A Survey on Identification topology through custom personal touch

Miss. Amruta S. Agrawal, Miss. Bharati I. Mendhe, Prof.Nilima V. Pardakhe

Abstract— Today's identification and authentication mechanisms for touchscreen-enabled devices are cumbersome and do not support brief usage and device sharing. Touch-based personal tokens would let devices unobtrusively identify who is interacting with the device at any given time. Devices could then tailor services to users and control access to sensitive information and online services. The use of devices such as smart phone, tablet etc. for storing sensitive information and accessing online services is increasing. At the same time, methods for authenticating users into their devices and online services that are not only secure, but also privacy and user-friendly are needed. In this seminar an approach for using a wearable personal token, in the form of a ring, to send an identification code to devices through touch. In conjunction with touchscreen receivers this ring serves as a user identification token that would be diversely compatible with a myriad of applications, such as user authentication for login, gaming, parental control, near-field communication (NFC) applications, etc. The ring will also serve as a single token or 'key' that would provide a unified access to multiple devices belonging to the user.

Index Terms— Signet Ring, Touchscreen, User Identification, Capacitive Touch, Distinguishing Users.

———————————— ◆ ————————————

1 INTRODUCTION

Pervasive computing is an advanced computing concept where it is made to appear everywhere and anywhere. In contrast to desktop computing, pervasive computing can occur using a particular device, in any location, and in any format. A user makes interactions with the computing device, which is in many different forms - laptop, tablets, smart phones, etc.The underlying technologies to support ubiquitous computing include Internet, new I/O (input / output), new user interfaces, networks, mobile protocols, location and position of new materials, etc.

In this era of pervasive computing, there is interaction with and rapidly switch among a diverse set of digital devices. People tend to transition from a smart phone to a notebook when arriving in the office, and when return to home, often switch to a tablet. In between, there is use of wall-mounted displays, car navigation systems, and home security or smart home controls. Many of these devices have multiple users even if only used in the home. Over the next decade, this range of devices will likely increase, and the time with any single device will grow shorter. It's time for touchbased personal tokens that let devices identify who is interacting with the pervasive device. We wants to share with you a very nice example, suppose that a child reportedly spent more than $1,000 on in-app purchases while playing games on his mother's smart Phone. Devices that identify their users can protect such spending from unauthorizeduser. The approach is to use a wearable personal token to communicatean identification code through touch.

2. History

In 1960's first time touch screen was developed for air traffic control systemsand is now a popular user interface technology on devices ranging from ATMs and self-service terminals in grocery stores or airports to cars, smart phones, and tablets. Even the touchpads used in laptops are based on similar technology. These products employ different touch screen implementations such as including analog resistive, surface capacitive, projected capacitive, surface acoustic wave, infrared and optical technology to mention a few. In 1988 Mark Weiser proposed the phrase "ubiquitous computing" around, during his tenure as Chief Technologist of the XeroxPalo Alto Research Centre (PARC). Both alone and with PARC Director and Chief Scientist John Seely Brown, Weiser was write in some of the earliest papers on the topic, largely defining it and sketching out its major concerns.

Identifying that the extension of processing power into everyday scenarios would necessitate understanding the nature, beyond its proper ambit, Weiser was influenced by many fields outside computer science, including "philosophy, phenomenology, anthropology, psychology, post-Modernism, sociology of science and feminist criticism". He was finding about "the humanistic origins of the 'invisible ideal in post-modernist thought'", referencing as well the ironically dystopianPhilip K. Dick novel Ubik.

Andy Hopper from Cambridge University UK gives and demonstrated the concept of "Teleporting" - where applications follow the user wherever he/she moves.

Roy Want, while a researcher and student studying under Andy Hopper at Cambridge University, worked on the "Active Badge System", which is an advanced location computing system where personal mobility that is merged with computing.

Bill Schilit (now at Google) also did some earlier work in this topic, and participated in the early Mobile Computing workshop held in Santa Cruz in 1996.

Dr. Ken Sakamura of the University of Tokyo, Japan leads the Ubiquitous Networking Laboratory (UNL), Tokyo as well as the T-Engine Forum. The joint goal of Sakamura's Ubiquitous Networking specification and the T-Engine forum is to enable any everyday device to broadcast and receive information.

