

**5A A2S**

**Sécurité des Serveurs :  
Sécurité des SGBD**

**Année 2014/2015**

**B. Nguyen**

**[benjamin.nguyen@insa-cvl.fr](mailto:benjamin.nguyen@insa-cvl.fr)**

# Plan

- Menaces et législation
- Attaques
  - Injection
  - Buffer Overflow
  - Attaques Statistiques
- Contrôle d'accès *et d'usage*
  - Modèles DAC, MAC, RBAC, *UCON*
  - implémentation dans les BD relationnelles
- *Protection cryptographique des bases de données*
- *Protection matérielle des bases de données*
- Autres formes de protection des données
  - *Audit*
  - Anonymisation de données
  - *Tatouage de BD*

# Les menaces

# Où/par qui nos données sont-elles stockées ?

- Des données disséminées partout, parfois silencieusement
  - SI nationaux (Impôts, fichiers de police, BaseEcole, DMP ...)
    - Les plus encadrés car focalisent toute l'attention
  - SI d'entreprise (employeurs, assurances, EDF ...)
  - BD personnelles (factures, fichiers perso ...)
  - BD "ambiantes" (Pass Navigo, Telco, télé-surveillance, log de requêtes Web ...)
- Des données bien organisées
  - Données centralisées, structurées, cohérentes, à jour
  - Facilement accessibles, exploitables, croisables
  - donc intéressantes !
  - Et ce qui est intéressant pour le gestionnaire l'est pour l'attaquant

# Sont-elles bien protégées ?

- **La négligence à l'origine de nombreux trous de sécurité**
  - 490.000 Bases de Données sans protection sur le Web (D. Litchfield, nov 07)
  - Données personnelles de 25 Millions de contribuables Anglais égarées (BBC, nov 07)
  - Données de 70 Millions de vétérans US égarées (DataLossDB, oct 09)
  - Achats d'or des clients du CIC (Canard enchaîné, déc 2011)
  - Playstation network hack : 77 million d'utilisateurs, infos perso et bancaires (2011)
  - LinkedIn (6.5 million de personnes, 2012)
  - eBay (145 millions de personnes, 2014)
  - Sites : Zataz.com, datalossdb.org, etc...
- **Même les sites les plus sûrs sont piratés**
  - FBI, NASA, Pentagone n'échappent pas à la règle
  - Rapport annuel CSI/FBI
    - Les SGBD constituent la 1<sup>ère</sup> cible des attaques
    - 45% des attaques sont internes

