Report on DIMACS* Workshop and Working Group on Usable Privacy and Security Software

Date of Workshop: July 7-8, 2004
Date of Working Group: July 9, 2004

Workshop Organizers

Lorrie Cranor, Carnegie Mellon University
Mark Ackerman, University of Michigan
Fabian Monrose, Johns Hopkins University
Andrew Patrick, NRC Canada
Norman Sadeh, Carnegie Mellon University

Report Authors:

Serge Egelman
School of Computer Science
Carnegie Mellon University
egelman@cs.cmu.edu

Ponnurangam Kumaraguru
School of Computer Science
Carnegie Mellon University
ponguru@cs.cmu.edu

Date of Report: January 11, 2005

*DIMACS was founded as a National Science Foundation Science and Technology Center. It is a joint project of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs, NEC Laboratories America, and Telcordia Technologies, with affiliated partners Avaya Labs, IBM Research, Microsoft Research, and HP Labs.

1 Introduction

Privacy and security have become increasingly popular issues. End-users are becoming more alert to various concerns, and the industry is responding by developing tools to allow individuals to better safeguard their privacy and security. However, these tools often go unused, and when they are used, they are frequently used incorrectly. This phenomenon was documented in Alma Whitten's "Why Johnny Can't Encrypt," in 1999. Since then, efforts have been made to make privacy and security software more usable. The key lies in creating a dialogue between usability professionals, and privacy and security professionals. For instance, at the 2002 Computer-Human Interaction Conferences, a small workshop was organized to discuss security and privacy issues. At the 2003 USENIX Security Conference, an informal birds of a feather session was held to discuss usability issues. But not until now has there been a conference held to explicitly discuss these issues.

The Workshop on Usable Privacy and Security Software (WUPSS) was held at DIMACS on July 7, 2004. The workshop brought together researchers in the fields of privacy, security, and human-computer interaction. The first two days consisted of invited talks, while the last day consisted of "break-out sessions" –individuals meeting in small groups to discuss various research problems. Around 85 people attended the conference, a diverse population coming from academia, government, and industry. The workshop talks were arranged into six sessions, which are discussed in the sections that follow: "Challenges, Approaches, and Mental Models," "Keynotes," "Authentication," "Privacy, Anonymity, and Encryption Tools," "Ubiquitous Computing (Ubicomp)," and "Administration and Access Control." The slides from most of these talks are available online at http://dimacs.rutgers.edu/Workshops/Tools/slides/slides.html

2 Challenges, Approaches, and Mental Models

2.1 Usable Security: Beyond the Interface

Speaker: Angela Sasse, University College London

Angela Sasse presented a talk on the various barriers to good security. The premise of the workshop was that security systems need better usability. Dr. Sasse argued that user behavior also must change. The first limitation is human memory. Passwords are hard to remember, so users often resort to either making very simple passwords that are easy to guess, or writing passwords down in an insecure manner (such as a Post-It note on a monitor).

The proliferation of password based systems forces users to either memorize dozens of passwords (and risk forgetting them) or use one password for everything (which is insecure).

Some solutions to these problems include setting up password reset mechanisms and mechanisms to "help" users remember their passwords. Password reminders make the system less secure by changing it from having to know the exact password to guessing based on clues. Rather than using reminders, some systems allow users to securely reset their password if they forget it. Often times help desks are used exclusively for solving authentication problems. These come at a very high cost.

The biggest problem though, is also a human one: users often try to undermine these systems because they see them as a nuisance. One example is sharing passwords; users will all use the same password so that they can use each others' accounts. Of course the solution would make it so that users wouldn't need to resort to reminding themselves or sharing passwords. Ideally, the systems would be more forgiving; giving the user feedback, providing hints, and forcing them to memorize fewer passwords across all the systems they use. The main research challenge is doing this while keeping the system secure. Biometric systems were created in part to solve this problem, but they create usability problems of their own.

Dr. Sasse suggests that it is the mental model of security that needs to change. People need to have a better perception of what security is, and how it applies to them. One common misconception is that security is only for those who are paranoid. This manifests itself with users choosing not to lock their computers at work becuse they are worried that their coworkers will think that they do not trust them. New metaphors need to be created so that people can relate to security terms and then integrate security into their daily lives. This must start by getting users interested and motivated. This can be accomplished by making security appealing and by changing its image— making it "fun."

2.2 Human-Computer Interaction Issues in Privacy

Speaker: Mark Ackerman, University of Michigan

Mark Ackerman spoke about some fundamentals of privacy: what privacy is, what the problems are, and why it is difficult. The first definition he cited is "the regulation of social interaction," or wanting to be alone. Next there is "unwanted personal disclosure," "freedom from surveillance," and "control over release and dissemination of personal data." He discussed a broad definition which seems to cover them all, "control over one's persona."

Users are becoming more and more concerned about privacy. In a 2000 Harris Poll, 41% of sampled US consumers said they were *very* concerned about their privacy, 57% wanted better legal protections, and 92% did not trust companies to keep personal data private. The main problem is that there is not just one problem with privacy. Current privacy concerns include unauthorized people accessing information, companies reusing personal data for unrelated purposes, sharing personal data with third parties, and creating profiles to track individuals.

