HotMobile 2006: 7th IEEE Workshop on Mobile Computing Systems and Applications

Summarized by Maria R. Ebling, Program Chair

Like the first WMCSA, the goal of this workshop was to foster interaction among practitioners of mobile computing. In keeping with this goal, we decided to return with a small, informal workshop, one with few papers but significant discussions. We accepted just nine papers, but we had two significant group discussions, two exciting panels, and an insightful keynote address. Approximately 40 people attended the two-day event on April 6–7, 2006, at the Semiahmoo Resort, Washington, USA.

To reflect these changes, during the opening remarks the organizers announced a name change for this workshop. They reported that the workshop will now be known as HotMobile 2006: The 7th IEEE Workshop on Mobile Computing Systems and Applications. USENIX is an in-cooperation sponsor of this workshop.

What follows is an overview of the workshop's proceedings summarizing the formal presentations, but omitting the discussions that followed. The vast majority of this overview focuses on the presentations that are not represented by papers. You will find that the paper summaries contained in this overview are extremely brief and are intended only to help you identify those papers you would like to read in full. Those readers interested in a longer summary should refer to the Digest of Proceedings that appears at the end of the workshop proceedings. This digest includes a summary of the discussions that followed each of the presentations.

This overview is based on the written notes taken by two student volunteers, Tapan Parikh and Alex Varshavsky. They took excellent notes, although they did not always know who was speaking and my notes were not always complete. If anything has been reported in error or omitted, the responsibility lies squarely on my shoulders and not theirs.

OPENING DISCUSSION

The workshop's initial discussion revolved around the following statement: "Resolved: The mobile phone is the only device people will carry in the future." We started by taking a quick straw poll in which only six attendees voted in favor of the resolution. After the straw poll, attendees began discussing the resolution. Each attendee had been randomly assigned to argue the Pro position or the Con position. The discussion period started with small groups of people from each position. After about 20 minutes, we then switched to having all the Pros gather their arguments and all the Cons gather their arguments. Again, after about 20 minutes, we opened the floor to debate. Each side had about 5 minutes to present its case and then open discussion ensued. It should be noted that, at times, certain members of the

groups argued in favor of the opposing side.

- *Pro Position*

  Cell phones are already ubiquitously deployed. Gartner believes that in 2005 the number of cell phones sold will have reached 780 million units and that the number will hit 2.6 billion by 2009. Also, in India and China, cell phones are believed to be the primary computing device. Given such a high penetration of mobile phones, application developers will concentrate on developing applications for the phones, especially since computing power and storage are not an issue.

- *Con Position*

  Today, people use a variety of different devices, including cell phones, watches, PDAs, MP3 players, and laptops. Combining the functionality of all these devices into a single cell phone device, resembling a Swiss army knife approach, may result in a device that may do many things, but none of them well. For example, it is unclear what a user interface of such a device would look like. Because the price of single-use devices will go down significantly, it may be more appropriate for users to carry specialized devices that have the right form factor and the right user interface for the task at hand (e.g., an iPod). Also, fashion has a say in what devices people carry with them. For instances, some people wear watches for reasons that have nothing to do with time (e.g., esthetics).

  After a lively and interactive discussion, with various attendees taking up their assigned position as well as occasionally arguing for the other side, we took another vote. This time the result included nine votes for the Pro position. Although one attendee jokingly noted that this was not a scientifically valid approach, the discussion was interesting and set the proper tone for the workshop: one of interaction and discussion.

MOBILE PHONES AS APPLIANCES

The theme of the first paper session, chaired by Gaetano Borriello, was considering mobile phones as appliances. John Barton presented the first paper, entitled "Mobile Phones Will Become the Primary Personal Computing Devices." He argued that because of increasing storage and computing power, mobile phones will eventually replace PCs. Users will utilize large displays and input devices available at public places for easier interaction with their mobile phone. After the talk, John took questions from the audience.

John Davis then presented the second talk, on "Supporting Mobile Business Workflow with Commune." The paper proposes a workflow management system for a mobile workforce that utilizes "mini-workflows," network-isolated components that can be offloaded onto mobile clients by leveraging Web services.

