WWW.ARTECH-GE.CH

Mot du Président

Chers membres,

Il y a un certain temps (mars 2003) que nous avons commencé une campagne publicitaire concernant notre association. Celle-ci commence à porter ses fruits. En effet, nous pouvons nous réjouir d'accueillir de nouveaux membres et c'est pourquoi, le comité a décidé de continuer cette campagne.

La prochaine assemblée des délégués suisse aura lieu à Olten le 15 mai 2004. Cette année, encore bien des changements se profilent au sein de l'ASET. Il est question que l'ASET revoie à la hausse ses cotisations. L'an passé nous avons refusé ce budget (nous n'étions pas les seuls !) et cette année l'ASET recommence. Nous voterons encore une fois non, car les nouveaux montants de la cotisation me semblent disproportionnés par rapport aux services rendus. Je ne suis pas négatif, mais j'estime être juste.

Ce n'est pas la première fois que l'ARTech a des différents avec l'ASET et chaque fois, après discussion, nous avons réussi à nous entendre. Il n'y a donc pas de raison que cela change !

De plus, nous avons créé une nouvelle rubrique sur notre site Internet. Cette rubrique est consacrée aux petites annonces (vente, achat, location …) de nos membres (exclusivement !). Il suffit simplement d'envoyer vos petites annonces à notre Webmaster (Thibault) qui se fera un plaisir de les placer sur le site se l'ARTech.

A bientôt

Didier Moullet
Président ARTech section GE

La biométrie

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que les autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. D'autre part, les caractéristiques physiques sont loin d'être si parfaites et si précises, et l'on atteint très vite des limites pour ces techniques.

Les techniques basées sur la biométrie jouissent à l'heure actuelle d'un engouement général favorisé par un phénomène de mode, principalement véhiculé par les films au cinéma et à la télévision. Ainsi, il n'est pas rare de voir des scanners rétiniens avec de superbes lasers rouges, des lecteurs d'empreintes digitales avec de très jolis voyants clignotants, etc… tout cela représentant le summum de la technologie du contrôle d'accès. Or, les techniques de biométrie sont belle et bien en train de se répandre dans notre vie quotidienne, et ce tout en gardant une image quelque peu trompeuse.

Car le problème est bien de savoir quelles techniques existent réellement, et quelles sont leurs limites.

CARACTÉRISTIQUES PHYSIQUES

Il existe plusieurs caractéristiques physiques qui se révèlent être uniques pour un individu, et il existe également pour chacune d'entre elles plusieurs façons de les mesurer.

1) – Les empreintes digitales (finger-scan).

La donnée de base dans le cas des empreintes digitales est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu. En pratique, il est quasiment impossible d'utiliser toutes les informations fournies par ce dessin (car trop nombreuses pour chaque individu), on préférera donc en extraire les caractéristiques principales telles que les bifurcations de crêtes, les "îles", les lignes qui disparaissent, etc… Une empreinte complète contient en moyenne une centaine de ces points caractéristiques (***les minuties***). Si l'on considère la zone réellement scannée, on peut extraire environ 40 de ces points. Pourtant, là encore, les produits proposés sur le marché ne se basent que sur une quinzaine de ces points (12 au minimum vis-à-vis de la loi), voire moins pour beaucoup d'entre eux (jusqu'à 8 minimum).
Pour l'histoire, le nombre 12 provient de la règle des 12 points selon laquelle il est statistiquement impossible de trouver 2 individus présentants les mêmes 12 points caractéristiques, même en considérant une population de plusieurs dizaines de millions de personnes.

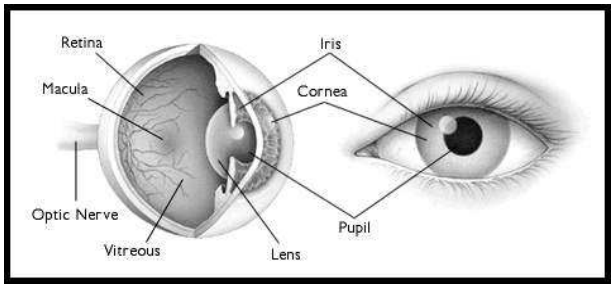
Les techniques utilisées pour la mesure sont diverses: capteurs optiques (caméras CCD/CMOS), capteurs ultrasoniques, capteurs de champ électrique, de capacité, de température…
Ces capteurs sont souvent doublés d'une mesure visant à établir la validité de l'échantillon soumis (autrement dit, qu'il s'agit bien d'un doigt): mesure de la constante diélectrique relative de l'échantillon, sa conductivité, les battements de cœur, la pression sanguine, voire une mesure de l'empreinte sous l'épiderme…

2) – La géométrie de la main (hand-scan).

