AMBASSADE DE FRANCE EN ALLEMAGNE
SERVICE POUR LA SCIENCE ET LA TECHNOLOGIE

Berlin, le 3 septembre 2012

Rédacteur : Charles Collet, Chargé de mission NTIC et nanotechnologie

Développement d'initiatives et programmes de recherche sur la cybersécurité en Allemagne

Le développement des technologies numériques pour – et par – la sécurité est un enjeu technologique, sociétal (acceptabilité des produits) et stratégique majeur régulièrement abordé lors des grandes rencontres des TIC en Allemagne.

Au cours des derniers 16 mois, le thème de la sécurité informatique, avec celui du Cloud Computing dont celle-ci légitimera ou non le développement, est devenu central dans les discussions politiques et technologiques outre-Rhin. Cette importance stratégique s'est notamment illustrée par une série de séminaires R&D sur les systèmes de sécurité ("*Sicherheitssysteme*") organisés au sein de l'Université Technique de Berlin par différents organismes de recherche (DLR, DFKI), des forums organisés par la Société allemande de politique étrangère (DGAP) sur la cybersécurité (en y invitant des experts américains et français du domaine), la venue à Berlin de la conférence internationale MCTA spécialisée sur la sécurité des communications et des paiements en ligne, le forum sécurité comme thème central au CeBIT 2012[1] ("*Managing Trust*"), ou encore le focus stratégique sur la sécurisation comme feuille de route technologique présenté par le symposium international des semiconducteurs (ISS) invité en Allemagne.

On distingue outre-Rhin deux centres de recherche principaux spécialisés sur la sécurité des réseaux, soutenu par le ministère fédéral de la recherche (BMBF) et l'Académie allemande des technologies (Acatech), l'un associé à l'université de Darmstadt (Hesse) et l'autre à l'université de Bochum (Rhénanie du Nord-Westphalie), qui récoltent la majorité des appels à projet dans ces thématiques. On note également l'expertise reconnu de l'Institut Hasso Plattner (HPI) de Potsdam qui tisse des collaborations stratégiques dans le développement de protocoles de sécurité et de technologies réseau (notamment avec la Chine), ainsi que celle de Deutsche Telekom qui se concentre de plus en plus sur ce thème, notamment pour fiabiliser ses services de Cloud Computing et de paiement digital. On constate enfin l'implantation de firmes TIC étrangères en Allemagne, s'intéressant à la position allemande et européenne sur les problématiques croissantes de sécurité et sur l'acceptabilité sociétale des services numériques proposés.

1. Les centres de sécurité informatique de Darmstadt et de Bochum

1.1 Le Centre de sécurité avancé à l'Université technique de Darmstadt

C'est un des centres les plus renommé en Europe dans le domaine de la sécurité informatique. Il est à l'origine de la création en 2011 du "Centre européen pour la sécurité et la confidentialité dès la conception - EC-SPRIDER", qui a pour but de traiter les procédures de développement, de vérification systématique et de tests de logiciels spécifiquement du point de la sécurité et de la confidentialité.

[1] "Bilan du CeBIT 2012 : focus sur l'internet des choses et la sécurisation des données", BE Allemagne n°563 - 14/03/2012 - http://www.bulletins-electroniques.com/actualites/069/69424.htm

Son objectif à long terme est d'assurer la sécurité des solutions informatique dès la phase de conception des systèmes logiciels.

a) Programme fédéral « EC SPRIDER » et attraction de jeunes talents en cryptographie

L'EC SPRIDER a débuté ses travaux en lançant le programme 'Claude Shannon pour jeunes chercheurs', soutenu par le BMBF à hauteur de 8 millions d'euros jusqu'à 2015. Choisissant leurs propres groupes de travail, les chercheurs talentueux allemands ou étrangers sélectionnés doivent développer des solutions de sécurité informatique à l'épreuve des fraudes ou des tentatives de sabotage et d'espionnage. La vision du BMBF est qu'il faut une recherche forte sur la sécurité informatique en Allemagne afin de développer des solutions sûres et fiables pour les systèmes informatiques critiques. **Avec plus de 200 scientifiques spécialisés sur ce thème, Darmstadt est en passe de devenir l'un des sites les plus importants en Europe pour la recherche sur la sécurité des TIC.**

b) "Internet Privacy" : culture de l'Internet et la protection de la vie privée (octobre 2011)