There also is not just one type of person concerned with privacy, but instead people can be put into three different groups: marginally concerned (27%), fundamentalists (17%), and pragmatists (56%). Grouping people based on preference is often difficult as stated privacy preferences usually differ from practice. Privacy preferences are also highly nuanced; users will give out information based on the context of the interaction. At the same time, users also pay attention to different details. This makes for a critical but incredibly difficult problem for Human-Computer Interaction (HCI): analysis is difficult, solutions are not clear.

2.3 Security as Experience and Practice: Supporting Everyday Security

Speaker: Paul Dourish, University of California, Irvine

Paul Dourish spoke about the differences between privacy and security. The two are different issues with a bit of overlap, though privacy problems are solved almost exclusively with solutions designed for security problems. Instead, we should try using privacy solutions to solve security problems.

Privacy is difficult because of many factors. There are no rules about how privacy should be handled in every conceivable situation; privacy requirements change based on the context. Posting personal information on a web page will prevent individuals from intruding because they do not need to ask questions via email– the information is already in the open. By maintaining one form of privacy, another is destroyed (in this example, minimizing intrusions come at the cost of disclosing information). Because it is hard to distinguish which privacy requirements fit into which specific situation, new systems need to be designed that make better decisions. Where possible, privacy decision making should be integrated with actions.

2.4 Best Practices for Usable Security In Desktop Software

Speaker: Simson Garfinkel, Massachusetts Institute of Technology

Simson Garfinkel spoke about the problems with usability in most software. It is widely known that programming errors lead to software security vulnerabilities, but Garfinkel postulates that poor user interface design also leads to security vulnerabilities. He uses a task as simple as deleting a file as an example. When a file is deleted, the two most common desktop operating systems use the "trash can" metaphor. But the user often does not realize that placing the file in the trash can is the same as deleting it. Furthermore, if the trash can is actually emptied, it is not clear whether the file can be recovered; there are many undelete programs available just for this reason. There is a huge difference between deleting the link to the file and overwriting the actual contents of the file, and most users do not realize this. What needs to be done is make the difference between "throwing away" and "shredding" clear to the user. But adding a new mechanism is not enough. Apple has added a "Secure Empty Trash" feature to OS X, just for this reason. However, it has failed in that it is not clear to the user what the difference is between it and the regular "Empty Trash" command. Additionally, its placement is not consistent throughout the operating system; it is obvious that this security feature was added as an afterthought, rather than from the ground up.

A similar situation can be seen when trying to delete the history, cache, and cookies from a web browser. The problem with many browsers is that a user has to specifically know ahead of time how to accomplish these tasks, as this functionality is not apparent from menus. Additionally, deleting some items (e.g. cookies) may cause the user to incorrectly think that others (e.g. history) have also been deleted. This creates a false sense of security.

Along these lines, the question was asked, what if software intentionally tries to obscure its activities? The example given was the GATOR eWallet program; in addition to the main stated use of the program, the fine print says that it "also occasionally displays pop up ads on your computer screen based on your online behavior." Of course, this is stated in the 6,645 word license agreement. Most users do not read legal documents such as license agreements, they simply click through them.

This is not a new problem. The 1906 Pure Food and Drug Act mandated that food product labels must be standardized and disclose the contents. In addition to nutrition facts and ingredients being in a standard format, certain icons have been adopted (e.g. to denote kosher products). Such symbols can be used for software. Symbols can be legally mandated to denote whether software monitors user actions, contacts other machines automatically, or even displays pop up ads. This allows the user to not have to rely on reading a legal document to find such disclosures. Of course this

can only be made possible through legislation, as most companies would not make disclosures voluntarily. And so Garfinkel proposes the Pure Software Act of 2006.

2.5 A Flock of Birds, Safely Staged

Speaker: Scott Flinn, National Research Council of Canada

Scott Flinn discussed "safe staging" and how desktop security may be increased by better announcing the potential risks. Users are falling prey to malicious email attachments, and various social engineering scams. Attempts are made to educate users to be more cautious, but to no avail. Many of the suggested solutions have been to strip emails of attachments and only read messages from known senders. Flinn argues that these solutions restrict the flow of information. Instead risks need to be better addressed.

Mostly users simply do not understand the problems that they are facing. If users were able to clearly see which actions were risky, what the risks are, and how to remedy the situation, Flinn believes users would be able to make better decisions. Privacy Bird attempts to solve this problem, but only for privacy issues; the user is alerted when a desired web page has privacy policies that are not in line with their preferences. A similar tool is needed for more general security issues.

3 Keynotes

3.1 Privacy and Security: Putting People First

Speaker: Elizabeth Mynatt, Georgia Institute of Technology

Elizabeth Mynatt discussed various difficulties involved in understanding the computation involved in everyday activities. Mynatt provided an overview of the "Aware Home" at Georgia Tech where they are performing various experiments involved in everyday computing. Many of the various actions performed by individuals relate to privacy.