Ce type de mesure biométrique est l'un des plus répandus, notamment aux Etats-Unis. Cela consiste à mesurer plusieurs caractéristiques de la main (jusqu'à 90) tel que la forme de la main, longueur et largeur des doigts, formes des articulations, longueurs inter-articulations, etc… La technologie associée à cela est principalement de l'imagerie infrarouge; d'une façon générale, le système présente des ***FAR*** (***False Acceptation Rate***) assez élevés, surtout entre personnes de la même famille ou bien des jumeaux.

3) – L'iris (iris-scan).

Pour les 2 techniques suivantes, il faut tout d'abord faire la distinction entre l'iris et la rétine.



En ce qui concerne l'iris, l'individu se place en face du capteur (caméra CCD/CMOS) qui scanne son iris. Celui-ci représente quelque chose de très intéressant pour la biométrie car il est à la fois toujours différent (même entre jumeaux, entre l'œil droit et le gauche, etc…), indépendant du code génétique de l'individu et très difficilement falsifiable. En effet, l'iris présente une quasi-infinité de points caractéristiques (que certains comparent en nombre à ceux de l'ADN), qui ne varient pratiquement pas pendant la vie d'une personne contrairement à ***la couleur de l'iris*** qui, elle, peut changer. Mais cela n'a aucune influence car les images d'iris obtenues par les capteurs sont en noir et blanc.
Le seul problème de cette technique est lié à la mesure en elle-même, qui peut être source d'erreurs ou de problèmes. Ainsi, on peut quasiment dire que le nombre de problèmes rencontrés lors de cette mesure augmente proportionnellement avec la distance entre l'œil et la caméra.

D'autres problèmes se posent à cause des reflets (nécessité d'avoir un éclairage restreint et maîtrisé), et lors de la détection de faux yeux (photos) et autres fraudes. Pour ces dernières, on peut faire appel à certaines caractéristiques dynamiques de l'œil qui prouveront son authenticité : réactivité de la pupille (dilatation/rétraction) par rapport à la quantité de lumière, étude de l'iris dans l'infrarouge et l'ultraviolet, etc…

4) – La rétine (retina-scan).

Cette mesure biométrique est plus ancienne que celle utilisant l'iris, mais elle a été moins bien acceptée par le public et les utilisateurs, sans doute à cause de son caractère trop contraignant: la mesure doit s'effectuer à très faible distance du capteur (quelques centimètres), qui effectue ensuite un balayage de la rétine. Il est physiquement impossible d'effectuer une mesure rétinienne à une distance de 30cm ou plus sur un sujet mobile comme on peut le voir dans certains films. Cette méthode requiert des sujets coopératifs et entraînés.

Pourtant, cette technique semble être tout aussi fiable que celle de l'iris; elle se base sur le fait que le schéma et le dessin formé par les vaisseaux sanguins de la rétine (la paroi interne et opposée de l'œil) sont unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne. La mesure peut fournir jusqu'à 400 points caractéristiques du sujet, que l'on peut comparer aux 30 à 40 points fournis par une empreinte digitale !

En conclusion, la mesure rétinienne est la plus difficile à utiliser mais également la plus dure à contrefaire.

4) – Le visage (facial-scan).

Il s'agit ici de faire une photographie plus ou moins évoluée pour en extraire un ensemble de facteurs qui se veulent propres à chaque individu. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage tel que le haut des joues, les coins de la bouche, etc… On évitera d'autre part les types de coiffures, les zones occupées par des cheveux en général ou toute zone sujette à modification durant la vie de la personne.