« Internet Privacy »[2], le nouveau projet de l'Académie allemande des technologies (Acatech) et porté par le Centre de sécurité avancé de Darmstadt, a pour objectif de proposer des solutions pour une meilleure confiance dans les technologies et services numériques. Il est mis en œuvre par un groupe de travail interdisciplinaire mené par Johannes Buchmann, directeur du Centre de sécurité avancé. Il repose sur le principe suivant : les effets d'une crise de confiance dans les TIC menaceraient le développement d'autres technologies en Allemagne, parce que l'Internet est étroitement lié à de nombreuses technologies clés: les réseaux électriques intelligents (Smart Grids), les futurs réseaux de transport urbain, l'harmonisation des soins médicaux par le Cloud Computing, les Smart phones, etc. Une perte de confiance éventuelle pourrait, selon le BMBF, dégrader de façon drastique le climat global d'innovation. Le projet financé par le BMBF se terminera le 31 Janvier 2013, les résultats finaux seront présentés d'ici juillet 2013. Les autres partenaires du projet sont Google et IBM Allemagne (Berlin).

1.2 L'institut de sécurité des réseaux et des données de l'Université de la Ruhr à Bochum

Le second centre allemand à Bochum[3] spécialisé sur la sécurité des réseaux, après celui de Darmstadt, est reconnu pour son expertise sur l'identification des vulnérabilités informatiques. Les projets majeurs actuellement portés sont décrits ci-dessous.

a) Cloud Computing : les chercheurs de Bochum ont découvert des failles de sécurité critiques (septembre 2011)

Plus de 25.000 « nuages » de données privées ont déjà été créés à travers le monde via la plateforme Cloud « Eucalyptus », l'une des 1ère à avoir été développé commercialement à grande échelle (environ 40% des 100 plus grandes sociétés cotées dans le magazine « Fortune » utiliseraient cette plate-forme logicielle pour leurs activités). Néanmoins, les scientifiques de l'Institut de sécurité des réseaux et des données de Bochum ont pu contourner son système de sécurité et ainsi accéder à toutes les données et fonctionnalités dans le nuage, qui a immédiatement du être fermé. Selon eux, un simple message XML caché dans la signature aurait suffi à infiltrer une lacune de programme qui leur a servi de passerelle afin d'entrer dans la zone de données hébergées par le nuage.
La lacune sécuritaire découverte à ce jour est l'une des nombreux cas potentiellement présents dans l'offre de Cloud et à laquelle les chercheurs de Bochum ont travaillé ces derniers mois. Le ministère fédéral de l'économie et de la technologie (BMWi) subventionne ainsi le projet « Trusted Cloud » (« nuage de confiance ») dans lequel l'Université de la Ruhr contribuera également à améliorer la sécurité de l'interface des serveurs partagés.

b) L'Université de Bochum forme des pirates informatiques (janvier 2012)

[2] Plus d'informations sur le projet sur : www.acatech.de/privacy

[3] Pour en savoir plus, contacts : Département de sécurité des réseaux et des données de l'Université de la Ruhr : http://www.nds.ruhr-uni-bochum.de/

La liste des sociétés ou administrations qui ont été récemment victimes d'attaques de pirates en Allemagne est longue : Sony, Rewe, Citigroup, voire même des ministères allemands. C'est pourquoi l'Université de Bochum a mis en place une formation au cours de laquelle les jeunes informaticiens talentueux apprennent légalement à cracker des mots de passe, à propager des virus et des chevaux de Troie, ou détourner des comptes bancaires en ligne. Avec près de 1100 candidats pour environ 20 places, cette filière est devenue une des plus sélectives et populaires. Une fois par semaine, les étudiants du Département de sécurité des technologies de l'information de l'université s'entrainent à pénétrer les systèmes informatiques des entreprises et des sites web et à manipuler leurs données.
Les deux chercheurs encadrant cette formation sont ainsi experts dans le domaine et consultants auprès de plusieurs entreprises du DAX pour la recherche de failles de sécurité, en plus de leurs activités d'enseignement universitaire sur la piraterie informatique et la sécurité des réseaux. C'est la première fois qu'une telle option est officiellement ouverte en Europe, et les étudiants signant un document les rendant pénalement responsables de l'utilisation de leurs recherches.

c) Cryptologie : Bochum développe un nouveau procédé pour sécuriser les puces RFID (juin 2011)

