ENER-GM
Consultant en énergie et en environnement

Régie de l'énergie du Québec

R-3770-2011

HQD - Demande d'autorisation pour réaliser le projet lecture à distance - Phase 1

Complément de preuve de l'ACEF de l'Outaouais

Préparé par :

Mounir Gouja, PhD

Assisté par l'expert-conseil Mohamed Ibnkahla, PhD

Pour

l'ACEF de l'Outaouais
109, rue Wright,
Gatineau (Qué.)
J8X 2G7

07 décembre 2011

6683, rue Jean Talon Est
H1S 0A5 St-Léonard (Qc)

Tél. : (514)249-8903 Fax : (514)448-7372
energm@gmail.com

INTRODUCTION :

Dans sa lettre en date du 12 octobre 2011 (pièce C-ACEFO-0010), l'ACEF de l'Outaouais (l'ACEFO) avait répliqué aux objections exprimées par Hydro-Québec dans ses activités de distribution (« HQD » ou « le Distributeur » ou « Hydro-Québec ») en réponse à certaines demandes de renseignements des intervenants dans le présent dossier, dont la question 10-a de la demande de renseignements no. 1 de l'ACEFO relative au sujet de la sécurité du système IMA (pièce C-ACEFO-0009).

À cet égard, l'intervenante a considéré pertinente cette question et a obtenu l'ordonnance de la Régie adressée au Distributeur pour qu'il réponde à cette question. L'ACEFO a alors obtenu une réponse à sa question dans la pièce B-072 (HQD-4, Document 13), mais cette réponse n'a pas était satisfaisante et a encore soulevé de nouvelles préoccupations de l'ACEFO quant à la sécurité de la solution proposée par le Distributeur dans son projet LAD.

Étant convaincue que la piraterie du système IMA de HQD constitue un risque certain et réel à prendre en compte, l'ACEFO a fait part à la Régie, suite à l'obtention de la réponse à sa question 10-a, que pour l'intervenante il ne suffit pas d'alléguer que la technologie du Distributeur est la meilleure ou la plus sûre. Il s'agit plutôt, pour le Distributeur, de démontrer la fiabilité de ses lignes de défense pour éviter et pallier, le cas échéant, à d'éventuelles défaillances.

L'intervenante ne cherche pas à obtenir de l'information d'ordre stratégique en soit. La demande de l'ACEFO porte sur la méthodologie et la déontologie de la prise en compte de la question de la sécurité du réseau; parce que l'électricité est une fonction vitale de la vie quotidienne du consommateur qu'il faut bien protéger. Elle est aussi un produit et un *input* stratégique de l'économie québécoise et il faut sécuriser sa distribution.

Des études récentes exigent que les modèles de sûreté et de sécurité des réseaux électriques intelligents soient aussi stricts que dans le domaine de l'aviation, dans lequel les risques sont minimisés et leur mitigation obéissent à des normes et procédures d'action et de prévention très rigoureuses.

Compte tenu du refus du Distributeur de déposer le rapport de la firme Lofty Perch dont elle a fait référence dans sa réponse à la question 10-a de l'ACEFO, même avec des procédures de respect de confidentialité, le présent document, venant en complément de preuve de l'ACEF de l'Outaouais (l'ACEFO), se base principalement sur la réponse d'Hydro-Québec à la question 10-a de l'ACEFO[1] ainsi que sur d'autres données et informations fournies dans la preuve en chef du

[1] HQD-4, Document 13

Distributeur. Dans l'élaboration de ce document, l'ACEFO a retenu les services de conseil du Dr Mohamed Ibnkahla, expert dans le domaine de la communication digitale et du traitement du signal appliqués au *Smart Grid*. Le curriculum vitae de Dr Ibnkahla est déposé au présent dossier, pièce C-ACEF-0017.

L'ACEFO considère que HQD n'a pas adressé la question de sécurité comme l'exigent les normes internationales en vigueur, et laisse plusieurs zones ambiguës à la fois dans ses réponses et dans les informations techniques fournies dans la demande du Distributeur.