Il existe plusieurs variantes de la technologie de reconnaissance du visage. La première est développée et supportée par le MIT et se nomme ***"Eigenface"***. Elle consiste à décomposer le visage en plusieurs images faites de nuances de gris, chacune mettant en évidence une caractéristique particulière.
Une autre technique appelée ***"Feature Analysis"*** se base sur la précédente en y rajoutant des informations sur les distances inter-éléments, leurs positions, etc… Elle se dit plus souple quant aux éventuelles modifications pouvant survenir: angle de prise de vue, inclinaison de la tête, etc… Viennent ensuite des techniques moins utilisées à l'heure actuelle, basée sur des réseaux neuronaux, sur des méthodes plus techniques et moins souples.

5) – Système et configuration des veines (vein pattern-scan).

Cette technique est habituellement combinée à une autre, comme l'étude de la géométrie de la main. Il s'agit ici d'analyser le dessin formé par le réseau des veines sur une partie du corps d'un individu (la main) pour en garder quelques points caractéristiques.

CARACTÉRISTIQUES COMPORTEMENTALES

Outre les caractéristiques physiques, un individu possède également plusieurs éléments liés à son comportement qui lui sont propres.

1) – Dynamique des frappes au clavier (keystone-scan).

Les frappes au clavier sont influencées par plusieurs choses; tout d'abord, selon le texte que l'on tape et, de manière plus générale selon sa nature, on aura tendance à modifier sa façon de taper au clavier. C'est d'ailleurs un des moyens utilisés par certaines attaques (***timing attacks***) pour essayer d'inférer le contenu ou la nature du texte tapé de façon à remonter jusqu'à un mot de passe par exemple. Ces techniques sont assez satisfaisantes mais restent néanmoins statistiques.
Ensuite, le facteur comportemental entre en jeu, et ce facteur va être différent pour chaque individu. Les facteurs sont, à peu de chose près, identiques à ceux évoqués précédemment: ce sont les durées entre frappes, la fréquence des erreurs, durée de la frappe elle-même… La différence se situe plus au niveau de l'analyse, qui peut-être soit statique et basée sur des réseaux neuronaux, soit dynamique et statistiques (comparaison continuelle entre l'échantillon et la référence).

2) – Reconnaissance vocale (voice-scan).

Les données utilisées par la reconnaissance vocale proviennent à la fois de facteurs physiologiques et comportementaux. Ils ne sont en général pas imitables.

3) – Dynamique des signatures (signature-scan).

Ce type de biométrie est à l'heure actuelle peu utilisé mais ses défenseurs espèrent l'imposer assez rapidement pour des applications spécifiques (documents électroniques, rapports, contrats…). Le procédé est habituellement combiné à une palette graphique (ou équivalent) munie d'un stylo. Ce dispositif va mesurer plusieurs caractéristiques lors de la signature, tel que la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total, etc… Bref, tout ce qui peut permettre d'identifier une personne de la manière la plus sure possible quand on utilise une donnée aussi changeante que la signature.

NOUVELLES TECHNIQUES

Il existe plusieurs techniques en cours de développement à l'heure actuelle; parmi celle-ci, citons la biométrie basée sur la ***géométrie de l'oreille***, ***les odeurs***, ***les pores de la peau***, et ***les tests ADN***. Sur ce dernier point, il est intéressant de souligner que le procédé peut se révéler menaçant tant au niveau de la vie privée des personnes, de leur liberté que des dérives informatiques éventuelles /et autres Big Brothers). En effet, même si cela dépend de la technique mise en œuvre, le test ADN est quelque chose qui peut se révéler comme exact et sûr à 100%, autorisant des ***FFR (False Rejection Rate)*** et des ***FAR (False Acceptation Rate)*** nuls. Il est également reconnu de façon universelle et permettrait très facilement d'effectuer des recoupements entre bases de données. Autrement dit, ce serait le moyen idéal pour "cataloguer" les personnes et détruire ainsi la vie privée que nous avons respectée jusqu'à présent.

INCONVÉNIENTS DE LA BIOMÉTRIE

La biométrie présente malheureusement un inconvénient majeur. En effet, aucune des mesures utilisées ne se révèle être totalement exacte car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant: on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins important, bref, on évolue et les mesures changent.