Privacy involves social communication, social networks, and frameworks. Acumen, a system that works similarly to ConsumerReports.org was mentioned. It provides information regarding privacy and security for various websites that have been rated by both regular users and experts. One of the interesting research questions is: Will average users prefer to listen to a large group of other users rather than a small group of experts?

The boundaries within which the community is working on privacy issues are constantly changing, which makes the problem of solving privacy and

security even more difficult. Social networks provide information regarding an individual in a particular group with certain characteristics. Using this we can form clusters, boundaries, and connections.

"Privacy mirrors" can help facilitate information sharing and keep users informed about privacy decisions. Individuals would see "reflections" of information about themselves and others, and therefore know the status of their private information. Similar to Paul Dourish's talk, privacy is a paradox; allowing more personal information to be publically available could reduce the number of privacy invasions.

3.2 Human-Scale Security

Speaker: Matt Blaze, University of Pennsylvania

Matt Blaze discussed various "human scale" security protocols and problems. These are security issues that arise in every day activities that do not directly involve computation, yet provide computer security researchers with good working models. The main issues discussed were security issues with physical locks and burglar alarms, and privacy issues with restaurant etiquette.

Blaze noted the similarities between denial of service attacks in the physical world and in computer security, to illustrate he used burglar alarms. There are two ways of circumventing a burglar alarm: cutting the wires thereby disabling the alarm, and overwhelming the system so that the authorities will think it is defective and thus ignore it. Attacks on the Internet were originally mostly the former; cutting off access to systems by virtually cutting wires. But now attacks have changed to overwhelming the systems to the point that they are useless.

Locks can be used to draw similar comparisons. A lock with a single key can be fairly difficult to circumvent; the best way is to try every possible combination with a lock pick. This can be accomplished in exponential time. But a lock with a master key (and thus two keys can open it), takes far less time as each bit has two possible positions. This is similar to authentication systems that use computers. When more than one "key" can access the system, it becomes that much easier to crack.

Restaurant etiquette is also a good comparison for a few privacy and security problems in the online world. When ordering wine with guests, the person paying for the wine must communicate the desired price range to the sommelier without divulging it to the rest of the dinner party. Similar protocols have been developed over the past few hundred years to deal with other security problems in the physical world. Computer security researchers are

quick to understand these systems and use them to model online protocols, yet the converse is usually not true.

4 Authentication

4.1 Some Practical Guidance for Improved Password Usability

Speaker: Mike Just, Treasury Board of Canada

Mike Just described various aspects of password management for single and multiple accounts. Users have various accounts for different purposes and are not in a position to handle a large number of passwords, so they usually have three or four passwords which they continue using for all accounts. Several conditions lead to an unusable or intolerable environment for the user. Each authentication system will often have its own rules for length, variety of characters, dictionary words, etc. Just discussed the various online and offline attacks to which these systems are subjected. Additionally, he went over solutions for safely organizing passwords, and compounding passwords with other authentication mechanisms.

4.2 Fingerprint Authentication: The User Experience

Speaker: Lynne Coventry, NCR Corporation

Lynne Coventry discussed usability issues with finger print scanners. Currently many different methods exist for fooling existing ATM systems. In this study, fingerprint recognition software was installed on ATM machines. Many usability issues were discovered during the study. The study showed that users need an explanation of the finger print "core" and what they are trying to achieve and why, rather than just how to do it. The study found significant problems enrolling elderly users. The findings suggest that supporting the user by positioning their finger print core centrally on the reader rather than using any acceptable image decreases the chances of the system falsely rejecting them. While biometric authentication holds promise for decreasing ATM fraud, many usability issues still stand in the way before widespread adoption can occur.

4.3 Authentication for Humans

Speaker: Rachna Dhamija, University of California, Berkeley

Rachna Dhamija presented her study on visual authentication systems. She studied a system where the user picks multiple images from a set of randomly generated artwork to use as their "password." Upon authentication, the user is presented with many such images and must choose their password out of the set. The correct pictures may or may not need to be presented in a fixed order. A similar commercially available system uses faces rather than random artwork. While humans are very good at remembering faces, it is easier to be confused with similar looking faces. The correct faces can also be more predicatable based on the demographics of the user. Future work involves a long term study about the usage of the random pictures, faces and various other pictures. It also involves creation of multiple portfolios for the same user as whether users can remember multiple sets of pictures across different systems is still an open question.

4.4 On User Choice in Graphical Password Schemes

Speaker: Fabian Monrose, Johns Hopkins University

Fabian Monrose presented a talk on the various security flaws in graphical password schemes due to the user choosing their own passwords. The study involved students making use of graphical schemes for accessing course materials, assignments, grades, etc. Permitting user selection of passwords in graphical password schemes can yield passwords with entropy far below the theoretical optimum. In some cases password choices can be highly correlated with the race or gender of the user. In addition to predictability, it was observed that memorability decreases as a function of the number of pictures used. This might imply that having to memorize many pictures for use across multiple systems might not be feasible. Longitudinal studies and more collaboration between security and usability researchers are needed for better uderstanding of the data collected.

