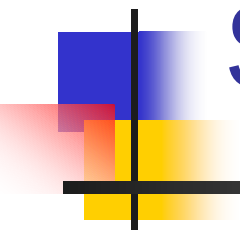
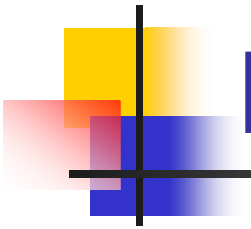


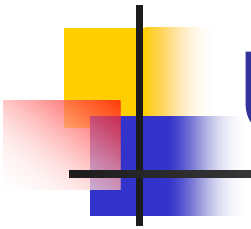
Sécurisation des nomades

IGC et certificats pour sécuriser les accès d'utilisateurs nomades



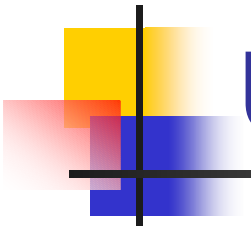
Plan

- Contraintes du nomadisme
- Certificats et IGC
- Solutions
  - Webmail
  - Accès sécurisés au courrier (imaps, pop3s, smtps)
  - Intranet
  - TLS, SSH
  - Portail captif
  - IPSec
  - Carte à puces
  - 802.1x
- Comparatif, bilan



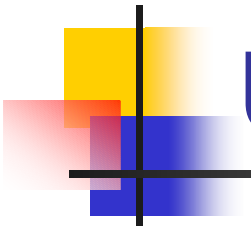
Utilisateurs nomades

- De partout
  - Bureau
  - Domicile
  - Autre laboratoire
  - Salle de conférence
  - Cyber-café
  - Hôtel
  - Hot spot



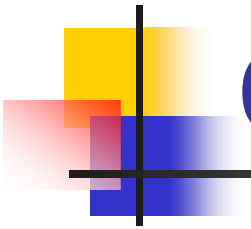
Utilisateurs nomades

- Divers média
  - Ethernet
  - Modem
  - ADSL
  - Wi-Fi



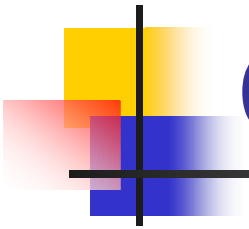
Utilisateurs nomades

- Stations de travail
  - Tendance : fixe → portable
- Invités
  - Accès à Internet



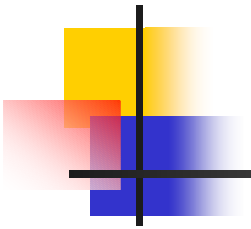
Considérations de sécurité

- Facilite la propagation
  - Virus, vers, chevaux de Troie, logiciels espion
- Périmètre
  - Plus de frontière bien définies
  - Coupe-feu : efficacité limitée
- Environnement universitaire
  - Pas de contrôle des gens
  - Culture libertaire



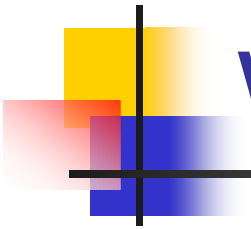
Considérations de sécurité

- Cauchemar
- Défi intéressant à relever
- Réponse possible
  - Cryptographie
    - Authentification
    - Confidentialité



IGC

- Cryptographie
  - Echange de clés
    - Le vrai défi
  - Créance
    - Autorité de certification
- Réponse : Infrastructure de Gestion de Clés
- Déploiement d'IGC
  - Lourde tâche
    - 80% organisation
    - 20% technique
  - Existe déjà → pas de nouveaux coûts

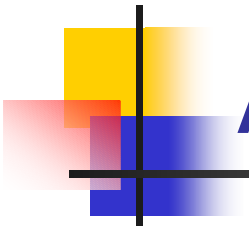


Webmail

- Application Web
- Sécurisé par HTTPS
  - Plus de mot de passe en clair
  - Le client est authentifié par un mot de passe et non par un certificat personnel
- Très facile d’utilisation
- Le premier service à offrir