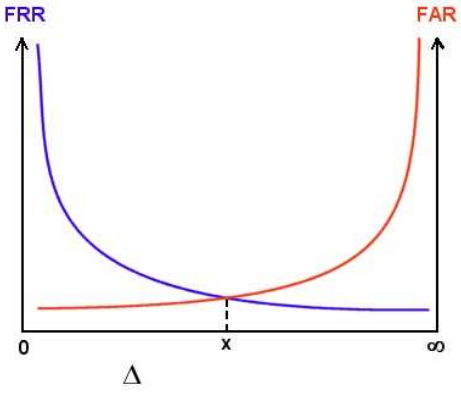
Prenons le cas le plus simple, celui des empreintes digitales. Suivant les cas, nous présentons plus ou moins de transpiration. La température des doigts est tout sauf régulière (en moyenne de 8 à 10°C au-dessus de la température ambiante) et il suffit de se couper pour présenter une anomalie dans le dessin de

ses empreintes. Bref, dans la majorité des cas, la mesure retournera un résultat différent de la mesure initiale de référence. Or il faut pourtant bien réussir à se faire reconnaître, et en réalité cela marchera dans la plupart des cas car le système autorise une marge d'erreur entre la mesure et la référence.

Les fabricants ne recherchent nullement la sécurité absolue, ils veulent quelque chose qui fonctionne dans la pratique. Ils cherchent donc à diminuer le taux de faux rejets ***(FRR)***, tout en maintenant un taux relativement bas de fausses acceptations ***(FAR)***.

Explications: Un ***FR*** est le fait de rejeter une personne autorisée en temps normal car sa mesure biométrique présente trop d'écart par rapport à la mesure de référence pour cette même personne. **Un système fonctionnel aura un FFR le plus bas possible**. D'autre part, un ***FA*** est le fait d'accepter une personne non-autorisée. Cela peut arriver si la personne a falsifié la donnée biométrique ou si la mesure la confond avec une autre personne. **Un système sûr aura un FAR le plus bas possible.**

Dans la vie courante, les industriels cherchent principalement à avoir un compromis entre ces 2 taux, FRR et FAR, qui sont liés suivant une relation illustrée ci-dessous.



Ce graphe est purement démonstratif; delta représente la marge d'erreur autorisée par le système, variant de 0 à l'infini. Très succinctement, on voit que plus la marge d'erreur autorisée est importante, plus le taux de fausses acceptations augmente, c'est-à-dire que l'on va accepter de plus en plus de personnes qui ne sont pas autorisées (et donc la sécurité du système diminue). Par contre, on voit que le taux de rejet des personnes autorisées diminue également, ce qui rend le système plus fonctionnel et répond mieux aux attentes des utilisateurs. A l'autre extrémité, si l'on diminue la marge d'erreur acceptée par le procédé de mesure biométrique, les tendances des 2 taux sont inversées: on va de moins en moins accepter des individus essayant de frauder mais on va également, par la même occasion, avoir un taux de rejet sur des personnes autorisées qui sera trop important pour être toléré dans la plupart des cas. Le compromis habituel est de prendre la jonction des courbes, c'est à dire le point X où le couple (FAR, FRR) est minimal.

En conclusion, toute la biométrie peut se résumer pour les plus pessimistes à ce seul compromis qui fausse toute la confiance que l'on pourrait porter à cette technologie.

EXEMPLE DE VULNÉRABILITÉ

Les empreintes digitales représentent sans aucun doute les données biométriques les plus couramment utilisées. De ce fait, on trouve un grand nombre de produits disponibles sur le marché mais également beaucoup de travaux sur le sujet et de contrefaçons dans ce domaine.

Il convient tout d'abord de se procurer les données fondamentales de la mesure, c'est-à-dire les points caractéristiques de l'empreinte digitale que l'on veut contrefaire, en fabriquant un faux doigt (fine couche de silicone reproduisant la géométrie du doigt). Je ne donnerai pas le mode opératoire, mais sachez qu'il est tout à fait possible et simple de créer un faux doigt à partir d'une simple empreinte sur un verre, sur un clavier, sur une poignée, … Ensuite, examinons les cas pour chaque type de capteur.

1) – Capteur de température.

La fine couche de silicone ne fait varier la température que de 1 à 3°C en moyenne. Ce qui n'est pas détectable par les capteurs sous peine d'avoir une FRR trop élevée (surtout en extérieur).

2) – Capteur de battements cardiaques.

