Michel Ugon, l'inventeur de la carte à microprocesseur nous a quittés

Jean-Louis Desvignes

Nous allions boucler ce bulletin quand une autre bien triste nouvelle est tombée.

L'un des plus illustres membres de l'ARCSI s'est éteint le 28 décembre dernier. Aucun article de presse, aucun flash n'a diffusé cette information et aucune autorité n'a salué le départ de cette figure pourtant reconnue mondialement.

Pourquoi ? Parce qu'il y a plus de cinquante ans, des journalistes ont préféré honorer l'un des leurs : un certain Roland Moreno qui, bénéficiant d'un accès à certaines informations industrielles avait réussi à déposer un brevet pour une carte à mémoire et ce faisant, à force de communication habile, à être déclaré inventeur de la carte à puce. Du moins d'une puce pas très douée puisqu'il ne s'agissait que d'une carte à mémoire.

Michel Ugon, ingénieur de génie, lui, a su doter le célèbre morceau de plastique d'un véritable calculateur implanté dans cette puce identifiable par ses connecteurs dorés que nous connaissons tous. Ce faisant Michel Ugon a érigé notre pays comme le berceau incontesté de cette technologie qui a inondé le monde. Aujourd'hui entre les cartes bancaires, les cartes SIM, les cartes de santé, les cartes d'identité, etc. ce sont des milliards de cartes qui sont en service à travers le monde. Pourtant

lorsqu'il aurait fallu monter au créneau pour faire reconnaître à qui en revenait vraiment le mérite aucun dirigeant de l'entreprise pour laquelle il avait travaillé, aucun responsable français de la recherche ou de l'industrie n'a eu la lucidité de le faire. Certes tardivement une petite fête a été organisée à l'observatoire de Meudon quand Michel a été admis à faire valoir ses droits à la retraite. Il lui fut offert un cadran solaire mais était-ce à la mesure de cette fantastique invention ?

La vie est ainsi faite, la blessure face à l'ingratitude et l'injustice fut profonde. D'autant que l'usurpateur ne cessait d'attirer les projecteurs sur sa piètre contribution. Pourtant lorsque vint le temps des épreuves pour la technologie de la carte à puce notre mystificateur faillit y laisser des plumes.