4.5 Secure Web Authentication with Mobile Phones

Speaker: Rob Miller, Massachusetts Institute of Technology

Rob Miller explained a new method for using mobile phones to authenticate over untrusted networks. In addition to concerns over sending data insecurely over untrusted networks, there are more and more reports of key loggers being installed on public Internet kiosks. People are increasingly relying on computers to do business over the Internet. Therefore transmiting authentication information under such circumstances should be avoided, as many cases of fraud have resulted.

In this approach, to prevent the password from being captured by the public Internet kiosk, the password is not sent at all through the client machine. Instead, a trusted security proxy is set up. The proxy mediates all aspects of the user's communication with the remote service, by storing the user's authentication information.

The proxy also stores the user's mobile phone number. The user uses her registered mobile phone to authenticate her web connection from the kiosk. Once authenticated, the proxy then operates like a traditional web proxy, with the exception that it maintains the user's web cookies in a secure "cookie jar" to prevent authentication information contained in the cookies from touching the kiosk. The proxy randomly chooses a word from a dictionary and displays it as a session name on the kiosk's browser. At the same time, the session name is sent to the user's mobile phone in a short message. This message is approved by the user by responding to the message. Once the proxy receives the approval, it logs in to the remote service as the user.

A controlled user study was performed using this system. Different kinds of attacks were also simulated in an attempt to trick the users. By asking the user to choose and approve a correct session name from her mobile phone, they provided a mobile phone authentication solution that is both secure and easy to use. This proxy is a flexible solution to web authentication. It can be deployed by an individual user, a third party, or a web service provider. Furthermore, when a user forgets her password, she can still log in using her mobile phone instead.

4.6 Toward Usable Security

Speaker: Dirk Balfanz, Palo Alto Research Center

Dirk Balfanz discussed setting up secure wireless LANs. It is widely known that wireless ethernet is notoriously insecure, however it remains as such because of the effort that is needed to enable encryption. Balfanz gave a firsthand account of setting up a wireless access point using the new 802.1x standard for key distribution, which aims to automate the task of enabling encryption on the client's end.

The new protocol works by first creating a trusted channel for facilitating a key exchange. Once certificates have been exchanged and access has been granted, the client will be able to freely access the wireless interface on the access point without having to worry about having to manually update their computer every time a new key is used. The trusted channels that were experimented with in this case were infrared, ethernet (wired), and USB.

Upon performing a usability test, it was shown that this system is far easier to set up as compared to traditional methods. Enabling the Wired Equivalent Privacy (WEP) protocol on a traditional client and base station took an average of over two hours, and many users could not complete the task. At the same time, using the new system took under two minutes. It can clearly be seen that providing a more automated system for enabling encryption on a wireless network will result in more users engaging in safer practices.

5 Privacy, Anonymity, and Encryption Tools

5.1 Anonymity Loves Company: Usability as a Security Parameter

Speaker: Roger Dingledine, Free Haven Project

Roger Dingledine spoke about tools for anonymity. The most pertinent question was, who needs anonymity? Individuals use anonymity for various advocacy campaigns, reporting, and even whistle-blowing. Businesses use anonymity for keeping track of employees, tracking customers, and hiding trade secrets. Governments use anonymity for law enforcement, reporting tips, and even conducting research.

But for anonymity tools to be successful, many people must also use them. Mixnets were created to obfuscate traffic. They rely on volumes of traffic to guarantee maximum anonymity. This creates a distributed trust system, users must carry other users' traffic in order to achieve maximum anonymity for themselves. At the same time, users cannot trust any one entity with their traffic, and so they must share traffic as much as possible.

The next issue is that the quality of the anonymity is directly proportional to the computation time, storage size, and available bandwidth. This allows for more computation using more cover traffic. However, users do not like waiting and do not like sacrificing their resources. And so there exists a paradox: anonymity takes time and requires many users, but users would prefer something that takes less time.

5.2 Cryptography and Information Sharing in Civil Society

Speaker: Marc Levine, Benetech

Marc Levine spoke about his company's product, Martus, a "human rights bulletin system." The goal of Martus is to allow individuals to report human rights violations in hostile territories. Martus aims to guarantee the

anonymity of the whistle-blower, maintain the integrity of the message, and make the information accessible. The software is similar to email from the client's perspective, however the interface is far simpler, and the underlying technology is far more complex. When a message is sent, it is automatically encrypted, delivered to the recipient, and archived on backup servers around the world. This allows for anonymity, confidentiality, and redundancy.