La fine couche de silicone permet au capteur de fonctionner normalement. De plus, toute discrimination basée sur cette mesure est physiquement impossible et infaisable. Infaisable car

dans le cas de sportifs, par exemple, leur rythme cardiaque peut descendre jusqu'à 40 battements/min, ce qui suppose une mesure durant plus de 4 secondes pour pouvoir évaluer la fréquence cardiaque. Impossible car quoi de plus changeant qu'un rythme cardiaque ? Le moindre effort le modifie ce qui le rend inutilisable dans notre cas.

3) – Capteur de conductivité.

Suivant le type de capteur, on estime la valeur normale pour la peau à 200 kOhms. Néanmoins, cette valeur sera de plusieurs MOhms pendant l'hiver (sec) pour descendre à quelques kOhms durant un été humide. Dans ces conditions, il est évident qu'un faux doigt pourra passer le test sans trop de soucis.

4) – Constante diélectrique relative.

Très succinctement, cette constante identifie dans quelle mesure un matériau concentre les lignes électrostatiques de flux. Ici, la silicone sera rejetée puisque présentant une valeur trop différente de celle de la peau. Or, il s'avère que la valeur de cette constante pour la peau se situe entre celle de l'eau (80) et celle de l'alcool (24). Autrement dit, il suffit d'enduire le faux doigt d'un mélange eau-alcool (80/20 ou 90/10), de poser le doigt sur le capteur et d'attendre que l'alcool s'évapore. En effet, lorsque l'alcool s'évapore, la valeur de la constante va remonter vers celle de l'eau (de 24 à 80) et atteindre au passage celle de la peau. CQFD !!!

De manière générale, les faiblesses de ces systèmes ne se situent pas au niveau de la particularité physique sur laquelle ils reposent, mais bien sur la façon dont ils la mesurent, et la marge d'erreur qu'ils autorisent. Là encore, il convient de ne pas se laisser impressionner par une image illusoire de haute technologie - produit miracle.

LIMITE DE CETTE TECHNOLOGIE

Les données biométriques ne devraient pas être utilisées seules pour de l'authentification forte car elles ne sont pas modifiables puisque par nature elles sont propres à chaque individu. On ne peut donc pas se permettre de se baser uniquement dessus, d'autant plus que nous avons vu qu'elles ne sont pas fiables à 100% (FAR/FRR). En règle générale, on préférera utiliser la biométrie dans le cadre d'un schéma d'identification plutôt que pour faire de l'authentification.

Les données biométriques sont comparables à tout autre système de contrôle d'accès comme des mots de passe, etc… , car du point de vue du système informatique, ce ne sont rien d'autre que des séries

de bits comme toute donnée. Autrement dit, la difficulté réside dans la contrefaçon de la caractéristique physique et biologique que l'on mesure, mais en aucun cas dans sa valeur numérisée (digitale).
Prenons l'exemple de notre vieil ami, le login/mot de passe. Ce système est souvent décrit comme peu sûr car une des principales attaques consiste à épier les transactions durant un processus de login pour récupérer les données utiles et les rejouer. On voit que même dans le cas des techniques basées sur la biométrie, cela reste possible ! A quoi bon se compliquer la tâche en essayant de reproduire une empreinte alors que l'on peut récupérer les données numérisées directement ? Ou si l'on peut attaquer les bases de données contenant toutes les données biométriques de référence ?

CONCLUSION

On peut retenir plusieurs faits marquants concernant la biométrie:

- Il ne suffit pas de remplacer un login/mot de passe par une mesure de biométrie. Il faut également repenser tout le système et sécuriser l'architecture complète.
- Il ne faut pas utiliser une mesure biométrique seule pour procéder à une authentification. On préférera la coupler avec une carte à puce, un ***token*** sécurisé (petit élément de stockage présentant une grande résistance aux attaques, même physiques), un mot de passe.
- On utilisera la biométrie de préférence pour les opérations d'identification plutôt que d'authentification.
- Enfin, perdons une fois pour toutes cette image de technologie ultra sûre faussement propagée par les médias. La biométrie n'est nullement une ***solution miracle et universelle***.

(Source : Web) C.B.

Reconnaissance des diplômes dans l'UE

L'accord sur la libre circulation des personnes, entré en vigueur le 1er juin 2002, entraîne la reconnaissance réciproque des diplômes et certificats de capacité entre la Suisse et l'UE, mais les dispositions varient d'un pays à l'autre.