LOCALIZATION

Natalia Marmasse chaired our second paper session, on localization. Nishkam Ravi presented the first paper, entitled "Indoor Localization Using Camera Phones." He proposed an indoor localization scheme based on camera phones worn as a pendant by the user. The camera phone automatically takes pictures and transmits them over GPRS to the centralized server, which localizes the user by matching the current picture to the database of preloaded pictures. The discussion following this paper focused on a few issues: training costs, accuracy, and whether the entire system can run on the phone.

Alex Varshavsky then presented a paper entitled "Are GSM Phones *the* Solution for Localization?" He argued that localization using GSM-based mobile phones may be adequate and sufficient for many interesting location-aware applications. The authors show that, with GSM-based fingerprinting, it is possible to achieve 2–5m median error indoors, perform room-level localization indoors and achieve 70–200m median error outdoors. Moreover, by tracking signal stability, it is possible to detect places people visit with very high accuracy.

IS LOCALIZATION A *SOLVED* PROBLEM?

Following our paper session on localization, Gaetano Borriello (University of Washington) moderated a panel session exploring the question of whether localization is a solved problem. Three people sat on the panel: Dieter Fox (University of Washington), Mike Hazas (Lancaster University), and Jeff Hightower (Intel Research Seattle). Gaetano opened the panel by presenting four questions to each of the panelists and giving them each a chance to respond.

Prefacing his first question with "Cell phones are the location-aware platform of choice. We should focus all our attention on improving location systems on phones (accuracy, privacy, performance, etc.). There are no other viable platforms." Gaetano asked, "If it doesn't work on a cell phone, why bother?" Dieter

responded that it does not matter because everything can be integrated into the cell phone, if not now, then in the not-too-distant future. Most of what can be done on a laptop will be appropriate for a cell phone. Techniques for providing context awareness should be independent of this sort of detail. Mike responded that people may need to interact with other devices besides phones. Other devices may want to know where they are (e.g., a car or bus). Jeff agreed with the statement and added that everything is converging into phones. He felt that phones are the way to go, except for some enterprise IT and asset-management usages.

"Indoor location systems will piggy-back whatever outdoor system becomes dominant," continued Gaetano, so "can special-purpose indoor infrastructure even be practical for deployment or will location systems have coverage?" Mike responded that indoor location systems are too expensive, especially the ones that require special hardware. So indoor localization systems may need to be different. Jeff stated that specialized infrastructure is reasonable in certain environments, but support for indoor and outdoor localization should be implemented on the same device. We don't want to carry one more device. If additional hardware is required, it should be integrated into mobile phones. Dieter argued that most applications will not require special infrastructure. WiFi signal-strength information will be available in virtually any building. We just need to be smart about how to use it. If necessary, binary sensors or RFID can give additional location context.

For the third question, Gaetano began, "Getting a coordinate is a solved problem. No more papers need to be published on the issue," asking "Shouldn't research now only focus on what to do with the coordinates to solve real problems?" Jeff agreed, stating that coordinate research is basically done. Research should focus on place detection, learning, and labeling; combining activity inference with location; and designing applications with location awareness. Mike argued that we are not yet done, because we still do not know how to deploy the coordinate-based systems, and today's solutions are often expensive or otherwise impractical. Dieter thought that we are mostly done with coordinate-based localization, but the devil is in the details. It is not clear how to combine location with activity recognition. It is also not clear how to learn and maintain personalized maps (predict the location to which the person is going). In addition, combining information from multiple people is interesting.

And now on to Gaetano's final question: "The only people who really care about location privacy are researchers, lawyers, and bloggers. When you get right down to it, regular people just don't care that much, so let's stop worrying about it, OK?" Dieter responded that it all depends on the context. He argued that most people have a problem with being tracked, though he noted that elderly people might accept it. He also felt that there will be continuous erosion of privacy. Gaetano interjected that the indirect use of information is possible and then reported that a professor had complained about his students being tracked because he can be indirectly tracked that way as well. Mike added that although regular people think that they care about privacy, they really do not. Paranoid users have few applications to choose from, because applications are often provided by third parties. The remaining users can be bought out (e.g., by customer "loyalty" cards). He added that Scott McNealy may have had it right when he said, "You have zero privacy anyway. Get over it." Jeff argued that privacy will always be an important design goal. Regular people are pragmatic, privacy is not all or nothing, and it is not solely a technology issue. The goal is to help people avoid socially awkward situations, to support clarity in interpersonal interactions, and to provide transparency and reciprocity. He noted that there were several findings in the Ubicomp Reno paper:

