Réunion du 10 janvier 2018

Normalisation de la sécurité de l'information

CLUBEBIOS

Réunion du SC 27 à Berlin

Réunion technique (non plénière) tenue à Berlin dans les locaux du DIN du **30 octobre au 3 novembre 2017**. 20 représentants français présents (et seulement une dizaine de Britanniques)

Création d'un **MAG (*Management Advisory Group*)** au SC 27 de 9 membres (membre français : Jean-Pierre Quémard)

Nouveau chairman du SC 27 : Andreas Wolf qui succède à Walter Fumy.

Prochaines réunions du SC 27 :
Chine (Wuhan), plénier, 16 au 24 avril 2018,
Norvège, technique, 1 au 5 octobre 2018 avec lieu à confirmer,
Corée du Sud, plénier printemps 2019 lieu et dates à préciser,
France, technique, automne 2019, Paris, dates à préciser.

Normes du WG 1

IS 27001 : Des questions préliminaires ont été posées. Elles portent principalement sur l'Annexe A et sur la nécessité du SoA. Il en résulte une *Study Period* de 6 mois ouverte pour examen à Wuhan (Chine), prochaine réunion du SC 27. Par ailleurs, il y a aussi la possible influence de la nouvelle version de l'Annexe SL.

IS 27002 : La *Study Period* est terminée le 1er novembre à Berlin. Il en découle une « *Design Specification* » réalisée à Berlin et un NWIP. Il est proposé de changer le titre du document, en particulier de supprimer « *code of practice* » dans le titre.

Normes du WG 1

IS 27005 (*Information security risk management*) : La *Study Period* en cours est close à Berlin. La situation est complexe : Initialement, une forte majorité (92%) a voté en faveur de la parution d'un corrigendum. Comme le document est trop ancien (2011), il ne peut plus s'agir d'un corrigendum et le document à paraître doit donc être une nouvelle version de la norme qui ne pourrait être disponible qu'entre mai 2018 au plus tôt et Q1 2019 au plus tard.
Considérant la parution comme acquise, une *early revision* peut être entamée. Il va donc y avoir une phase de *design specification* qui peut être close à Berlin. Après quoi, un document (sans statut de *working draft*) pourra être produit. Il changera de statut quand, après la parution de la norme, un NWIP sera émis qui pourra être accompagné d'un WD.

Pas d'IS 27005 vraiment nouvelle avant 2020-2021.

Normes du WG 1

IS 27009 (*Sector-specific application of ISO/IEC 27001 – Requirements*) porte sur l'extension du champ de la certification 27001. Elle a été publiée. Sa mise en œuvre rencontrant des difficultés, une révision précoce a été décidée.

A Berlin, un calendrier a été proposé qui fait aboutir le projet de **norme en avril 2020** (WD à Berlin, CD pour Wuhan, DIS en avril 2019).

Normes du WG 1

IS 27014 (*Governance of Information Security)* entre en révision.

Le document est entré en révision à Berlin. La révision est menée de façon efficace et constructive par Bridget Kenyon (ensemble des commentaires traités en moins d'une heure, prise en compte du contexte SC 40 et TC 309)

NWIP 27102 (*Guidelines for cyberinsurance*) : ce document est une proposition britannique.

C'est actuellement un projet de TR (PDTR). Il y avait à Berlin 46 pages de commentaires. Ils ont été traités assez minutieusement.

Normes du WG 1

Study period on cybersecurity La définition de la cybersécurité fait toujours débat. Deux groupes d'experts, l'un en faveur d'une définition préalable à toute étude, l'autre en faveur de démarrer un *framework* en parallèle des travaux sur la définition. Deux ateliers ont été créés qui ont permis de conclure sur trois projets :

New Study Period 1 **:** un document en charge d'une *design specification* d'un *standalone* TS : « *Cybersecurity – Overview and Concepts* – TS ». Son statut sera lié à ce qui adviendra de la 27032. A noter le fort leadership de Bridget Kenyon.

NWIP pour un TS « *Cybersecurity – Guidelines for Frameworks*" Ce NWIP n'est pas un *framework* en soi, mais un guide pour la définition d'un *framework* (*Practical guidance on how to create a cybersecurity framework, including the components*). En principe, la proposition du *National Body* US sera utilisée pour ce NWIP.

New Study Period 2 : un document visant à clarifier la définition de la Gouvernance Cybersécurité : « *Cybersecurity – Societal considerations and responsibilities* »

Normes du WG 2

Environ 16 *National Bodies* présents et 63 experts

IS 18032 (*Prime number generation)*

En cours de révision, texte en CD édité par N. Gajcowski (US)

Commentaires JP, GB, RU et MY très majoritairement éditoriaux

Suite au désastre de la librairie RSA OBKG d'Infinéon et du scandale de la carte nationale d'identité estonienne, des changements de fond dans la 18032 sont suggérés, en particulier d'utiliser systématiquement des générateurs pseudo-aléatoires pour pouvoir tester les implémentations avec des vecteurs de test. Finalement, il est décidé de laisser le texte en CD et de lancer un appel à contributions sur des suggestions de fond. A l'issue, un CD2 sera produit, à temps pour un vote CD2 avant Wuhan.

