



Solidarity, Independence, Democracy

SID :
Independent Trade Union of EU
Institutions Staff

Building: BECH - Kirchberg
Office: A3/166 or B2/327
tel. (+352) 4301-33907 / 33567
fax (+352) 4301-32999
e-mails: reza.fardoom@ec.europa.eu
michael.ashbrook@ec.europa.eu

15/11/2007

Democracia Ltd.



Abuso de la RFID

Durante el primer día del CeBIT 2007, Viviane Reding , Comisaria responsable de la Información, dijo " Cuando vengo a CeBit la gente me pregunta ¿Qué reglamento va usted a proponer hoy? Y continuó diciendo "no traigo ningún reglamento, no debemos sobre-regular RFID. Tan sólo tenemos que dar a la industria una seguridad legal".

Ref:

http://scenariothinking.org/wiki/index.php/Viviane_Reding's_speech_on_ubicomput_during_the_first_day_of_CeBIT_2007

En un futuro inmediato, podremos ser vigilados gracias a que vestiremos, comeremos y portaremos objetos que han sido diseñados concienzudamente para tal propósito.

El nombre genérico para este tipo de tecnología es RFID, que significa Identificación por Radio Frecuencia.

Las tarjetas RFID son minúsculos microchips, reducidos ya al tamaño de la mitad de un grano de arena.

Permanecen a la escucha de ciertas frecuencias de radio a las que responden transmitiendo su unívoco código de identificación.

La mayoría de las tarjetas RFID no tienen batería: Para transmitir su respuesta, utilizan la energía de la señal de radio inicial.

Todos deberemos familiarizarnos con la tecnología RFID puesto que muy pronto vamos a oír hablar mucho de ella.

Las actividades de vigilancia pueden basarse en buenas intenciones y ser beneficiosas. Pueden ser necesarias o deseables, por ejemplo para combatir el terrorismo y el crimen, para mejorar el control de acceso a servicios públicos y privados, y para mejorar los cuidados sanitarios.

Pero, una vigilancia invisible, incontrolada o excesiva puede crear un clima de sospecha y minar la confianza mutua. Puede crear serios problemas para ciertas personas - exclusión social, discriminación y un impacto negativo en sus vidas.

Desgraciadamente los modos de vigilancia predominantes en el siglo XXI producen situaciones en las cuales se aumentan e institucionalizan las distinciones por motivos de clase, raza, género, geografía y ciudadanía.

Los expertos predicen que los empleados se verán sujetos a barreras biométricas y pruebas psicológicas para determinar sus capacidades.

Quienes se nieguen a someterse a las pruebas o quienes sean considerados no saludables no obtendrán el empleo.

¿Deberían usarse los identificadores de radiofrecuencia en las tarjetas de identificación?

¿Servirá la RFID integrada en las tarjetas de identificación para facilitar la suplantación de la identidad?

Mientras que unos alaban la tecnología como una excelente forma para proteger a las personas, otros la califican de una pesadilla para la seguridad.

El Senador por el estado de California, Joe Simitian, dijo en Octubre de 2007 "Esto parece escrito por Orwells", pero es real, y ahora es el momento de hacerle frente.

No podemos permitir que los patronos "etiqueten" a sus empleados.

Hay otras formas de mantener la seguridad de las propiedades físicas e intelectuales de una empresa – desde luego no debe hacerse a costa del derecho de las personas a su privacidad.

Ref: <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=202402856>

El programa de televisión Holandés "Nieuwslicht" en cooperación con la firma Riscure consiguió descifrar un pasaporte prototipo holandés provisto de RFID.

En este caso, el intercambio de datos entre el lector RFID y el pasaporte, pudo ser interceptado, registrado y posteriormente, en tan solo 2 horas, se pudo averiguar la contraseña con la ayuda de un ordenador personal, obteniendo un completo acceso a la huella digital, fotografía y otros datos tanto encriptados como en formato de texto procedentes de la tarjeta RFID – todo dispuesto para crear un pasaporte clonado.

