
Sécurité réseaux et applications: Perspective africaine

Alain Patrick Aina

aalain@trstech.net

Addis Abéba, le 14 Mars 2006

Agenda

Problématique

Services de sécurité

Mécanismes de sécurité

Protocoles et applications de sécurité

La situation en Afrique

Les initiatives

Conclusion



Problématique (1)

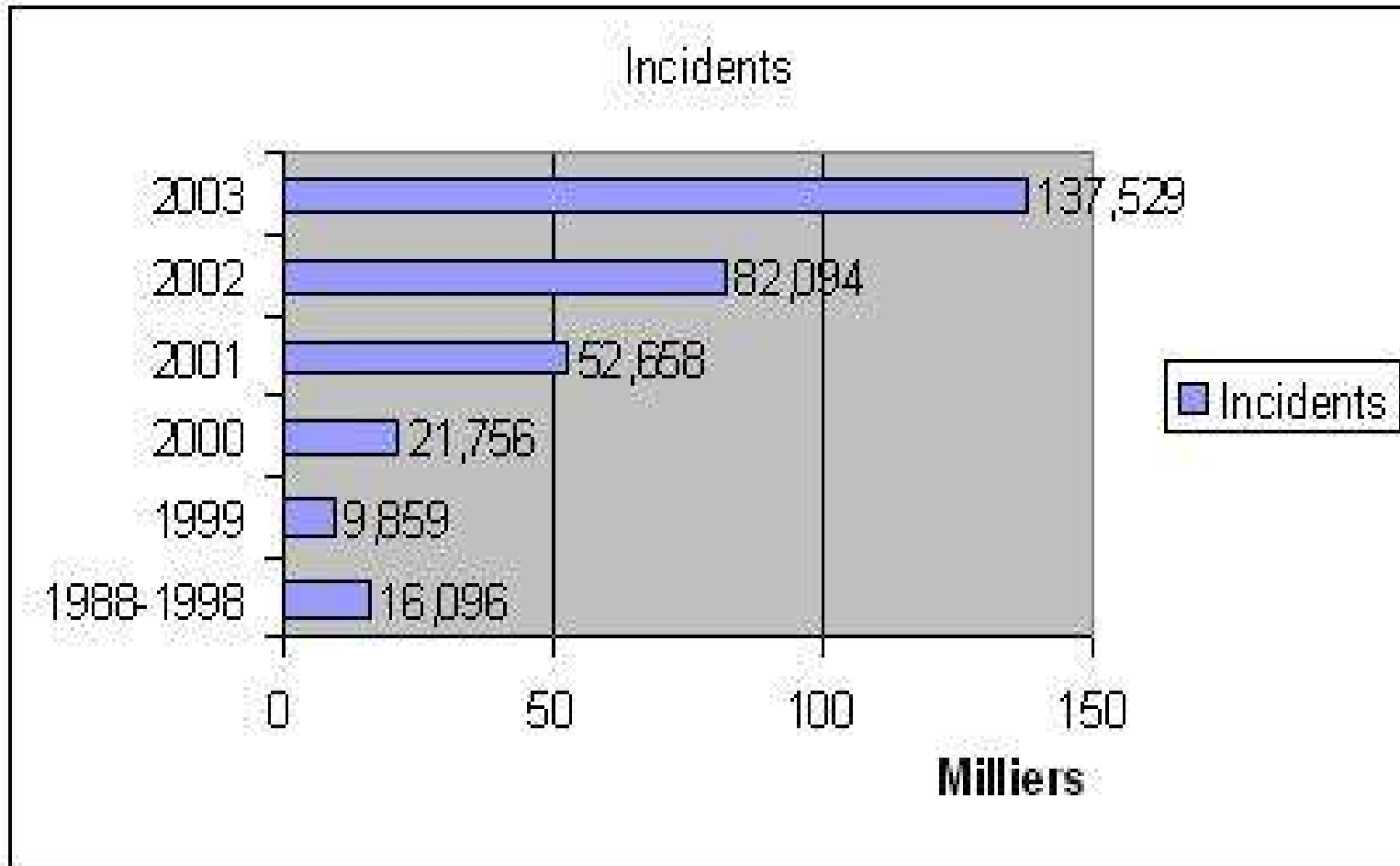
Le changement majeur ayant affecté la sécurité des informations est l'introduction des systèmes distribués, l'utilisation des réseaux et outils de communication pour transporter des données entre les terminaux et les ordinateurs et entre ordinateurs.

