Cyber Risks to Secure and Private Universal Access

G. Susanne Bahr[1], Liam M. Mayron[2], and Hannah J. Gacey[1]

[1] Psychology
Florida Institute of Technology
Melbourne, Florida, USA
[2] Government Communications Systems Division
Harris Corp.
Melbourne, Florida, USA
gbahr@fit.edu, lmayron@harris.com, hgacey2010@my.fit.edu

Abstract. The overarching goal of UA is affording all individuals, regardless of disabilities, geographic status, infrastructure, age or training background, the use and benefit of information technology. The goal of this paper is to raise awareness of *the security and privacy cyber risks in the everyday use of UA technology.* The challenge of UA technology transfer from the laboratory to real world setting leads us to identify vulnerabilities of UA users and to present examples of cyber security strategies to safeguard data. The principles of confidentiality, integrity and availability guide our non-exhaustive review of concrete UA approaches and their security and privacy implications for everyday use. We examine the cyber risks to privacy and security of brain computer interfaces and UA home networking and conclude with call to interdisciplinary collaboration between the security and UA expert communities to ensure the transitioning of safe and secure UA technologies to the end-users.

Keywords: Universal Access, Privacy, Security, Technology Transfer, Brain Computer Interfaces, Networks, Hacking, Interdisciplinary Research.

1 Introduction

The overarching goal of universal access (UA) in human computer interaction (HCI) is affording all individuals, regardless of disabilities, geographic status, infrastructure, age or training background, the use and benefits of information technology. The UA research agenda has prolifically generated new ideas, methodologies and solutions for universal access to technology [1], [2], [3], [4]. At the same time, there remain facets of the UA challenge that are conspicuous by their minor treatment in the UA literature: privacy and security. For instance, in the 2009 Handbook of Universal Access, only one of sixty-one chapters deals explicitly with security [5]. In fact, with the exception of Maybury's concise chapter on international security policies the topic is mentioned implicitly or treated superficially, if at all.

It is difficult to deny that the privacy and security concerns of users and their families will likely emerge from the UA axioms of inclusiveness and diversity. Clearly, universal access is not intended as a bidirectional flow of information

C. Stephanidis (Ed.): Universal Access in HCI, Part I, HCII 2011, LNCS 6765, pp. 433–442, 2011.
© Springer-Verlag Berlin Heidelberg 2011

resulting in being universally accessible. Potential issues may be less evident in laboratory settings because researchers are accountable to institutional review boards which are governed by federal and international laws. Instead, privacy and security issues become tangible and consequential as UA solutions migrate from the laboratory to the real world, i.e., commercially available technology and real networks. This challenge is at the core of this paper: *What are the security and privacy cyber risks for the everyday use of UA technology?* For example, should advertisers have access to interaction data that allows them to determine which users have sensory impairments or where they are located? How do we protect health related data collected in non-traditional interaction paradigms such as brain computer interfaces from unwanted disclosure or corruption? These questions not only introduce privacy concerns, but also raise security matters. For example the site "pleaserobme.com" educates its users how to easily track the current location as well as location trails of a mobile device, i.e. its user, using Google maps [6]. The site suggests that lack of location privacy makes users' homes vulnerable to burglars. Such information, in combination with health information, may be exploited for other dark purposes left to the reader's imagination.

Another example deals with health-related data collection and storage: the US Department of Health has recorded 216 violations of health Information privacy since 2009 for databases that have been hacked or left unprotected. The range of records, i.e., confidential data of real people, reaches above one million for a case of hard drive theft from BlueCrossBlueShield, Tennessee. Other types of breaches include loss, improper disposal, hacking, and unauthorized disclosure [7].