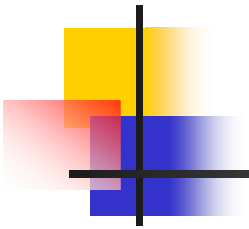
Accès sécurisé au courrier

- Version sécurisée de POP3, IMAP
  - Chiffré
  - Possibilité d'authentification forte (certificat)
- SMTPS
  - Amplification de SPAM $\Rightarrow$ interdiction du relais
  - Authentifié $\Rightarrow$ relais permis
- Très commode pour l'utilisateur
  - Outil unique
  - La configuration ne change pas



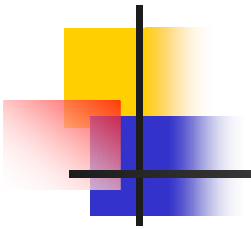
Accès sécurisé au courrier

- Clients
  - De plus en plus d'implémentation
  - Automatique (STARTTLS)
- Service qui mérite d'être installé
  - Le courrier est la première, sinon unique demande pour les utilisateurs nomades
  - Un cas où la sécurité apporte un plus en matière de confort d'utilisation



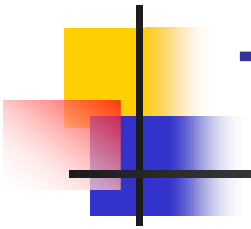
Intranet

- HTTPS (version sécurisée de HTTP)
  - Chiffré
  - Authentification du serveur
  - Authentification du client
- Historiquement le premier protocole sécurisé
  - Implémenté dans pratiquement tous les clients et serveurs



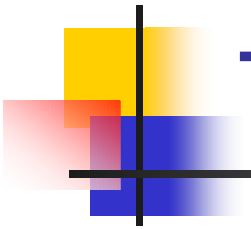
Intranet

- Web
  - Nouveau paradigme
  - Toute application a une interface web
- Uniformisation des accès aux applications
  - Authentification unique



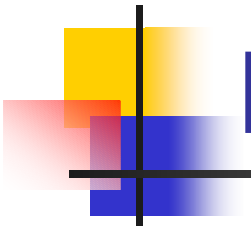
TLS, SSH

- SSL/TLS
  - Presque chaque protocole a une version TLS
  - Correctement implémentés
    - https, imaps, pops3s, smtps
  - Manque d'implémentations satisfaisantes
    - FTP, telnet
    - Où est rangé la clé privée ?
      - Parfois elle n'est même pas protégée par un mot de passe



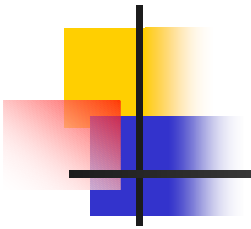
TLS, SSH

- SSH
  - A la fois protocole, application et société
  - Aujourd'hui la seule alternative sécurisée à telnet, rlogin, rsh, rcp
  - Propres méthodes pour gérer les clés
  - Certificat X509 n'est pas encore implémenté (opensll)



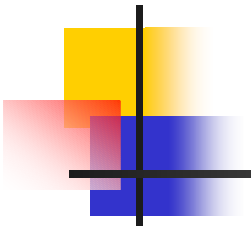
Portail captif

- L'utilisateur commence par s'authentifier auprès d'un serveur web
  - Mot de passe
  - Certificat
- Le serveur informe l'équipement de routage
  - Pour autoriser la connexion
  - Facturation
- Utilisés par les fournisseurs d'accès Internet
  - Hôtels, hot spots



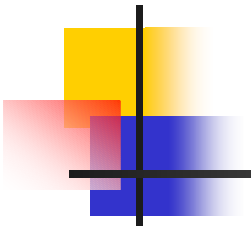
IPSec

- Conçu pour sécuriser IP
  - Niveau réseau (couche 3)
    - Pas de changement pour les applications
  - 2 modes
    - Transport
    - Tunnel
  - Echanges de clés
    - Secrets pré-partagés
    - Certificats