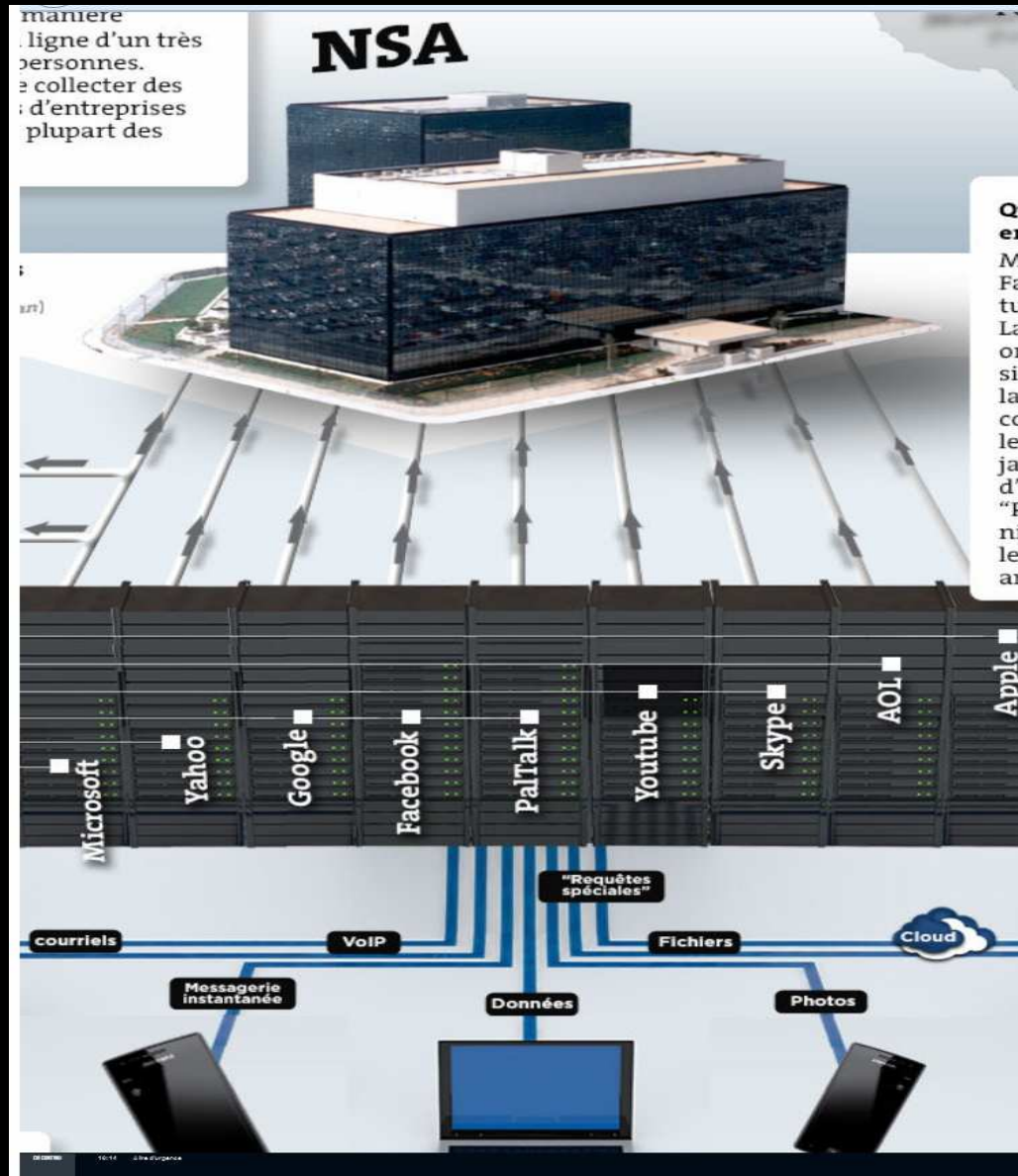
# Existe-t-il une parade technique fiable ?



ORACLE®

- Le côté 'Unbreakable' a attiré les Hackers (2002)
  - Les tentatives d'attaque sur Oracle ont augmenté de 30,000 per week.
- Quelques jours plus tard ....
  - 'When they say their software is unbreakable, they're lying.'
  - Bruce Schneier
  - David Litchfield (chercheur anglais en sécurité) a montré qu'un buffer overflow existait dans le serveur Oracle.
  - [http://www.theregister.co.uk/2002/02/07/how\\_to\\_hack\\_unbreakable\\_oracle/](http://www.theregister.co.uk/2002/02/07/how_to_hack_unbreakable_oracle/)
  - N'existe plus depuis 2005 ...

# Et le problème est-il uniquement technique ?



# Qui est responsable ?


- Dilution des responsabilités

- Hébergement de données: un modèle qui tend à s'imposer aux particuliers, aux entreprises, aux administrations
- Vulnérabilité aux attaques internes
  - *Dossiers médicaux menacés de publication par l'employé d'un sous-traitant Pakistanais d'un hôpital Californien (San Francisco Chronicle)*
- Quelle législation appliquer ?
- Flou des chartes de confidentialité
  - *“We will not share your health data with individuals or third parties unless you explicitly tell us to do so or except in certain limited circumstances described in our [privacy policy](#). “*
  - *“Certain features of Google Health can be used in conjunction with other Google products, and those features may share information to provide a better user experience and to improve the quality of our services. “*
- Et aussi : rachat de sociétés, changement de législation, pressions gouvernementales



# Mais qui s'intéresse à ces données ?

## ... Pourquoi des attaques ?



[Login to Intelius](#) | [Manage Account](#)  
 Customer Service: 425.974.6100 | [View My Reports](#)

| Verification Services       | Information Services   | Protection Services     | Business Services           |
|-----------------------------|------------------------|-------------------------|-----------------------------|
| Background Information      | People Search          | IDWatch                 | Employee & Tenant Screening |
| Phone Number Verification   | Search By Phone Number | Background Check        | DMV Driving Records         |
| Property & Area Information | Criminal Records       | All Products & Services | Batch & Lead Generation     |


### Background Check

Personal Background Check
Employment Background Check

First Name  MI  Last Name  State Select a State

Current/Previous Address (Optional)  City (Optional)

SEARCH



**The right knowledge can make all the difference.**

That's why millions of people rely on Intelius to deliver the information they need to protect their interests and maneuver in a complex world.

**Background Check By Social Security Number**

Background Check Includes: Criminal report, sex offender check, lawsuits, judgments, liens, bankruptcies, home value & property ownership, 30 year address history,

Que voulez-vous savoir sur vos amis, voisins, nourrice, employés, assurés ...?

# Le marché des données personnelles

**Search Summary**

|                |                                    |
|----------------|------------------------------------|
| <b>Name</b>    | Lori Ortiz                         |
| <b>Aliases</b> | 1) Lorry Ortiz<br>2) Samatha Ortiz |
| <b>Age</b>     | 37                                 |

**REPORT CONTENTS**

- Address History
- Single State Criminal Check
- Single State Civil Judgments
- Property Report
- Personal Pub
- Area Sex Off
- Relatives and
- People Search

| OFFENSE             |    |
|---------------------|----|
| <b>Court Name</b>   | SP |
| <b>Case Number:</b> | CC |
| <b>Offense ID</b>   | W  |
| <b>Offense Date</b> | 12 |
| <b>Offense Code</b> | 42 |
| <b>Offense</b>      | DI |

**Background Report**

Includes all 3 records for **Dennis Shasha** in **New York, NY**.

**Report includes: (when available)**

- ✓ Full Name
- ✓ Age & DOB
- ✓ Relatives
- ✓ Avg. Income
- ✓ Criminal Check
- ✓ Liens
- ✓ Aliases
- ✓ Neighbors
- ✓ Marriage
- ✓ Address
- ✓ Phone Number
- ✓ Address History
- ✓ Property
- ✓ Bankruptcies
- ✓ Judgments
- ✓ Lawsuits
- ✓ Death Records
- ✓ Divorce

[View Sample](#)

**Possible Relatives and Associates**

| Name         | Address   | Phone          | Background        |
|--------------|---|----------------|-------------------|
| BRENDA ORTIZ | 13014 STOCKPORT ST<br>REDMOND, WA 98052<br><b>Property Report</b> | (425) 663-XXXX | <b>Background</b> |
| TODD ORTIZ   | 98 EDGAR ST.<br>BELLEVUE, WA 98005<br><b>Property Report</b>      |                |                   |

**Property Report**

|                  |                                   |
|------------------|-----------------------------------|
| Property Address | 18565 SE PL<br>Bellevue, WA 98005 |
| Owner Name       | ORTIZ LORI                        |

**\$39.95**

**\$10 off**

**Special Price!**  
[Learn More](#)

**Add to Cart**

**With FREE Identity Protect Trial**

| Neighbor        | More Reports      | Address                                 | Phone #        | From       | To         |
|-----------------|-------------------|---|----------------|------------|------------|
| NANCY RODRIGUEZ | Background Report | 525 108TH AVE. SE<br>BELLEVUE, WA 98005 | (425) 555-XXXX | 03/29/2003 | 08/21/2006 |
| JOHN GATES      | Background Report | 419 108TH AVE. SE<br>BELLEVUE, WA 98005 | (425) 949-XXXX | 12/10/2002 | 08/21/2006 |

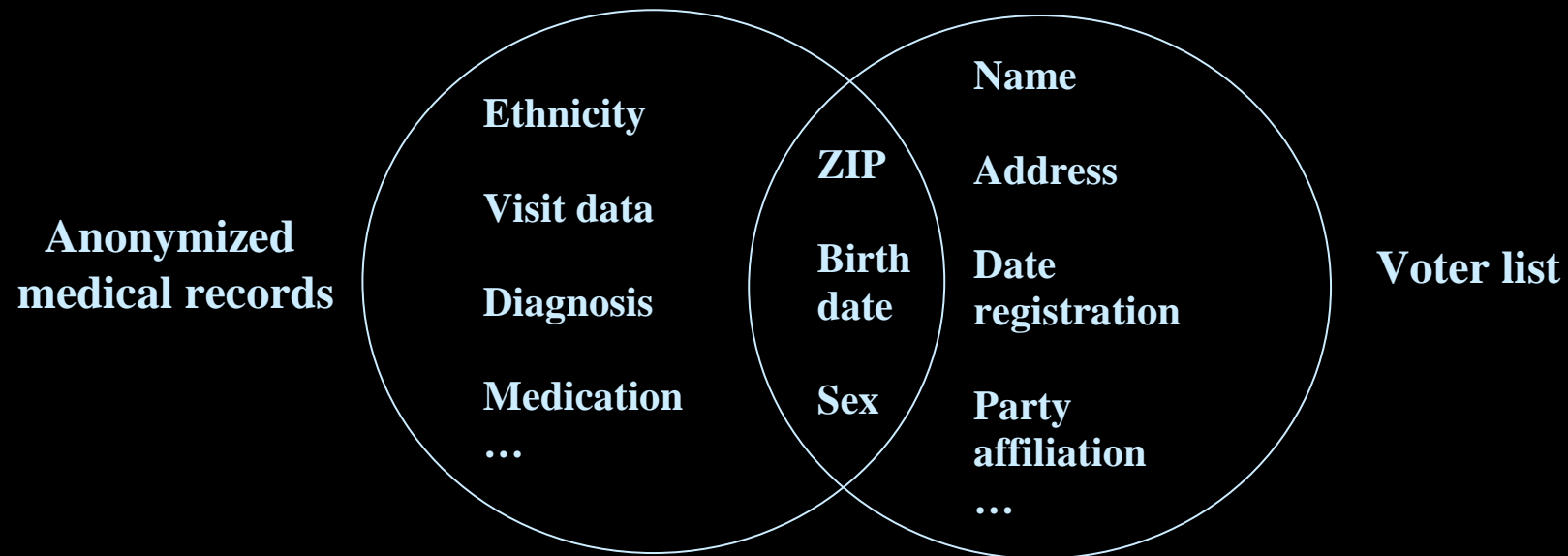
|             |           |
|-------------|-----------|
| Total Value | \$400,000 |
| Tax Amount  | \$2,557   |

« The data within the report is compiled from thousands of different sources that include government, property, and other public record repositories. »

Et la parade (lucrative) s'organise => ORM (Online Reputation Manager) e.g. reputation.com

# Un risque démultiplié par l'Open Data

- Anonymiser (pseudonymiser) les données ne suffit-il pas ?
- L'existence de quasi-identifiants permet de croiser des sources anonymisées avec d'autres qui ne le sont pas



- « 87% of the population in the US had characteristics that likely made them unique based only on {5-digit Zip, gender, date of birth} » [Sweeney, 2002]
- Antagonisme entre anonymisation et usage

# Généralité du problème

- La préservation de la vie privée est un problème emblématique
- Quid de la protection des données industrielles, commerciales, artistiques, administratives, militaires, diplomatiques ... ?
  - Se prémunir contre les fuites de confidentialité mais également contre la falsification, la destruction, la copie et plus généralement l'usage illicite
- Peut-on sécuriser efficacement ?
  - Pas de sécurité ultime
  - Une équation économique : Coût / Bénéfice de l'attaque
  - ... et sociologique : risque législatif / Bénéfice de l'attaque