- Use binary choice—disclose what is most useful or don't disclose.
- Levels of denial are needed (say that the system is "busy" as opposed to "deny").
- Blurring is used for clarity, not privacy ("I am in Seattle" may be more meaningful to outsiders than "I am on 45th and 30th").
- Actions convey complex meaning and/or intention.

At this point Gaetano opened the panel to questions and comments from the audience. An active discussion ensued.

KEYNOTE: MOBILE APPLICATIONS SUPPORT FOR ENTERTAINMENT

Frederick Kitson, Vice President and Director of the Applications Research Center at Motorola Labs, gave the keynote address on Friday morning. He focused on the future of mobile applications and showed us a wide variety of the kinds of research his team is working on at Motorola. This overview presents a sample of the visions he shared with us.

More than 70% of i-mode revenue comes from entertainment applications, such as music,

sports, personalized TV, imaging, and games. One of the goals of Motorola's research is to drive seamless mobility: to simplify effort, satisfy full mobility, and amplify the user experience. In fact, Motorola requires seamless mobility within its own product lines.

He described a vision of "cache and carry" that transparently "mobilizes" dynamic content. Users consume only a fraction of the content they pay for, in part because the content they capture is not located where they want to consume it. This research focuses on what might happen if they could provide a mobile content experience that moves the content to the user transparently, economically, and just before it is needed. Such a vision requires that the system behave intelligently with respect to battery, storage, and bandwidth consumption as well as with respect to the user's interests and consumption history.

He also described iRadio, in which users have six channels of dynamic content. Each channel has 90 minutes of cached content that can be streamed from the collection device (a PDA) to the user's car radio.

He described the "Push to X" technology, which was originally called iDEN. With this technology, you might have an existing audio connection and, while you are talking, you add visual content to it. He pointed out that standards are changing to increase bandwidth to support these types of services.

Fred then defined a vision of "Ambient Communication." Today, communication is intentional and conscious. It requires that one person call, text, or chat with another person. It requires that other person to interrupt his or her day to receive the communication. He argued that tomorrow communication might be unintentional or subconscious. In this world, one person might send a message to another person without knowing it and the other person might receive that message peripherally, or "ambiently." People will feel more connected in a less obtrusive manner and will have social awareness through context disclosure.

He then presented some interesting and daunting statistics: In the United States, fewer than 10% of WAP phone users actually use the browser; furthermore, among those that do, 50% are lost with each additional click. To address these challenges, Motorola has been working on a system called SCREEN3, which transmits data to idle cell phones in the background, with no noticeable effect on the handset's performance. The data is personalized and scrolls by as the user looks at the screen. If the user pushes any button, the scrolling stops. If the user clicks on something, more content is displayed. The analogy Fred used to represent the amount of data displayed with each additional click is "bite, snack, meal, feast." The "bite" and "snack" are cached on the phone. As the user requests the "snack," the "meal" is prefetched, and so on.

Motorola has considered combining this model for content delivery with location-based services. Services in the user's vicinity could scroll across the phone. The interested user can then easily obtain additional information with a single click. Another important application domain is advertising. Approximately $400 billion each year is spent on advertising. Mobile advertising is a big market and has the potential to be far more effective than billboards, magazine ads, and the like.

He also described integrated content consumption, which would allow users to capture more content "like this" across all of their devices, including both mobile and home devices. The content could be previously stored content as well as upcoming broadcasts that could be recorded. It would aggregate that content with Web images, news articles, songs, and the like.

BREAKOUT DISCUSSIONS

During the last afternoon session on Thursday, we introduced the breakout discussion topics:

- Impact of various networking technologies (gold)
- Application issues (green)
- Device symbiosis (silver)
- Cross-disciplinary research (blue)
- Privacy (red)

Each attendee had been assigned to a team prior to arrival, indicated by a colored star on the name badge. After the discussion questions and team assignments were introduced, each team of approximately eight members broke off to begin discussion. With the weather so pleasant, many teams chose to sit outside on the benches and rocking chairs. On Friday, each team was allotted 10–15 minutes to present a summary of their discussion and allow other attendees a chance to ask questions and to voice their own opinions.

