Antonin MILZA
51 Bd Auguste Blanqui – Hall D
75013 Paris

06 32 90 85 76
antonin.milza@telecom-paristech.fr
Paris, le 02/02/2014

Objet : Note mettant en évidence le travail personnel le plus important réalisé pendant le cursus de formation à Telecom ParisTech

Monsieur le vice-président du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies,

Le secteur des industries de souveraineté et plus particulièrement la sécurité numérique m'attire depuis longtemps. J'ai été frappé ces dernières années par l'augmentation du nombre d'attaques informatiques, de plus en plus ciblées et sophistiquées, contre nos entreprises et administrations. L'attaque sur le ministère de l'Economie et des Finances lors du sommet du G20 de février 2011 en est un parfait exemple. Par ailleurs, lors de mes stages en laboratoire, PME et administration, j'ai remarqué que le chiffrement des données sensibles n'est aujourd'hui que très rarement utilisé. Ce que j'ai voulu comprendre, c'est pourquoi, face au danger des cyber-attaques, certaines de nos entreprises et organisations continuent de ne pas utiliser cet outil à leur disposition pour se protéger C'est cette question qui m'a motivé à effectuer mon stage ingénieur dans le domaine de la cybersécurité et plus particulièrement chez Airbus Defense&Space.

Airbus Defense&Space, la division du groupe Airbus en charge des produits et services destinés aux usages militaires et astronautiques, a créé il y a 2 ans un département de cybersécurité composé d'une centaine d'experts dont la mission est de développer des solutions innovantes pour protéger les entreprises, gouvernements et infrastructures critiques contre le cyber espionnage et le cyber sabotage (anciennement Cassidian Cybersecurity). Des recherches sont effectuées en permanence dans ce département pour repérer comment de nouvelles découvertes scientifiques permettraient de déboucher sur des solutions innovantes et de lever des contraintes actuelles.

Le sujet de stage qui m'a été proposé portait sur comment explorer un domaine de la cryptographie moderne, encore cantonné au monde de la recherche académique, appelée Cryptographie Basée sur l'Identité (ou IBC pour *Indentity Based Cryptography*). Ce domaine, que j'avais repéré lors de mes lectures, me semblait extrêmement prometteur et j'avais l'intuition qu'il pourrait m'aider à répondre à mon interrogation sur la faible utilisation du chiffrement des données. Ma mission a consisté à faire un état de l'art du domaine, à en identifier les opportunités industrielles et les contraintes sous la forme d'un livre blanc, et pourquoi pas à aller plus loin en développant un prototype d'application.

La conclusion de mon étude a montré qu'il existe aujourd'hui deux mouvements antagonistes. D'un côté la bataille pour la sécurisation des données dans un contexte d'espionnage mondial, et de l'autre la volonté de pouvoir s'échanger toujours plus facilement et à moindre frais les données entre individus et organisations. C'est cet antagonisme qui me semble à l'origine de la faible utilisation du chiffrement que j'ai pu constater lors de mes différentes expériences. Mon étude, ainsi que le prototype que j'ai développé, tendent à montrer que la Cryptographie Basée sur l'Identité constitue un début de réponse permettant de réconcilier ces deux enjeux apparemment contradictoires.

Ce stage, constitue pour moi le travail le plus abouti de ma formation. J'ai pu y mettre à profit mes connaissances de scientifique et d'ingénieur pour transformer la recherche fondamentale en Cryptographie Basée sur l'Identité en un prototype de chiffrement innovant des emails pour Microsoft Outlook. Avoir pu contribuer à mon échelle, avec mon prototype et mon étude, à une meilleure protection de nos entreprises contre le cyber espionnage est une grande fierté et c'est qui me pousse à vouloir vous en parler davantage si j'en ai l'opportunité.