MIT has also contributed significant research in this field, notably Things That Think consortium (directed by Hiroshi Ishii, Joseph A. Paradiso and Rosalind Picard) at the Media Lab and the CSAIL effort known as Project Oxygen. Other major contributors include University of Washington's Ubicomp Lab (directed by Shwetak Patel), Georgia Tech's College of Computing, Cornell University's People Aware Computing Lab, NYU's Interactive Telecommunications Program, UC Irvine's Department of Informatics, Microsoft Research, Intel Research and Equator, Ajou University UCRi & CUS.

3. User Identification Challenges

Current user-identification techniques are based on logins and PINcodes or passwords. It becomes headache oflogging in again and again whenthe user used to sit down for long sessionsof work in front of a computer, but many users forgot any authentication on their mobile devices.Similarly, in biometrictechniques, such as fingerprint readersor face recognitionare more resourceintensive and face their own usabilitychallenges. Fingerprint readers requirespace on a device, and cost of this device is very high, and it can bedifficult to use in low-humidity environments.Face recognition has higherprocessing requirements and can be difficultin low-lighting conditions. The goal is to finda way to identify users during their regular interactions with pervasive devices. Capacitive touch sensors have emerged as a dominant user interface technology for mobile and pervasive devices. Touch sensors reside in hundreds of millions of smart phones and tablets as well as in ATM machines, car dashboard displays, and even home appliances such as televisions, microwaves, and refrigerators. Touch is the predominant way of navigating and interacting with today’s computer-embedded devices, the approach seeks to identify who touches a device, which can be more accurate (or secure) than user-proximity sensing with short-range radios such as Bluetooth or NFC. When there are several potential users near a device, one of the most easiest ways to identify who’s really interacting with the device is to identify who is touching it.

4. A Touch-Identification Token

The pervasive capacitive touchscreen and touchpad input devices are used as receivers for an identification code or password. The current token is in the form of a ring, but other devices are also possible, such as wristbands or watches. The token transmits signals when brought in contact with a device’s touchscreen or when the user’s finger touches the screen. The signal is transmitted from the human skin. The transmitted electrical signal from the token essentially spoofs the device’s touchscreen, mimicking the signalsfrom up and down movements of afinger, while the finger (or token) itselfremains stationary on the device.

Capacitive touch screen comprisesan array of conducting electrodesbehind a transparent insulating glasslayer, which form a capacitor with thehuman finger when the user touches thescreen. The finger is in turn capacitivelycoupled through the human body (andsometimes through the ground) to thedevice’s case. A touch can therefore bedetected by driving the electrodes withan AC signal to repeatedly charge anddischarge the capacitor and measurethe change in capacitance through thechange in charge voltage. Where onthe electrode array this change occursreveals the location of the touch.

Owing to the small capacitance involved, a charge integration circuitmight be necessary.[1] When this changein voltage exceeds a certain thresholdand meets several other filtering criteria the screen’s firmware reports thepresence of a new touch event to thedevice’s operating system, which thetraverses up the software stack to the application level. As wearable hardwaretoken comes in contact with thescreen, its own AC signal charges anddischarges the capacitor formed withthe screen’s electrodes, leading to repetitivebut irregular touch events capturedby the touchscreen controller.

The system then exploits this abilityto generate touch events through electricalsignals to modulate these evenstand communicate a short identificationcode between the token and device. This system can be viewed as a classical communication system with a

• Transmitter (a hardware token);

• Communication channel (the hardware and firmware of the device’s touch screen, the software stack and its operating system); and

• Receiver (the software component demodulating the sequence of touch events to receive the originally transmitted bit sequence).

The transmitter generates electrical pulses that are modulated tocarry the input bit sequence using onoffkeying modulation, that is, a onebit is represented by the electricalsignal is turning on, and a zero bit is representedby switching that signal off. As a result,the pattern of the sequence of touchevents generated follows the original bitsequence. These events thus can be usedto reconstruct the originally transmittedbit sequence on the receiver side otherwise unknown to the screen. Thesoftware component, act as thereceiver, counts the number of touchevents in each bit period to determinewhich bit was transmitted. It receives aone bit if the number of events appearing in that bit period is greater than acertain threshold otherwise, it receivesa zero bit.

5. Decoding Challenges

Because touchscreens weren’t designedfor communication purposes, thetouchscreen responded differently tothe same input, generating different received bit patterns. Consider for example, the number of touch events registered whena one bit is sent after a long sequence ofzeros is lower than that of a one bit thatcomes after a long sequence of ones.The variable delay between the transmission of a bit and its reception at the receiver makes it even more challenging to demodulate it to retrieve the original bit sequence.