➤ Des mesures de sécurité réseau sont donc nécessaires:

- Pour protéger les données pendant les transmissions
- Pour contrôler l'accès aux données et systèmes

Problématique (2)

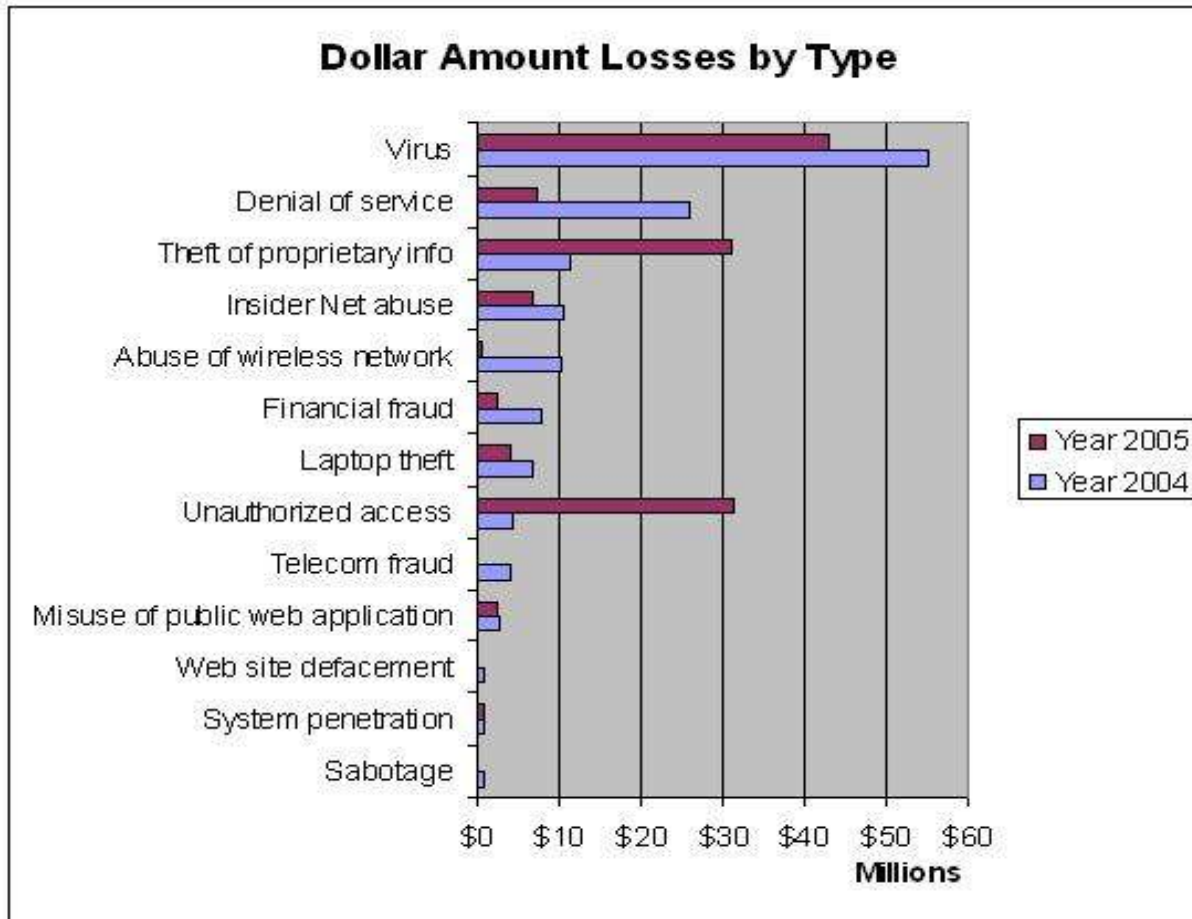
(Incidents de sécurité rapportés depuis 1988)



Source: <http://www.cert.org/stats/certstats.html>

Problématique (3)

(Pertes financières par type d'incident de sécurité)



2005:

Losses: \$130,104,542

Respondents: 639

2004:

Losses: \$141,496,560

Respondents: 269

Source : 2005 CSI/FBI Computer crime and security survey

<http://gocsi.com>

Services de sécurité(1)

➤ Confidentialité

- Protection des données transmises contre les attaques passives

➤ Authentification

- Assurer l'authenticité des communications.
- Permettre au destinataire de vérifier l'authenticité de l'expéditeur
- Dans le cadre d'une transaction, permettre aux parties de vérifier l'authenticité de leur interlocuteur.

