BY E-MAIL

Jai Singh
Editor-in-chief
CNET News.com
235 Second Street
San Francisco, CA 94105

May 25, 2005

Dear Mr. Singh,

We are writing in response to Phil Libin's CNET News.com column on May 17, 2005, "Technology alarmism in spades."[1] In it, Mr. Libin criticized the Electronic Privacy Information Center's April 2005 Spotlight on Surveillance report, "Homeland Security ID Card Is Not So Secure," which is an evaluation of the Department of Homeland Security's Access Card (DAC).[2] Mr. Libin also posted a longer criticism of the report on his blog, "Vastly Important News"[3] Mr. Libin's column and blog entry contain several errors, and EPIC takes this opportunity refute his criticisms.

Mr. Libin's most significant error is his assertion that the DAC's ISO 14443 technology is not Radio Frequency Identification (RFID).[4] However, technology experts, the industry and CNET News.com itself, label ISO 14443 as RFID.[5]

[1] Phil Libin, *Technology alarmism in spades*, CNET News.com, May 17, 2005 *available at* http://news.com.com/Technology+alarmism+in+spades/2010-7348_3-5710529.html (hereinafter "column").

[2] EPIC, *Spotlight on Surveillance: Homeland Security ID Card Is Not So Secure*, Apr. 2005 *available at* http://www.epic.org/privacy/surveillance/spotlight/0405.html.

[3] Phil Libin, *EPIC report is not so good*, Apr. 11, 2005 *available at* http://www.vastlyimportant.com/vastly/2005/04/epic_report_is_.html (hereinafter "blog").

[4] Blog.

[5] Ari Juels, David Molnar, and David Wagner, *Security and Privacy Issues in E-passports*, at 2 (2005) prepublication draft *available at*: http://eprint.iacr.org/2005/095 ("The standard for e-passport RFID chips (ISO 14443) stipulates ..."); Press release, *Texas Instruments to Deliver RFID Solution for MasterCard PayPass*, Texas Instruments, Jan. 17, 2005 *available at* http://www.ti.com/tiris/docs/news/news_releases/2005/rel01-17-05a.shtml ("Texas Instruments today announced plans to deliver ISO/IEC 14443 compliant radio frequency identification (RFID) chips …"); John G. Spooner, *Visa readies*

RFID is a generic category that encompasses many types of chips: some are passive (they are dormant until read at close range), some are active (they are always ready to be read at a greater distance), some offer plaintext or encrypted data in addition to authentication mechanisms (ISO 14443 A&B). What they have in common is that they use radio waves to request and transmit data, as opposed to contact cards, which require physical contact with a reader to receive and transmit information.

ISO 14443 is RFID. The flaws stated in the EPIC report regarding RFID are applicable to ISO 14443. First, tests have proved that ISO 14443 chips can be read at up to 30 feet away, not merely a few inches away.[6] Second, the ISO 14443 specifications state that the contents of the chips *can* be encrypted; it is not the case that they must be encrypted, much less encrypted well. Finally, to assume that because the contents of an ISO 14443 chip are safe from prying eyes because they are encrypted is as foolish as assuming that a house is able to withstand a stiff wind simply because it is built. It is as important to take into consideration how a cryptographic system is implemented as much as what components it is built from. A hastily built house of straw offers significantly less protection from intruders than one that is carefully built of brick.

Mr. Libin stated that the DAC does not use Bluetooth. Mr. Libin is correct, and we apologize for the error. However, the Department of Homeland Security, as reported in Mr. Libin's column and the CIO Insight article Mr. Libin previously referenced, is considering using Bluetooth-enabled card holders for the DAC.[7] The problems that the EPIC report stated concerning Bluetooth are applicable to these card holders. The central security flaw is in using Bluetooth at all in connection with the DAC. If the Bluetooth transmissions are not encrypted, it has been proved that anyone can access those transmission from up to a mile away.[8] If

wireless smart cards, CNET News.com Sept. 19, 2002 *available at* http://news.com.com/Visa+readies+wireless+smart+cards/2100-1017_3-958612.html ("The credit card company said Thursday that it plans to set up a new system that uses smart cards fitted with radio-frequency chips (sometimes called RF identification, or RFID, tags) … The new smart cards will use wireless chips that conform to an international wireless standard known as ISO 14443.").

[6] *See* Ziv Kfir and Avishai Wool, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, Feb. 22, 2005 *available at* http://eprint.iacr.org/2005/052; Scott Bradner, *An RFID warning shot*, Network World, Feb. 7, 2005 *available at* http://www.networkworld.com/columnists/2005/020705bradner.html.