The remainder of this paper presents UA vulnerabilities and reviews cyber security strategies and objectives, which lead to a brief, non-exhaustive review of UA approaches and their security and privacy implications for everyday use. Some of our ideas may seem grotesque, overstated, or paranoid. We do acknowledge that media confessions of hackers and anecdotal evidence suggest that hacking into confidential and secured spaces is perceived as a challenge without intend to harm or the harboring of sinister intentions. For transcripts of interviews see [8]. However, such observations trivialize the problem and remain insufficient evidence to dismiss the need to protect the unsuspecting UA user from being unethically universally accessed. Hence, to protect privacy and security we have to enter the dark side of universal access technology in the real world network of networks.

2 Universal Access Targets and Vulnerabilities

Universal access includes those individuals who are otherwise unable to gain access to information technology. They are offline and perhaps even unlisted or "ungooglable", as epitomized in *The New Yorker* cartoon by Roz Chast [9]. What makes these disconnected individuals unique or excludes them from access? Primarily, they do not represent the average user of standard interfaces for high speed networks. Apart from making a deliberate decision against technology access, non-accessing individuals may be socioeconomically or geographically without access, or are virtually disconnected due to low speed or low bandwidth connections. It appears

reasonable to argue that the UA users who are the most vulnerable and require the most protection from exploitation are individuals with motor or sensory disabilities or cognitive impairments and medical issues. For example, the elderly have been invisible disconnected due to unfamiliarity with technology, training issues, and lack of age-appropriate interfaces. Consequently, a paramount UA approach to empower "all" to avail themselves of information technology is by overcoming barriers through user models and interface design. Such efforts are not without introducing risks that require identification and management.

Concerns dealing with consumer privacy, health data privacy, demographic data privacy and location privacy are not new to the modern networks of networks but may escalate as UA succeeds. In this context, one might think of "cyber-patients" and their physical or psychological safety when depending on the web-based services. While Internet practices and safeguards are ongoing discussion topics, reliance on unverified assumption about user knowledge, skills, abilities, security awareness, or compliance are unlikely to control risk. Instead, research must become sensitive to security issues and invoke processes for designing with security in mind, thereby making networks, including the internet, relatively safe places for interactions and transactions.

Fig. 1. The Ungooglable Man by Roz Chast (reprinted with permission of The Cartoon Bank, a New Yorker Company/Condé Nast Publications Inc.)

3 Cyber Security Today

Security is a fundamental consideration in contemporary computation. For example, malware is a major concern for systems because, as the name suggest, it is software designed to do harm. Harming the system may involve harvesting private or sensitive data, altering or corrupting of data, compromising the processing of data, or denying access. Malicious code may traverse networks such as the Internet to seek a host. Indeed, being offline seems like a safe place for users and their computers. However, as malware such as Stuxnet has shown, even systems that are isolated from an external network (called "air gapped") are vulnerable [10]. For background, Stuxnet is a worm that self-replicates and appears to attack control systems. Its discovery in 2010 was high-profile news because it infested the internal networks of nuclear power plants. Isolation from the Internet may seem a safe strategy to protect data and software from misuse and corruption, however the Stuxnet example illustrates even air-gapped system may be vulnerable. The question arises, *how do we protect privacy and data*?

The states of science and practice have identified many ways to secure a system [11]. The following is an overview of the "how to" secure systems health and data assuredness [12]. They include at least seven strategies: network intrusion detection, perimeter defense, encryption, malware detection, patch management, backups, and file reputation systems. This overview starts at the highest (network) level and ends with the assurance of individual files.