Impact of Various Networking Technologies

The gold team was asked to consider the impact of various networking technologies. The initial questions they were asked to consider included the following:

- What is the impact of community-based networks?

- What might be the impact of having wireless connectivity at highway speeds? Does such functionality create new application scenarios?
- Will we, as a research community, need to support disconnected operation in ten years?

They addressed each of these questions.

With respect to the impact of community-based networks, Nina Bhatti reported that the team had two schools of thought on why these networks are important. The first is that such networks provide special content or special values for local communities. The second had to do with improving the cost structure so that more people have access to the network, thus reducing the digital divide.

Regarding having wireless connectivity at highway speeds, the gold team predicted that it would increase traffic accidents but thought it could provide value in the form of additional information from signs as the car drives past, or by enabling distributed content to be shared among vehicles. They thought it might be more useful to think about traffic-routing scenarios using vehicle-to-vehicle communications (e.g., sharing information on traffic speeds or avoiding congestion on freeways). They also wondered whether the question was addressing the car networking or the people networking across this wireless connectivity. [Editor's note: It should be noted that the gold team's discussion took place before the paper on this topic was presented.]

The gold team also discussed the need for disconnection research. They pointed out that there are two types of disconnected operation: visible and invisible. Invisible disconnection attempts to hide the discontinuous operation from the user (e.g., Outlook uses this approach). Alternatively, visible disconnection makes users aware of discontinuous operation and allows users to act in a way that respects the paradigm (e.g., users do not expect immediate receipt or response of SMS messages). The gold team felt that we still need caching research as we design for disconnection and for vehicular computing. They also identified store and forward as a very powerful idea in this work. Finally, they pointed out that users want to be disconnected at times.

- *Application Issues*

The green team was asked to consider application issues. The initial questions they were asked to consider included the following:

- Why don't we see more applications research?
- What are future directions for mobile applications?
- What is needed from the research community for mobile applications to succeed?
- What characterizes a good application paper?
- What makes good application research?

James Scott reported on the discussion of "Team Green." In response to why we do not see more application research, the team felt that users are tricky. Evaluation of application research suffers from measurability and repeatability challenges. They noted that you need long periods of time to interact with users and that it often goes wrong the first few times. They also observed that good application ideas typically lead to products and patents, but not to open research. Further, applications are generally regarded as engineering rather than research, so you will see "Usage patterns of XX" or "Privacy issues of XX" but not simply "XX" itself.

For future directions of mobile applications, they see health and fitness as well as elder care as important areas. They also see interest in social mobile applications, although they noted that the value proposition of these applications is weak. Finally, they see numerous research issues around thin clients as replacements for PCs.

Next they discussed what is needed from the research community for mobile applications to succeed. The first need was for people, as employees of start-up companies. They also noted a need for a shift in expectations and rewards toward more rigorous, deep research rather than least-publishable units. Such a shift should benefit applications research, which already has significant overhead.

They identified the characteristics of good applications research. The biggest one was iterating on the application. They also noted that it was important that researchers resist the temptation to stop after a single iteration.

They made some suggestions of how things could change to better support application research. One suggestion was for review forms to ask for ratings regarding the extent to which a paper describes a piece of work that contributes a building block or builds on top of an existing body of work. Review forms could also assess the extent to which the research provides suitable levels of comparison against other work, using common quantitative measures whenever possible. The second suggested change is to create a journal of impactful research, which contains papers describing only work that was created by one institution or group and also used

by *another* institution as an enabler for their work.

- *Device Symbiosis*

  The silver team was asked to discuss device symbiosis. The initial questions they were asked to consider included the following:

  - What role will mobile phones play in the future?
  - Will we ever attain the vision of exploiting devices in the user's environment? Why or why not?

  The silver team answered a completely different, though related, set of questions.

  John Barton reported that the team began by defining device symbiosis as two or more devices being combined, as peers offering independent value, for a task. Device symbiosis happens opportunistically and spontaneously; it is not configured. It happens wirelessly because mobility causes dynamics.