Pour aider les personnes concernées à y voir plus clair, le Bureau de l'intégration ***DFAE/DFE*** a rédigé une brochure comprenant des informations utiles et des adresses relatives à la reconnaissance des diplômes dans les pays de l'UE.
Chaque pays membre de l'Union décerne ses propres titres permettant l'exercice de diverses professions, ce qui entrave la mobilité des travailleurs. Pour surmonter cet obstacle, l'UE a mis en place un système de reconnaissance réciproque des diplômes et certificats de capacité. Suite à l'accord sur la libre circulation des personnes, la Suisse fait partie de ce système.

Les nouvelles brochures intitulées ***"Diplômes suisses dans l'UE"*** et ***"Diplômes de l'UE en Suisse"*** explique les règles qu'il convient d'observer. Elle donne également les adresses des principales instances de Suisse et de l'étranger qui sont compétentes pour examiner les demandes de reconnaissance des diplômes.

Ces brochures sont disponibles sur le site de l'Artech (**www.artech-ge.ch**) dans la rubrique "Liens" ou sur le site **www.europa.admin.ch/pub/best/f/index.htm**

C. Battagliero

Sorties et activités

Cette année, nous organisons une sortie "fun et familial" d'une journée à la ***Forêt de l'Aventure*** à Talloires (près d'Annecy).

A 1000 m d'altitude, le site de Talloires offre une vue plongeante sur le lac d'Annecy. Une magnifique forêt de montagne aux essences variées vous attend pour des moments inoubliables dans les arbres…

Le site comprend : **1 grand parcours** pour adultes et jeunes (minimum 1.40m)
1 parcours kids pour enfants et plus petits (minimum 5 ans et 1.10m)
1 parcours X' Trem Equilibre pour les … courageux !

La date de la sortie est fixée au **Samedi 5 juin 2004 !!!**

La date limite d'inscription est fixée au **Samedi 22 mai 2004 !!!**

Une partie de l'inscription (pour les membres) sera prise en charge par l'ARTech. Conjoints et enfants sont les bienvenus.

Pour tout renseignement et inscription vous pouvez me contacter aux numéros suivants:

022 / 780.78.15 (prof.)
079 / 729.79.38

Amicalement

M. Berchten

PAUSE – CAFÉ

1– Carré naturel

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Le carré naturel ci-dessus peut-être qualifié de naturel, car on y a écrit les entiers strictement positifs dans l'ordre, ligne après ligne, d'une façon toute "naturelle".

Calculez la somme de 5 nombres de ce carré choisis de telle façon que deux quelconques d'entre eux n'appartiennent jamais à la même ligne ni à la même colonne.

2– Les cartons

Le nouveau matériel informatique vient d'être livré ! Il est emballé dans plusieurs cartons parallélépipèdiques tous différents et dont les dimensions sont toutes des nombres entiers de décimètres. De plus, fait surprenant, chaque carton satisfait à la propriété suivante: le nombre de dm^2 de son aire totale est égal au double du nombre de dm^3 de son volume !

Combien y-a-t-il de cartons au maximum ? Et quelles sont alors leurs dimensions ?