5.3 Giving Johnny the Keys

Speaker: Alma Whitten, Google

Alma Whitten gave a presentation that outlined the next steps after her usability study of PGP 5.0, "Why Johnny Can't Encrypt." The goal of secure email software is to allow the user to retrieve public keys, encrypt with the correct public keys, sign messages, and verify keys. One of the problems with understanding cryptography is understanding all of the terminology; the metaphors "public" and "private" keys can be very confusing to the unfamiliar. Whitten created new metaphors for a sample email encryption program: the public and private keys are color coded black and white, and fit together to form a yin-yang (indicating that the two pieces fit together). Messages that are encrypted are shown with a colored lock on them (black means that the private key is needed to decrypt, and white means that the public key is needed to verify a signature).

Additionally, users are greeted with a tutorial that aims to educate them on the basics of cryptography. This is all part of safe staging: as they become more familiar with the software, more advanced features become available to them. At each stage, users are made aware of which actions are available to them and what the risks of those actions are. The example program has three such stages, starting with no email security and ending with key signing. Finally, the software underwent a usability test and was shown to be far easier to use than PGP.

5.4 Techniques for Visual Feedback of Security State

Speaker: Tara Whalen, Dalhousie University

Tara Whalen presented a talk on visualizing security information. In order to better give users feedback about the security of a system, visual information may make action and assessment more accurate and timely. Whalen discussed creating a "security lens" that will allow the user to see security information from various perspectives: their own, an affiliated party, or the rest of the world. One suggested application for this technique would

be integrating a widget into a secure messaging application. The user can type up an encrypted message, and then use the lens to view how the message would look to the outside world (a bunch of random characters) or the intended recipient (the text as the sender typed it).

5.5 Privacy Analysis for the Casual User Through Bugnosis

Speaker: David Martin, University of Massachusetts, Lowell

David Martin presented a talk on Bugnosis, a tool that highlights "web bugs" inside a web browser. The problem is that most users do not know what to expect in regard to online privacy, and there are two ways of solving this: improve online privacy or make privacy invasions more visible. A common online privacy threat is the web bug, which is often a third party image or cookie used to track referrer information. Bugnosis aims to make the user more aware by warning when the web browser encounters a page with such content. The software was designed with journalists in mind, so that more attention might be drawn to this problem if they could see firsthand evidence. The software itself was basically a proof-of-concept to show the general public concrete evidence of privacy invasive web sites. Out of a sample of 84 popular sites, 58% contained web bugs, while 29% did not disclose them in their privacy policies. Martin is interested in the idea of integrating Bugnosis with a P3P user agent, as well as an email client.

5.6 Protecting Privacy in Software Agents: Lessons from the PISA Project

Speaker: Andrew Patrick, National Research Council of Canada

Andrew Patrick reported on aspects of the Privacy Incorporated Software Agents (PISA) project. This project studies trust factors and the adoption of various software agents. Trust is built based on many perceived factors; interface layout, ease of navigation, and even color choice all contribute to the user's trust bias. The user's sense of risk is also based on perception; the autonomy of the system and the amount of information collected from the user may increase or decrease the perceived risk.

An agent for contacting potential employers was created to test these theories. The goals were to keep the design as simple as possible, yet completely functional, in order to gain the user's trust. To accomplish this, various help dialogs were included. These helped to guide the user through the process, and provided warnings as soon as users needed to enter potentially sensitive information. A group of 50 users participated in a usability

test. Over 90% of them understood how to use the major functions of the system, and 86% of them found the help dialogs useful (80% thought that this contributed to understanding the privacy terminology). At the same time, many users did not like the pop up dialogs warning them about sensitive information. Some thought that the dialogs were simply annoying, while others associated them with advertisements.

5.7 Architectural Issues in Distributed, Privacy-Protecting Social Networking

Speaker: Lenny Foner, Massachusetts Institute of Technology

Lenny Foner is the designer of Yenta, which is a distributed network that protects privacy. This enables users to share information and collaborate without having to explicitly trust anyone. Creating a decentralized system has many advantages over systems that require a central server. While they are harder to implement, they allow greater reliability and greater usage. Having a central server also opens the system up to targeted attacks, insider attacks, equipment failure, and even legal threats. This can be seen with file sharing systems.

Yenta takes this decentralized approach and creates a system for finding people with similar interests. The system works by automatically organizing users in clusters. Each agent can send broadcast messages to anyone in the cluster to advertise their interests, or respond to someone else's broadcast. This guarantees some amount of anonymity as it is difficult to pinpoint the source of a message.

Recently we've seen an increase in social networking on the Internet; LiveJournal and Friendster are just a few such sites. But because they are maintained centrally by a corporation, they are created for profit and often have unfriendly clauses in their terms of service. Peer-to-peer systems are currently only used for file sharing, and not social interaction. Yenta, which predates most of these systems, offers the potential to provide the best of both worlds— a privacy-friendly social networking system.

5.8 Privacy in Instant Messaging

Speaker: Sameer Patil, University of California, Irvine

Sameer Patil spoke about privacy issues with instant messaging. Instant messaging programs are currently in widespread usage, both at home for personal use, and at work for collaboration. For work related use, users need to be highly available in order for all parties to communicate efficiently and

effectively. At the same time, individuals have a sense of privacy which might conflict with this. Patil questions what the balance is between awareness and privacy.

