Radio Frequency Identification (RFID) technology appears in a huge array of contactless payment products ranging from subway tickets and credit cards to mobile phone NFC payments. Security and privacy for contactless payments are important to both protect consumer privacy and manage fraud. Unfortunately, poorly designed security is difficult to distinguish from well-designed security --- especially by consumers who are inundated with misleading information about the security and privacy of contactless payment systems. How can a consumer or researcher determine whether an RFID-enabled, contactless payment system is actually secure and privacy preserving, or whether a system is merely advertised as secure?

An estimated 20 million contactless credit cards are already in circulation in the United States, but until last year no public study had thoroughly analyzed the contactless mechanisms that provide both security and privacy. Using samples from a variety of such cards, my research team observed that (1) the cardholder's name and often credit card number and expiration were leaked wirelessly; (2) our homemade device costing around $150 effectively cloned one type of skimmed card thus providing a proof-of-concept implementation of a replay attack; (3) information revealed by the contactless card contaminated the security of card-not-present transactions; and (4) contactless credit cards are susceptible in various degrees to a range of other attacks such as skimming and relaying. Moreover, low-cost devices can be bought on eBay that enable unsophisticated criminals to mount advanced attacks without needing any specialized, technical knowledge.

Consumers lack sufficient opportunities today with respect to contactless payments: Personal privacy, informed consent, and consumer choice.

1. Consumer privacy should be a high priority for contactless payments. Many consumers are concerned about their personal privacy. Would you feel violated if the person next to you on a subway could wirelessly read the contents of your wallet through your clothing? That's precisely what our attack did to obtain cardholder information. Moreover, the attacks in our report skimmed cardholder information despite that the cards are designed to work at short distances. Thus, short read ranges cannot be relied upon for security. While fraud directly affects the bottom line of credit card companies, violation of consumer privacy does not have a direct cost because consumers have few choices. There should be stronger incentives for credit card companies to protect the consumers against violation of their personal privacy rather than just protection against fraud.

Example: A professor of electrical engineering told me that he did not have a contactless card. My research group scanned his wallet and pointed out that he was already carrying an RFID-enabled, contactless credit card. The next day he disabled the RFID portion of the card with a hammer. He felt violated by the lack of information about privacy of contactless cards. If an engineer with a PhD has difficulty maintaining privacy of a contactless card, then how can we expect the average consumer to guard their privacy without stronger requirements for privacy in contactless payments?

2. Consumers should be fully informed about the risks and benefits of contactless technology so that consumers can make informed decisions. My experiences show that companies offering contactless payments have often provided misleading or partial information. Whether unintentional or just out of incompetence, some credit card companies have given consumers a misleading "education" program that touts the benefits of contactless technology but downplays or hides the risks to consumer privacy.

Example of misleading information:
http://www.paymentsnews.com/2006/06/wells_fargo_ann.html
A press release from Wells Fargo on June 2006 reads,

"Visa Contactless is enabled by radio frequency (RF) technology. The Visa Contactless RF payment chip uses industrial strength encryption technology -- 128-bit and triple DES encryption -- the highest level encryption allowed by the federal government. The chip contains the same minimal personal information found on a traditional magnetic stripe card -- just the account number and cardholder's name."

The press release implies that all Visa contactless cards were using strong encryption, and yet our report examined a number of Visa cards and found no observable encryption protecting confidentiality of basic information such as the cardholder name, credit card number, and expiration date. Who verifies such claims that a contactless card properly uses the security as advertised?

Example of denial from a credit card company: A co-worker in my department called her credit card company to disable the RFID technology in her card. She was told by a customer support representative that "the security report on contactless credit cards is not true." Who is instructing support representatives to mislead customers about published research that received thorough peer review? On the contrary, our report demonstrated real security and privacy vulnerabilities, and none of the results in our report have been disproven.

3. Consumers should have the ability to make informed choices about contactless payments. Today, consumers are like airline passengers who are told they "have a choice of chicken." The consumers receive advertising from credit card companies such as, "Our cards are capable of strong encryption." Does that mean the card actually uses secure encryption? Or does it mean that the card could but does not necessarily provide secure encryption? How does the consumer know? One type of consumer cares deeply about personal privacy and vehemently wishes to opt-out of contactless technology regardless. Another type of consumer unknowingly carries a contactless credit card. Neither of these types of consumers receive appropriate information and customer service to make informed choices.

Example of botched handling of opt-out requests: A woman complained to me that she called her credit card company for a non-RFID-enabled credit card. The customer support representative explained that she would receive a new card that did not include RFID technology. When the card arrived, it still included RFID technology. It is difficult for consumers to even determine whether RFID-enabled card is present. In this case the woman was able to carefully inspect the card for evidence of RFID, but such visual indicators are not universal. Consumers do not have enough information to make informed choices. Consumers lack well-trained customer service and adequate information to make informed choices about security and privacy of contactless technology.

In summary, the promise of convenient payments with contactless technology needs justified security and privacy that is subject to public scrutiny. Analysis has proven that the proprietary systems from payment associations have failed to protect information such as the credit card holder name, card number, and expiration date. Will consumers remain the unwilling and unwitting beta-testers of underdeveloped contactless technology? Or will regulations and other incentives encourage credit card companies to give more serious attention to consumer privacy before millions more cards are deployed? Contactless payments need stronger privacy and security mechanisms.

Bio:

Dr. Kevin Fu, PhD, is an assistant professor in the Department of Computer Science at the University of Massachusetts Amherst. He serves as the director of the RFID Consortium on Security and Privacy (RFID-CUSP.org) and the co-director of the Medical Device Security Center (secure-medicine.org). Dr. Fu investigates how to ensure security and privacy for devices that must defend against determined,

malicious parties. His contributions include the security and threat model analysis of several systems ranging from contactless "no swipe" credit cards and wireless medical devices to access-controlled Web sites and automated software updates. Dr. Fu's research has led to improvements in security and privacy of pervasive devices, promoting the vision of safer and more effective technology for consumers. Dr. Fu received his Ph.D. in Electrical Engineering and Computer Science at the Massachusetts Institute of Technology. He has served on numerous program committees of prestigious conferences in computer security and cryptography, and has given dozens of invited talks world-wide to industry, government, and academia on the topic of security and privacy. His research has appeared in The New York Times and The Wall Street Journal.

References:

[1] "Researchers See Privacy Pitfalls in No-Swipe Credit Cards."
In New York Times, October 23, 2006.
http://www.nytimes.com/2006/10/23/business/23card.html

[2] "Vulnerabilities in first-generation RFID-enabled credit cards."
by Thomas S. Heydt-Benjamin, Dan V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare.
In Proceedings of the Eleventh International Conference on Financial Cryptography and Data Security, Lowlands, Scarborough, Trinidad/Tobago, February 2007.
http://prisms.cs.umass.edu/~kevinfu/papers/RFID-CC-manuscript.pdf
http://prisms.cs.umass.edu/~kevinfu/talks/FC-RFID-CC-slides.pdf
http://prisms.cs.umass.edu/~kevinfu/video/RFID-CC-clips.mov

[3] "Summary of Vulnerabilities in First-Generation RFID-Enabled Credit Cards."
by Ari Juels.
October 23, 2006.
http://www.rfid-cusp.org/blog/blog-23-10-2006.html

[4] "Chip and Pin Take-over and Fraud Risk"
Newsnight, BBC2, 26 February 2008
http://www.cl.cam.ac.uk/research/security/banking/ped/
http://youtube.com/watch?v=L7QzOcZAwbg
http://youtube.com/watch?v=pHdX3ZYEvXw