- Network intrusion detection: Here an intrusion detection system (IDS) analyzes network traffic (information flowing into and out of the network). The purpose of this analysis is to identify suspicious patterns of behavior that may be an indication of an attack or probe of system vulnerabilities. A sophisticated IDS may include a honeypot system that simulates vulnerabilities in order to attract and identify hackers.
- Perimeter network defense: This type of defense includes systems such as firewalls that reside between the internal network and the internet. A firewall may be installed on a computer or around an internal network of a group of computers. Authorized traffic may pass through a firewall, whereas unauthorized traffic will be denied [13]. Firewalls can be implemented in hardware, software, or both. The rules for categorizing traffic vary and can be set to different levels of permissiveness and scrutiny.
- Encryption: Encryption is an approach for securing data by transforming an intelligible pattern into an apparently random one [14]. The goal is to create and use secrecy to protect information that could is vulnerable to being tapped or stolen. In general, cyphers (algorithms used to transform plain text into something unreadable) have a long history of being invented and broken [Simon Singh,2000, the code book]. An everyday example of the use of encryption is the Hypertext Transfer Protocol Secure (HTTPS). HTTPS is used as the scheme for secure transactions such as online banking, e.g., *https://www.bankofamerica.com* [15].
- Host-based malware detection: Host-based (residing on one's computer) malware detection, includes antivirus software. It typically consists of actively-running software processes that detect and, if possible, contain hostile infections as they

occur. Antivirus software often includes defenses against Trojans, Worms, and other malicious viruses program and requires regular updates to be prepared to deal with new developments, which leads directly to the next item.

- Patch management: To remain secure, a system must have a way to update itself in order to correct vulnerabilities that have been identified and exploited since the system was originally deployed. Generally, the majority of resources in the lifetime of a software system are expended after the initial development [16].
- File reputation systems: Systems, particularly those encountering large amounts of data of unknown provenance, must be able to judge, with reasonable certainty, the risk of opening a file, executing a process, or communicating with a remote host. File reputation systems can reference remote risk databases in order to augment results.
- Backups: In the event a system is compromised beyond repair, a security strategy must include backups and the ability to restore a system to a known working state. The backups must be updated and checked regularly and systematically and hence require maintenance to be of use.

The objective of using and integrating these strategies is to secure data and system health against four types of cyber-attacks: Disclosure, theft, intentional damage and denial of service [17]. In order for a system to be resistant to such attack threats it must satisfy three universal security and privacy requirements [18]:

1. Confidentiality: Certain data must not be made public or should be restricted to only certain users or groups of users. Hackers, malware (malicious programs), or unauthorized insider activity are several of the threats to confidentiality.
2. Integrity: Data must remain impervious to unauthorized alteration or damage. Users must have the confidence that the data they are interacting with has not been tampered with in an improper way.
3. Availability: A system must be able to provide access to data when it is needed. System downtime, either intentional or otherwise, interrupts availability. Although a power outage or natural disaster may be natural causes for an interruption in system availability, it is possible to intentionally disrupt a system, such as through a distributed denial-of-service attack.

As the UA user group grows and its inherent diversity multiplies, the principles of confidentiality, integrity and availability are waiting to be addressed and may become more challenging as seen in the next section.

4 Universal Access Users under Attack

The purpose of this section is to visit UA concepts and research to consider emerging privacy and security concerns. We return to the question that is at the core of this chapter: *What are the security and privacy risks for the everyday use of UA technology?* The examples presented here examine security and privacy implications of brain computer interfaces and home networking for UA.

4.1 Brain Computer Interfaces

The concept of the Brain Computer Interface (BCI) is based on the measurement and interpretation cortical activity of a human user *in real time* so that this human may

interface with a system using his or her brain activity. Thus, interfacing changes from motor activities, such as typing and clicking, to *thinking about typing or clicking*. It has been noted that BCIs are of particular benefit to individuals with disabilities or in extreme circumstances that involve severe communication and motor control problems. Likewise, as a non-traditional human-to-system communication tool, BCIs become an additional input/output alternatives for traditional computer users. For an overview of BCIs see [19].