**Que dit la législation ?**

# Nature des infractions de la cybercriminalité

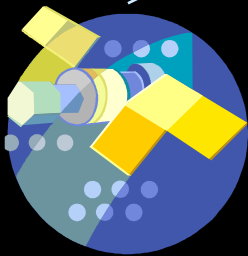
## Cybercriminalité

Infractions pour lesquelles les Technologies de l'Information et de la Communication (TIC) sont l'objet même du délit

Infractions pour lesquelles l'Internet est le moyen de commission

Caractéristiques : nature des technologies utilisées

Caractéristiques : criminalité de droit commun, de nature juridique traditionnelle



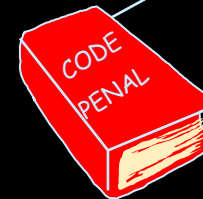
Infractions liées à la télécommunication



Infractions liées à la téléphonie cellulaire



Infractions informatiques



Infractions prévues par le code pénal



Infractions prévues par des textes spécifiques

# Infractions pour lesquelles l'Internet est le moyen de commission

- Les atteintes aux libertés individuelles
  - Diffamation et injure
  - Atteintes à la vie privée
  - Haine raciale, négationnisme, révisionnisme
- Les atteintes aux biens
  - Escroquerie
  - Menace de commettre une destruction, une dégradation ou une détérioration
- Les atteintes à l'ordre public
  - Protection des mineurs
  - Terrorisme
  - Paris clandestins et Jeux d'argent
- Les infractions au code de la propriété intellectuelle
  - contrefaçon

# Infractions pour lesquelles les TIC sont l'objet du délit : loi Godfrain, 5 janvier 1988

- Intrusion ou maintien frauduleux dans un système de traitement automatisé de données (STAD) == SGBD !
  - 1 an d'emprisonnement et 15 000 € d'amende
  - 2 ans d'emprisonnement et 30 000 € d'amende s'il ya dommage
- Supprimer, introduire ou modifier frauduleusement des données dans un STAD et/ou tenter d'entraver son fonctionnement
  - 3 ans d'emprisonnement et 45 000 € d'amende
- Détenir, offrir, céder ou mettre à disposition un équipement, programme informatique ou toute donnée en vue de commettre les infractions sus-citées
  - article 323-3-1 du code pénal (Loi sur l'économie numérique du 24 juillet 2003)
  - Peine en fonction de la nature de l'infraction
- Association de malfaiteurs
  - Article 323-4 du code pénal
  - Peine en fonction de la nature de l'infraction



# Législation internationale concernant la protection<sup>17</sup> des données à caractère personnel

- Situations très différentes selon les pays
- USA dotés d'une législation sectorielle
  - **Right to Financial Privacy Act, 1978**
  - **Health Insurance Portability and Accountability Act, 1996**
  - **Children's Online Privacy Protection Act, 1998**
  - ...
- Union Européenne dotée d'une législation globale
  - **Data Protection Directive 95/46/EC, 1995**
  - **Nouvelle réglementation européenne (General Data Protection Regulation, encore en cours de réalisation...)**
  - **Agences nationales (ex: CNIL) imposant l'enregistrement des bases de données et la déclaration préalable des traitements**
- Principe de « Safe Harbor » permettant l'échange d'information avec des entités hors UE tout en offrant des garanties fondamentales de préservation de la confidentialité

# Principes généraux de la directive 95/46/EC

- *Finalité*

- les **finalités** des traitements doivent être **légitimes, explicites et déterminées** lors de la collecte des données. Un traitement ultérieur à des fins **historiques, statistiques ou scientifiques** n'est pas réputé incompatible pour autant que les Etats membres prévoient des **garanties appropriées**. La **période de conservation** des données sous une forme permettant l'identification des personnes concernées **ne doit pas excéder la réalisation des finalités** pour lesquelles elles sont collectées.

- *Information et consentement*

- La personne reçoit toutes les informations concernant la finalité de la collecte et le traitement ne peut être effectué que si elle donne son **consentement explicite et éclairé**.

# Principes généraux de la directive 95/46/EC

- *Droit d'accès*

- la personne concernée a le droit d'obtenir la confirmation que ses données font, ou non, l'objet d'un traitement et peut demander la rectification, l'effacement et le verrouillage de données lorsque le traitement n'est pas conforme à la directive.

- *Exactitude*

- Les données doivent être exactes, à jour et non excessives au regard des finalités pour lesquelles elles sont collectées.

- *Non discrimination*

- Tout traitement portant sur des catégories particulières de données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale d'une personne sont interdits.

# Principes généraux de la directive 95/46/EC

- *Sécurité*
  - le responsable de traitement doit assurer la sécurité des données contre toute destruction accidentelle et l'accès non autorisé.
- *Transfert vers des pays tiers*
  - Principe de Safe Harbor.
- *Dérogation*
  - Intérêts vitaux de la personne, intérêt public, sécurité nationale, recherche scientifique ...
- *Champ d'application*
  - au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

# La législation face à la réalité (ex 1 : droits d'accès)

| Catégorie de document   | Annuaire IPR<br>1944<br>199-426<br>Code<br>CLASS A | Annuaire OIF<br>1944<br>197-423<br>Code<br>CLASS A | Régimes de cotisations (Maladie, invalidité, vieillesse) - 23, 40, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000 |      | Ergonomie (activité de diagnostic) |      | Chirurgie (activité de diagnostic) |      | Soins infirmiers |      | Pharmacie (activités de diagnostic) |      | Radiologie |      | Diagnostiqueur |      | Technicien d'imagerie médicale |      | Anesthésie-réanimation, Pathologie, Diététique |      | Prévention et promotion |      | Médicament (activité de diagnostic) |  |
|---|--|--|---|------|------------------------------------|------|------------------------------------|------|------------------|------|-------------------------------------|------|------------|------|----------------|------|--------------------------------|------|--|------|-------------------------|------|-------------------------------------|--|
|   |  |  | L10   | L10B | L10C                               | L10D | L10E                               | L10F | L10G             | L10H | L10I                                | L10J | L10K       | L10L | L10M           | L10N | L10O                           | L10P | L10Q   | L10R | L10S                    | L10T | L10U                                |  |
| <b>DOMAINE D'IDENTIFICATION</b>   |  |  |   |      |                                    |      |                                    |      |                  |      |                                     |      |            |      |                |      |                                |      |  |      |                         |      |                                     |  |
| Identification de l'état  |  |  | X   | X    |                                    | X    |                                    | X    |                  | X    |                                     | X    |            | X    |                | X    |                                | X    |  | X    |                         |      |                                     |  |
| <b>DOMAINE MEDICAL GENERALISTE</b>  |  |  |   |      |                                    |      |                                    |      |                  |      |                                     |      |            |      |                |      |                                |      |  |      |                         |      |                                     |  |
| Antécédents médicaux et chirurgicaux personnels, symptômes (y compris certains de l'ICD), anamnèse médicale |  | 10, 11, 12   | 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120  | X    | X                                  | X    | X                                  | X    | X                | X    | X                                   | X    | X          | X    | X              | X    | X                              | X    | X  | X    |                         |      |                                     |  |
| Historique des consultations médicales et chirurgicales   |  | 13   | 121   | X    | X                                  | X    | X                                  | X    | X                | X    | X                                   | X    | X          | X    | X              | X    | X                              | X    | X  | X    |                         |      |                                     |  |
| Allergie et intolérances alimentaires, médicaments  |  | 14   | 1038, 1039  | X    | X                                  | X    | X                                  | X    | X                | X    | X                                   | X    | X          | X    | X              | X    | X                              | X    | X  | X    |                         |      |                                     |  |
| Prothèses et appareils  |  | 15   | 181   | X    | X                                  | X    |                                    | X    | X                | X    |                                     | X    | X          | X    | X              | X    | X                              | X    | X  | X    |                         |      |                                     |  |
| <b>DOMAINE DE SOINS</b>   |  |  |   |      |                                    |      |                                    |      |                  |      |                                     |      |            |      |                |      |                                |      |  |      |                         |      |                                     |  |
| Éducation à l'examen histologique (y compris groupe sanguin, histologie et virologie)                       |  | 16, 17   | 341, 342  | X    | X                                  | X    | X                                  | X    | X                | X    | X                                   | X    | X          | X    | X              | X    | X                              | X    | X  | X    |                         |      |                                     |  |
| CE d'aide diagnostique (radiologie, imagerie médicale, analyses para-cliniques, labos)                      |  | 18, 19, 20   | 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000   | X    | X                                  | X    | X                                  | X    | X                | X    | X                                   | X    | X          | X    | X              | X    | X                              | X    | X  | X    | X                       | X    |                                     |  |
| Plans d'intervention de la police d'urgence   |  | 16   | 101   | X    | X                                  | X    |                                    | X    |                  | X    | X                                   | X    | X          | X    | X              | X    | X                              | X    | X  | X    |                         |      |                                     |  |
| Plans d'intervention par satellite médical  |  | 17   | 101   | X    | X                                  | X    |                                    | X    |                  | X    | X                                   | X    | X          | X    | X              | X    | X                              | X    | X  | X    |                         |      |                                     |  |
| Contributions de l'expertise (LMD - see analysis)   |  | 18   | 333   | X    | X                                  | X    | X                                  | X    | X                | X    | X                                   | X    | X          | X    | X              | X    | X                              | X    | X  | X    |                         |      |                                     |  |
| CE d'aide thérapeutique (CE opérationnel, CE d'accompagnement, labos)                                       |  | 19   | 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702,   |      |                                    |      |                                    |      |                  |      |                                     |      |            |      |                |      |                                |      |  |      |                         |      |                                     |  |

