If this page does not print out automatically, select Print from the File menu.

# Researchers craft first RFID virus

RFID systems open to viruses

Tom Sanders in California, vnunet.com 15 Mar 2006

Researchers at the VU Amsterdam university claim to have crafted the world's first RFID viruses and worms.

Organisations are using or looking to use the wireless identification tags at checkout stands in stores, for inventory control in warehouses or for luggage tagging and routing at airports.

In an airport scenario, one maliciously crafted tag on a suitcase could infect the scanning system, which could then be instructed to spread the exploit code to all suitcases in the system. This could cause a global RFID infection within 24 hours, researcher Melanie Rieback cautioned.

As the wireless tags are scanned, a specially crafted tag could inject infected code into the middleware, exploiting security vulnerabilities in components such as the web server or database, researcher Rieback demonstrated on Wednesday at the IEEE Conference on Pervasive Computing and Communications in Pisa, Italy.

The tag could also embed javascript to execute code on RFID systems incorporating web based components. The Javascript code could instruct the system to surf to a specific internet address hosting a malicious payload, or for instance format the system's hard drive.

Another possible attack method would be to launch a buffer overflow attack against the RFID reader. The sensor networks typically don't expect buffer overflow attacks because an RFID tags offers only a limited storage capacity, but it could be used to cause a system crash.

RFID worms require careful programming. Because of the limited storage space available, attackers will most likely create code that instructs the system to download additional exploit code off the internet.

Rieback recommended that software engineers pay close attention to how they design RFID systems. They should use security practices that are common in other software implementations, such as limiting privileges for applications and the removal of features that aren't required.

The university has published a special website on RFID viruses, which also offers a ten-page paper on the subject that has been submitted to the IEEE.

- Also read: Experts unconcerned by RFID virus

Permalink to this story

www.pcmag.co.uk/2152061

Close this window to return to the website