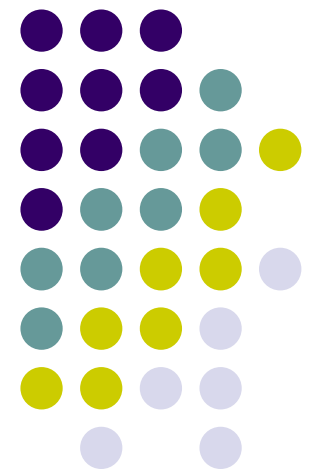


CS 525M Mobile and Ubiquitous Computing: The Wi-Fi Privacy Ticker: Improving Awareness & Control of Personal Information Exposure on Wi-Fi

Shengwen Han

*Computer Science Dept.
Worcester Polytechnic Institute (WPI)*

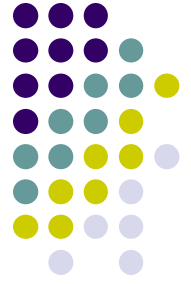




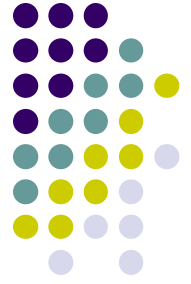
Abstract

- Problem: Unaware of the risk while using Wi-Fi
- What this paper aims:
 - Improve their awareness
 - Provide with control—Wi-Fi privacy ticker
 - Display + prevent transmission
- To verify: 3-week field study with 17 participants

Why—Easy to get people's information?



- Public Wi-Fi hotspots which provide little protection
- Provide personal info to use web services
- Freely available tools for eavesdropping



Related Work

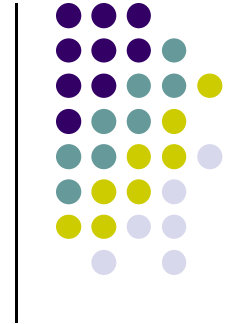
- Understanding & behavior on Wi-Fi
- Technologies to improve awareness & control
- Commercial solutions



The Wi-Fi Privacy Ticker

- **Workflow**

- User provides terms to monitor;
- System monitors network traffic when using Wi-Fi
- When it detects that any term is being sent or received in the clear, it is shown on a peripheral “ticker” display and added to an archive
- User-control



- **The Network Monitor**

- Hook NtDeviceIoControlFile—handle network-related requests
- For 3-week field study—Internet Explorer and Firefox browsers

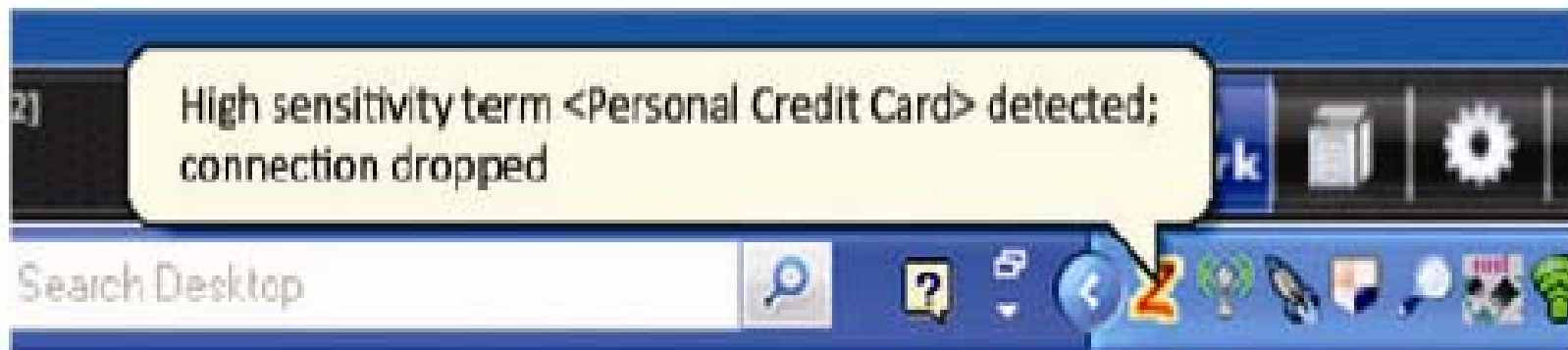


- **The Control Mechanism—Zapper**

- Implemented in Windows kernel
- Close socket device handle when it detects a highly sensitive term in the socket's "send" buffer
- Drops connection



- To indicate a “zapped” term, the term appears in *Ticker display* with a strikethrough and a balloon tip appears in system tray



- Cannot prevent terms from being received in the clear



- **The Ticker Display**

- Real-time alerts of potential data exposures
- Scrolling text that moves from right to left
- Implemented by *.NET Windows Presentation Foundation*



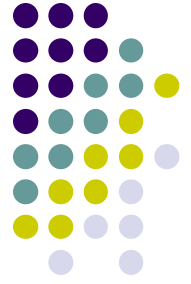
- Terms:
 - *Watch List* terms—user specifies (a sensitivity level, displayed name)
 - search terms
- Color reflects term's sensitivity level
- Rules to prioritize display of terms:
 - First detected, first appear (sensitivity level > detection order)
 - time-out of *Ticker display's* queue—90 seconds

- 'out' / 'in', times, IP of the server and other details
- Network encryption
 - Open or Closed Network—bright shade
 - Secure Network or VPN—darker shade



```

adsite1.net, mktresearch1.com, adsite2.net, mktresearch2.com, mktresearch3.net
Via www.eventplanning.com
September 27, 2010 9:15am
ZIP Code> :: [in ,3]
multiple senders
:: <Work ZIP Code> :: [out ,7]
multiple destinations
  
```



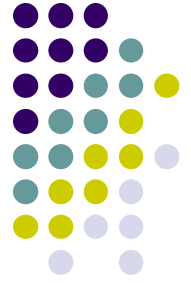
- **The Archive**

- Review past exposures
- Any detected *Watch List* terms including which were dropped from the queue for time-out reasons



- **Considerations for Protecting Users' Data**

- User's *Preferences* are password-protected
- Particularly sensitive term types are never shown in the clear
- Database in which system stores user's terms remains encrypted



3-Week Field Study

- Study Procedure & Data Collection
 - Survey + data logs
- Participants
 - chosen from company
 - have option of using a VPN



- Participants' Watch Lists
 - 186 unique *Watch List* terms

Term Type	# of Participants	# of Terms per Type	# of Terms per Sensitivity Level		
			High	Med	Low
Email address	17	28	1	13	14
Password	16	30	19	9	2
Social Security #	14	14	10	3	1
Street address	13	15	2	7	6
Birth date	12	13	3	5	5
ZIP Code	12	14	0	1	13
Last name	11	11	0	5	6
First name	10	16	0	2	14
Username	9	13	2	4	7
Credit Card #	6	11	5	6	0



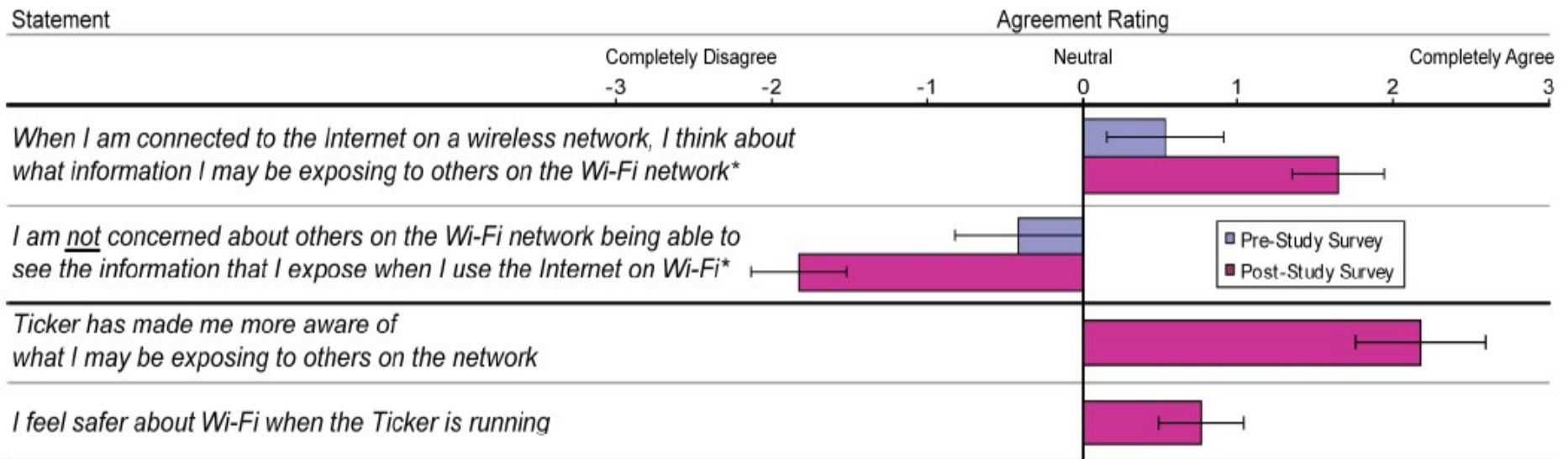
Results

- **Watch List Term Exposure**
 - Average of 1,054 unique search terms were detected for each participant
 - Personal data was transmitted with high frequency
 - Many websites sent personal data in the clear

