

Sécurité et protection de la vie privée sur Internet

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS



La sécurité des réseaux s'améliore

- ❖ Législation (mars 2000) sur les signatures électroniques -> IGC (PKI)
- ❖ IP-Sec -> IPv6
- ❖ Progrès de la détection d'intrusions

... mais croissance des menaces

- ❖ DDoS
- ❖ Fraude dans l'e-Commerce
- ❖ Criminalité transfrontière
- ❖ ... et les failles sont nombreuses!

... d'où encore plus de sécurité

- ❖ Filtrage à la source
- ❖ "Traçabilité"
 - Par les fournisseurs d'accès Internet (FAI)
 - Par les serveurs
- ❖ Danger pour la vie privée

Sommaire

- ❖ "Privacy" :
 - Définition
 - Législation
- ❖ PETs : Privacy Enhancing Technologies
 - Protéger les adresses IP
 - Protéger la localisation
 - Accès anonyme à des services
 - Autorisation respectant la vie privée
 - Accès aux données / Gestion des données
- ❖ Projet PRIME

"Privacy" : définitions

- ❖ Intimité, protection de la vie privée, du domaine privé
- ❖ Critères Communs (ISO 15408):
une classe fonctionnelle, 4 propriétés :
 - Anonymat : impossibilité (pour d'autres utilisateurs) de déterminer le véritable nom de l'utilisateur associé à un sujet, une opération, un objet
 - "Pseudonymat" : idem, sauf que l'utilisateur peut être tenu responsable de ses actes
 - Non-"chaînabilité" : impossibilité (pour d'autres utilisateurs) d'établir un lien entre différentes opérations faites par un même utilisateur
 - Non-observabilité : impossibilité (pour d'autres utilisateurs) de déterminer si une opération est en cours

Législation

- ❖ Protection des **données nominatives** : loi "Informatique et Libertés" du 06/01/78, en cours de révision + loi 94-548 (recherche médicale): <http://www.cnil.fr/>
- ❖ Protection des **données à caractère personnel** : Convention 108 du Conseil de l'Europe (26/01/81), directives 95/46/EC (libre mouvement) et 2002/58/CE (communications électroniques) (remplaçant la directive 97/66/CE)
- ❖ Secret professionnel (N^{eu} Code Pénal, art. 226-13) et secret des correspondances (NCP art. 226-15) + code des postes et télécommunications (secret des correspondances + art. L-32-3-1, inséré par la "Loi relative à la sécurité quotidienne" 2001-1062 du 15/11/2001, révisé par la "Loi pour la sécurité intérieure" 2003-239 du 18 mars 2003)

PETs : Privacy Enhancing Technologies

- ❖ **Principe** : "besoin d'en connaître" ("need-to-know") ne transmettre une information qu'à ceux qui en ont besoin pour réaliser la tâche qu'on leur confie
-> **Minimisation des données personnelles**
puis **destruction/oubli**
- ❖ ... sur Internet comme dans le monde réel
- ❖ ...avec des limites : certaines informations personnelles doivent pouvoir être fournies aux autorités judiciaires en cas de litige ou d'enquête (lutte contre le blanchiment d'argent sale, par exemple) : **pseudonymat plutôt qu'anonymat**

Exemple : commerce électronique (1)

- ❖ Parties impliquées :
un client, un marchand, un service de livraison, des banques, émetteur de carte de crédit, fournisseur d'accès Internet, ...
- ❖ Le marchand n'a pas besoin (en général) de l'identité du client, mais doit être sûr de la validité du moyen de paiement.
- ❖ La société de livraison n'a pas besoin de connaître l'identité de l'acheteur, ni ce qui a été acheté (sauf les caractéristiques physiques), mais doit connaître l'identité et l'adresse du destinataire.

Exemple : commerce électronique (2)

- ❖ La banque du client ne doit pas connaître le marchand ni ce qui est acheté, seulement la référence du compte à créditer, le montant ...
- ❖ La banque du marchand ne doit pas connaître le client...
- ❖ Le f.a.i. ne doit rien connaître de la transaction, sinon les caractéristiques techniques de la connexion ...