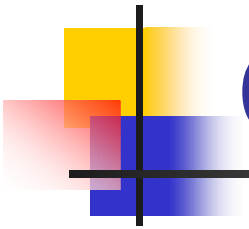
IPSec

- VPN
  - L’ordinateur est vu comme appartenant au réseau interne
- Restrictions
  - Protocoles 50 (ESP), 51 (AH)
  - UDP 500
  - Fragmentation IP



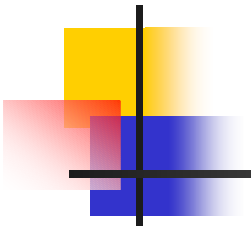
IPSec

- Déploiement
  - Relativement compliqué
- Usage
  - Plus pour les fournisseurs d’accès que les utilisateurs finaux
  - Installation sur le poste de travail par des spécialistes



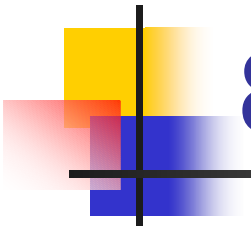
Cartes à puces, token USB

- La clé privée doit être conservée en lieu sûr
- Magasin sur le disque de l'ordinateur
  - Chiffrée (mot de passe)
  - Sauvegardes
- Dispositifs matériels
  - Cartes à puces, token USB
  - La clé privée est générée et conservée dans le dispositif matériel
  - Protégé par un code (PIN)



Cartes à puces, token USB

- 2 sécurités
  - Possession du dispositif
  - Connaissance du code
- Cohérence
  - IGC
    - Déploiement coûteux
    - Sécurité accrue
  - Clé privée
    - Disque : trop faible
    - Dispositif cryptographique : seule alternative cohérente
    - On commence à trouver des portables vendus en standard avec un lecteur de carte à puce



802.1X

- Norme Ethernet
  - Authentification du matériel connecté
    - Mot de passe
    - Certificat
- Port sur un commutateur
  - Non-autorisé : avant authentification
    - Seul le trafic nécessaire à l'authentification est permis
  - Autorisé : après authentification
    - Tout trafic

802.1X

- Rôles
  - Supplicant
    - Station de travail
  - Authenticator
    - Commutateur, borne d’accès Wi-Fi
  - Serveur d’authentification
    - RADIUS

802.1X

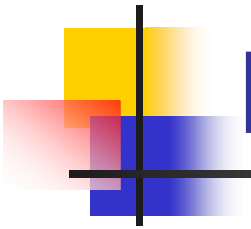
- Wi-Fi
  - Authentification
  - Echange de clés WEP
- LAN
  - Plus sûr que l'adresse MAC
  - Affectation
    - VLAN
    - ACL

Comparaisons

	Sécurité	Usage	Instal.	Dispo.	Versatilité
Webmail	**	**	***	***	*
Courrier sécurisé	**/***	***	**	**	*
Intranet	***	***	**	***	**
Portail captif	*	*	**	***	**
IPSec	***	**	*	*	***
802.1x	*	***	*	*	***

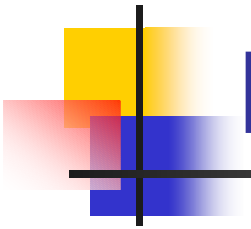
Critères de choix

	Webmail WebFTP	TLS	IPSec	SSH
Courrier (publique)	***			*
Courrier (personnelle)	**	***	*	*
Transfert de fichiers	*		**	***
Intranet		***	*	
Tout protocole			***	*



Bilan

- Certificats et IGC pour sécuriser les accès des utilisateurs nomades
  - Opérationnel
  - Encore des difficultés
- Pas de solution universelle
- Une IGC est un projet important et coûteux
  - Justifiée si on a de multiples usages



Réflexions

- Alternatives à la cryptographie pour sécuriser les accès nomades ?
  - Chiffre utilisé depuis très longtemps
    - Militaires
    - Ambassades
- Peux-t-on se passer d'IGC ?
  - Nécessaire au delà d'une communauté de quelques individus se connaissant tous