[7] Emigh, *supra* note 5; Mark Baard, *RFID Invades the Capital*, Wired News, Mar. 7, 2005 *available at* http://www.wired.com/news/privacy/0,1848,66801,00.html?tw=wn_tophead_2.

[8] Humprey Cheung, *How To: Building a BlueSniper Rifle – Part 1*, Mar. 8, 2005 *available at* http://www.tomsnetworking.com/Sections-article106.php; Robert Siegel, Michele Norris and Melissa Block, *All Things Considered: 'Rifle' Sniffs*

they are encrypted, it would be harder to access the transmissions, but as with anything, not impossible.

Bluetooth is designed to enable two implementing devices to communicate with each other. As the use of weak (8-128-bit) encryption is optional, the technology itself could be vulnerable to unauthorized eavesdropping and proxy attacks.[9] As such, it is inappropriate to use Bluetooth in conjunction with an ID card intended for securing government resources.

Mr. Libin stated in his column that with the DAC, "[e]very time you scan your finger, the system only tries to match it to the already enrolled fingerprint securely stored on your card."[10] If DHS keeps an entire photo-realistic scan of your fingerprint in electronic format, that is a significant security flaw because new fingerprints can be created from that scan without you or your finger ever being there.[11] It would be more secure for DHS to store a mathematical calculation (called a hash), which is based upon a scan.[12]

Mr. Libin asked what it means for a biometric to be stolen.[13] The above fingerprint example is one way a biometric can be stolen. Another answer also lies in a previous EPIC report that Mr. Libin cited in his column. The problem is that Mr. Libin cited only part of a paragraph; the rest, which contains the answer to his question, states:

It would be difficult to remedy identity fraud when a thief has identification with a security-cleared federal employee name on it, but the thief's biometric identifier. Or, in a more innocuous scenario, the identities of employees with different security clearances and their biometric identifiers are mismatched in their files due to human or computer error. Allowing employees access to their records would help ensure the accuracy of the information collected and used.[14]

Out Vulnerability in Bluetooth Devices, NPR, Apr. 13, 2005, *available at* http://www.npr.org/templates/story/story.php?storyId=4599106.

[9] Ziv Kfir and Avishai Wool, *supra* note 6.

[10] Column at 2.

[11] *See* Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino, *Impact of Artificial "Gummy" Fingers on Fingerprint Systems*, Jan. 24, 2002 *available at* http://cryptome.org/gummy.htm.

[12] Eric Butterfield, *Biometrics finds its niche*, ZDNet, Sept. 24, 2002 *available at* http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2881275,00.html.

[13] Column at 2.

[14] Marc Rotenberg, EPIC Executive Director; Marcia Hofmann, Director: Open Government Project; Melissa Ngo, Staff Counsel, *Comments of the Electronic Privacy Information Center on Docket No. TSA-2005-20485*, at 8, Mar. 17, 2005 *available at* http://www.epic.org/privacy/biometrics/tsa_comments31705.html.

Mr. Libin's answer to EPIC's question of what happens if a biometric is stolen is to revoke the invalid card and issue a new card. EPIC agrees with this solution; however, there is the potential problem of the difficulty with which an employee would be able to prove his identity and that the biometric is false to his employer, and then receive a new card.

Mr. Libin and EPIC have a difference of opinion concerning the DAC's use of PINs. Mr. Libin stated that this is just another authentication choice for the system. But, the use of a short (4 to 6 character) PIN allows for a complete circumvention of biometric as an authentication device. It is the weakest link that breaks an otherwise secure system.

Finally, we would like an explanation as to why Mr. Libin made a full disclosure of his relationship with the Department of Homeland Security on his blog, but not on the CNET News.com column. Column readers as well as blog readers need to know all possible conflicts of interest. From the blog:

Full disclosure: although I am not directly involved in the DHS card program, DHS is a customer of ours and we are working on several products that will make use of the card. In other words, I may be biased but I kind of know what I'm talking about.

The main point of the EPIC report is that the federal government is spending a tremendous amount of money on these new systems of identification with little consideration of the security or privacy risks. The report seeks to highlight these problems. Mr. Libin stated, "Indeed, an ID card that uses RFID and Bluetooth is a really bad idea."[15] We agree with him. Such an ID card, like the DAC as initially proposed by the government, used with a Bluetooth card holder, is a really bad idea.

Sincerely,

Bruce Schneier
CIO, Counterpane Internet Security
EPIC Advisory Board Member

Melissa Ngo
EPIC Staff Counsel

[15] Column at 1.