5 types de PETs

- ❖ Protéger les adresses IP
- ❖ Protéger la localisation
- ❖ Accès anonyme à des services
- ❖ Autorisation respectant la vie privée
- ❖ Accès aux données / Gestion des données

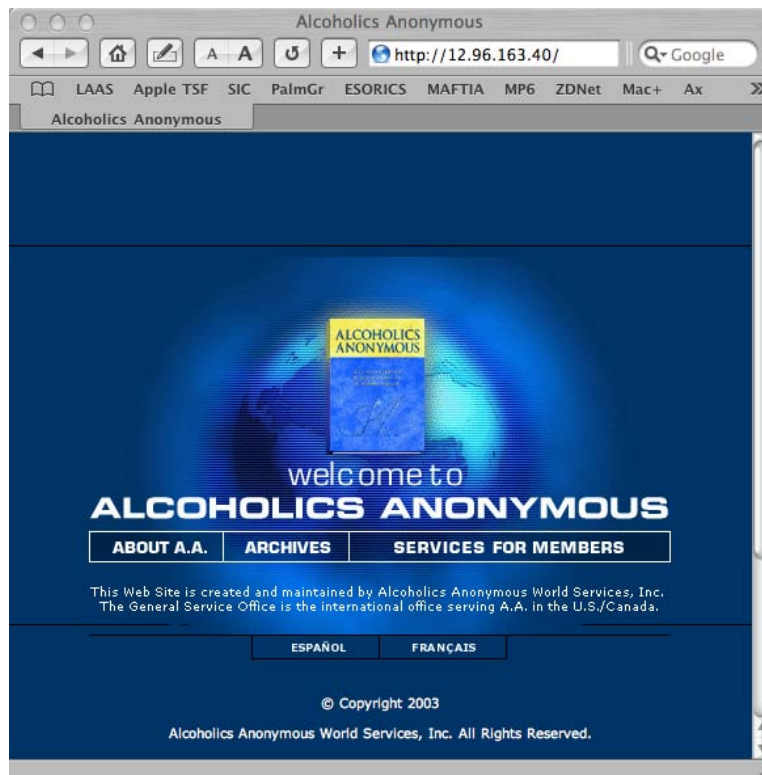
Adresse IP= "donnée nominative"

Exemple :

```
Return-Path: <Yves.Deswarte@laas.fr>
Received: from laas.laas.fr (140.93.0.15) by mail.libertysurf.net
(6.5.026)
        id 3D518DEF00116A4D for yves.deswarte@libertysurf.fr; Tue, 13 Aug
2002 13:44:40 +0200
Received: from [140.93.21.6] (tsfyd [140.93.21.6])
        by laas.laas.fr (8.12.5/8.12.5) with ESMTTP id g7DBid1D001531
        for <yves.deswarte@libertysurf.fr>; Tue, 13 Aug 2002 13:44:39 +0200
(CEST)
User-Agent: Microsoft-Entourage/10.1.0.2006
Date: Tue, 13 Aug 2002 13:44:38 +0200
Subject: test
From: Yves Deswarte <Yves.Deswarte@laas.fr>
To: <yves.deswarte@libertysurf.fr>
Message-ID: <B97EBDC6.2052%Yves.Deswarte@laas.fr>
Mime-version: 1.0
Content-type: text/plain; charset="US-ASCII"
Content-transfer-encoding: 7bit
```

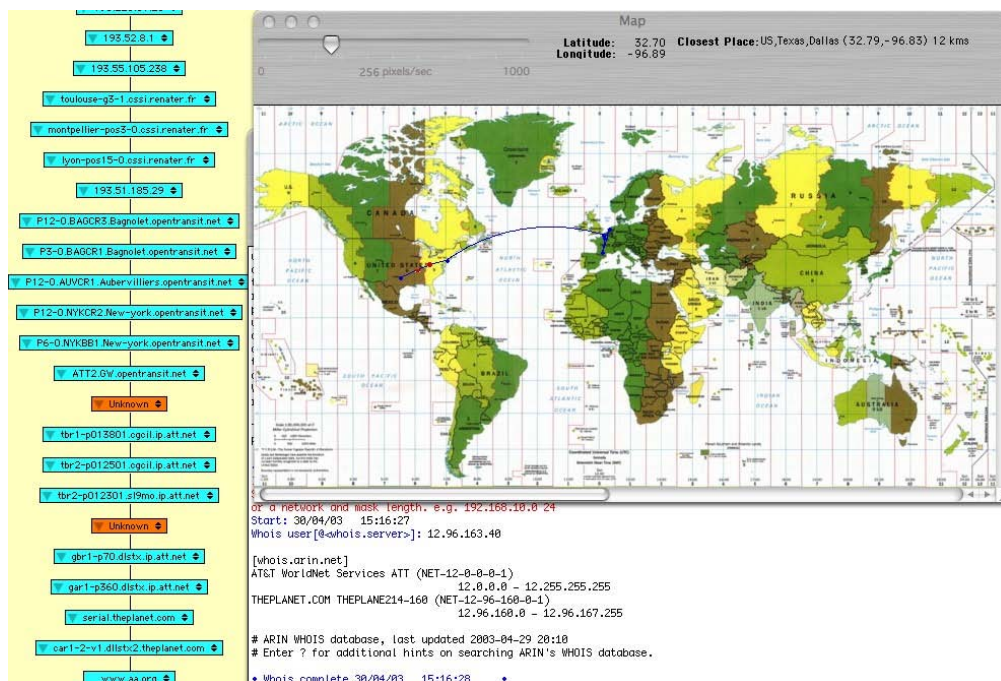
Adresse IP= "info sensible"