Site	% of Total Matches (out of the 353 sites observed)	Watch List term types matched						
		Email Address	First Name	Last Name	Password	Street Address	Username	ZIP Code
Web search & portal	22.39%	●	●	●		●	●	●
Social networking	21.07%	●	●	●	●	●		
Sports	16.66%	●	●					
Newspaper	6.41%	●						
Company	3.81%		●	●			●	
Airline	2.83%		●	●				
eCommerce (apparel)	2.53%	●	●	●				
eCommerce (technology)	2.09%		●	●				
Manufacturer	1.35%	●	●	●				
Auction	1.34%		●		●		●	●



● Change in Awareness



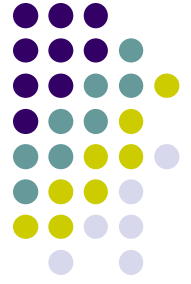
* - Difference between pre- and post-study surveys is significant ($p < .01$)

- Pay attention to network encryption
- Form more accurate mental models of the circumstances in which data get transmitted
- Positive to Zapper



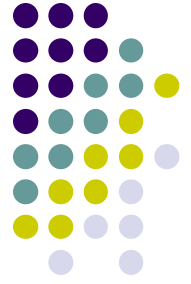
- **Change in Behavior**

- ≠long-term behavior change
- Upgrade encryption of home wireless network
- Start using VPN
- More careful about types of networks
- Not stay logged in
- Close browser windows more frequently
- Educate friends



Discussion & Future Work

- **Improve the Control Mechanism**
 - pop up a window to ask if dropping connection or proceeding
 - rule-based systems



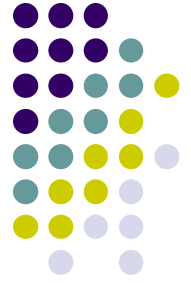
- **Extend the Ticker Concept**

- Detect transmitting of personal data which is not in *Watch List*
- Monitor additional applications
- Develop system used by parents to monitor and keep children safe on the Internet
- Change or augment user experience



- **Provide Education**

- Educate users about phishing attacks by *PhishGuru* and *Anti-Phishing Phil*
- Making suggestions based on user's activities



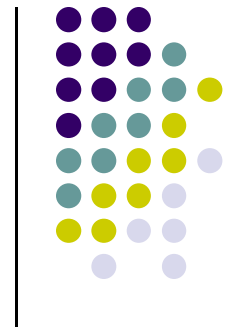
Conclusion

- Wi-Fi Privacy Ticker
- How to help users become more aware of the unencrypted transmission of terms and how to prevent
- Three-week field study with 17 participants verified that participants' awareness improved and their behavior on Wi-Fi changed



References

- Kindberg, T., O'Neill, E., Bevan, C., Kostakos, V., Stanton Fraser, D., & Jay, T., "Measuring Trust in Wi-Fi Hotspots," *Proc. of CHI '08*, Florence, Italy, (2008), pp. 173-82.
- Klasnja, P., Consolvo, S., Jung, J., Greenstein, B., LeGrand, L., Powledge, P., & Wetherall, D., "'When I am on Wi-Fi, I am Fearless:' Privacy Concerns & Practices in Everyday Wi-Fi Use," *Proc. of CHI '09*, Boston, MA, USA, (Apr 2009), pp. 1993-2002.
- Kowitz, B. & Cranor, L., "Peripheral Privacy Notifications for Wireless Networks," *Proc. of the WPES '05*, Alexandria, VA, USA, (2005), pp.90-6.
- Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A., & Pham, T., "School of Phish: A Real-World Evaluation of Anti-Phishing Training," *Proc. of SOUPS '09*, Mountain View, CA, USA, (2009).
- Maglio, P.P. & Campbell, C.S., "Tradeoffs in Displaying Peripheral Information," *Proc. of CHI '00*, The Hague, The Netherlands, (2000), pp. 241-8.
- Palen, L. & Dourish, P., "Unpacking "Privacy" for a Networked World," *Proc. of CHI '03*, Ft. Lauderdale, FL, USA, (2003), pp. 129-36.



Thanks!
Questions?