



August 2009

DEFCON's RFID Sniffing, Door Frame Antenna and Long Range Reader make Feds Nervous.

(New York, NY) Three major RFID Hacks were showcased by RFID security experts at this year's DEFCON 17 conference, one of which had Federal Agents attending the events so nervous that they broke their RFID enabled identity cards – just to be on the safe side. What did these researchers do to raise such concerns about the security of RFID enabled cards?

1. RFID Sniffing at the Wall of Sheep

In 2007, renowned hacker “Major Malfunction,” cracked the UK passport and proved that RFID chips in government issued passports could be skimmed, copied and hacked. At DEFCON 17, the vulnerability was put on display when Major Malfunction set up RFID sniffing gear at the Wall of Sheep, a service that Aries Security provides to its customers and a fixture at the DEFCON conferences. The RFID skimming conducted at the Wall of Sheep displayed information read off of RF identity badges of individuals who walked by and along with a picture of the person whose data was skimmed. Paring this up with the information taken from the RFID cards would have allowed hackers to create a duplicate identity badge, in many cases. The demonstration was stopped after a former Federal Agent suggested that Major Malfunction “do the right thing.” It is unknown whether information from any of the Feds attending the conference was actually obtained, since the SD card that stored the data was destroyed immediately upon shutting down the project; however, it is known that some nervous individuals were breaking their RFID cards after the demonstration – just to be safe.

2. Long Range RFID Skimming

Chris Paget, of the security consultancy H4rdw4re, gave a talk titled “RFID Mythbusting” in which he discussed and later demonstrated long-range RFID skimming capabilities. In the demonstration, Paget handed an RFID card to an attendee approximately 20 feet from the stage and successfully skimmed the tag using a high-powered reader.

Presentation: <http://seclists.org/bugtraq/2009/Aug/0112.html>

3. RFID Door Frame Skimmer

Later, at the hardware hacking area, Chris Paget spearheaded the creation of an RFID skimming doorframe antenna that would capture information from anyone who walked through the door carrying an RFID card. The reader in the lab was set up to beep to raise awareness and prove that the reader was working; however, in a non-lab setting, a malicious hacker might set up an door frame skimmer that stores all information from those who pass through it to be collected later, with the victim none-the-wiser.

Video: http://www.youtube.com/watch?v=W_HVPubYpPY

DIFRwear, a manufacturer of RFID Blocking Wallets and Passport cases exhibited at the conference and saw a significant increase in sales after the skimming demonstrations and the government's recent warning that RFID enabled passports should be stored in electronically opaque sleeves, such as DIFRwear's RFID blocking passport case. Several hackers attending the event, including Major Malfunction, tested DIFRwear's RFID blocking products and were unable to skim any chips through the products.

DIFRwear – Because what you wear matters.

DIFRwear is the leading supplier of RFID Blocking wallets, passport cases and badge holders. Founded in 2005, DIFRwear's mission is to give individuals the ability to maintain privacy and ensure security in a world of insecure contactless devices. DIFRwear's products are sleek, sexy, stylish, and SECURE.

Through our growing line of RFID Blocking products, DIFRwear ensures that RFID tags within the wallet, passport case or sleeve can NOT be read while the product is closed. This gives you the ability to control when, how and by whom your cards are accessed. To learn more, visit us at www.difrwear.com.

For press inquiries contact Diana.Kearns@difrwear.com or 347-623-5998.

#