Exemple :



Adresse IP= localisation

Exemple :

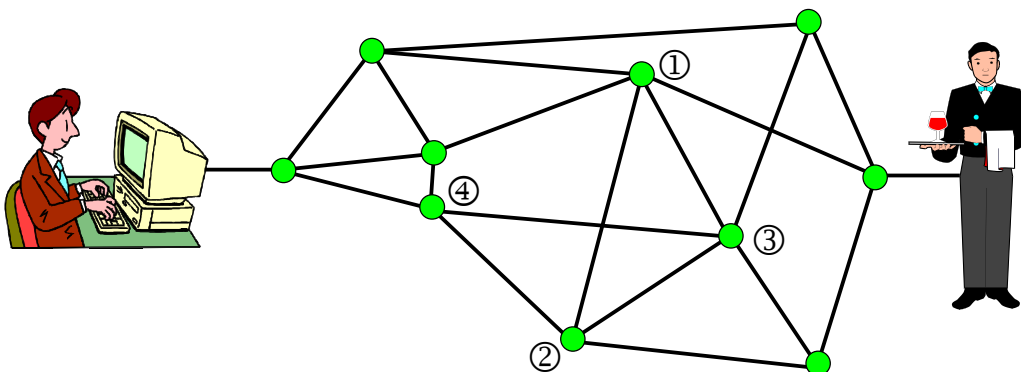
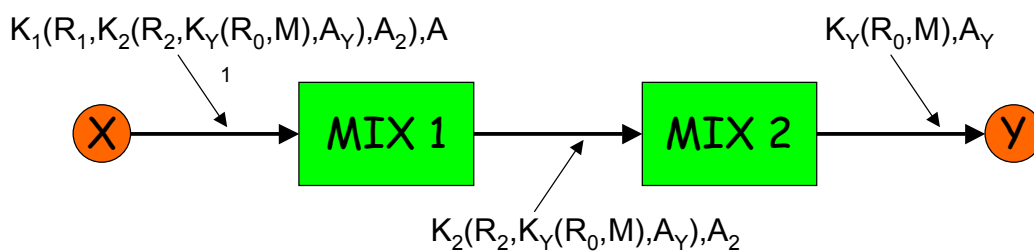


1° PET : Protéger les adresses IP

- ❖ PET : affectation dynamique des adresses IP (DHCP, PPP, NAT, ...)
- ❖ Routeurs d'anonymat :
 - MIX
 - Onion Routing
 - Crowds