Le présent document va d'abord focaliser sur les failles remarquées avant de dresser un bilan et des conclusions sur la solidité de la preuve du Distributeur en matière de sécurité de son IMA.

LISTE DE CRITIQUES RELATIVES À LA SECURITE À PARTIR DES INFORMATIONS FOURNIES DANS LA DEMANDE R-3770-2011 ET DANS LA RÉPONSE DU DISTRIBUTEUR À LA QUESTION 10-A DE LA DEMANDE DE RENSEIGNEMENTS NO.1 DE L'ACEFO :

1. Réponse d'Hydro-Québec, HQD-4, Document 13, page 24, lignes 26-27 :
   Afin de préciser que les données transitant sur le réseau IMA ne sont pas déchiffrables, la réponse d'Hydro Québec stipule que « Les données qui transitent sur le réseau IMA sont chiffrées en tout temps à l'aide de clefs personnalisées et d'un algorithme particulier. »
   Cela n'empêche pas pour autant que les données soient déchiffrables par un intrus ayant des connaissances assez avancées dans ce domaine. En fait, les algorithmes d'encryptage sont connus en général. La seule chose inconnue, c'est la clef d'encryptage qui reste la même pour un compteur donné. Donc si les intrus ont accès aux clefs, ils peuvent très bien déchiffrer le signal. La connaissance de la clef peut être facilement déterminée grâce à la connaissance de mots de référence qui sont inévitablement utilisés dans ce genre de communications. Parmi ces mots de référence, on peut citer "BEGIN", "END", "SESSION", "FLAG", "ESCAPE", etc. Le problème de détermination des clefs serait réduit, par conséquent, à un simple système linéaire de M équations à N inconnues (ces dernières sont les bits des mots d'encryptage), le système étant paramétré par les mots de référence.
   Cette tâche devient encore plus facile si l'un des pirates possède lui même un compteur IMA, donc ayant directement accès au signal avec le numéro de client, l'identité (*stamp*) du compteur. Il peut ainsi avoir accès aux premiers paquets échangés qui contiennent

des références importantes sur le protocole utilisé et la référence des clefs d'encryptage et de décryptage.

Dans le cas où le pirate est lui même client d'Hydro-Québec, il peut même forcer certains échanges de données et certaines initialisations. Par exemple, il peut provoquer l'arrêt du compteur puis sa remise en marche, ce qui va provoquer certains échanges d'initialisation (des paquets spécifiques) entre le compteur et le réseau. Ce sont bel et bien ces premiers échanges qui sont capitaux dans le décryptage de l'information et sa généralisation.

Le client pirate peut aussi faire usage d'un compteur parallèle hors réseau (pas nécessairement intelligent) qui peut mesurer les mêmes données que le compteur IMA. En recoupant les données transmises par IMA avec celles du compteur parallèle du pirate, le pirate peut avoir à résoudre un simple système d'équations linéaires afin de remonter aux familles de clefs utilisées.

2. Réponse d'Hydro Québec, HQD-4, Document 13, page 24, lignes 28-30 :

   Afin de nous convaincre du haut niveau de sécurité, la réponse d'Hydro-Québec stipule que « Les équipements (compteurs de nouvelle génération, routeurs et collecteurs) qui agissent comme relais, ne détiennent aucune information sur l'origine topologique de l'information.»

   Cela représenterait un premier niveau de sécurité. Il est tout à fait normal que les paquets transmis ne détiennent pas les données topologiques et les lieux des compteurs. Cependant, ces paquets détiennent bien certaines références (comme par exemple le numéro de compte du client) qui peuvent très bien être décodées et les pirates peuvent remonter aux données topologiques qui correspondent à ces numéros de comptes. D'autre part, même si le pirate n'arrive pas à relier les numéros de comptes aux lieux topographiques, il est relativement facile de faire ce lien grâce à la technique appelée RSS (*Received Signal Strength*) qui se base sur la puissance du signal numérique pour déterminer son origine (grâce à un modèle de propagation de signal). En utilisant cette méthode, un pirate (ayant une formation de base en télécommunications sans fil) peut facilement identifier les sources des signaux sans fils et associer un signal donné au compteur IMA transmetteur.