Liste des membres

ANDREETA Pierre	Plan-les-Ouates	Electronique
BACHMANN Jean-Jacques	Grandson	Electronique
BAEZA Alexandre	Le Lignon	Electronique
BAJULAZ Alain	Aire-la-Ville	Génie Civil
BARRAS Pierre Léon	Carouge	Génie Civil
BASSO Roberto	Meyrin	Génie Chimique
BATTAGLIERO Christophe	Valleiry (F)	Génie Chimique
BERCHTEN Marc	Challex (F)	Génie Chimique
BOCHATAY Olivier	Vernayaz	Mécanique
BORDIGNON Alain	Grand-Saconnex	Génie Civil
BOUNAB Deif	Prilly	Génie Civil
BUCLIN Marc	Bernex	Electronique
CARNEIRO SOARES Paulo	Genève	Génie Civil
CARRETI Robert	Gaillard (F)	Mécanique
CHARLET Manuel	Bellevue	Electronique
COMINA Michel	Genève	Génie Civil
CRETTAZ Raphaël	Chardonne	Graphisme
DAENZER Frédéric	Les Moulins	Electronique
DE FARIA Luis Miguel	Genève	Electronique
DECAILLET Alain	Genève	Electronique
DESCHENAUX Jean-Paul	Carouge	Génie Civil
DESIMONE Laurent	Epalinges	Informatique
DEVAUD Daniel	Fribourg	Mécanique
DI LUCA Serge	St Genis-Pouilly (F)	Electronique
DIVOUX Jean-Noël	La Chaux-de-Fonds	Electronique
DONADELLI Igor	Renens	
DUMONT Laurent	Monthey	Mécanique
ESSELBORN Philippe	Mies	Génie Chimique
FERRIERO Giuseppe	Coppet	Electronique
FRATERNALE Olivier	Vernier	Mécanique
FREIHOLZ Alain	Founex	Informatique
GIROUD Jean-Louis	Vandoeuvres	Mécanique
GUIDI Marco	Perly	Mécanique
GUISOLAN Alain	Sergy Haut (F)	Mécanique
HARTH René	Genève	Mécanique
HARVEY Mark	Genève	Instrumentation
HAUSAMANN Laurent	Villars-Burquin	Electronique
HEIMO Philippe	Croix-de-Rozon	Informatique
IMBRUGLIA Piero	Genève	Génie Chimique
JANUSZEWSKI Yves	Bernex	Mécanique
KUNZ Philippe	Chêne-Bourg	Génie Civil
LANZILLOTTA Agostino	Corsier/Vevey	Génie Civil
LEGRAND Christian	Châtillon-sur-Cluses (F)	Electronique
LEVRAT Olivier	Genthod	Electronique

MAURY Christian	Préverenges	Génie Civil
MEYLAN Mathieu	Renens	Informatique
MONVAL Robert	Bellegarde (F)	Génie Civil
MONNET Raphaël	Bex	Mécanique
MOSER Marc-André	Petit-Lancy	Electronique
MOULLET Didier	Carouge	Electronique
NINO Francisco Javier	Genève	
NUSBAUMER Jean-Marc	Carouge	Génie-Civil
PASCHE Michel	Chexbres	Electronique
PAULY Alain	Petit-Lancy	Graphisme
PERRIER Eric	Orbe	Mécanique
PIACENZA Alain	Saint-Cergue	Génie Civil
PONCE Jorge	Nyon	Electronique
PRADERVAND Alain	Vandoeuvres	Mécanique
ROESSLI Pierre-Alain	Sierre	Informatique
ROULET Thibault	Thônex	Informatique
SCHÄR Frédéric	Meyrin	Electronique
SCHWOB Jean	Bassins	Mécanique
SEGATORI Jean-François	Denens	Mécanique
SIEGFRIED Catherine	Yvoire (F)	Génie Chimique
STEULET Christophe	Grand-Lancy	Electronique
VAGNI Giorgio	Genève	Electronique
VILLAR Elias	Lausanne	Mécanique
VON WARTENSLEBEN Aurélie	Grand-Saconnex	Génie Chimique
VUAGNAT Olivier	Carouge	Génie Civil
ZEHNDER Jacques	Bellevue	Genie Civil
ZILTENER Joseph	Dielsdorf	Mécanique

Liste des nouveaux membres

Nous avons le plaisir d'accueillir 8 nouveaux membres cette année :

DAENZER Frédéric	Les Moulins
DEVAUD Daniel	Fribourg
FRATERNALE Olivier	Vernier
HARVEY Mark	Genève
LANZILLOTA Agostino	Corsier/Vevey
MEYLAN Mathieu	Renens
MONNET Raphaël	Bex
VILLAR Elias	Lausanne

Le comité de l'Artech leur souhaite la bienvenue dans notre association.