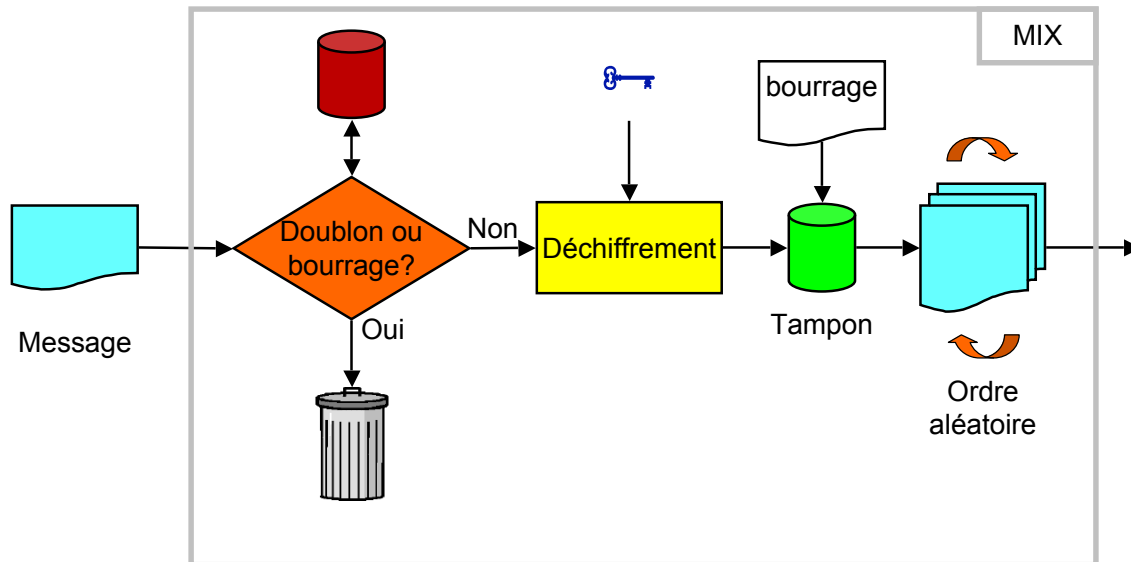
MIX / Onion Routing / Crowds

<http://www.vote.caltech.edu/wote01/pdfs/juels2-wote.ppt>



MIX : comment ça marche ?

<http://www.inf.tu-dresden.de/>



2° PET : Protéger la localisation

- ❖ Aujourd'hui : une @ IP \leftrightarrow localisation (pcq: routage)
- ❖ De nombreux services connaissent la localisation de leurs clients
 - Aujourd'hui : fournisseurs d'accès Internet, GSM, ...
 - En cours de déploiement : gestion de flotte, navigation, surveillance (anti-kidnapping), ...
- ❖ Demain : IP partout (*ubiquitous computing, intelligence ambiante...*) : chaque "machin" aura une adresse IP permanente (nomade), chaque personne aura plusieurs machins, qui se connecteront aux machins proches (réseaux ad-hoc), qui s'identifieront, routeront leurs communications, fourniront des infos contextuelles, etc.
- ❖ Il faudra développer des PETs pour protéger la localisation.

3° PET: Accès anonyme à des services

- ❖ Relais d'anonymat (*anonymity proxy*) : unidirectionnels (ou bidirectionnels?)
 - Web
 - ftp
 - e-mail
 - ...
- ❖ Serveur de pseudonymes :
 - e-mail
 - Identités multiples fournies par des f.a.i.
 - Identités virtuelles multiples :
Liberty Alliance <<http://www.projectliberty.org>>
vs. Microsoft Passport

