Frequently Asked Questions (FAQ) about CUSP’s RFID credit-card report

Q: *Does the CUSP report mean that RFID is a fundamentally flawed technology?*
A: Our analysis does not mean that RFID is categorically flawed or insecure. RFID, like other technologies, can be deployed in a variety of ways, with varying degrees of security and privacy. CUSP believes that highly secure RFID credit cards are practically achievable. Further, we believe that it is important to build RFID systems that incorporate strong security and privacy from the start.

Q: *Who was involved in the credit-card study?*
A: Professor Kevin Fu and PhD student Thomas Heydt-Benjamin at the University of Massachusetts Amherst collaborated with RSA Laboratories scientists Daniel Bailey and Dr. Ari Juels to perform the analysis. As members of CUSP, they undertook this analysis in order to learn more about RFID credit cards and inform the public of potential flaws and problems. While not a member of CUSP, Thomas O’Hare of Innealta also collaborated in the research.

Q: *Why do these experiments?*
A: The CUSP study is, in effect, a product safety report. RFID is a budding technology of high promise. CUSP scientists believe that it is important to help ensure strong privacy and security in RFID systems as early as possible. As credit card fraud is already a widespread problem, it is particularly important to ensure that RFID does not introduce new vectors of attack.

Q: *How many credit cards are affected?*
A: The credit cards analyzed spanned all three major U.S. payment associations and several major issuing banks. All were issued in 2006. While the 20 cards under study do not represent 100% of the RFID credit cards issued, they are enough to raise significant concerns about the present security of RFID credit cards. CUSP would welcome the opportunity to analyze other types of RFID credit cards.

Q: *What’s the range at which these attacks can be perpetrated?*
A: The cards are designed to work reliably at a range of only a couple inches. But the maximum achievable range is greater. Some research papers report read ranges of up to 15 cm, while some newspaper reports claim up to 26 inches. Feasible read ranges are an open research problem, and not the focus of the CUSP study.

Q: *How do I know if my credit cards have RFID?*
A: Some RFID-enabled credit cards bear visible microchips. Others do not. If in doubt, you may wish to contact your credit card issuer.

Q: *How can I protect myself?*
A: Perhaps the best course of action is to contact your credit card issuer. They may be able to provide some options, like a replacement card without RFID, or some more detail on your precise level of exposure.

Q: *What expertise and equipment is needed to perform these attacks?*
A: No complicated cryptographic algorithms or security measures were broken. RFID readers for credit cards are available inexpensively online. Certain types of attack are feasible with such off-the-shelf readers. Others require more specialized devices. We assembled a simple electronic device that clones cards for about $150.

Q: *The credit card companies claim they use Triple-DES or 128-bit AES encryption. Don't these measures defend against hackers?*
A: None of the cards we examined encrypted the cardholder name. Instead, some cards use encryption to create changing authentication values, i.e., changing transaction numbers. This protective measure does prevent certain forms of attack, but still leaves cards vulnerable to various forms of cloning.

Triple-DES and 128-bit AES encryption are powerful cryptographic building blocks. Used correctly, they could effectively prevent nearly all of the attacks described in the CUSP paper. We did not observe the optimum deployment of these algorithms in any of the cards under study.

Q: *Will the researchers' findings lead to a wave of RFID credit card fraud?*
A: The RFID credit-card vulnerabilities in the CUSP report probably do not pose a major, imminent threat. Others forms of credit-card fraud represent a more serious systemic problem--particularly the frequent compromise of credit-card information on the Internet. What is particularly significant about the CUSP report is the new *physical* dimension of vulnerability that it reveals in RFID credit cards.

It's important to note that the RFID-CUSP report did not create any new flaws. It just reported existing ones that others could very likely have discovered independently.

Q: *Have the researchers tried their experiments in real-life situations, or just under laboratory conditions?*
A: The research team has performed a real-life "cross-contamination" experiment. We skimmed the data from a card in a sealed envelope (one of our own cards) and then made a purchase using the resulting data. The team has also created a credit-card "clone," that is, a radio device that spoofs a point-of-sale terminal into accepting previously skimmed data from a valid card.

What the team has not undertaken is field testing of a "clone" card, i.e., an in-store purchase using a spoofing device. The team believes that such experiments are feasible, but has refrained from mounting them because of their uncertain legality.

Q: *What projects does RFID-CUSP anticipate undertaking in the future?*
A: Scientists in the consortium have already performed a substantial body of research on RFID, including the development of RFID privacy and anti-counterfeiting techniques and analysis of vulnerabilities in other RFID systems. Information on this work is available at www.rfid-cusp.org.

The ongoing mission of the consortium is to make RFID safe for consumers and industry through open, peer-reviewed research, experimentation, and education of new generations of RFID security experts.