At the core of this chapter is the question which cyber threats and safe guards may affect UA technology transfer or UA solution that are commercially deployed. In the case of BCIs all three requirements (confidentiality, integrity and availability) seem relevant. For instance, a BCI system whose confidentiality has been compromised may provide physiological and interaction data of the user to outside parties. Such a breach is similar to accessing medical records without obtaining consent or HIPAA-like (Health Insurance Portability and Accountability Act) agreements. This offense is not trivial and in the USA, violators of patients' privacy rights can be held accountable with civil and criminal penalties [20]. Encryption of the nervous system may be a defense but it has been shown that even encrypted communications are susceptible to the man-in-the-middle attack [21]. In order to execute a man-in-the-middle attack, the perpetrator intercepts communications between two parties (or in the case of BCIs, the user and the system) and relays them as intended or altered. Eavesdropping alone without alterations, even in closed-loop interfaces, may not be detectable. The questions for technology transfer are at a minimum whether BCI users are aware of the risks and how to implement safeguards to protect these data.

Next, BCIs whose integrity has been corrupted may not disclose private information but act and function is an undesirable or harmful manner. BCIs require calibration and user profiles to match brain activity to the desired interaction. A compromised system may actuate undesirable inputs in response to brain activity. An example of an unwanted, perhaps harmless command would be the sending of an email draft instead of the final and intended communication. Other scenarios of mismatched intended and actuated input due to system compromise may include deleting instead of saving or typing erroneous characters in the case of BCI speller [22]. In addition to BCI use at home, BCI have been explored for driving and aviation tasks. We leave the consequences of compromised system integrity of a BCI to operate a motor vehicle to the reader's imagination [23].

Not only integrity issues but also availability limitations may have considerable influence not only over user frustration levels but impact safety. For a BCI to transcend novelty as an alternative and perhaps chic input device, it has to be reliably available. Users who depend on BCIs to connect to services, to work, and with friends and family, cannot be subjected to noticeable maintenance and downtimes, i.e., intermittent availability.

In summary, when considering the transfer of BCI technology from the laboratory to real world setting, we meet challenges regarding confidentiality, integrity and availability of the UA systems. Without resolving the privacy and security concern outlined, the deployment of BCIs may enhance the quality of life of potential users but also introduce unmitigated risks with uncertain consequences to the user. Next, we explore UA vulnerabilities in the context of home networking.

4.2 Universal Access and Home Networking

Technology and innovation are rapidly presenting consumers with new products for interfacing with the Internet, with many marketed for their ease of use. One such product is low-level home monitoring, which lets consumers invite information gathering artifacts into their personal space (their home) for small scale telemonitoring and the ability to "watch" their spaces [24]. Monitoring may also be accomplished with mobile devices and to the benefit of off-site caregivers who wish to keep a virtual eye on the activity of, e.g., their elderly or disabled family member [25]. In addition to surveillance, such systems may be smart, i.e., equipped with (a) sensors to detect user state and (b) actuators to make adjustments to the environment or artifacts in line with user needs [26]. Data gathered can be made intentionally available to a range of parties from emergency services to the individual consumer using or example a web browser enabled mobile phone. In this context, Baillie, Pucher and Képesi (2004) point out that, "the user should feel a sense of privacy and control over any artifacts proposed for their home space." [24, pg. 377]. Unfortunately, this reasonable expectation is not a trivial security problem.

The ease of penetrating a home that is connected to the Internet has been demonstrated recently in a high profile court case in Germany. The incident involved approximately 150 underage women whose privacy was invaded by taking external control of in-home webcams. The individual charged had approached his teenage targets using social networking sites [27]. The case demonstrated that granting control to one's personal webcam is as easy as clicking on an attached photo. This click not only opens the desired picture but also (without knowledge of the user) installs a virus that enables control of one's webcam by a remote user. This remote user then has the choice to turn the camera on and off, and if so inclined to record one's personal space and post the video, for instance, on *www.youtube.com* [28].