  They continued by describing possible applications of device symbiosis. The applications ranged from home and consumer applications (e.g., phone headsets, games, music, and entertainment), to mobile-travel applications (e.g., mobile radio, electronic wallets, and location-based advertising), to business applications (e.g., face-to-face groupware, HotMobile projectors, and opportunistic augmentation).

  They continued with a discussion of the importance of standards to the success of device symbiosis and the need to achieve critical mass. They then made an analogy to the Web. Prior to DNS, networking was for geeks who could make sense of things like 196.192.13.10, and they argued that this is the state of device symbiosis today. DNS gave us human-understandable names for devices. Further, we have search engines that allow people to search all sources known to the search engine. Device symbiosis will require similar functions to support spontaneous connections forced by mobility. Similarly, when they discussed the role of location technology, they noted that searches for symbiotic devices must be constrained by the user's location and that with device symbiosis, users will be able to physically identify spammers.

  Finally, the team identified challenges facing device-symbiosis researchers. The first challenge was how to create critical mass. The second concerned standards. The third challenge focused on user experience.

- *Privacy Issues*

  The red team was asked to consider privacy issues. The initial questions they were asked to consider included these:

  - What mechanisms do we need to support privacy?
  - How should we evaluate the privacy of mobile systems/applications? What is the value/price for privacy?
  - Have we solved the privacy problem with location-based (and other context-aware) services?

  Like the silver team, the red team devised their own approach to the breakout discussion. Mark Corner reported that they first asked themselves what makes this environment different. The answer they came up with is that, although there is some overlap with traditional privacy concerns, mobile computing presents much greater integration with daily activities. In addition, although many attacks are not new, the barriers are lower. Furthermore, they found that the risks are much more subtle. The risks include behavioral information and not just bank records and the like. As in traditional privacy concerns, users often do not understand the risks involved (especially the new risks related to mobile privacy), their exposure often goes unnoticed, they do not understand how to protect themselves, and they cannot make informed decisions.

  The team then advanced three proposals.

  Symmetric Privacy: In this scheme, there would be full disclosure of all disclosures. In other words, all requests for information are disclosed to the user. This scheme brings to mind the "watch the watcher" model. There would be a mandatory audit trail that records all disclosures of personal information and activity scans that look for exposures the user may have missed.

  Aggressive User Interfaces: In this scheme, the system would inform the user about leaked information. It would create an N map for people and/or mobile devices and produce embarrassing reports about their lives. It would rely on social networking. It could even create phishing attacks against a user's own phone.

  Help the User: This scheme uses the information collected from the Aggressive User Interface scheme to show how the information was leaked and demonstrate better behavior. It would actively obfuscate to spread disinformation and provide digital anarchy for mobile devices. In fact, mobile devices should impersonate others (e.g., by swapping grocery store loyalty cards).

- *Cross-Disciplinary Research*

  The blue team was asked to consider issues concerning cross-disciplinary research. The initial set of questions they were given included the following:

  - How do techniques from other fields (e.g., machine learning) ap-

ply to mobile computing research? Which ones are most important?

- If you could make one change in your previous mobile computing research projects, what would that change be and why?
- In what field do you see mobile computing making the most inroads?

In response to how techniques from other fields might apply to mobile computing and which ones are most important, the blue team thought control theory provided the basis for adaptive mobile applications (e.g., as bandwidth changes, so does behavior) and that statistical inference techniques provided the basis for fusing location sensor data. They also identified security, networking and operating systems, machine learning, human-computer interaction, industrial engineering, sensor systems, robotics, game theory, and social psychology as providing fertile grounds for cross-disciplinary research.

Regarding the ability to change history, the blue team offered a number of thoughts. The first would be to have anticipated the Web mindshare by engaging earlier and more deeply with the early Web developers and embracing Web practitioners. The second was to pay more attention to issues of data revocation and caching (e.g., erasing an address on Google). The remaining ones included performing more user studies, focusing on existing hardware, contributing more to open source, focusing more on applications, and providing controlled exposure rather than complete transparency.