In addition, the channel adds an unknown delay between the receiver and the transmitter due to the unknown processing delay of the device, which depends on the device's workload. Asa result, traditional demodulation techniques aren't applicable. Instead a two-step process is devised to decode the originally transmitted data: first calibration,then correlation. During offline calibration, the software component selects a threshold, which is used for bitdetection during the correlation phase.The offline calibration step computesthe expected number of touch eventswhen a one bit or zero bits are transmitted.To determine this number, the stepmust be performed once per device,per data rate, during initialization. Thehardware token repeatedly transmits abit sequence that's known to the receiver.

Upon receiving a sequence of touchevents corresponding to that known bitsequence, the receiver software synchronizeswith the transmitter, then countsthe number of touch events in each oneand zero bit to calculate the averagenumber of expected events in each.During the actual communication, assuming all possible messages areknown, the software decoder thencomputes the correlation between thetouch event sequence and all possiblemessages using the expected numberof events. The message that yields thehighest correlation value is selected asthe originally transmitted bit sequence.

6. Applications

The work demonstrates the feasibility of communicating short codes from the tokens to touch receivers. This technique can be directly applied to parental-control applications, games which are played by more than one user, and weak authentication for any devices. Further improvement in the rate of data transfer, reliability, and security would result in immense opportunities to create a unified user identification and authentication scheme around personal tokens rather than passwords.

In today's SIM cards, which are identification tokens for devices in a cellular network, wearable tokens can provide personal identification for users. Conceptually, SIM cards were an adequate solution for users to accessing a network through a device. However, with access to diverse devices. There are many devices such as smart phones, laptops, tablets, and cars, which might be shared among multiple users, it's more important to understand which user is interacting with the device.

In addition, with future shared data plans (shared across devices), data usage from any device can be charged to a user-specific (rather than device specific) account. This type of billing model can be realized with proposed techniques, using the signet ring as a personal identification token a portable SIM-ring worn by users.

Beyond networking, the token could also allow payment functions and replace credit cards (becoming a credit ring). It can authenticate transactions on mobile phones and ATM machines and could even be used to access a smart home, to open the door for authorized access and loading user-specific preferences on certain devices, such as the home appliances.

7. Advantages

- It can allow users to access their device anywhere and anytime (hence it is ubiquitous).
- It is more secure than password or pin code system.
- No need to handle the token because of its small size unlike smart phones or tablets.
- It is wearable (i.e. hands free device) therefore users don't need to take additional efforts for taking it from one place to another.
- It can overcome limitations of biometric techniques.
- It provides authentication to user who wants to access a particular device.

8. Limitations

- It works only on touch screen devices.
- There is possibility of losing the token if the user is careless.

9. Conclusion

Integrating identification and authentication functions into a wearable item, such as a ring or wristband. The token should reduce the probability of losing the device especially as compared to smartphones and thus reduce the security risks related to unauthorized users.In applications with higher security requirements, these tokens could be one part in a multifactor authentication system. Thus, ubiquitous computing is responsible for the automatic personalization of computer infrastructure to create a customized user experience that's better suited to the task at hand.

References

[1] Tam Vu and Marco Gruteser, "Personal Touch – Identification Token", Roy Want, April-June 2013;1536-1268/13/$31.00 © 2013 IEEE
[2] C. Newton, "Google's Password Proposal: One Ring to Rule Them All," Cnet News, 18 Jan. 2013; http://news.cnet.com/8301-1023_3-57564788-93/
[3] C. Cornelius et al., "Who Wears Me? Bioimpedance as a Passive Biometric," Proc. 3rdUSENIX Workshop onHealth

Security and Privacy, 2012.
[4] T. Vu et al., “Distinguishing Users with Capacitive Touch Communication,” Proc.18th Ann. Int’l Conf. Mobile Computingand Networking (MobiCom 12), ACM, 2012, pp. 197–208.
[5]C. Foresman, “Apple Facing Class- Action Lawsuit Over Kids’ In-App Purchases,” ArsTechnical, 15 Apr. 2011; http://arstechnica.com/apple/2011/04/ apple-facing-class-action-lawsuit-overkids- in-app-purchases.
[6] W. Westerman and J.G. Elias, Capacitive Sensing Arrangement, US patent2006/0232,567,2006.
[7]http://en.wikipedia.org/wiki/Ubiquitous_computing