3. Réponse d'Hydro-Québec, HQD-4, Document 13, page 25, lignes 1-8 :

   Hydro-Québec conclut sa réponse en affirmant que « le Distributeur a pris tous les moyens nécessaires afin de minimiser les types de risques liés à la sécurité des équipements et des informations.»

Ici, Hydro-Québec reconnaît (pour la première fois) qu'il y a des risques (à minimiser certes, mais implicitement ils existent). Avoir reconnu que les risques existent et sont à minimiser est bien en soit, mais Hydro-Québec n'a jamais spécifié ou décrit ces risques.
Reconnaître, quantifier et spécifier les risques, d'une part, et prévoir une approche claire, réaliste, efficace et implantable pour mitiger les risques, d'autre part, sont deux règles de base pour assurer une sécurité avancée dans les systèmes de télécommunications, car le risque Zéro n'existe pas.
Cela contredit bien entendu les documents fournis par Hydro-Québec qui affirment clairement qu'il y a Zéro risque.

4. Demande R-3770-2011, HQD-1, Document 1, page 22 lignes 22 et 23, et Annexe A pages 53-54 :
   Cette annexe donne une liste de normes techniques « applicables » à ce projet. Cette liste inclut des « mesures » canadiennes, des « normes » d'Hydro-Québec, ainsi que des recommandations internationales. Toutefois le document ne précise pas si ces normes sont appliquées dans ce projet, ni l'endroit de leur application si c'est le cas.
   Du point de vue de l'ACEFO et de son expert-conseil, il est très invraisemblable que ce soit le cas, car il y a, parmi ces normes et recommandations certaines, qui sont très récentes et il serait très étonnant que les systèmes IMA commercialisés d'aujourd'hui obéissent aux plus récentes d'entre elles (et bien entendu les plus élaborées en termes de sécurité). Ces normes (par exemples NISTIR 7628) n'ont été établies que très récemment (moins d'un an).

5. Demande R-3770-2011, page 43 : Analyse de risque et mesure de mitigation :
   Le terme « Sécurité des TI et de télécommunication » qui figure en quatrième lieu dans le tableau reste très général et vague. On n'y sous-entend même pas que Hydro-Québec reconnaît que les risques existent. Les « mesures de mitigation » dressées par Hydro-Québec sont aussi bien vagues que générales : « respect des normes propres à ce domaine d'activité dont le chiffrement de données » ou «le contrôle d'accès », etc. Ces mesures ne montrent rien d'extraordinaire ou d'exceptionnel dans le cas d'attaque réussie : que ce soit une attaque ciblant la vie privée des gens ou une attaque qui causerait une paralysie locale ou générale du réseau de distribution. Que faire dans des cas pareils ? Quelle réponse Hydro-Québec apporterait à ses millions de clients?
   Les documents sous-entendent une négation de l'éventualité d'une attaque.

Il ne paraît pas évident, à partir de ces documents, que Hydro-Québec a même simulé sur ordinateur des scenarios types d'attaques virtuelles, ni mesuré ses étendues sur la vie privée des gens, la vie collective ainsi que sur l'économie du Québec en général.

Il est clair, donc, que l'éventualité d'une attaque, aussi minime soit-elle, a été complètement négligée et l'on n'identifie pas, dans la preuve du Distributeur, de mesures et/ou procédures claires pour les mitiger.

CONCLUSION :

À partir des points indiqués ci-dessus, la sécurité dans le projet lecture à distance d'Hydro-Québec présente des faiblesses techniques indéniables.

En plus de ces faiblesses techniques, Hydro-Québec a vraisemblablement misé sa politique en termes de sécurité sur la sophistication des technologies existantes, sans imaginer une éventuelle défaillance dans ces technologies (qui sont par ailleurs développées par des fournisseurs).

Le point le plus faible de la preuve du Distributeur reste, de l'avis de l'ACEFO et de son expert-conseil, Dr Ibnkahla, l'absence d'une procédure de mitigation de risques, la non quantification des dégâts qui seraient causés par ces risques et, par conséquent, l'absence d'estimation de la capacité de ces procédures à limiter les dégâts.