Un défi complexe a été résolu par le mathématicien Eike Kiltz, chef du groupe de travail « Fondements et Applications de la théorie de cryptographie » à Bochum[4], qui a réussi à développer un processus d'authentification simple et totalement sécurisé pour un très grand nombre de puces RFID. Le chercheur a ainsi élucidé un problème jusqu'alors insoluble de la théorie du codage. Car si les puces RFID sont au cœur de nombreux dispositifs électroniques d'identification, par exemple dans les passeports électroniques, ces puces miniaturisées sont souvent simplifiées, l'espace y manquant pour introduire des algorithmes cryptographiques complexes qui pourraient protéger efficacement les données sensibles. Des cryptographes renommés avaient tenté dans la dernière décennie de résoudre ce défi d'équilibre entre économie d'espace, calcul complexe, et mécanisme de protection efficace, avec des niveaux de sécurité spéculatifs.

La nouvelle méthode cryptographique de Bochum est d'un niveau de sécurité extrêmement élevé, les ordinateurs de haute performance testés auraient besoin de calculer pendant plusieurs millions d'années pour en percer la solution, selon l'équipe de recherche. Un prototype de la puce avec la nouvelle méthode d'authentification est actuellement en conception en collaboration avec le département « Embedded Security » de l'université de Bochum. Après avoir travaillé aux Etats-Unis, Eike Kiltz est retourné à l'Université de la Ruhr en 2010, soutenu par le prix Sofya Kovalevskaya de la Fondation Alexander von Humboldt qui soutient des scientifiques choisis pour développer leurs projets de recherche dans l'institution allemande de leur choix.

2. Les activités des instituts privés allemands dans le domaine de la sécurité informatique

2.1 - L'Institut Hasso Plattner de Potsdam (HPI)

L'Institut Hasso Plattner (HPI), centre de recherche rattaché à l'Université de Potsdam, a été fondé par H. Plattner, co-fondateur de l'entreprise SAP, le géant allemand des logiciels de gestion de données. Reconnu pour son expertise en programmation informatique et en technologies de traitement de bases numérisées, l'HPI a été sélectionné en 2012 par la Chine pour développer des collaborations de R&D en sécurisation de Cloud Computing. Dans ce contexte, les possibilités de co-développement en termes de technologies pour les mémoires seront explorées. Une rencontre, financée par le Centre sino-allemand pour la promotion de la recherche (*Chinesisch-Deutsches Zentrum für Wissenschaftsförderung*) s'est tenue à Shanghai. Du côté allemand, ce centre est soutenu par la *Deutsche Forschungsgemeinschaft* (DFG). Le Département des technologies Internet et des systèmes de l'HPI, ainsi que le Centre de calcul de haute performance et la faculté des sciences informatiques de l'Université de Shanghai organisent cet atelier conjoint.

Sur la même période, l'HPI a pris en charge un projet de recherche lancé par le BMWi dans le cadre du programme « confiance dans le nuage » (« *Trusted Cloud* ») et financé à hauteur de 30 millions d'euros. En collaboration avec trois autres partenaires, le Département de l'HPI consacré aux technologies Internet et aux systèmes prend en charge l'accompagnement de 14 projets pilotes pour

[4] Pour en savoir plus, site internet du département de cryptographie à l'Université de Bochum : http://www.cits.rub.de/

développer des prototypes de technologie de sécurisation des réseaux et des services de Cloud Computing.

2.2 - Le développement de la sécurité par Deutsche Telekom

Le centre R&D de l'entreprise Deutsche Telekom à Berlin « T-Labs », modèle de PPP entre l'entreprise de télécommunications et l'Université technique de Berlin (TUB), est actif sur ces thématiques,. En effet, les "T-Labs" appartiennent conjointement aux deux partenaires dans laquelle Deutsche Telekom y emploie des chercheurs venant de l'université dans sept domaines de R&D, dont un sur le Cloud, avec sept professeurs de la TUB les encadrant. Les principales recherches s'orientent vers le développement d'infrastructures et services de cloud, ainsi que sur les nouveaux besoins en termes de protection de données privées ou de pertinence de l'information. Tous domaines confondus, les T-Labs présentent de bons résultats en termes de R&D : plus d'une publication par jour (392 en 2010), un brevet par semaine (57 en 2010), et une décoration scientifique par mois, dont le prix Leibniz 2011 décerné au Pr. Anja Feldmann (une des plus hautes reconnaissances scientifiques au niveau national, dotant le récipiendaire de 2,5 millions d'euros pour mener ses recherches).