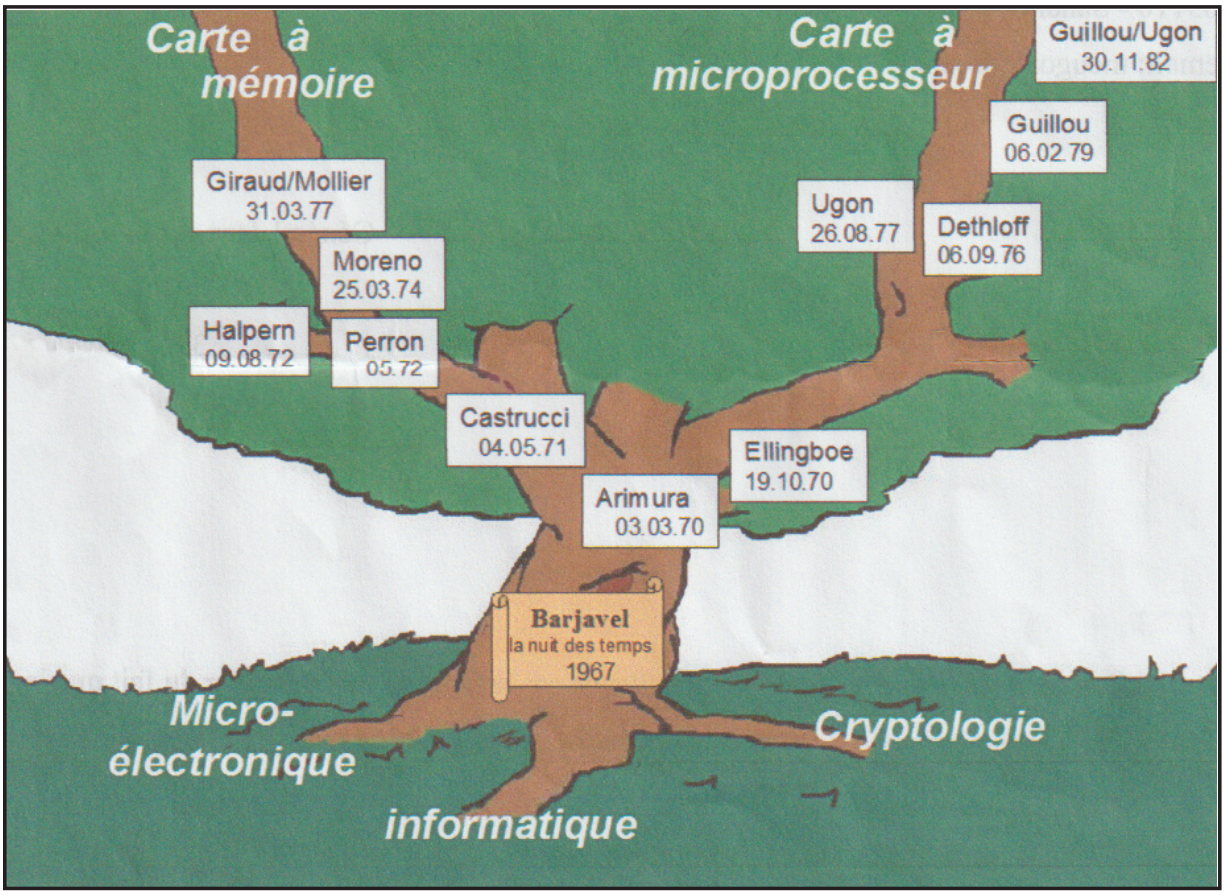
En effet, à la fin du siècle dernier, un informaticien curieux que l'on qualifia un temps de pirate, avait fait trembler le monde bancaire en réussissant à fabriquer de fausses cartes capables de leurrer certains automates. Serge Humpich était son nom. L'affaire fit grand bruit et le pouvoir décida de punir l'audacieux comme ce fut rapporté lors de notre dernier colloque à la Bibliothèque nationale de France en présence de l'intéressé. Flairant l'occasion de se faire de la publicité Moreno offrit alors un million de francs à qui casserait ses cartes. Son défi fit de gros titres dans la presse mais le lendemain il demandait à me voir. Il avait appris que le SCSSI pouvait le faire en 5 minutes. En fait c'était l'équipe de France Télécom que nous avions sauvée en la faisant racheter par le LETI qui faisait couramment la démonstration de révéler le code de cartes non sécurisées.

Je le reçus donc en le remerciant chaleureusement de nous offrir l'occasion d'arrondir nos fins de mois. Livide, il me demanda comment nous faisions. Malgré son insistance je me bornai à lui dire qu'il y avait les cambrioleurs qui n'hésitaient pas à combiner différentes techniques pour ouvrir un coffre. Il était clair que cet inventeur de génie n'avait pas encore entendu parler de DPA, attaque fondée sur l'analyse de la puissance consommée. J'avais ainsi la confirmation que cet imposteur avait du mal à suivre. Aussitôt il s'appliqua à durcir a posteriori les conditions de son offre…

Je dispose d'ailleurs d'une de ses lettres prouvant noir sur blanc qu'en 1978 il ne croyait pas à la carte à microprocesseur, et en tout cas pas avant 1985 disait-il, alors que Michel Ugon était en phase de finalisation de la réalisation de celle-ci. . . Mais Paix à son âme puisque décédé en 2012, et parce qu'il savait communiquer il a malgré tout contribué à la réputation de notre pays.

Michel Ugon lui, était de surcroît un être exquis, discret, d'une grande simplicité, d'une grande culture et d'une parfaite clarté dans ses explications. Il me fit l'honneur d'utiliser pour ses conférences quelques dessins humoristiques et pédagogiques que j'avais réalisés pour l'une des inaugurations des salons dédiés à la carte : CARTES 199x. dont il était en tant que président d'Eurosmart, l'un des principaux organisateurs.

Lui de son côté m'avait fait cadeau de l'arbre généalogique des brevets de la carte à puce reproduit ci-après. Il se trouve qu'un esprit malin a subrepticement modifié cet arbre en faisant disparaître les brevets antérieurs à celui de Moreno pour le reproduire dans un des panneaux de l'exposition sur la cryptologie de Rennes en 2012. À la grande fureur de Michel on s'en doute.