El fallo, al menos en parte, se debe al algoritmo usado al generar la clave secreta que debe proteger los datos.

Se puede predecir la clave dado que se construye a partir de la fecha de expiración del pasaporte, la fecha de nacimiento, el número de pasaporte y un dígito de control.

Ref: <http://www.engadget.com/2006/02/03/dutch-rfid-e-passport-cracked-us-next/>

Una firma consultora de seguridad informática en Alemania ha demostrado que puede clonar los pasaportes electrónicos que los Estados Unidos y otros países han empezado a distribuir este año.

Los controvertidos pasaportes electrónicos contienen un chip de identificación de radio frecuencia, o RFID, que el Departamento de Estado de los EE.UU., entre otros, afirma contribuye a evitar la falsificación del documento.

Pero Lukas Grunwald, consultor de seguridad de DN-Systems en Alemania y experto en RFID, dice que los datos del chip pueden copiarse fácilmente.

"Todo el diseño del pasaporte es débil", dice Grunwald.

"Desde mi punto de vista todos estos pasaportes RFID son una enorme pérdida de dinero. No aumentan la seguridad en absoluto.

Ref: <http://www.wired.com/news/technology/0,71521-0.html?tw=rss.index>

Los Microchips RFID biométricos de transferencia a distancia en un pasaporte británico aportan los mismos riesgos para la privacidad y seguridad que los pasaportes biométricos de los Estados Unidos, haciéndonos más vulnerables a criminales y terroristas que usando los conocidos microchips de tarjeta "de contacto", por ejemplo los de las tarjetas de crédito, etc.

Ref:

http://www.rfidbuzz.com/news/2005/spy_blog_contactless_rfid_biometric_passports_in_the_uk_same_risks_as_us_rfid_passports.html

Es difícil de imaginar el maremagnum de escenarios legales que se pueden generar.

Los futuros casos de divorcio pueden generar que una parte pida los registros RFID para probar que el cónyuge estuvo a una hora concreta en un lugar determinado.

Los ladrones en el futuro podrían buscar por las calles, con la ayuda de detectores RFID, tarjetas en contenedores de basura que indiquen la presencia cercana de caros equipos electrónicos. En todos estos casos, la posibilidad del anonimato queda mermada.

Las tarjetas RFID son, en su conjunto, un desarrollo útil y una tecnología provechosa. Permiten a los comerciantes reducir los niveles de inventario, evitar robos, que cierto grupo industrial estima en 50.000 millones de dólares anuales.

Con tarjetas RFID generando eficiencia económica para las empresas, los consumidores seguramente terminen teniendo más opciones y más baratas. Además, ¿no sería cómodo coger los productos de la tienda y simplemente salir por la puerta con el importe de la compra cargado en la, esperemos que segura, tarjeta de crédito RFID?

La amenaza a la privacidad empieza cuando las tarjetas RFID continúan activas al salir de la tienda.

Esa es la situación que debería hacer saltar las alarmas – y en estos momentos la industria de RFID no está dando claras señales de si las tarjetas se desconectarán o se dejarán en funcionamiento por defecto.

La Comisión Europea también reconoce algunos de estos riesgos

Ref:

http://www.cc.cec/home/dgserv/jrc/dwnld/docs/dss/ipr/presentations/200504_ep_wilikens.pdf

El comunicado del Sr. Kallas a los miembros de la Comisión en Marzo, indicaba que la Comisión está considerando el uso de tarjetas con identidad biométrica para identificación de seguridad personal.

Ref:http://www.cc.cec/sq_vista/cgi-bin/repository/getdoc/COMM_PDF_C_2007_0797_1_XX.pdf

¿ Está usted seguro de que la Comisión Europea nunca usará RFID con usted ?

¿ Está usted seguro de que no han empezado ya ?



Senador por el Estado de California Joe Simitian, prominente crítico contra la RFID



Comisaria Vivienne Reding, promotoroa de la RFID