Many different messaging programs have different mechanisms to protect the user's privacy: AOL allows senders to be "warned," and ICQ requires approval before adding an individual to your buddy list. A study was conducted using seven subjects of varying backgrounds who were interviewed about their instant messaging habits. All of them stated that they were concerned about people messaging them who are not on their contact lists, being distracted from their current task, and keeping conversations private. Overall, users only added contacts who were trusted, and didn't maintain a public profile. Regarding being interrupted, users had different behaviors when they were engaged in a task as opposed to relaxing. Additionally, recreational conversations often occurred during work hours, but work related conversations rarely occurred while not at work. While behaviors were influenced by the client's default settings, the user's self-impression structured the balance between privacy and awareness. Finally, it was determined that providing better suited default settings, and a way for the user to switch between profiles would better address the privacy concerns of most instant messenger programs.

6 Ubiquitous Computing (Ubicomp)

6.1 Knowing What You're Doing: A Design Goal for Usable Ubicomp Privacy

Speaker: Scott Lederer, University of California, Berkeley

Scott Lederer spoke about how ubiquitous computing is infusing new interactive technologies into everyday life. The main focus was the design goals for privacy mechanisms in ubiquitous computing systems. It has become very difficult to design and implement policies and mechanisms provided in privacy statements. Correctly doing this requires recognizing that end-users know more about their own privacy management practices than designers can know, even as that knowledge remains implicit in the practices themselves.

Separating policy from mechanism conflates policy with practice; it is always better to have the data and the control over the data to go together, as it becomes very difficult to have the control over the data if they are separated. He pointed out that people are aware of steps and consequences during usage of credit cards with respect to privacy. Using credit cards in

a way provides a tacit disclosure of some information to others. But we are not sure whether they are aware of the secondary uses of the data like banks misusing your personal information for other analysis or providing this information to other organizations for usage.

6.2 Privacy Challenges in Ubiquitous Computing

Speaker: Marc Langheinrich, ETH Zurich

Marc Langheinrich discussed privacy challenges related to Radio Frequency Identification (RFID) systems. RFID systems are used to capture information regarding the status of products and where they are located. Since it's fairly unlikely that this technology would be used for surveillance or by criminals, the main threat model in RFID systems is staying in control of personal data. This technology could allow corporations to seamlessly track individuals without their knowledge for the purpose of building profiles.

Langheinrich proposed a transparent protocol that could read only targeted RFID commands when and if initiated. The system would be able to understand RFID privacy policies encoded with P3P and would be able to make decisions accordingly. Watchdog tags are necessary for reading the policies and interpreting them so that the system can provide correct implementations. The system works by extending the RFID format so that each tag's ID number fits into a hierarchy. This way the reader can only scan for tags fitting a certain mask, thus preventing arbitrary tags from showing up. Additionally, fields will be added for specifying the purpose and collection intent for the particular tag. The goal is to allow each tag to be able to function like a P3P policy. Since the hardware can already support these features, it is simply a matter of updating the software on the readers.

6.3 Semantic Web Technologies to Reconcile Privacy and Context Awareness

Speaker: Norman Sadeh, Carnegie Mellon University

Norman Sadeh discussed various semantic web technologies to reconcile privacy and context awareness. There are many mobility challenges in designing a system, for instance: users have various distractions in performing an activity, tasks need to be completed in a short period of time, and there is limited input/output functionality.

The MyCampus project is designed to enhance campus life through context-aware services accessible over the WLAN using HTTP. The e-Wallet

program is a three layer architecture having core knowledge, a service layer, and a privacy layer. The system allows visualizing, editing preferences and also editing based on existing ontologies. The initial prototype was implemented at Carnegie Mellon University. The evaluation provides context awareness which requires access to a broad range of resources/attributes.

Contextual information can be obtained through a calendar, location tracking, an address book, a buddy list and weather information. Available resources vary from one user to another over time. Ontologies could be used to represent personal and contextual resources, contextual attributes, and personal and privacy preferences.

Context awareness helps overcome the limitations of mobile devices and the time criticality of mobile scenarios. Context awareness makes privacy even more critical. The experiments indicate that user preferences are often complex. The semantic web approach allows for policies that refer to concepts introduced in any number of domain-specific ontologies.

7 Administration and Access Control

7.1 Better Tools for Security Administration: Enhancing the Human-Computer Interface with Visualization

Speaker: Bill Yurcik, National Center for Supercomputing Applications

Bill Yurcik discussed the importance of keeping in mind system administrators when designing security and privacy tools. A recent survey of three Internet sites showed that 51% of all failures are caused by operator errors. Delay in the human-computer interface can adversely affect system security so an important goal is to enhance this interface to reduce the delay. Methods are needed to help security operators more quickly extract vital information from large amounts of data and translate this information into effective control actions. Visualization tools can aid in analyzing large data sets by identifying areas that need further scrutiny and enabling sophisticated decisions. Users should be provided with features for overviews, summaries, zoom-in and zoom-out, and filters to provide details of any particular section on demand. Research on cluster security is very sparse but this is a key area for aiding system administrators in improving overall security.