Au niveau des applications, et dans le cadre particulier de la compétition pour l'affectation des fréquences numériques en Allemagne, Deutsche Telekom a obtenu 10 blocs de fréquence pour 1,3 Md€, ce qui le place en 3ème position derrière deux opérateurs étrangers, ce qui n'est pas négligeable sachant qu'une connexion performante est la clé de développement des services de Cloud. Elle s'attaque maintenant aux problèmes de sécurité dans les Smart phones.
Au niveau stratégique, le géant chinois des matériels de télécommunication Huawei et Deutsche Telekom ont signé à la mi-septembre 2011 un accord stratégique afin de développer conjointement des services Cloud pour le marché des entreprises.

3. Localisation de firmes étrangères en Allemagne, s'intéressant à la position allemande et européenne sur ces problématiques

Après la récente vague d'attaques de pirates informatiques (ou hackers) sur des entreprises et administrations à travers le monde, dont en Allemagne, **Microsoft** compte renforcer ses efforts de recherche sur la sécurité des technologies de communication, et notamment des réseaux informatiques. Dans cette optique, l'entreprise américaine a annoncé fin juillet 2011 l'ouverture à Munich d'un laboratoire de recherche consacré à la sécurité des réseaux, où les experts se concentreront sur l'étude des nouveaux types d'attaques et les stratégies de protection appropriées. Microsoft explique ce choix, tout comme **Google** à propos de l'ouverture de son « Institut pour l'Internet et la Société » à Berlin, par une conscience allemande accrue sur les problématiques de protection des données privées, et la motivation des chercheurs allemands dans ce domaine.

CONCLUSION

Suite aux différentes attaques ciblant des administrations allemandes, à la montée du parti Pirate, et à la sensibilité de sa population quant à la protection des données privées, l'Allemagne, via le BMBF et le BMWi, s'est doté d'une R&D en sécurité informatique les plus performantes et reconnues d'Europe, notamment par ses 2 centres visibles de **Darmstadt** et de **Bochum** travaillant sur les infrastructures de données et la cryptologie. Ses instituts de R&D privés, tels les **T-Labs** (PPP entre Deutsche Telekom et la TU Berlin) ou le **HPI** (entre SAP et l'Université de Potsdam) ont également atteint une reconnaissance internationale notable. Profitant de ce terreau dynamique et voulant comprendre les attentes locales pour mieux les servir, les firmes de TIC globalisées telles **Google** et **Microsoft** ont également implanté des centres de R&D autant tournés sur les technologies de sécurisation que sur la sociologie des barrières à l'acceptabilité.

Majeure rencontre européenne des TIC et de l'électronique et vitrine de la R&D allemande, le **CeBIT** avait en 2012 pour thème transversal "**Managing Trust**" (Gérer la confiance), illustrant l'importance actuelle du sujet de la sécurité informatique. Il fut d'ailleurs inauguré par la Chancelière Angela Merkel, la Présidente du Brésil Dilma Rousseff, Dieter Kempf (Président du Bitkom, la puissante fédération allemande des TIC) et Eric Schmidt (Président du Conseil d'administration de Google). La

R&D présentée lors de l'évènement se focalisait sur le développement de **systèmes cyber-physiques** (interconnexion des équipements physiques et du cloud computing, visant la gestion flexible et automatisée des usines de production, de la mobilité), et la **sécurisation des infrastructures de données**, nécessaire à l'acceptabilité de ces services Cloud et de gestion délocalisée. Les multinationales des NTIC **Deutsche Telekom** et **SAP** ont ainsi fait du terme "sécurité" le mot-clé de leur R&D et de leur communication publique, le système d'email sécurisé avec accusé de réception de Deutsche Telekom ayant même été finalement certifié par le gouvernement fédéral.

Volonté de passer un cap dans l'interconnexion des systèmes physiques par le numérique, besoin de sécurisation et sensibilisation des utilisateurs aux efforts de R&D dans la protection des données traitées, tels sont les piliers de la R&D en Allemagne sur les réseaux informatiques, qui s'inscrivent parfaitement dans les problématiques actuelles des NTIC./