



Université Libre de Bruxelles
Faculté des sciences appliquées

BA2 orientation ingénieur civil

Visite d'entreprise

STMicroelectronics



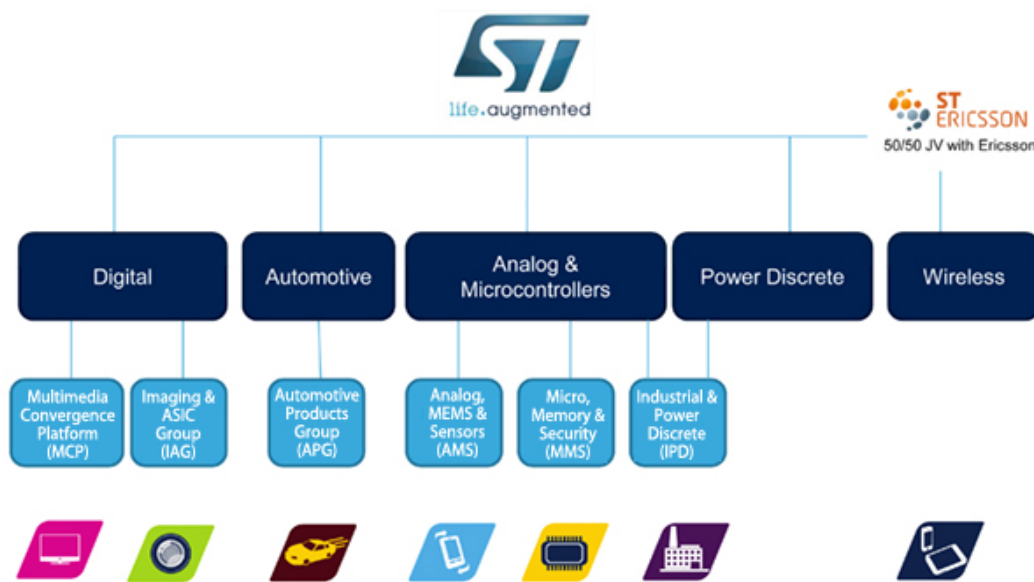
Delhayé Quentin
MECAH201

Bruxelles, 23 mars 2012

1 STMicroelectronics

ST STMicroelectronics est une société franco-italienne employant près de 50000 personnes dans le monde. C'est l'une des plus importantes entreprises dans le monde des semi-conducteurs, et elle a su au fil des 30 dernières années asseoir une réputation certaine autour de la marque.

ST officie dans différents domaines : computers, Home entertainment, automotive, wireless, MEMS, MCU et non-flash memories. En 2009, ST et Ericsson se sont associés pour fonder la co-entreprise *ST-Ericsson*, en charge de la division wireless. Si la division wireless est en perte de vitesse ces derniers temps, les MEMS sont en pleine expansion avec un chiffre d'affaire de 600 millions de dollars en 2011. Ces microcontrôleurs se retrouvent dans toute sorte d'appareils qui font la part belle d'un secteur en pleine expansion. Ce sont par exemple les capteurs gyroscopiques des smartphones et autres périphériques portables et ces derniers se vendent actuellement formidablement bien.



[www.st.com]

Zaventem Zaventem est la section Secure Microcontrollers, « Secure Software Solutions » (SSS), elle développe des logiciels dans et autour de puces (MCU). De telles puces se retrouvent par exemple sur les cartes de banque ou d'identité. La sécurité est donc très importante pour protéger les données contenues dans la puce du piratage tant software que hardware. Si le piratage matériel est bien plus difficile à mettre en œuvre, il ne faut pas le négliger pour autant. Il suffit d'un maillon faible dans la chaîne de sécurité pour rendre tout le système exposé.

Les ingénieurs aux commandes de ce département développent des modules ou des systèmes entiers de cryptographie, le tout le plus sécurisé possible. Cette cryptographie comporte deux grandes branches : la première développe les algorithmes et la seconde tente de les casser. Cette seconde étape subit une première batterie de tests en interne avant que la puce ne soit envoyée dans un laboratoire indépendant qui va pouvoir tester la sécurité du produit et lui apposer les labels idoines le cas échéant.

Ces tests reposent sur des scénarios très précis comportant jusqu'à plusieurs centaines de commandes. Il existe donc un besoin d'automatisation important afin d'être le plus efficace. Les résultats sont ensuite envoyés dans des logs pour analyse. Durant ces tests, on mesure à la fois l'endurance du chip et ses performances.

Le design des puces peut se faire à Zaventem, mais n'étant pas doté de ligne de production, il faut compter sur la fonderie la plus proche se trouvant à Grenoble. Cette distance implique de nouvelles difficultés lors du développement et des tests ; en effet, si c'est la partie matérielle qui s'avère déficiente, le projet doit être mis à l'arrêt jusqu'à la rectification de ces erreurs par une division externe.

TPM Un autre produit très important de la firme est le TPM (Trusted Platform Module). Ce module sert à la fois de vérificateur de l'intégrité physique de la plateforme sur laquelle il est installé (typiquement une carte mère, sur laquelle sont branchés divers périphériques), et de coffre-fort pour des clés de chiffrement ou pour générer ces clés. Il forme alors avec le BIOS une « chaîne de confiance », principe si cher à l'entreprise, qu'il faut respecter avant de pouvoir amorcer le démarrage du système d'exploitation.