IS 18033 (*Encryption algorithms)*

Part 6 *Homomorphic Encryption*

Commentaires du Japon, de la Russie, de la Grande-Bretagne et des USA, résolus par P. Paillier et A. Miyaji sur le CD2.

Passe en **DIS**.

Normes du WG 2

CLUBEBIOS

IS 29192 (*Lightweight cryptography)*

Part 2 *Block ciphers* (Simon/Speck)

Le projet le plus clivant actuellement au WG2. Objectif : inclusion des *blockciphers* Simon et Speck par les US. Edité par Louis Wingers et Doug Shors de la NSA.

Votes reçus sur le ballot PDAM2 ::Votes OUI : 13, Votes OUI Avec Commentaires : 2 (RU, GB), Votes NON : 9 (dont IL, DE, JP, BE, CH), Abstentions : 31 (dont FR, CN, SG)

Les éditeurs estiment avoir déjà fourni toute l'information nécessaire à la conduite de l'AMD et refusent dorénavant de produire de nouveaux documents informatifs sur la conception du *block-cipher.*

Une discussion générale très animée a eu lieu dès le début de la semaine, avec une opposition essentiellement menée par Israël (Orr Dunkelman et Tomer Ashur) qui tentait de mettre en évidence un mensonge technique de la part des éditeurs sur les marges de sécurité des *blockciphers*. Le point culminant de la session semble avoir été le moment où Dunkelman a demandé à Wingers : « *Are you aware of an attack more efficient than the publicly known ones, on either Simon or Speck?*» et où Wingers a répondu : « *I am not authorized to answer that question*».
Finalement, Israël a proposé que le texte reste au niveau PDAM (**PDAM3 pour Wuhan donc**) et Wingers a accepté immédiatement.

Normes du WG 2

CLUBEBIOS

Study Period on Quantum computing resistant cryptography

Progresse doucement en raison d'absence de ressources. *Hash-based et lattice-based schemes* sont les premières cibles pour les futurs standards.

La SP est terminée. Elle débouche finalement sur la **rédaction d'un nouveau *Standing Document* (le SD8)** dédié à la cryptographie post-quantique, avec un découpage en chapitres dédiés aux différentes techniques de construction : les codes, les lattices (treillis), le multivarié, etc.

Lily Chen reste éditrice du SD8 « *Post-quantum cryptography* » mais a identifié, consensuellement avec le WG2, des co-éditeurs sur chaque chapitre sur la base du volontariat.

L'objectif premier du SD est de fournir au WG2 une base documentaire solide sur les mécanismes prometteurs en vue d'une préparation à une standardisation ultérieure. Le format SD est facilement mis à jour et fournit un « réservoir à mécanismes » en attendant que ceux-ci gagnent en maturité.

Il n'y a donc pas de NWIP pour l'instant, mais plutôt une « préparation à dégainer plus tard ».

Normes du WG 3

Très forte affluence, plus de 50 délégués : un record, dont France (6 délégués)

IS 15408 (*Evaluation criteria for IT security* - version norme des Critères Communs)

Gros travail d'édition, salle comble (60 personnes), DoC préparés avant la réunion.

Part 1 - Introduction and general model,
Part 2 Security functional components,
Part 3 Security assurance components,
Part 4 Framework for the specification of evaluation methods and activities,
Part 5 Pre-defined packages of security requirements.

Normes du WG 4

IS 27031 (***Guidelines for ICT readiness for business continuity*)** est entrée en révision.
La révision est lancée avec difficulté par manque d'éditeur. La séance a cependant été constructive et deux coéditeurs se sont proposés (Alain De Greve, Thierry Maxime). Il semble qu'ils reçoivent le soutien de l'éditeur Brian Cusack (NZ) et les 2 co-éditeurs Alain De Greve (BE) et Thierry Maxime (FR) ont été « endorsés » par leur NB respectif et par le co-convener du WG4 (Francois Lorek)

Une dizaine de *Study Periods* sont en cours au WG4, notamment :

Study Period on Guidelines for Security in IoT
Un NWI doit être finalisé. On notera que la partie *privacy* et la partie *security* sont deux parties distinctes. Sur la partie *privacy,* il sera à charge du WG5 de fournir les contributions.
On s'acheminerait vers un projet commun avec SC41 et dont la RA (*Reference Architecture*) servirait de base pour les travaux (par exemple réunion SC27 et webex SC41)

Study period on Big Data security capability maturity model
Nouvelle *Study Period* lancée pour 12 mois, dont les rapporteurs sont Kepeng Li (CN) et Luc Poulin (CA). Il sera nécessaire de vérifier si le WG9 a des modèles de maturité générale dont il faudra alors tenir compte.

CLUBEBIOS

Merci