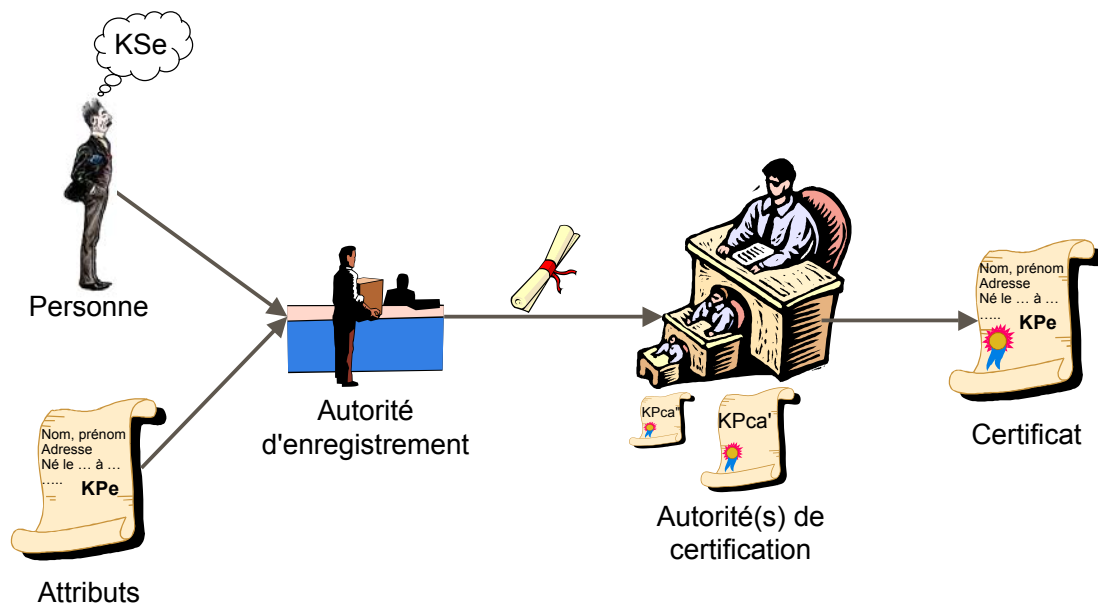
4° PET: Autorisation sur Internet

- ❖ Aujourd'hui : **client-serveur**
le serveur accorde ou refuse des privilèges au client en fonction de son identité déclarée (éventuellement vérifiée par des mécanismes d'authentification)
- ❖ Le serveur doit enregistrer des données personnelles :
preuves en cas de litige
- ❖ Ces données peuvent être utilisées à d'autres fins (profilage des clients, marketing direct, revente de fichiers clients, chantage...)
- ❖ **Action P3P (W3C) : Platform for Privacy Preferences Project**
vérification automatique de politiques de sécurité/privacy
"déclarées"

Ce schéma est dépassé

- ❖ Les transactions sur Internet mettent en jeu généralement plus de deux parties (ex : commerce électronique)
- ❖ Ces parties ont des intérêts différents (voire opposés) : suspicion mutuelle
- ❖ Nocif pour la vie privée : opposé au "besoin d'en connaître"

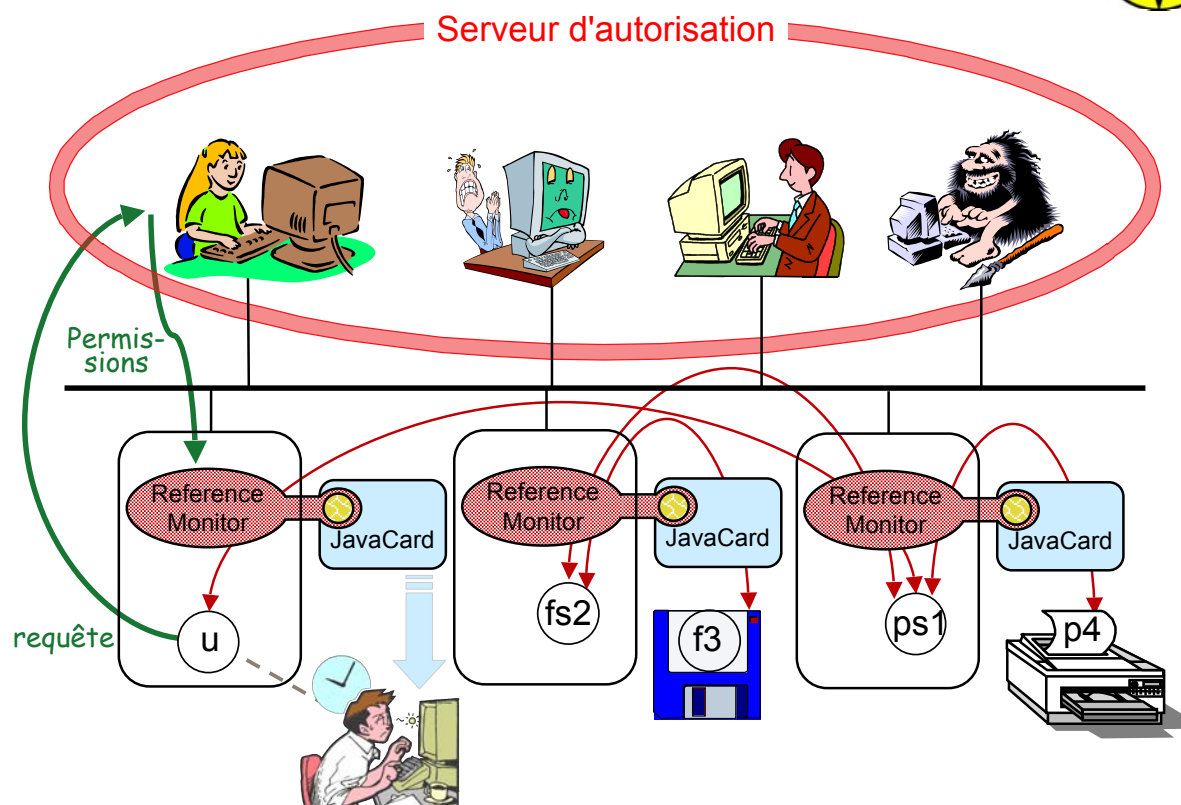
Certificats (ex: X509)