Services de sécurité(2)

➤ Intégrité

- S'assurer que les messages sont reçus tels qu'ils sont envoyés
 - Sans duplication, insertion, modification, changement d'ordre et retransmission.

➤ Disponibilité

- S'assurer que l'information est disponible et accessible par les utilisateurs légitimes

Services de sécurité(3)

➤ Non répudiation

- Empêcher l'émetteur ou le destinataire de nier la transmission ou la réception d'un message.

➤ Contrôle d'accès

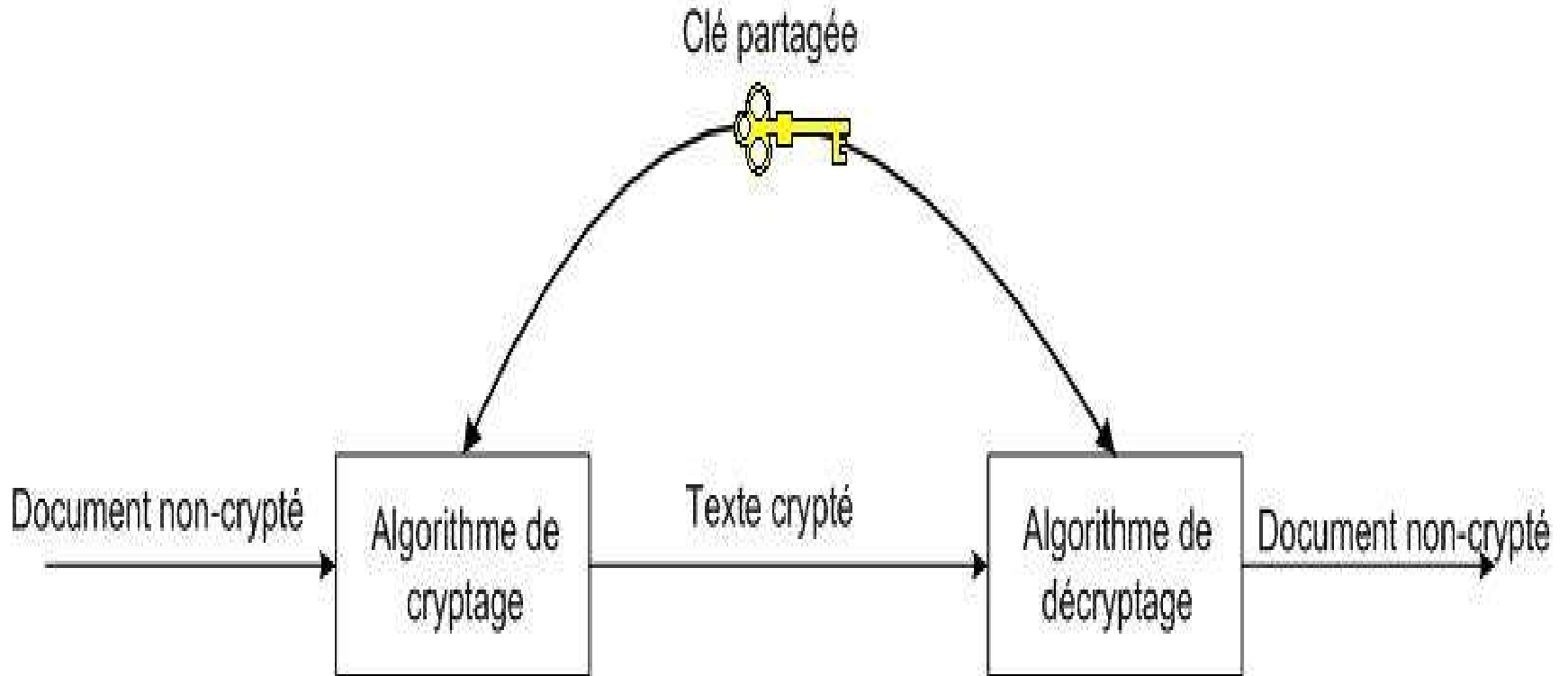
- Limiter et Contrôler l'accès aux systèmes et applications via les canaux de communication.
- Identifier, authentifier les accès.