7.2 Approaches for Designing Flexible Mandatory System Security Policies

Speaker: Trent Jaeger, IBM

Trent Jaeger discussed his work on Linux 2.6 using the Security Module Framework and SELinux. He described the approach for designing SELinux security policies to meet high-level security goals and a policy analysis tool called Gokyo that implements the approach. The system was designed with the following in mind: using flexible policy expressions, finding problems that might compromise integrity, and assisting in problem resolution.

Gokyo is a policy analysis tool that enables SELinux polices to be compared to high-level security goals. It supports the resolution of differences between the SELinux example policy and those goals. Gokyo takes the input as the entire SELinux example policy and finds Biba conflicts in that policy. It also displays the conflicts in terms of a minimal cover set. Gokyo will then compute the basic impacts for nodes and assigns them expressions for resolution and re-evaluation. The resulting policies provide Clark-Wilson integrity.

7.3 Useless Metaphors: Why Specifying Policy Is So Hard?

Speaker: Patrick McDaniel, AT&T Labs-Research

Patrick McDaniel presented his research on why representing security policies is difficult and a specific way by which we could improve the situation. Security policy is defined as statements of expected or desirable behavior within some defined scope. A policy system is a collection of abstractions, representations, interfaces and implementations used to specify and enforce the policy.

A policy system is effective if it has the following:

1. Interface – Allows users to state the policy.
2. Intent – What the user wants to do.
3. Vocabulary – Terms which are used in understanding the information.

Security policy systems largely fail because designers fail to present a clear narration to the user. The problem could be solved by having the following axioms as guidelines:

1. Audience Knowledge – Policy must be defined in the users language and also the complete scope of the information for making the decision should be made available in the policy.
2. Focus – Policy should focus on the users interest.

3. Simplicity – Representation should be simple but not so simple that it looses information.

4. Structure and Tone – The interface for the user is the key for success, it should be made as simple and narrative as possible.

Using the above axioms we could have a policy design system which could be narrative and descriptive for the users, thus improving usability.

7.4 Chameleon: Towards Usable Role-Based Access Control (RBAC)

Speaker: Chris Long, Carnegie Mellon University

Chris Long spoke about his system for decreasing the effects of malicious software on desktop computers. In the age of email viruses and worms, the advice to users has generally been, "do not open unknown attachments and make sure that your anti-virus program is up to date." This however, does not work. Instead, Long aims to mitigate the effects of such programs through Chameleon.

The main reason why malicious programs are allowed to propagate is because once installed on a desktop computer, they essentially have permission to do anything. Chameleon changes this by creating "sandboxes" for groups of programs. The computer is partitioned into roles; currently there are roles for communication, system utilities, the Internet, storing files, and testing. Each role cannot access files in other roles or the rest of the operating system. This means that if a virus is opened in the role that the email client is using, it can only effect things in this role (e.g. it cannot delete documents stored in other roles).

A usability test was performed on the prototype for this system using six users. Five participants said they would use the system on their desktops. However, it was unclear how resistant the system was to being tricked, as most users were unaware of tricks such as camouflaging a program to make it appear as though it were running under a different role. Overall, the user feedback was very positive though. The remaining research questions are: What is the optimum number of roles to use; Should users be allowed to add and remove roles; and How do you let some programs, e.g. anti-virus software, run across multiple roles without creating a vulnerability?

8 Working Group

The following are summaries of the small group discussions.

8.1 Privacy, Ubiquitous Computing, and Encryption Tools

At the highest level, better education is the best solution for getting users to exercise better security habits. But to facilitate this, designers need to make security easier to learn. The current terminology and metaphors seem to confuse people, new metaphors need to be researched. For instance, the term "key" makes it hard for users to differentiate between private keys and public keys. A key in the physical world is almost always synonymous with a private key, and as such many users are apprehensive about which key they should share. There are some terms that still might be salvageable as they have not yet caught on with the general public. These include terms like digital signatures and access control lists.

Another problem is making users aware of security by properly integrating it into the application. Security needs to be integrated from the ground up, and not as an afterthought. It therefore needs to be taken into consideration during every stage of design. Additionally, the security mechanisms should not confuse the user by forcing them to make unnecessary decisions. Security should function with minimal user interaction, but at the same time the user must know that it is functioning correctly. The corollary is that security tools are often created without the interface in mind. HCI designers need to be a part of the process from the very start in order to guarantee both security and usability.

Regarding privacy, users need a way of indicating their own privacy preferences to the system. Policies allow the system to explain what it will do; instead the users should explain to the system what they expect the system to do. Additionally, users need assurances that their data was only used for very specific purposes. This is a very difficult task as it can be very difficult to keep track of secondary purposes. A possible solution is better training. Security and privacy can be compared to driving a car: it seems like a daunting task in the beginning, but after proper training individuals drive regularly and do not think twice about it. One solution might be to teach children about security concerns when they are first introduced to the computer and are still motivated and enthusiastic.