Preuves d'autorisation

- ❖ Certificats multiples : "**credentials**"
ex: SPKI : certificats d'attributs/d'autorisation
 - o cartes d'abonnement, de membre d'association, ...
 - o permis de conduire, carte d'électeur...
- ❖ Certificats restreints :
 - o "Partial Revelation of Certified Identity"
Fabrice Boudot, CARDIS 2000
- ❖ Problèmes: "chaînabilité" (une seule clé publique pour plusieurs certificats?), gestion des certificats/clés, authentification, préservation des preuves, révocation, ...

Autorisation dans MAFTIA



5° PET : Accès aux données

- ❖ **Minimisation** des données personnelles
-> répartition : séparation des pouvoirs,
fragmentation des données
- ❖ **Auto-détermination** : celui qui fournit des informations sur lui-même doit pouvoir contraindre l'usage qui pourrait en être fait :
ex: à effacer dans 48 h.
- ❖ **Négociation** entre l'individu et l'entreprise
ex: coupons de réduction en échange d'une publicité ciblée

5° PET-bis : Gestion des données

- ❖ **Principe du moindre privilège** : un individu ne doit avoir que les droits minimaux nécessaires à sa tâche
- ❖ **Politique de sécurité et mécanismes de protection** : le détenteur d'une information en est **responsable**
- ❖ **Ces données peuvent être très critiques** :
ex: dossiers médicaux
 - Disponibilité : temps de réponse (urgence), pérennité
 - Intégrité : nécessaire à la confiance, éléments de preuve
 - Confidentialité : vie privée <-> intérêts économiques

Projet PRIME (03/2004 - 02/2008)

- ❖ Privacy and Identity Management for Europe
 - Aspects juridico-socio-économiques
 - PET Côté utilisateur (développement, utilisabilité)
 - PET Côté système, réseau, serveur
 - Applications réelles

- ❖ 21 Partenaires, subvention : 11,5 M€
 - Fournisseurs (IBM, HP, ...)
 - Labos (KUL, U. Dresde, U. Milan, Eurécom, LAAS...)
 - Utilisateurs (Lufthansa, T-Mobile, Swisscom, HSR)

Bibliographie

- ❖ Simone Fischer-Hübner, *IT-Security & Privacy*, LNCS n°1958, 2001.
- ❖ Stefan A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates*, MIT Press, 2000.
- ❖ David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, 24/2 (1981) 84-88.
- ❖ M. K. Reiter and A. D. Rubin. "Crowds: Anonymity for web transactions", *ACM Transactions on Information and System Security*, 1(1):66-92, November 1998.
- ❖ Fabrice Bodot, "Partial Revelation of Certified Identity", *4th IFIP WG8.8 Working Conference on Smart Card and Advanced Applications (CARDIS-2000)*, Sept. 2000, Bristol (UK), Kluwer (Eds: J. Domingo-Ferrer, D. Chan, A. Watson), pp.257-269.
- ❖ Yves Deswarte, Noredine Abghour, Vincent Nicomette, David Powell, "An Internet Authorization Scheme using Smartcard-based Security Kernels", in *Smart Card Programming and Security*, Eds. Isabelle Attali and Thomas Jensen, Proc. e-Smart 2001, Cannes (France), 19-22 septembre 2001, Springer, LNCS n°2140, pp. 71-82.
- ❖ MAFTIA Deliverable D6 <<http://www.research.ec.org/maftia/deliverables/index.html>>

Call for Papers

- ❖ IFIP/Sec 2004 : 23-26/08/2004, Toulouse
<http://www.sec2004.org/> (deadline 09/02)
- ❖ CARDIS 2004 : 23-26/08/2004, Toulouse
<http://www.cardis.org> (deadline 09/02)
- ❖ ESORICS 2004 : 13-15/09/2004, Sophia-Antipolis
<http://esorics04.eurecom.fr> (deadline 26/03)
- ❖ RAID 2004 : 15-17/09/2004, Sophia-Antipolis
<http://raid04.eurecom.fr> (deadline 31/03)