Identity Issues in Collaborative Natural User Interface Environments

[Extended Abstract]

Zach Harbort
The University of Tulsa
800 S. Tucker Drive
Tulsa, Oklahoma 74104
zach-harbort@utulsa.edu

David Greer
The University of Tulsa
800 S. Tucker Drive
Tulsa, Oklahoma 74104
david-greer@utulsa.edu

ABSTRACT

Devices featuring Natural User Interfaces (NUIs) are emerging as viable tools to conduct business processes, information exchange, and data interaction. When utilized in a collaborative environment, unique security concerns arise as new dimensions are introduced (e.g. gestures, spatial location). In a clearance-restricted space, how might access controls be enforced as data is shared between devices via hand gestures? Policies would need to reflect all relationships between users, gestures, and devices based on these new interfaces. This paper describes a research platform developed to foster collaboration through the use of NUIs on multi-touch, multi-user surfaces. It also introduces common scenarios and discusses accompanying security implications.

1. INTRODUCTION

The utilization of natural user interfaces to conduct business has increased within the last few years. In a January 2011 study by Morgan Stanley, two-thirds of chief information officers surveyed expected to purchase tablets for employees and/or allow personal tablets onto their corporate network(s) [1]. As more organizations adopt NUI technologies, we expect to see a growth in applications that allow for seamless data interaction and sharing. Unfortunately, very few models and methodologies exist which map entities to varying forms of NUI devices in an environment containing sensitive data. The notion of “who is touching what” is not only a concept that can help improve user interface design, but also combat access control concerns which abound in collaborative workspaces.

In traditional government or military office spaces, the relationship between a user and workstations is fairly straightforward: access is typically granted via Common Access Card (CAC), which represents that person’s identity in the organization. In a multi-touch, multi-surface environment, a user’s identity would need to persist not only across devices, but also with the data being shared. For example, if sensitive data is sent from a subject’s tablet to a large-scale screen for viewing, security permissions would need to travel with it. If this scree has multiple active viewers (users), the ability to open data around should be moderated based on their clearance levels.

The remainder of this paper is organized as follows. Section 2 gives background information on types of NUI devices, how NUIs are used for collaboration, and a description of our HCI lab where testing is being performed. Section 3 presents a new research platform and common scenarios. Finally, Section 4 discusses future work and conclusions.

ID360 ’12, April 23-24, Austin, Texas, USA

2. BACKGROUND

2.1 Natural User Interface Devices

Natural User Interface (NUI) devices can range from handheld to wall-sized. All can be tailored for specific tasks so long as their size and/or orientation does not introduce a sense of inhibition (e.g. limited screen space). Popular device forms include mobile phones (e.g. Apple iPhone), tablets (e.g. Apple iPad), and tables (e.g. Microsoft Surface). Factors to take into account when choosing a NUI device for a specific task can include:

- **Scalability** - number of supported users/touches
- **Portability** - mobility of the device
- **Interaction** - touch recognition/data manipulation capabilities
- **Analysis** - forms of analysis to be performed

2.2 Collaborative Natural User Interfaces

A number of institutions and organizations have active research and development efforts in multi-user applications for natural user interface devices. These include Apple Inc., Microsoft Corporation, The University of Canterbury, and The Upper Austria University of Applied Sciences whom have all constructed their own interactive tables with several in-house applications designed for collaboration. Their results proved the merit of using such devices [3], but users were restricted to a single space and developers to a single platform.

The semantics of collaboration vary on an application basis. To clarify, a multi-touch table may only support a local collaborative experience (e.g. solving a virtual puzzle with others on the same device) while a tablet could support both a local and remote collaborative experiences (e.g. solving a problem locally and sharing the answer to other tablets and tables). This research relies on discovering similar scenarios to help develop and improve a unified collaborative experience, independent of platform.

2.3 CAVE

The Collaborative Analytical Visualization Environment (CAVE) is an immersive collaborative laboratory developed with the ultimate goal of platform independence. This laboratory contains hardware research platforms centered on innovative, unobtrusive, and intuitive user interfaces for varying systems. At the heart of the CAVE is a 4x10 ft. multi-touch wall to test not only collaborative software, but also provide the means to test hardware/software interoperability, as well as advance multi-touch hardware solutions. All testing for this paper occurred in this laboratory.

3. CURRENT WORK

3.1 Gesture-Oriented Data Sharing

Gesture-Oriented Data Sharing (GODS) is a unique research platform developed to support the sharing of data via simple hand gestures on NUI devices. It "removes" the physical medium (e.g. USB flash drive) and gives users the illusion that their data is travelling with them by storing information in a private cloud. The innovative aspect of this research approach is based on its platform independence through the use of a Service-Oriented Architecture (SOA). One of the major goals GODS strives to accomplish is a sense of device interoperability.

3.1.1 *Architecture*

The GODS architecture includes four main components: clients (e.g. mobile phones, tablets, multi-touch wall), a web service, a file server, and a database. This modular design helps to separate the components into non-conflicting development environments where each section acts as a point in the aggregation process.

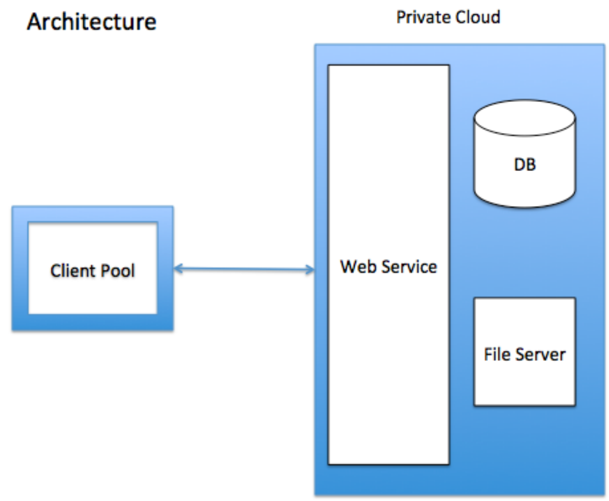

Figure 1: Architecture of GODS

3.1.2 *Interface*

The GODS user interface contains a workspace and configurable "hotspots", or drop zones that are paired with active devices on the network. To share data with one of these active devices, a user will simply drag the object and drop it onto the corresponding hotspot, as shown in Figure 2.