La généalogie des inventions

Michel Ugon nous avait fait le plaisir de participer en 2006 au colloque que j'avais décidé de tenir à Rennes au cours d'un week-end. Durant celui-ci nous eûmes le bonheur d'entendre l'un de ses complices Louis Guillou prononcer une conférence sur le *Zéro Knowledge*. Malheureusement leur autre complice dans cette aventure de la carte à puce n'était pas encore membre de l'ARCSI je veux parler de Jean-Jacques Quisquater bien évidemment. C'eut été fantastique de rassembler sur scène les trois héros de cette épopée d'un temps où l'Europe éclairait encore le monde.

Mais quelque temps plus tard Michel a vu sa santé s'altérer et m'a exprimé ses regrets de ne pouvoir continuer à participer à nos activités.

C'est Jean-Jacques qui m'a appris le décès de notre ami lui-même averti bien trop tard pour qu'on puisse organiser quelque hommage. Nous n'avons pu que partager notre grande tristesse.

Notre souhait bien évidemment est que son nom ne soit pas oublié et que chaque fois que possible justice lui soit rendue en rappelant que Michel Ugon est le véritable père de la carte à puce.

ELSEVIER

Computer Networks 36 (2001) 437–451

COMPUTER NETWORKS

www.elsevier.com/locate/comnet

Cryptographic authentication protocols for smart cards

L.C. Guillou [a,*], M. Ugon [b], J-J. Quisquater [c]

[a] *France Télécom R&D, DMI/DIR BP 59, 4 Rue du Clos Courtel, 35512 Cesson Sévigné, France*
[b] *Bull CP8, Louveciennes, France*
[c] *Math RiZK and UCL Crypto Group, Louvain La Neuve, Belgium*

Abstract

Today, cryptology is essential for security of information and communication systems. But 25 years ago, it was a classified and highly confidential activity. Presented here from the point of view of smart cards, this quick evolution of cryptology reflects the revolution of digital information, e.g., mobile phone and MPEG television. The link between smart cards and cryptology is very strong: smart cards efficiently confine keys and algorithms. Their security relies on a specific software, named here *secure-ware*, which demonstrates the value of the Common Criteria methodology. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Authentication; Identification; Digital signature; Local-area network; Smart card; Zero-knowledge protocol

1. Introduction

When integrity is threatened in a system transmitting information through time or space (see Fig. 1), at least the prover must protect its operation and keep it secret [6].

Depending on whether the prover is a user or a computer, we can distinguish user authentication and computer authentication.

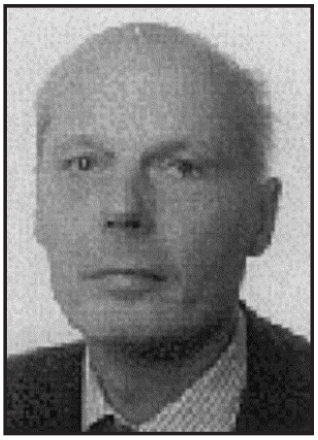
- A verifying computer, e.g., a server, a personal computer, a smart card, must recognize a user, i.e., a human being who has been previously registered. User authentication is based upon passwords and/or biometry; it is non-cryptographic, even if cryptography enforces security in any specific implementation.
- A verifying computer must be convinced that a proving computer, e.g., a server, a personal computer, a smart card, is authorized to perform a specific action, e.g., genuinely represents an authorized user; the verifying computer controls access to resources. Computer authentication is cryptographic: then both proving and verifying operations are beyond human-brain capability.

This paper considers computer authentication where at least one computer is a smart card: a prover (*claimant*) knows a secret; it wants to convince a verifier without revealing the secret so as to use it over and over.

- In *symmetric authentication*, the verifier knows either the secret (e.g., a *secret key*) or an image of the secret (e.g., a *password* image).
- In *asymmetric authentication*, the verifier knows a *public key* corresponding to a *private key*

* Corresponding author. Fax: +33-2-9912-3600.
E-mail addresses: louis.guillou@francetelecom.com (L.C. Guillou), michel.ugon@bull.net (M. Ugon), quisquater@dice.ucl.ac.be (J.-J. Quisquater).

PII: S1389-1286(01)00165-7



Première page de l'article « *Cryptographic authentication protocols for smart cards* » (Computer Networks - Volume 36-4, 16 juillet 2001, pages 437-451) et photos des trois auteurs