Mécanismes de sécurité (1)

- Il n'existe pas un simple mécanisme qui fournit les services de sécurité ci-dessus.
- Cependant, un élément particulier est à la base de la plupart des mécanismes de sécurité :

Les Techniques de cryptographie

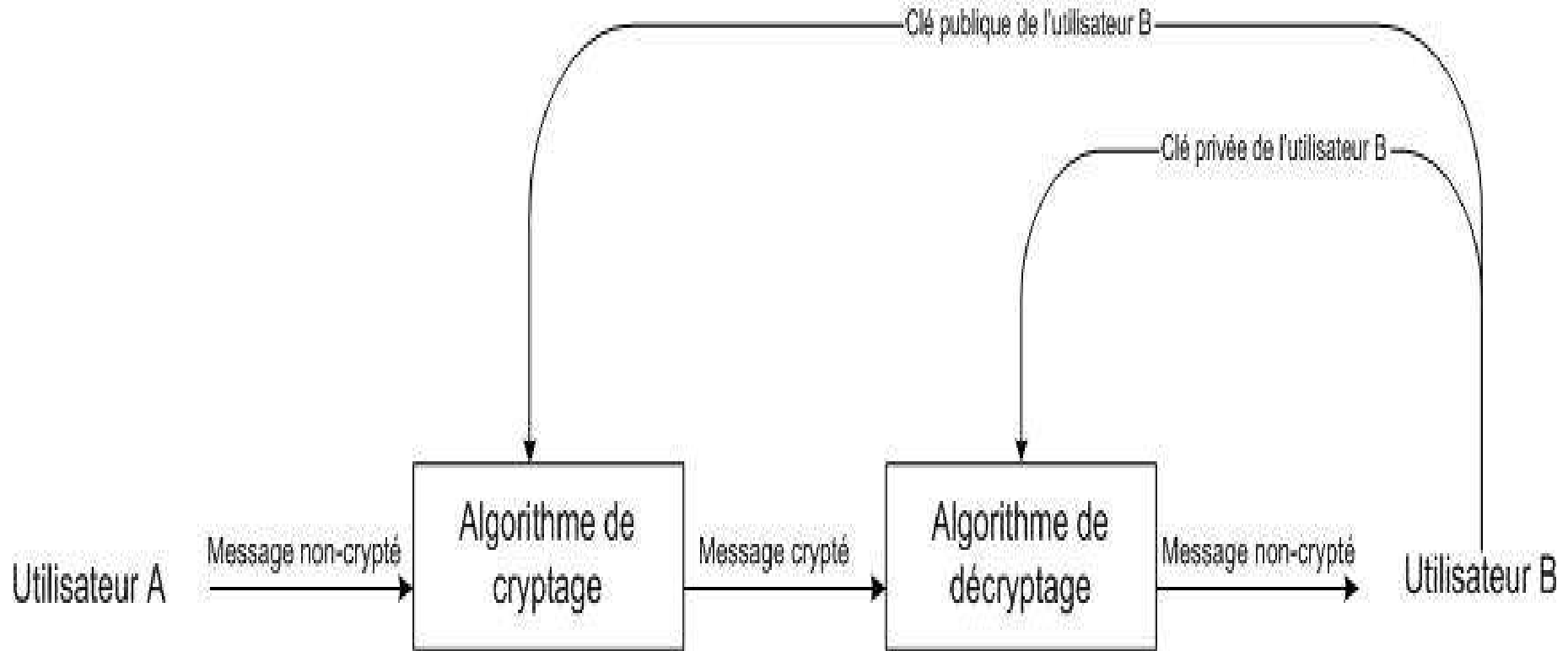
Mécanismes de sécurité (2): (Chiffrement symétrique)



Mécanismes de sécurité (2): (Chiffrement symétrique)

Algorithme	Taille de la clé
DES	56 bits
Triple DES	112 ou 168 bits
IDEA	128 bits
Blowfish	Jusqu'à 448 bits
RC5	Jusqu'à 2048 bits
CAST-128	40 à 128 bits
AES	128bits, 192 bits et 256 bits

Mécanismes de sécurité(3): (Chiffrement asymétrique ou à clé publique)



Mécanismes de sécurité(3):

(Chiffrement asymétrique ou à clé publique)