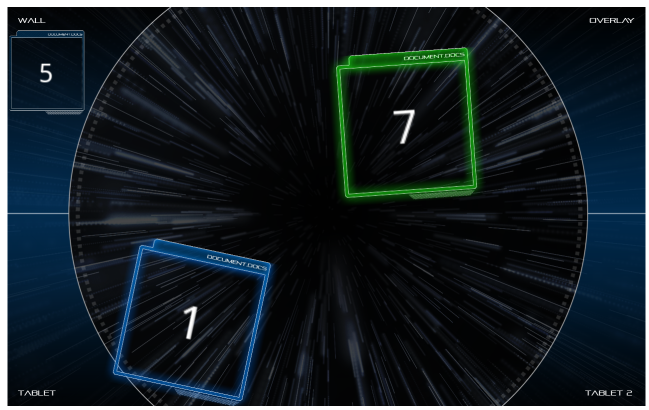

Figure 2: Interface of GODS, displaying data objects and hotspots

3.1.3 *Gestures*

The GODS platform supports several gesture patterns to interact with and manipulate data. For purposes of this paper, two globally accepted gestures will be discussed: swipe and pinch. A "swipe" (or drag) is generally representative of moving an object through space. In the GODS environment, a swipe invokes a "SEND" action, meaning a piece of data is copied and sent from a subject device to an object device (or devices). A "pinch" is generally representative of collapsing an object into a state of nothingness. In the GODS environment, a pinch is more of a personal gesture as it invokes a "STORE" action, meaning data is removed from the current system and stored in a fileserver for later retrieval. An entry is then added to the database containing a user-data pair. Only that particular user who performed the pinch can retrieve it later on a GODS-enabled device.

3.2 Scenarios and Security Implications

In an office environment where data sensitivity is typically low (unfiled papers, etc.), one might not worry about who has visibility of what, at least between employees in the same department. In a command and control environment where clearance levels vary from person to person, both a sense of collaboration and security needs to be maintained. To enforce this, data is tagged with information such as clearance level, privileges, and/or user ID. Therefore, whenever data is "swiped" from a subject device to a shared device, the system would scan all users sharing the receiving device and redactions made accordingly based on the lowest active clearance level.

Another scenario may be that an individual is presenting at a conference across the country. He "pinches" a file and sends it to the private cloud as shown in Figure 3. A unique user-data pair is then created to link the file to the individual. When he arrives at his destination, he authenticates with a GODS-enabled device and retrieves the file. Because

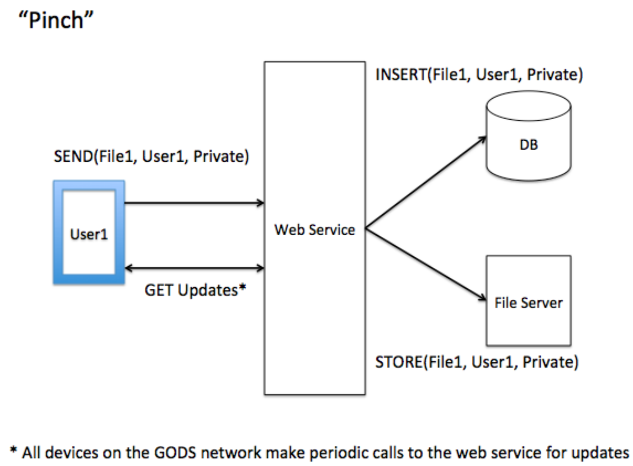

Figure 3: Flow of data after a file object is pinched

the user claims ownership of the file, he has the right to adjust privilege and redaction settings. For example, a fail-safe could be implemented in the case that an individual of lower clearance exists in close proximity (e.g. restricted access).

4. CONCLUSIONS AND FUTURE WORK

Gesture-Oriented Data Sharing (GODS) has served as an effective platform for developing software applicable to all sectors. It demonstrates that device interoperability is possible through a robust service-oriented architecture. It also opens the doors to future research into identity verification, access controls, etc. for these types of emerging collaborative environments.

Research will continue focus to on improving the GODS user experience, strengthen the data structure to better support security policies, and perform outreach projects to assess the effectiveness of natural user interfaces for collaboration.

Other future additions and improvements will be to develop unique forms of authentication based on biometric modalities (gesture patterns), near field communication, RFID, and QR codes.

5. ACKNOWLEDGEMENTS

This material is based on research sponsored by DARPA under agreement number FA8750-09-1-0208. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

6. REFERENCES

[1] K. Hubert. Tablet demand and disruption: Mobile users come of age. Technical report, Morgan Stanley, February 2011.

[2] S. Scott, K. Grant, and R. Mandryk. System guidelines for co-located, collaborative work on a tabletop display. In *Proceedings of the eighth conference on European Conference on Computer Supported Cooperative Work*, pages 159–178. Kluwer Academic Publishers, 2003.

[3] M. Waldner, J. Hauber, J. Zauner, M. Haller, and M. Billinghurst. Tangible tiles: design and evaluation of a tangible user interface in a collaborative tabletop setup. In *OZCHI '06: Proceedings of the 20th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artifacts and environments*, pages 151–158, New York, NY, USA, 2006. ACM. [BEST PAPER AWARD].