As an example of how we could have done a better job as a community, Satya asked us to consider the dawn of mobile computing. He pointed out that people were addressing interesting questions but that the Web was ignored by most of us. He thinks that if we had engaged earlier, many deep aspects of this model would have been done in a better way.

The third question the blue team addressed was in what fields they saw mobile computing making the most inroads. The team identified medicine and health (e.g., personal sensors for the elderly, personal fitness, and chronic illness), transportation (e.g., a traffic signal adjusting to the passage of a bus), business processes and workflows (e.g., mobile Web services), gaming and entertainment, logistics and distribution, and privacy models.

FINDING THE RIGHT BALANCE FOR USERS

Our next paper session, chaired by Eyal de Lara, examined how to find the right balance for users. The first paper of this session, presented by Varun Marupadi, was entitled "Presence-Exchanges: Toward Sustainable Presence-Sharing." Varun and his colleagues suggested introducing a trusted broker into presence-sharing applications, so that misbehaving users could not learn about the presence of others without sharing their own identity.

For our second paper in this session, Anthony Nicholson presented "Exploiting Mobility for Key Establishment." He observed that most Internet traffic today is unencrypted, and he blamed the lack of easy-to-use tools available to users. He and his colleagues propose a model in which keys are established insecurely and are then automatically confirmed by exchanging cryptographic hashes of the keys over many different paths, utilizing inherent user mobility and overlay networks.

SECURE MOBILE COMPUTING

Ramón Cáceres (IBM Research) moderated a panel session exploring the question of whether we might attain secure mobile computing anytime soon. Four people sat on the panel: Carl Ellison (Microsoft), Steve Gribble (University of Washington), Helen Wang (Microsoft Research), and Jason Hong (Carnegie Mellon University).

Ramón opened the panel with a brief discussion of why we should talk about mobile security. He noted that the following articles appeared in the popular press:

- The New York Times had recently reported on a study that found that RFID tags are vulnerable to viruses (15 March 2006).
- PC World found that a virus can pass from PCs to mobile devices (28 February 2006).
- Yahoo! News reported on a virus that can jump from mobile devices to PCs (23 September 2005).
- BBC News reported that the first mobile phone virus had been created (16 June 2004).

Ramón also presented the panelists with a list of questions:

- Can we achieve secure mobile computing anytime soon?
- Is security in mobile computing different from security in general computing?
- Can we build usable security and privacy functions into mobile environments?
- Will trusted computing hardware and virtual machines play a big role in security mobile systems?

He then invited each panelist to make a short presentation.

Carl Ellison compared mobile computing platforms to 1980s PCs. They both support single users; they have a handful of software providers; they have

low CPU power as compared to "real" computers; they have a small amount of memory; they hunger for features; and they use tricks to achieve features in spite of their limitations. The result of these limitations is that they have significant security vulnerabilities. These platforms also differ in that mobile computing platforms have been networked from day one. Consequently, they are not physically protected via isolation and face even worse potential security problems. He argued that our industry needs discipline. We need to assume hostile users from day one; we need to partition the platform; we need TPM-style measurement of partitions; we need to ensure that all channels are access-controlled using strong authentication, strong authorization, and thorough ceremony analysis.

Steve Gribble opened his remarks by saying, "Hold on a minute . . . we still haven't figured out secure *nonmobile* computing!" He named spyware, phishing, worms, denial-of-service attacks, and flawed software as examples that support his statement. He identified three wide-open issues that have nothing to do with mobility. These include giving users a conceptual model of security, building attributable networks, and enabling safe sharing in a hostile environment. He argued that mobile devices exacerbate security issues. They tend to be much more promiscuous. They are generally built on weaker, closed systems. They face greater physical threats, such as theft. But he also pointed out some opportunities. For example, mobile devices may allow us to use the physical context of the device together with digital security by requiring the user to touch the device to authorize a communication. He also observed that cell networks at least feel better guarded than the Internet, though he admitted that may simply be an illusion. Finally, he felt that there is still time to design before we get into the same mess we have with the Internet. He ended his presentation with three open questions that he would like to answer. First, why did his IMAP client complain about a bogus certificate from Romania? Second, if he leaves his mobile device in another room for 15 minutes, what's the worst that might have happened? Third, if he receives an SMS message with the subject "Remember to upgrade your Treo OS software," how does he know who sent it, whether he should read it, and whether he should believe it?