# La législation face à la réalité

## (ex 2 : anonymisation des données)

- Des règles plus permissives
  - L'exploitation de données anonymisées ne requiert plus le consentement de la personne dès lors que ce dernier a été donné pour l'objectif initial de la collecte
  - Plus de période limite de rétention
- Données concernées
  - directement nominatives (nom, prénom, date de naissance,..) ou indirectement nominatives (matricule, adresse, n° de téléphone, élément biométrique, adresse IP, les traces des données de connexion, etc)
- Préconisations de la CNIL
  - Ne collecter les données qu'au niveau de finesse strictement nécessaire
  - Ne pas fournir systématiquement un logiciel d'interrogation généraliste
  - Utiliser une fonction de hachage à sens unique (pseudonymisation)
  - Dans les requêtes d'interrogation, ne pas fournir de résultat de cardinalité inférieure à 10 ! (ou  $k=5$ ,  $l=3$ )
  - ...

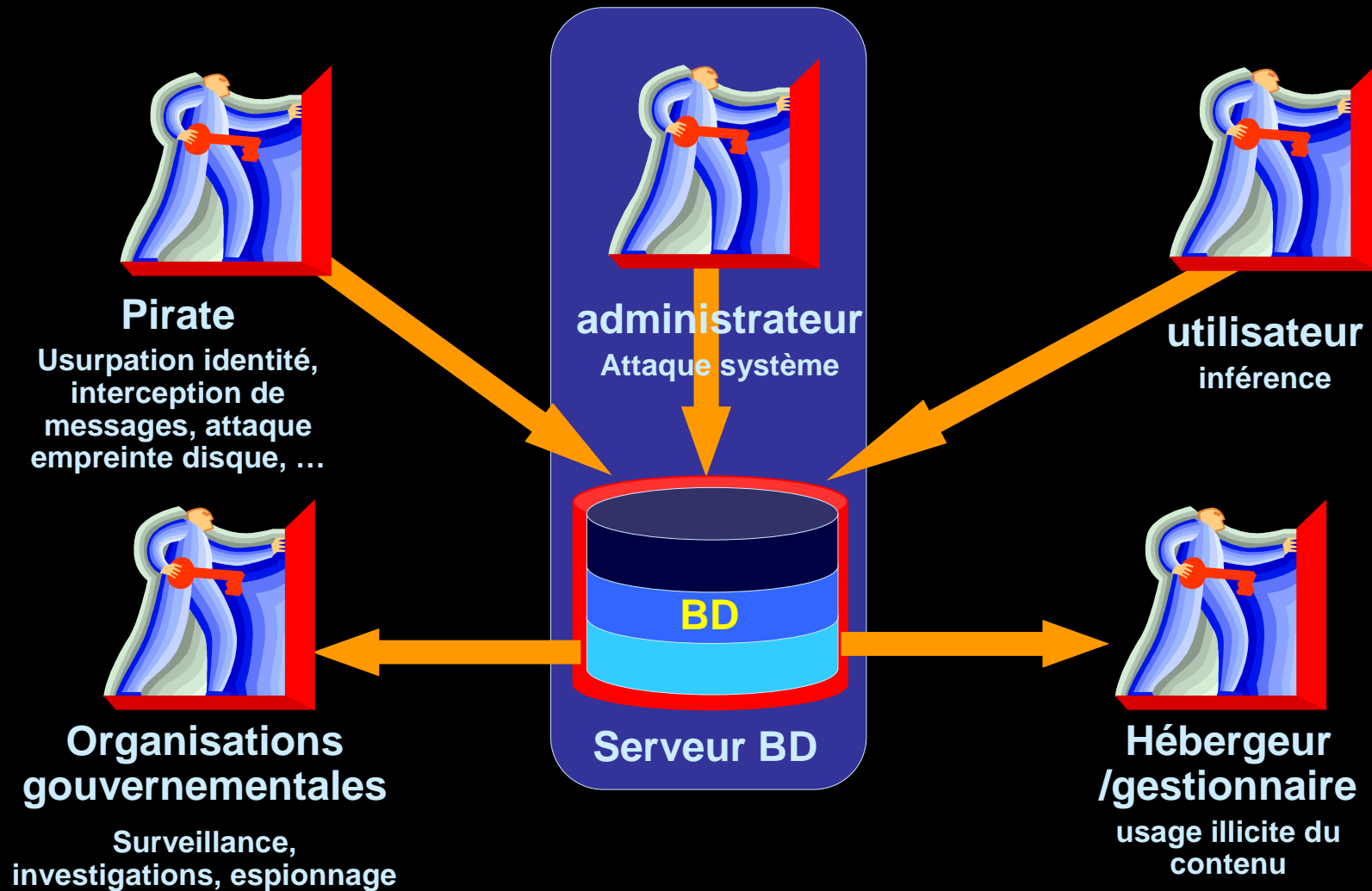
# **Attaques et défenses informatiques**

# Principales classes d'attaques

- Difficile d'être exhaustif
- Principales classes d'attaques
  - Interception de signaux ou brouillage physique
  - Usurpation d'identité
  - Mystification (simulation d'un terminal ou d'un site web)
  - Rejeu de messages
  - Déni de service
  - Fouille du disque ou de la mémoire
  - Cryptanalyse
  - Cheval de Troie, Virus, Ver
  - Etc...



# Principales classes d'attaquants



# Sécurité des Systèmes d'Information : définition

26

## *Information Technology Security Evaluation Criteria (ITSEC)*

- **Confidentialité**
  - Seules les personnes autorisées ont accès aux ressources du SI
  - *Ressources BD: données stockées dans la base ainsi que traitements activables sur ces données*
- **Intégrité**
  - Les ressources du SI ne sont pas corrompues
  - *BD: les données stockées et échangées doivent être protégées de toute modification illicite (destruction, altération, substitution, rejeu)*
- **Disponibilité**
  - L'accès aux ressources du SI est garanti de façon permanente
  - *BD: idem*
- **Et dans certains contextes**
  - *Auditabilité, imputabilité*

# Principales défenses

