Government Computer News

Wednesday August 30, 2006 | Updated 5:08 PM EST August 30　　　　　　**Login** | **Register**

Current issue　▼ Subscribe | ▼ Blogs　Events　eSeminars　White papers　RSS / XML　Jobs　**Post**Newsweek Tech Media | ▼ Visit our sites

Technology / Products

Tech/Products Home
Communications / Networks
Enterprise Hardware
Enterprise Software
IT Security
Mobile & Wireless
Storage Management

Hot Topics
Acquisition / Contracts
Authentication/Identity Mgt.
Business Process Mgt.
Content/Record Mgt.
Defense IT
E-Government
Enterprise Architecture
Health IT
Homeland Security
IPv6
Lines of Business
Open Source
Policy / Regulation
Program/Project Mgt.
RFID
State & Local
VOIP
Web Services / XML
Work force/Training

Archives
Print edition
E-letters
Forums

GCN Events/Seminars
GCN Events
PostNewsweek Awards

Sponsor Reports
Product/Services Finder
Custom Supplements
Juniper Networks
Citrix
Adobe

GCN Home > Tech Blog　　　　　　　　　　　　　　　　RSS | XML

Tech Blog

08/09/06 -- 08:28 AM
By Brad Grimes & Joab Jackson

Black Hat demo ruffles feathers

According to an observer of trends in homeland security, whose expertise and opinions we trust and value above others, a demonstration at last week's Black Hat Briefings in Las Vegas has set off something of a controversy. Actually, the controversy has always been there, but according to this observer, "in some quarters it has not really been simmering, but rather boiling over."

Last week a German security expert demonstrated how data could be hacked from electronic passports. GCN's senior writer William Jackson was there to see it.

This week, the demo brought a flurry of responses, one of which arrived yesterday from the Smart Card Alliance, an industry group. Here's what executive director Randy Vanderhoof had to say, and it's representative of the Black Hat demo's critics:

"People do not need to be concerned about the security or privacy protection features of the new e-passport program," Vanderhoof said in his statement. "Recent reports that there is a 'major vulnerability' that criminals could use to 'enter countries illegally' are untrue and demonstrate a lack of understanding of how the multiple security layers in place at the U.S. border work in the new e-passport system."

Vanderhoof continued, "Even if someone could copy the information on your e-passport chip, it doesn't achieve anything, because all of the information is locked together in such a way that it can't be changed. It's no different than someone stealing your electronic passport and trying to use it. No one else can use it because your photo is on the chip and they're not you."

He concluded, "People need to be cautious about some claims made by so called 'experts' when it comes to RF-enabled applications. There is too much misleading and inaccurate information being reported, simply because fear gets people's attention."

Fair enough. This blog has taken the position that fear-mongering has limited the progress of RFID-based solutions, but it would never go so far as to say, as Vanderhoof has, that people "do not need to be concerned about the security or privacy protection features" of e-passports. Just as we'd never say that the Veterans Affairs Department doesn't have to be concerned about the privacy protection of data stored on a desktop computer in a secure

RECENT POSTS TO THIS BLOG

- **The Dell battery recall, one week later**
- **The future of virtualization**
- **Why we don't defrag Unix**
- **Muni WiFi gets a boost**
- **Decoding AMD's new Opteron model numbers**

ARCHIVES FOR THIS BLOG

- August 2006
- July 2006
- June 2006
- May 2006
- April 2006
- March 2006

environment at a VA contractor's offices.

The German security expert, Lukas Grunwald, has a vested interest in vulnerabilities because his company is in the security consulting business. The Smart Card Alliance has a vested interest in e-passport adoption because its members make and sell the technology behind them.

Somewhere there's a middleground, where engineers working on behalf of the government must be analyzing it from both ends of the argument, evaluating the security risks of the new technology as well as its strengths/limitations.

Posted by Brad Grimes

Comments (0) | Post Comment | Link to this Page | Trackback

Post a Comment

If you are currently registered, click here to login and post your comment.

If you are new to GCN, click here to register and post your comment.

Home | About GCN | Contact GCN | Customer Help | Privacy Policy | Careers | Editorial Info | Advertise | Link policy / Reprints | Site Map