

# Pro Hackers Take On RFID Down Under

An Australian firm has begun using its information-security consultancy to perform RFID system audits, which include probing vulnerabilities.

By Mary Catherine O'Connor

Aug. 29, 2006—Companies pay Joshua Perrymon and Robert McAdam for performing ruinous acts on their infrastructures. The pair's firm, Pure Hacking, does what is known as ethical hacking, or penetration testing, and serves it up with a consultation service, detailing the holes in the companies' existing security measures and providing steps they can take to protect their data better.

Pure Hacking has, in the past, focused on corporate firewalls and security protections for onsite servers and applications, both in wired and wireless networks. Now, they've begun testing the vulnerabilities of RFID systems and are performing security audits for companies deploying RFID technology.

Perrymon says Pure Hacking is focusing on both the operational and technological risks associated with insecurities in an RFID system, and that the company uses a structured auditing process similar to those performed by the National Institute of Standards and Technology (NIST) the International Standards Organization (ISO). He says that aside from enabling its clients to improve information security, Pure Hacking can also save them significant amounts of money by "identifying security risks early, instead of down the road of when an attack comes."

Perrymon and McAdam interview executives and key employees at the firm being audited and perform surveys in order to understand how its RFID system is deployed. From this information, they ascertain the operational risks linked to its operation. "We ask about policies and procedures, and recommend new ones," says McAdam.

The client's technological risks are assessed through hands-on penetration testing. "We'll identify possible attack areas, and then go in with a rogue reader and simulate an attack," says McAdam. This consists of trying to read one of the firm's deployed tags with an unauthorized interrogator, trying to clone or change data encoded to the tag, or using an interrogator to manipulate the tag to identify the configuration of the data encoded to its chip.

Pure Hacking is marketing its RFID auditing service to all end users of RFID, such as those in the retail supply chain, as well as to users such as casinos or chemical companies, whose use of RFID might be linked to highly sensitive or proprietary information.

Pure Hacking has a large market opportunity in Australia, where Perrymon says roughly 1,300 companies are piloting RFID technology today. But he and McAdam say they are interested in running the RFID system audits around the world.

Thus far, Pure Hacking has completed one audit of a high frequency (13.56 MHz) RFID-based access-control system. After the consultation, Pure Hacking advised the company on a number of matters, such as how to

store access cards and how to restrict access to them. Pure Hacking was also able to clone one of the cards in deployment, then use the clone to enter the building. Its recommendations to the company included upgrading its system to support data encryption so cards could no longer be cloned.

McAdam says that going forward, Pure Hacking wants to focus RFID audits on EPC Gen 2 tags and readers. "We're seeing several risks with Gen 2 systems," says McAdam, "in the way the tag handles access and kill passwords. The system is subject to manipulation. We are currently analyzing the GEN2 protocol using custom in-house scripts to identify risks and possible attack scenarios."

Pure Hacking plans to submit the Gen 2 security risks it identifies to [EPCglobal](#), in the hope that the organization will use the information in future development of RFID standards.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved