, HelloWorld.ic, FooBar.ic