8.2 Privacy Preferences vs. Policy vs. Practice

Privacy policies for various online content have been in existence for a reasonable amount of time. However, many people are still confused about online privacy and concerns have increased rather than decreased. This can be attributed to the difference between what is stated in the policy, and

what is done in practice. Additionally, users have a hard time correlating their own privacy preferences with a stated policy.

Users seem to have a good idea of what their personal privacy preferences are, they just have difficulty articulating them in terms of a set of rules. Additionally, personal preferences are context sensitive, which makes it even harder to enumerate specific rules.

There are also problems with enforcement of privacy rules, from both sides. While many businesses state their privacy policies, whether they actually abide by them is a completely different story. There currently are few real consequences of failing to abide by a stated privacy policy (or even much motivation to state a privacy policy at all). Companies have few motivations to commit to good privacy policies. Legislation may be needed in this area. At the same time, individuals need motivation to develop better privacy habits. Change agents can help with the adoption of new technologies, but basic concepts still need to be understood. Positive reinforcement is needed to aid in developing better privacy habits.

8.3 User Authentication

Having multiple accounts on multiple domains is often a problem for users as this often entails having to remember multiple passwords. As such, research has begun on using graphical passwords to replace text passwords. The hope is that graphical passwords are easier to remember. However, preliminary research only shows that this is the case for a single account or a few accounts. No research has been done to find whether this holds true for many different accounts with different passwords. With the current state of graphical password technology, it could be trivial for others to predict passwords that use photographs (as opposed to abstract art).

It is not clear whether a serious problem exists using multiple passwords across multiple accounts; analysis has to be done to verify that there is in fact a problem, as many technologies currently exist to mitigate it. For instance, personal electronic devices such as palm pilots could be used to store multiple passwords securely, so that the user is not forced to memorize them. Mobile phones are being used in token based authentication so that users can respond through mobile phones by text messages in order to securely authenticate without knowing a password. Additionally, future research could be directed at creating a scheme or standard by which we could share passwords. Large numbers of discussions in this area are being conducted, yet very little research or analysis is being done. More research needs to be directed at analyzing the problem and finding solutions. Com-

mon metrics are needed for evaluating these solutions for usability, security, and social acceptance.

8.4 Evaluation for Human-Computer Interaction and Security (HCISEC)

Evaluation plays a key role in the development of new technologies. The types of evaluations include:

1. Lab
2. Real World
3. Cognitive Walkthrough
4. Heuristic
5. Low Fidelity
6. Cognitive Models
7. Hybrid Lab/Field

Each type of evaluation has its pros and cons, but they all have a few problems in common. Security is often a secondary goal for most evaluations, and therefore does not get the same consideration that many other aspects do. One direct result of this is that it is hard to set particular metrics for security aspects; if a quantitative study is conducted, what exactly is measured? Security is also separated from the rest of the system, so usability is measured with and without the security features and might not be representative of the actual use of the application.

Additionally, the need for security is often misunderstood. It is hard to tell if individual users expect the level of security that is actually needed. This plays in to evaluations as risks do not often get as much attention as they should. Creating an incomplete threat model results in an incomplete evaluation, thus lowering overall security.

8.5 Terminology

One of the major barriers to increasing usability is terminology. While part of the problem is that users are confused by terms that they do not understand, the main problem lies in using terms with multiple definitions. Policies, preferences and practices are terms that often have an aura of

ambiguity as applied to privacy research. We have attempted to define them in the following ways:

1. Policies are statements written by the organization for customers (outside), employees (inside) and lawyers for legal purposes. Policies are short notices which inform the reader regarding the usage of any information collected from the customers. They should also be machine readable as they could then be easily converted into other formats.

2. Preferences are statements made by the customers. They indicate what the customer will permit the data recipient to do with their data.

3. Practices are the actual behaviors of the customers and organizations. They represent what is actually done regarding the policies and the preferences.

Research must focus on getting the customers to do what they would like, instead of telling them what the data recipient will do. There is a huge gap between practice and solicited preferences. Risk of user profiling using the collected data could cause following problems: identity theft, nuisance, manipulation and price discrimination.

9 Conclusion

While many topics were touched on, it is clear that many future research challenges remain. Authentication schemes need to be studied so that a good median between usability and security can be reached. New tools need to be created for system administrators that increase security by allowing them to easily visualize problems. Finally, studies need to be conducted to educate users on more of the privacy and security issues. This can be accomplished by making consequences more apparent and by creating tools to aid in policy development.

The workshop concluded with a discussion on how to best organize another such conference. Most people agreed that the workshop was a success and another one should be planned for 2005. A venue with peer-reviewed publications would be preferred. In the meantime, attendees should try and organize birds of a feather and panel sessions at various other HCI and security conferences in an attempt to create more interest in the topic.

10 Acknowledgements

The authors and the DIMACS Center acknowledge the support of the National Science Foundation under grant number CCR 03-14161 to Rutgers University.