Unprotected home networks that reveal user activity put confidentially at stake. Moreover, integrity must be questioned due to unintentionally authorized access to network activity. It is perhaps counterintuitive, but in this context the requirement of system availability can create a threat to confidentiality. For example, a system that is reliably available but compromised may not only provide access to the user as intended, but also expose user actions and data to outside parties. Similarly, being visible during UA requires user knowledge of the data that are being revealed and collected. Profile Extractor (PE) is an example of user profiling based on internet behaviors. Here information learned from users is collected and analyzed to attempt the construction of accurate and comprehensive profiles and usage patterns. Such profiles can be leveraged in the interest of the user to capture user preferences but may also be exploited to expose private patterns of behavior and decision making. Particularly for UA, the use of profiles in E-commerce may include individuals whose executive functioning is impaired, which may involve suboptimal decision making and lacking control of impulsive behaviors. Such profile data can be used to safeguard individuals, e.g., protect against out of control shopping sprees or irresponsible transactions in general. Likewise, the same information may also facilitate target identification for phishing, cyber stalking or other forms of exploitation.

In summary, UA with home networking creates another layer of complexity to the challenge of safeguarding confidentiality, integrity and reliability. Not all aspects of

home networking that are critical to UA were covered here. For instance, network speed and bandwidth raise concerns for UA that will be addressed in future work.

5 Conclusion

As the UA field continues to grow, solutions are more likely to transfer from the laboratories to the commercial markets. In these every day, non-laboratory environments, it is plausible that increasing amount sensitive personal information are generated and possibly exposed. Preventing misuse is imperative to an overall system security strategy. Intentionally or not, end-users may execute or disclose information that is damaging to the network, system or, more importantly, to themselves. Attacks can involve social components and create even greater weaknesses in any system and hence potentially exploiting vulnerabilities of users. In the absence of UA systems that are capable of truly ensuring confidentially, integrity, and availability, the protection and security against "universally accessing" the user cannot be guaranteed.

The purpose of this paper is the exploration and identification of privacy and security concerns that are likely to influence the success of transitioning UA research to real world users living with real world networks. We did not focus on the security adage that *users must be instructed in proper protocols for remaining secure*. One reason is that although user education is important, it is unlikely the optimal and only strategy: It requires development, knowledge of the trainees' cognitive and motor abilities, unimpaired user agency for decision making and last but not least, that trainees have access to training. Our main reason for this paper topic is that UA scientists and security experts have not yet developed a rich dialogue or interdisciplinary projects. As a result, the awareness, identification, elimination and management of cyber risks to privacy and security have not been addressed for UA. It appears that interdisciplinary collaboration between the security and the UA expert communities is the necessary next step to controlling cyber risks, thereby enabling the successful, safe and secure transitioning of UA technology to the end-users.

References

1. Universal access: theoretical perspectives, practice, and experience. In: Carbonell, N., Stephanidis, C. (eds.) 7th ERCIM International Workshop on User Interfaces for All. Springer, Berlin (2003)
2. User-centered interaction paradigms for universal access in the information society. In: Stary, C., Stephanidis, C. (eds.) 8th ERCIM Workshop on User Interfaces for All. Springer, Berlin (2004)
3. Stephanidis, C. (ed.): Universal access in HCI: Towards an information society for all, vol. 3. Lawrence Erlbaum Associates, Mahwah (2001)
4. Stephanidis, C. (ed.): User interfaces for all: concepts, methods, and tools. Lawrence Erlbaum Associates, Mahwah (2001)
5. Maybury, M.T.: Security and Privacy for Universal Access. In: Stephanidis, C. (ed.) The Universal Access Handbook, pp. 1–11. CRC Press, Boca Raton (2009)
6. Please Rob Me: Raising Awareness about Over-sharing, `http://pleaserobme.com/` (retrieved January 7, 2011)

