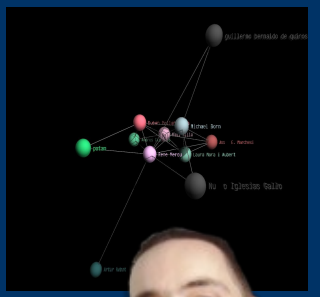
GnuPG + Coloquio privacidad



Juan MartínezRené Mérou
h.says.it

- Ideas para contagiar la defensa de la privacidad.
- Intro al GnuPG
- Anillos de claves
- Signing parties - cómo participar.

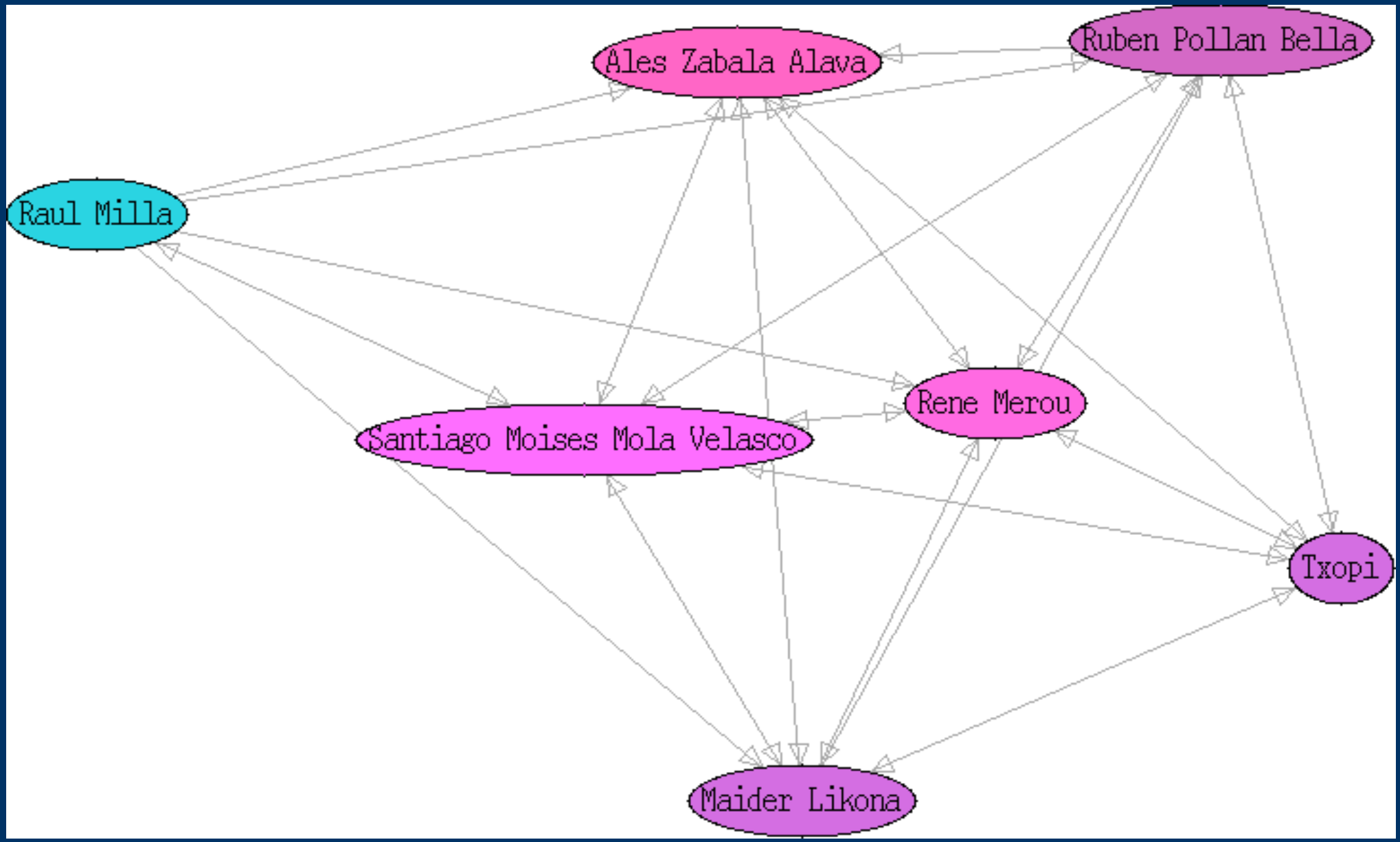
IV Jornadas por el Software libre de Elche

Rápida introducción al GnuPG

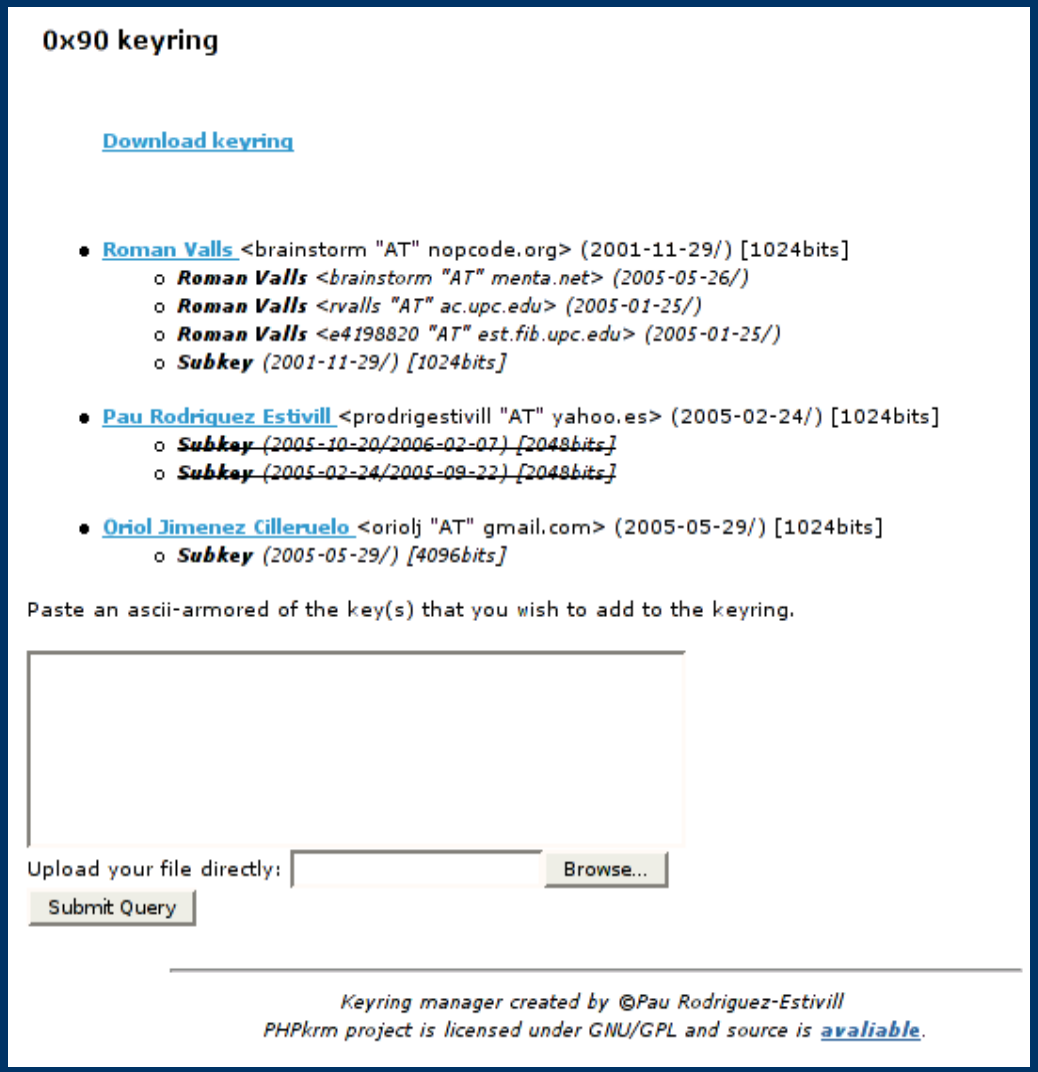
- gpg –gen-key asimétrica, par de claves, revocar ...
- gpg --output cert_revoc_arch.asc --gen-revoke -armor aa8e6a57
- gpg --send-keys aa8e6a57
- gpg --recv-keys aa8e6a57
- gpg --fingerprint aa8e6a57
- gpg --sign-key aa8e6a57 gpg --edit-key aa8e6a57 entonces lsign, adduid
- gpg –refresh-keys

Ref.: http://bulma.net/body.phtml?nIdNoticia=1684

Signing Parties:
Gráfico 2D de la red de confianza HM2006



Llaveros/anillos de claves/llaves



-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: AsterX phpkrm keyring at https://asterx.upc.es/keyrings/AsterX

mQGiBEIduQ4RBADZUNW8omhveuh/K2NXDm/bu1v9Lc8mKHr9gde6OLbIar/w7ewg
6L/Czonp8G6Ojm3qm17CQUOZlAaBmFO1M4Cm8oe30THLd3ZWBOAid1ksypZ8/o6u
jrLb880JS03yZOPCRm31Af0cGYxyeojxSwBa7hLaXcIFgSNyWpR6SnaALwCg7WA/
ysax+XSo0ieTnq4hG0jFeuUEAJzdiZQqfOc2YUUPs6x/ctSzK9JvMUrJ2cO0dZRu
FrcgQRB/2Gct70TsFBg5OW5FqB/QWfncvKbzzBSJiPe4IsquUdPZfA/IBL/9hDBH

. . .

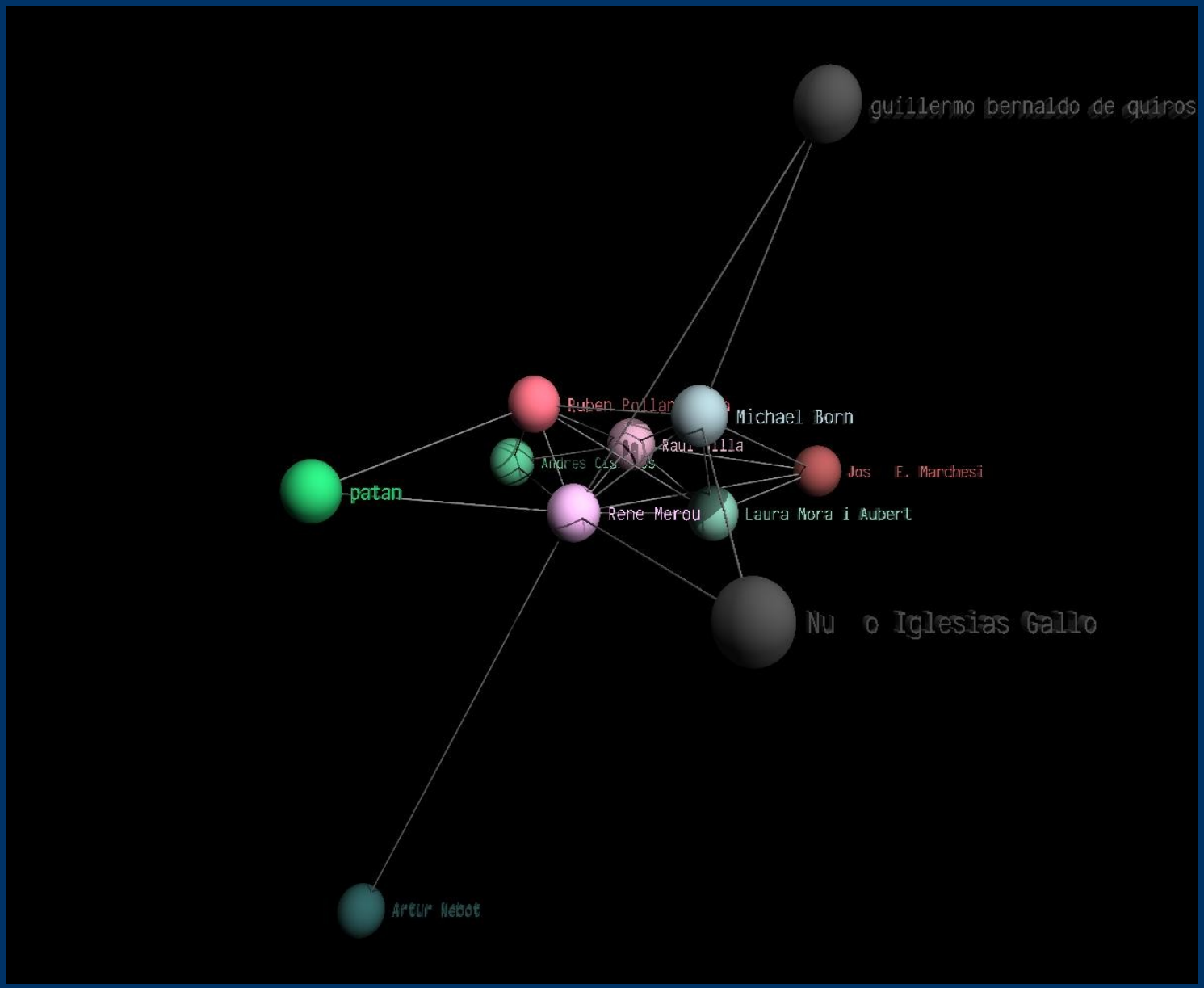
sgfXpFLzD8D4Z6zuvvL1hZPT6NgM1ad6p0E+h8yleDRm2cv6Bny6wRoKEFAl6DCs
ZAMNw3T03/mkzWFdunT4moKtkvlQCbaU+yAEP12gqMh+Y03iaZh7zGbzeobHRIhM
BBgRAgAMBQJA1BtgBRsMAAAAAAoJENkcS8QkiwGtTXkAoMEkfTR3YFAgjo2pgb2u
kLtkLAT6AJwML90/IIZLAVVooNgT5zpRoo0FxA==
=zlrI
-----END PGP PUBLIC KEY BLOCK-----

http://asterx.upc.es/keyrings/source/INFO.TXT

gpg --no-default-keyring --keyring bulmaring.gpg --recv-key 2DA367B7 67d8e867

gpg --no-default-keyring --keyring bulmaring.gpg --export -a > llavero

Signing Parties:
Gráfico 3D de la red de confianza HM2005



Signing Parties: Organización modelo Participando

- Participando en el Grupo
  - ¿Qué preparar?
  - ¿Por qué no llevar PCs?
  - ¿Qué hacer después?

Signing Parties - Referencias

- GPG Keysigning Party HOWTO
  http://www.cryptnet.net/fdp/crypto/gpg-party.html
- GnuPG Grupos de Firmas (Keysigning Party) COMO
  http://www.gnupg.org/howtos/es/gpg-party.html
- Debconf 5 (Helsinki) http://debconf.org/debconf5/
- 21C3 GPG Key Signging Party
  http://21c3.ccc.de/wiki/index.php/GPG_Key_Signing_Party

Herramientas PGP

- apt-get install signing-party
  - Pequeño manual traducido al español y catalán:

  http://pgp-tools.alioth.debian.org/index.html.es
- caff <options> `cat ksp-fingerprints.txt`

Valores

- ¿Cómo promocionar el valor de la privacidad?

  Los valores humanos no siempre es fácil comunicarlos =>

  - Usa el contagio.
  - Pídeles ayuda para resolver el problema, lo entienden antes, lo hacen/reconocen suyo y hacen equipo contigo.
  - Yo uso la historia de la ciencia para demostrar que

Sin privacidad no hay libertad

Valores
Panorama Personal

- Texto borrado en Word - Iraq -
- Timofónica - Mis datos-
- Vodafone - Siiii, no se preocupe -
- Bancos - Listas negras -
- Títulos DVDs - Viajan por internet

Valores
Panorama Profesional

- Comercio
- Ventaja técnica - Enviar un password -
- Navegación - Logeada -
- Obligación de entregar la clave privada si la piden

Valores Privacidad

Durante la charla mostré un par de imágenes de la revista de este mes *muy interesante* que vi en el aeropuerto:

1- Funcionalidades e Inseguridad

Imagen de gente vestida con ropa trasparente vigilada por escesivas cámaras (Al princípio de la revista). Para poder introducir el valor de la privacidad y la sensibilidad necesaria.

2- Biochips y Gattaca

Imagen de un grupo de personas con tablas con pixels de colores indicando genes o marcadores químicos. Es un perfecto ejemplo de lo que nos puede llevar la falta de privacidad y el dejar la funcionalidad sobre los valores humanos. Gattaca es una película muy buena para entender el problema.

Para ver las imágenes ir directamente en la revista o a su web:
http://www.muyinteresante.es/intro_port.htm

(por cierto que la revista usa una foto de stallman para hablar de altruismo y usa una definición de la wikipedia)

Más información tambien en el blog de carmen: http://ceugenio.wordpress.com/2006/12/04/iv-jornadas-de-software-libre-en-elx-elche/

Valores Privacidad

- Coste de tus datos en internet

Data	Amount
Address	$0.50
Phone number	$0.25
Unpublished phone number	$17.50
Cell phone number	$10
Date of birth	$2
Social Security number	$8
Driver's license	$3
Education	$12
Credit history	$9
Bankruptcy details	$26.50
Lawsuit information	$2.95
Sex offender	$13
Workers' comp history	$18
Military record	$35

http://turbulence.org/Works/swipe/calculator.htm

Valores Privacidad

- brechas seguridad (captura de la web de Zone-h)

Full list of Security Breaches from February 15th 2005 to July 7th 2006 :

DATE MADE PUBLIC	NAME (Location)	TYPE OF BREACH	NUMBER
Feb. 15, 2005	ChoicePoint (Alpharetta, GA)	Bogus accounts established by ID thieves	145,000
Feb. 25 , 2005	Bank of America (Charlotte, NC)	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx (Miramar, FL)	Exposed online	25,000
March 8, 2005	DSW/Retail Ventures (Columbus, OH)	Hacking	100,000
March 10, 2005	LexisNexis (Dayton, OH)	Passwords compromised **UPDATE** (06.30.06): Last week, five men were arrested in connection with this breach.	32,000
March 11, 2005	Univ. of CA, Berkeley (Berkeley, CA)	Stolen laptop	98,400
March 11, 2005	Boston College (Boston, MA)	Hacking	120,000
March 12, 2005	NV Dept. of Motor Vehicle	Stolen computer, later recovered.	[8,900] Not included in total below
March 20, 2005	Northwestern Univ. (Evanston, IL)	Hacking	21,000
March 20, 2005	Univ. of NV., Las Vegas (Las Vegas, NV)	Hacking	5,000
March 22, 2005	Calif. State Univ. (Chico, CA)	Hacking	59,000
March 23, 2005	Univ. of CA. (San Francisco, CA)	Hacking	7,000
March 28, 2005	Univ. of Chicago Hospital (Chicago, IL)	Dishonest insider	Unknown
April ?, 2005	Georgia DMV	Dishonest insider	465,000
April 5,	MCI	Stolen laptop	16,500