Helen Wang continued with a presentation about the threats of smart phones. She showed that smart phones are gaining ground fast: 30 million were shipped in 2004, and it is estimated that 100 million will ship in 2007. They combine the portability of cellular phones with the computational and networking power of PCs. They offer rich functionality and features. She then pointed out some of the many threats that can compromise smart phones: attacks from the Internet (e.g., worms, viruses, and Trojan horses), infections from the desktop via sync (e.g., compromise one and you can compromise both), and peer attacks or infections. She then showed a substantial list of mobile malware from 2004–2005. She then talked about smart-phone zombies and the problems they can cause, which range from SMS spamming, to identity theft, to denial-of-service attacks (e.g., to base stations) and distributed denial-of-service attacks (e.g., to call centers), to remote wiretapping.

Jason Hong opened by summarizing his opinion: "Outlook not so good." He argued that secure mobile computing faces significant challenges that range from mobile devices containing important information to having significant usability, cultural, and economic issues. He showed three news articles showing loss of important data, all from March 2006, and talked about the strong incentives for theft because of it. He shared statistics that approximately 20% of WiFi access points are returned because people couldn't figure out how to make them work and he guesstimated that about 80% of WiFi access points are not secured. He continued with the observation that phishing attacks are stunningly effective. He argued that we need security models that are invisible and *extremely* easy to use. He also discussed some of the cultural issues around cookies, which were originally meant for maintaining state and have become a pervasive means for tracking people online. He also pointed out that the algorithm that the United States seems to use with respect to handling important society issues is to wait for a disaster and then legislate, which is both slow and suboptimal. He then discussed the economic issues. One of the problems we face is that although the estimated cost of phishing in the United States is about $5 billion and although solutions for this problem already exist, the estimated cost of implementing those solutions is greater than $5 billion.

MAKING THE CONNECTION

Our final paper session was chaired by Carla Ellis. This session focused on making connections. The first paper, "Measurements of In-Motion 802.11 Networking," was presented by Richard Gass. This paper studies the ability of a commodity laptop to communicate with 802.11 APs while being driven in a car

traveling at speeds between 5 and 75 mph. The findings reveal that a significant amount of data can be pushed through the wireless link, but the performance suffers owing to application-related problems, such as protocols with hand-shaking and long round-trip times.

The second paper was presented by John Barton and examined "Connection Time for Strange Devices." John presented experiences connecting small mobile computers to other computers. The results show that the benefit of connecting phones to larger displays and keyboards may outweigh the burden of making the connection.

CLOSING THOUGHTS

The formal and informal feedback I received after the workshop indicates that people enjoyed the return to the informal, highly interactive workshop format. That success came because of the hard work of numerous individuals. This includes the members of the program committee: Michael Beigl, Nina Bhatti, Gaetano Borriello, Yatin Chawathe, Mark Corner, Carla Ellis, Adrian Friday, Hiromichi Hashizume, Jason Hong, Yih-Chun Hu, Natalia Marmasse, Bhaskar Raman, M. Satyanarayanan, and Doug Terry. They had a very difficult task and did a great job of choosing papers consistent with the new vision for the workshop. Panels are tricky to organize and are generally either really good or, well, not so good. Gaetano Borriello and Ramón Cáceres both did an outstanding job in putting together two very successful panel discussions. Special thanks go to Fred Kitson for sharing his visions of the direction in which mobile applications are heading and to Nina Bhatti for recommending such an outstanding speaker.

Anthony Joseph, Kay Beck-Benton, Eyal de Lara, and Paul Castro, all members of the organizing committee, deserve thanks for their efforts in organizing the workshop and ensuring that the event ran smoothly. A special thanks goes to Kay Beck-Benton, our Local Arrangements Chair, who helped with tasks too numerous to mention and went above and beyond the call of duty. Her help was invaluable and much appreciated.

Finally, I am pleased to report that Nina Bhatti and Eyal de Lara have agreed to be the General Chair and Program Chair, respectively, for HotMobile 2007. They plan to keep the same informal, highly interactive format. I hope to see you there next year!