THE PHYSICAL ACCESS SECURITY TO WSIS: A PRIVACY THREAT FOR THE PARTICIPANTS.

PRESS RELEASE, Immediate distribution
URL: http://www.contra.info/wsis | wsis@contra.info

PRESS CONFERENCE
Friday 12th December 2003 at 11.30 am
à « La Pastorale », Route de Ferney 106 à Genève
http://www.pressclub.ch/menu/sub_menu/adresse_csp.html

- **Ass. Prof. Dr. Alberto Escudero-Pascual**, Researcher in Computer Security and Privacy, Royal Institute of Technology, Stockholm, Sweden (EN, SP) Tel: + 41786677843,+46 702867989
- **Stephane Koch**, President Internet Society Geneva, Executive Master of Economic Crime Investigations, Geneva, Switzerland. (FR, EN) Tel: +41 79 607 57 33
- **George Danezis**, Researcher in Privacy Enhancing Technologies and Computer Security, Cambridge University, UK. (FR, EN, GR)

GENEVA, 10th DEC 2003

An international group of independent researchers attending the Word Summit on the Information Society (WSIS) has revealed important technical and legal flaws, relating to data protection and privacy, in the security system used to control access to the UN Summit. The system not only fails to guarantee the promised high levels of security but also introduces the very real possibility of constant surveillance of the representatives of the civil society.

During the course of our investigation we were able to register for the Summit and obtain an official pass by “just” showing a fake plastic identity card and being photographed (via a webcam), with no other document or registration number required to obtain the pass. The limited personal data required to produce the fake ID and thus register was easily obtained - a name from the WSIS website of attendees.

However this is only half of the story.

More photos of the WSIS Access Control

The official Summit badges, which are plastic and the size of a credit card, hide a “RF smart card” [1] - a hidden chip that can communicate its information via radio frequency. It carries both a unique identifier associated with the participant, and a radio frequency tag (RFID) that can be "read" when close to a sensor. These sensors can be located anywhere, from vending machines to the entrance of a specific meeting room allowing the remote identification and tracking of participants, or groups of participants, attending the event.

The data relating to the card holder (personal details, access authorization, account information, photograph etc.) is not stored on the smart card itself, but instead managed by a centralized relational database. This solution enables the centralized system to monitor closely every movement of the participants at the entrance of the conference center, or using data mining techniques, the human interaction of the participants and their relationship. The system can potentially be extended to track participants' movements within the summit and detect their presence at particular session.

Because all of the personal data is stored in a centralized database, any part of the database can be replicated locally, or transferred to future events - for example the next WSIS Summit hosted by the Tunisian authorities in 2005.

During the registration process we requested information about the future use of the picture and other information that was taken, and the built-in functionalities of the seemingly innocent plastic badge. No public information or privacy policy was available upon our demands, that could indicate the purpose, processing or retention periods for the data collected. The registration personnel were obviously not properly informed and trained.

Our main concern is not only that the Summit participants lack information about the functionalities of this physical access system implemented, or that no one was able to answer questions of how the personal data would be treated after the Summit. The big problem is that system also fails to guarantee the promised high levels of security while introducing the possibility of constant surveillance of the representatives of civil society, many of whom are critical of certain governments and regimes. Sharing this data with any third party would be putting civil society participants at risk, but this threat is made concrete in the context of WSIS by considering the potential impact of sharing the data collected with the Tunisian government in charge of organizing the event in 2005.

That a system like this gets implemented without a transparent and open discussion amounts to a real threat for the participants themselves, and for our Information Society as a whole.

More information is available at:
http://www.contra.info/wsis wsis@contra.info

NOTES TO EDITORS

- The World Summit of Information Society has contracted SportAccess, a Company of Kudelski Group, as the main responsible of an integrated solution for physical access control solution during the United Nations Summit of Information Society. The MultiSpAK system has already been deployed in other meetings as the World Economic Forum in previous years and was globally designed and developed by NagraCard and NagraID.
- The procedures of how personal data is being handled during WSIS break the principles of the Swiss Federal Law on Data Protection of June 1992 [2], the European Union Data Protection Directive 95/46/EC [3] and the United Nation guidelines concerning Computerized personal data files adopted by the General Assembly on December 1990.
- The Electronic Privacy Information Center [1] has an extensive news archive and background material on the subject of privacy threats and RFtags. Usage of RFtags in supermarkets, to tag products for purposes of stock management and security, has already attracted oppositions on privacy grounds by CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) [5] and has lead to campaigns for customer boycott of tagged products [6].

REFERENCES

[1] Electronic Privacy Information Center Website about RFID Identification http://www.epic.org/privacy/rfid/

[2] Swiss Federal Law on Data Protection, http://www.edsb.ch/e/gesetz/schweiz/index.htm

[3] European Union Data Protection Directive,

http://europa.eu.int/comm/internal_market/privacy/index_en.htm

[4] Guidelines for the Regulation of Computerized Personal Data Files, http://www.unhchr.ch/html/menu3/b/71.htm

[5] - http://www.nocards.org/AutoID/overview.shtml
[6]The Boycott Gillette Campaign - http://www.boycottgillette.org/