Si ces modules sont encore actuellement principalement destinés au marché professionnel, ça pourrait bien changer dans les mois à venir avec la sortie du nouveau système de Microsoft, Windows 8, qui nécessiterait un tel module pour lancer l'amorçage du système. On se retrouverait alors avec une nouvelle part de marché pour ces puces et de nombreux nouveaux clients parmi les constructeurs de cartes mères.

SHA-3 Notons enfin que quelques-uns des développeurs de ST participent au « NIST hash function competition », dont le but est d'imposer un nouveau standard de fonction de hachage. Le fait qu'ils soient arrivés en finale démontre leur talent, et si ST n'y est pas directement liée, la publicité qu'elle peut en tirer est tout de même importante.

2 Rôle de l'ingénieur

Relation client, commandes Typiquement, quand un client les contacte, il faut tout d'abord essayer de comprendre ce qu'il veut exactement et voir dans quelle mesure son projet est réalisable. Cette étape de *reverse engineering* est essentielle pour correctement décrypter la demande du client et lui faire comprendre, le cas échéant, où sont les faiblesses de sa requête.

Vient ensuite la phase de modélisation du chip et du listing des opérations sur le chip. Ces specs évoluent tout au long du développement. Ces spécifications sont réutilisées un maximum car elles coûtent très cher en temps de développement, et il existe de toute façon de nombreux standards. Néanmoins, ces standards sont plus ou moins modifiés et personnalisés en fonction de l'importance du client, afin de rendre le produit fini vraiment unique de se démarquer de la concurrence.

Standards La mise à jour constante de ces standards entraîne des modifications régulières de l'architecture en cours de développement. Les développeurs doivent donc être constamment au courant de ces mises à jour et faire preuve d'une réactivité et adaptabilité suffisante pour adapter leur projet en conséquence sans accumuler trop de retard.

Contre-mesures Il faut ensuite implémenter la partie cryptographique sur la puce en y adjoignant un maximum de contre-mesures pour garantir sa sécurité. De telles contre-mesures permettent de masquer le fonctionnement réel de la puce à la vue de mesures extérieures. On peut par exemple mettre en place un système qui masquerait la consommation de la puce et l'intensité du courant parcourant ses circuits, évitant ainsi qu'on puisse déterminer le contenu d'un bit en fonction de sa consommation électrique. D'un point de vue logiciel, on peut masquer le fonctionnement du programme en fractionnant ses variables en partie aléatoirement. Chaque sous-variable sera ensuite traitée séparément avant d'être finalement assemblée aux autres.

Endurance Le chip est ensuite passé à une autre équipe d'ingénieurs chargés de tester son endurance et sa sécurisation. Outre la démarche exposée au chapitre 1, il faut aussi tester les capacités de la puce à fonctionner dans des situations pathologiques, comme en cas de coupure brusque de courant dans le circuit (on pense au retrait de la carte d'un lecteur alors qu'elle travaille). Différents mécanismes de sauvegarde et de sécurité sont censés assurer l'intégrité du système et ces mécanismes doivent bien entendu être vérifiés.

Expérience La moyenne d'âge des ingénieurs tourne autour des 40 ans. Il est donc évident qu'il faut « rouler sa bosse » et réussir à se faire une place dans l'entreprise. La plupart des intervenants ont d'ailleurs construit leur carrière en suivant les différentes restructurations de l'entreprise, depuis le rachat de Proton ou Banksys jusqu'à aujourd'hui.

Enfin, l'ingénieur n'a pas tant été présenté comme un créatif (les standards à respecter étouffant bien souvent cette créativité) que comme un expert technique dans un domaine somme toute très complexe.

3 Conclusion

Intérêt Cette présentation de l'entreprise fût très riche en informations diverses, tant au niveau des procédés de fabrication de leur produits, que de leur programmation. L'accent a été très largement mis sur la sécurité inhérente à leur travail ; celle-ci nous a été exposée par plusieurs intervenants principalement du point de vue de la cryptographie et des TPM, pour le côté matériel.

Publicité Ce qui était aussi important c'est l'attention portée à la présentation du travail effectué, sans publicité ou volonté affichée de recrutement. Ils ont beau eu nous présenter leur avantages et leurs points forts sur le marché, ils ne nous parlaient pas comme à des clients potentiels. C'est surtout le domaine de la micro-électronique dans lequel ils travaillent qui a été présenté en détails.

Spécialisation En ce qui concerne la spécialisation des ingénieurs, on a pu voir que la spécialisation de sortie n'était finalement pas si importante, et que c'est sa capacité à se former rapidement qui fait la plus grande force de l'ingénieur. On a aussi eu l'exemple d'un docteur qui s'est finalement retrouvé sur-qualifié en sortie de doctorat. Ce genre d'études post-maîtrise est donc à entreprendre en connaissance de cause, ou, comme dans le cas d'un second docteur, en mi-temps avec une entreprise. Ces conseils seront très certainement d'une aide précieuse le temps venu de choisir ou non de commencer un doctorat.