Algorithme	Chiffrement Déchiffrement	Signature digitale	Echange de clés
RSA	OUI	OUI	OUI
Diffie-Hellman	NON	NON	OUI
DSA	NON	OUI	NON
Elliptic Curve	OUI	OUI	OUI

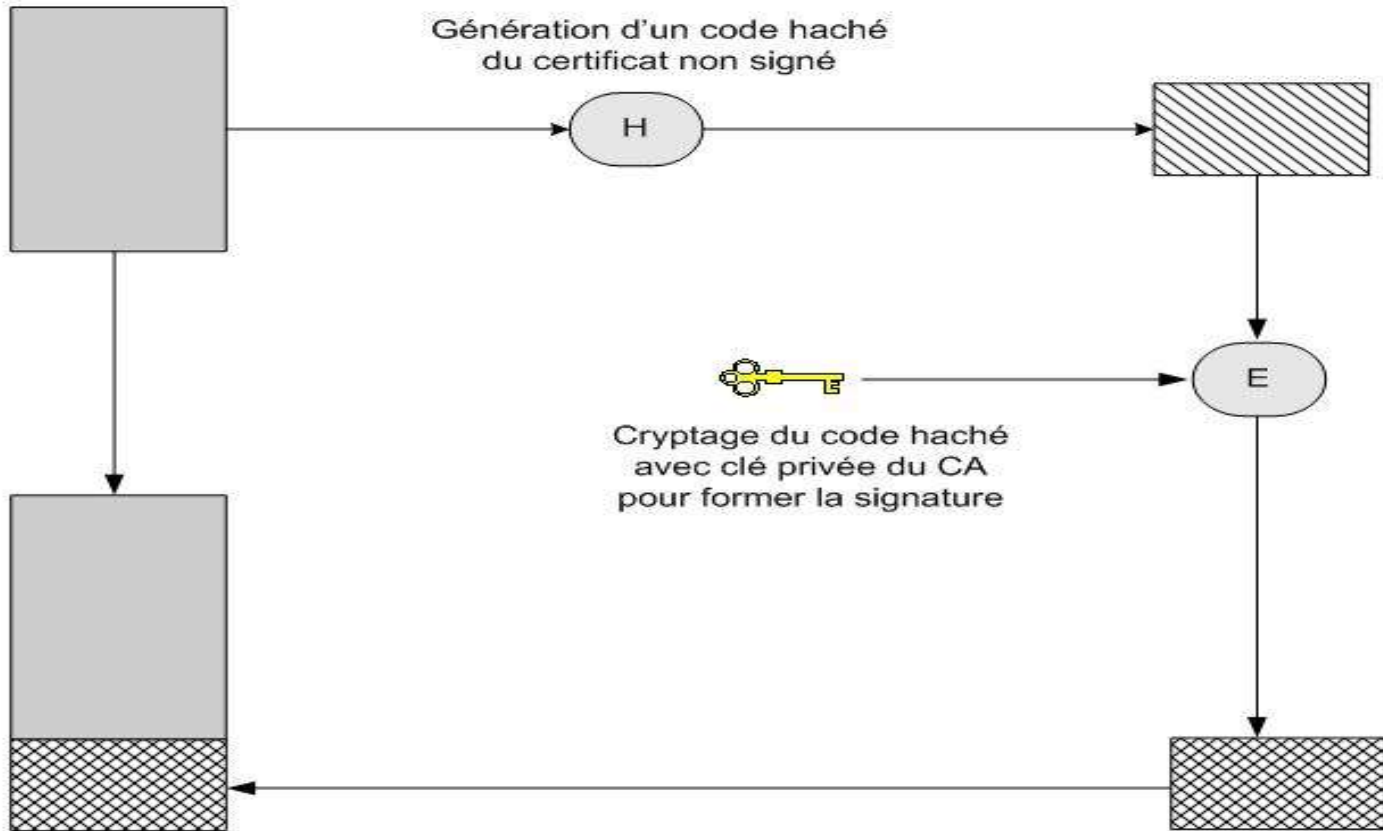
Mécanismes de sécurité (4)

(Fonction de hachage à sens unique)

- MD5, produit un code de 128 bits avec une taille de message infinie
- SHA-1, produit un code de 160 bits avec une taille de message de 2^{64} bits
- RIPEMD-160 , produit un code de 160bits, avec une taille de message infinie
- SHA-2(SHA-224, SHA-256, SHA-384, SHA-512)

Mécanismes de sécurité (4): (infrastructure à clés publiques)

Certificat non signé:
Contient l' ID utilisateur,
la clé publique utilisateur



Certificat signé:
Le sujet peut vérifier la signature
utilisant la clé publique du CA.