7. U.S. Department of Health & Human Services. Breaches Affecting 500 or More Individuals, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html (retrieved February 6, 2011)
8. Frontline by PBS, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/ (retrieved February 13, 2011)
9. Chas, R.: The Ungooglable Man. Reprinted with permission from The Cartoon Bank/Conde Nast, The New Yorker (March 22, 2010)
10. Falliere, N., Murchu, L.O., Chien, E.: W32.Stuxnet Dossier. Symantec Security Response, 1–69 (2011)
11. Pfleeger, C.P., Pfleeger, S.L.: Security in computing, 4th edn. Prentice Hall, Upper Saddle River (2006)
12. Mayron, L.M., Bahr, G.S., Balaban, C., Bell, M., Ford, R., Fox, K.L., Henning, R.R., Smith, W.B.: A hybrid cognitive-neurophysiological approach to resilient cyber security. In: The 2010 Military Communications Conference – Unclassified Program – Cyber Security and Network Management (MILCOM 2010-CSNM), San Jose, California (October 2010)
13. Cheswick, W., Bellovin, S., Rubin, A.: Firewalls and internet security: Repelling the wily hacker, 2nd edn. Addison-Wesley Longman Publishing Co., Inc., Boston (2003)
14. Mayron, L.M.: Secure Multimedia Communications. IEEE Security & Privacy 8(6), 76–79 (2010)
15. Bank of America, https://www.bankofamerica.com/ (retrieved January 7, 2011)
16. Schach, S.: Object-Oriented and Classical Software Engineering. McGraw-Hill, New York (2010)
17. Amoroso, E.: The Effects of Cyber Attacks. In: AT&T, Cyber Security, ch. 3. Silicon Press, Summit (2007)
18. Greene, S.S.: Security Policies and Procedures: Principles and Practices. Prentice Hall, Englewood Cliffs (2006)
19. Adams, R., Bahr, G.S., Moreno, B.: Brain Computer Interfaces: Psychology and Pragmatic Perspectives for the Future. In: Proceedings of the Artificial Intelligence and Simulation of Behaviour (AISB) 2008 Symposium on Brain Computer Interfaces and Human Computer Interaction: A Convergence of Ideas, vol. 5(1-6). The Society for the Study of Artificial Intelligence and Simulation of Behaviour, Aberdeen (2008)
20. U.S. Department of Health & Human Services. What does the HIPPA Privacy Rule do?, http://www.hhs.gov/ocr/privacy/hipaa/faq/privacy_rule_general_topics/187.html (retrieved February 6, 2011)
21. Asokan, N., Niemi, V., Nyberg, K.: Man-in-the-middle in tunnelled authentication protocols. In: Christianson, B., Crispo, B., Malcolm, J.A., Roe, M. (eds.) Security Protocols 2003. LNCS, vol. 3364, pp. 28–41. Springer, Heidelberg (2005)
22. Thulasidas, M., Guan, C., Wu, J.: Neural Signal Process. Lab., & Inst. For Infocomm Res., Singapore. IEEE Transactions on Neural Systems and Rehabilitation Engineering on Robust classification for EEG signal for brain-computer interface 14(1), 24–29 (2006)
23. Augmented Cognition International Society, http://www.augmentedcognition.org/ (retrieved February 12, 2011)
24. Baillie, L., Pucher, M., Képesi, M.: A supportive multimodal mobile robot for the home. In: Stary, C., Stephanidis, C. (eds.) User-Centered Interaction Paradigms for Universal Access in the Information Society: 8th ERCIM Workshop on User Interfaces for All, pp. 375–383. Springer, Berlin (2004)

25. Becker, S.A., Webbe, F.M.: Designing for Older Adult Users of Handheld Technology. In: Proceedings of the 28th IEEE Engineering in Medicine and Biology Society Annual International Conference, pp. 3297–3300 (2006)
26. Cook, D., Das, S.: Smart Environments: Technology, Protocols and Applications in the Wiley Series on Parallel and Distributed Computing. Wiley-Interscience, Hoboken (2005)
27. Hacker spannt junge Mädchen per Webcam, http://www.stern.de/digital/online/150-faelle-hacker-spannt-junge-maedchen-per-webcam-1584091.html (retrieved January 6, 2011)
28. YouTube, http://www.youtube.com/ (retrieved January 6, 2011)