Composition du comité 2004

Président	**Didier MOULLET**	Tél. privé	:	022 343 82 86
	3 rue du Pont-Neuf	Tél. prof.	:	022 709 06 96
	1227 Carouge	Natel	:	079 442 10 47
		Fax	:	022 343 82 88
		E-mail	:	didier@artech.ch
Attaché relation ASET	**Philippe ESSELBORN**	Tél. privé	:	079 518 95 07
	10 route de Suisse	Tél. prof.	:	022 363 46 51
	1295 Mies	E-mail	:	
	philippe@agtech.ch			
Trésorier	**Serge DI LUCA**	Tél. privé	:	+33 450 20 33 60
	11 rue de Pouilly	Tél. prof	:	022 767 56 40
	F-01630 St Genis-Pouilly	Natel	:	079 201 40 00
		E-mail	:	serge@artech.ch
Secrétaire	**Laurent DUMONT**	Tél. privé	:	024 471 08 46
	6 route du Tonkin	E-mail	:	laurent@artech.ch
	1870 Monthey			
Rédacteur bulletin / Archiviste	**Christophe BATTAGLIERO**	Tél privé :	:	+33 450 04 39 27
	Les Erables Bât. D	Tél prof.	:	022 780 21 95
	F-74520 Valleiry	E-mail	:	
	christophe@agtech.ch			
Rédacteur bulletin	**Marc BERCHTEN**	Natel	:	079 729 79 38
	15 rue Gourgas	Tél prof.	:	022 780 78 15
	1205 Genève	E-mail	:	marc@artech.ch
Webmaster	**Thibault ROULET**	Tél. privé	:	022 348 31 23
	22 ch. Edouard-Olivet	E-mail	:	thibault@artech.ch
	1226 Thônex			

Solution carré naturel p 10

Chaque case du carré peut-être repérée par son numéro de ligne (de haut en bas par ex.) et son numéro de colonne (de gauche à droite). Ainsi la case A2;3 est la 3^{e} case de la 2^{e} ligne, qui contient le nombre 8. En assimilant chaque case au nombre qu'elle contient, on peut montrer que pour tout "i" et pour tout "j" variant de 1 à 5, Ai;j = 5(j-1)+i . Si on choisit 5 nombres tels que 2 quelconques d'entre eux n'appartiennent jamais ni à la même ligne, ni à la même colonne, on a 5 valeurs de Ai;j telles que l'on n'ait jamais deux fois le même i ni jamais deux fois le même j . Toutes les valeurs de i et toutes les valeurs de j sont donc représentées. En additionnant les 5 nombres, on obtient alors une somme S égale à (1+2+3+4+5) + 5(0+1+2+3+4) = 65 .
Dans un carré de n cases de côté, on obtiendrait une somme égale à n (n^2+1)/2 , qui est … la constante des carrés magiques d'ordre n .

Solution les cartons p 10

Désignons par a, b, c les dimensions d'un carton (on suppose a ≥ b ≥ c). On doit avoir ab + bc + ca = abc, avec a, b et c entiers positifs. On en déduit :

$$a = \frac{bc}{bc - (b+c)} \quad \text{d'où} \quad b < \frac{bc}{bc - (b+c)} \quad \text{et } 1 \leq c \leq b/(b+2)$$

Le nombre c devant être entier, on est conduit aux seules valeurs du tableau ci-dessous.

a	**b**	**c**
3	3	3
6	3	2
-3	3	1
4	4	2
-4	4	1

Le matériel a donc été livré dans 3 cartons au maximum, de dimensions respectives: (6 dm ; 3 dm ; 2 dm), (4 dm ; 4 dm ; 2 dm) et (3 dm ; 3 dm ; 3 dm).

ON THE WEB…

Windpower …

Tout sur l'énergie éolienne. L'association danoise de l'industrie éolienne vous propose visite guidée, quizz et matériel pour se familiariser avec cette énergie dans le vent.

www.windpower.org

Aéronautique

Pour tous savoir sur les sillages laissés par les avions et pour le plaisir des yeux …

www.onera.fr

Minéraux

Pour les amateurs de minéraux, cette énorme base de données vaut le détour. Plus de 11'000 substances listées et 4'000 décrites (localisations, propriétés physico-chimiques, structure cristalline, etc.). Outre une importante galerie de photos, la base de données est régulièrement mise à jour.

www.mindat.org

C.B.

Impressum	
Editeur :	comité ARTech
Rédaction :	Christophe Battagliero Marc Berchten Didier Moullet
Mise en pages :	Ch. Battagliero
Correspondance :	ARTech Case postale 5490 1211 Genève 11 Stand
e-mail :	contact@artech.ch
Le bulletin de l'AGT :	parait 2x par an
Tirage :	80 exemplaires