Protocoles et applications de sécurité(1)

➤ Applications d'authentification

- Kerberos
- Authentification avec certificats X509
- Secure-ID

➤ Session distantes

- ssh

➤ Sécurité web

- TLS,SSL

➤ Sécurité E-mail

- PGP,S/MIME



Protocoles et applications de sécurité (2)

➤ Sécurité IP - VPN

- IPsec

➤ Contrôle d'accès

- Pare-feu
- Système de détection d'intrusion
- Système de prévention d'intrusion
- Anti-virus

➤ Paiement électronique

- SET(Secure Electronic transaction)

➤ Etc....



La situation en Afrique (1)

- Multiplication des infrastructures réseau depuis les années 90, accompagnée par la pénétration de l'Internet
- Généralement mal déployées
- Sans dispositifs de sécurité adéquats
- Aux moyens limités et dans un environnement peu favorable
 - Capacités systèmes, connectivités, etc...
 - OS, outils et applicatifs non à jour
 - Difficultés de gestion des licences et des mises à jour

La situation en Afrique (2)

- Difficultés d'accès aux informations de sécurité
 - Absence de CERT
- Mauvaise qualification des techniciens surtout sur les aspects sécurité
- Absence de politique et de stratégie de sécurité
- Budget sécurité Informatique ~ 0
- Absence de formation des utilisateurs à la sécurité informatique
- Absence de législation sur les crimes informatiques et la cybercriminalité
- Etc....

La situation en Afrique (3)

Ces Infrastructures sont également confrontées aux difficultés et problèmes liés aux incidents de sécurité

- Complices d'attaques(zombies, amplificateurs)
- Victimes souvent faciles
- D'importants dégâts subis
- Des incidents de sécurité généralement mal gérés

Les initiatives (1)

- De nombreuses initiatives de formation et de renforcement des compétences sur le continent avec des ateliers sur les réseaux et la sécurité de l'information
 - AfNOG, (www.afnog.org)
 - Plus de 350 ingénieurs de 34 pays formés en six ans:
 - RALL (logiciels-libres.aul.org)
- De nombreux fora d'échange et de collaboration entre les opérateurs réseaux
- La vulgarisation des logiciels et systèmes ouverts

Les initiatives (2)

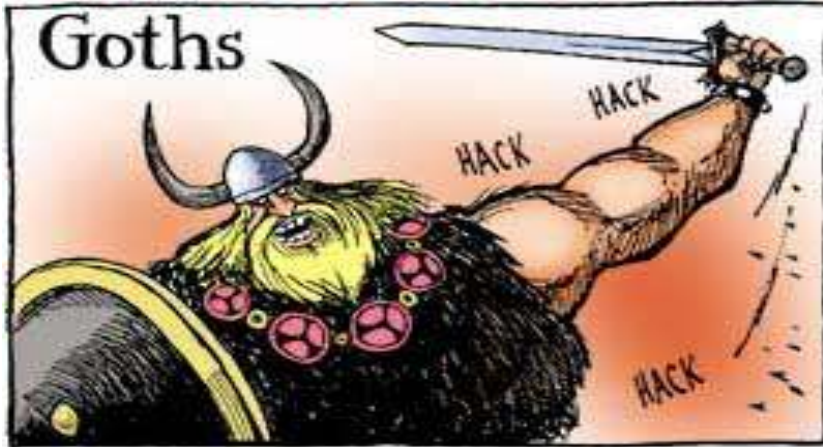
- La multiplication des rencontres sur la sécurité des transactions électroniques et les PKIs
- Le lancement des initiatives comme AfriPKI pour encourager le développement des PKIs sur le continent

Sont autant des éléments favorables qui concourent au renforcement de la sécurité de l'information et des transactions en Afrique.

Conclusions

- La situation de la sécurité de l'information au plan mondial n'est pas reluisante
 - Celle de notre continent l'est encore moins
- Des efforts sont faits, beaucoup reste à faire
- Renforcer les compétences techniques
- Sensibiliser davantage
- Créer un cadre propice
- Il faudra encore plus de moyens et d'initiatives

BRINGING CIVILIZATION TO ITS KNEES...



Je vous remercie