C&ESAR 2008

Computer & Electronics Security Applications Rendez-vous

Compte-rendu pour l'OSSIR

Olivier Heen

Les figures reproduites ici sont extraites ou adaptées des actes et des supports de la conférence. Les photos des orateurs reproduites ici ont été prises pendant la conférence. Les nuages de mots sont réalisés sur www.wordle.net en Creative Commons. Pour toute question sur cette présentation contacter olivier(.)heen(@)inria(.)fr. Pour toute information sur la conférence, consulter le site officiel www.cesar-conference.fr

C&ESAR 2008

Computer & Electronics Security Applications Rendez-vous

2-3-4 décembre

15èmes Journées SSI

Rennes - France

« Informatique... de confiance ? »

« Can we trust... trusted computing ? »

C&ESAR 2008
Computer & Electronics Security Applications Rendez-vous

En chiffres

3	jours
15ième	édition
27	intervenants
100 €	ministères, universitaires
190 €	autres participants
228	pages d'actes
250	participants
976	hits C&ESAR 2008 dans Google

C&ESAR 2008
Computer & Electronics Security Applications Rendez-vous

En images

olivier(.)heen(@)inria(.)fr

En 25 mots (FR)


anonymisation
comme
matériel
sécurité
OS
exemple
données
accès
réseau
architecture
entre
confiance
hôte
exploitation
virtualisation
mémoire
système
niveau
Applications
mesure
processeur
TPM
mécanismes
informations
fonction

En 25 mots (US)


User
security
MAC
RFID
reader
attacks
access
secure
system
example
Privacy
memory
mobile
also
data
used
Contactless.
attack
control
Proof
TPM
trust
species
tags
trusted

C&ESAR 2008
Computer & Electronics Security Applications Rendez-vous

Informatique… de confiance?

Jour 1 : problématique
- Qu'est-ce que la confiance ?
- Où se posent les problèmes et lesquels ?

Jour 2 : technologies
- Architectures, virtualisation, composants…
- Attaques

Jour 3 : applications
- Preuves, transactions mobiles, DRM, Vote…

C&ESAR 2008

Computer & Electronics Security Applications Rendez-vous

Jour 1 : problématique

Qu’est-ce que la confiance ?

Où sont les problèmes ?

C&ESAR 2008

C&ESAR 2008
Computer & Electronics Security Applications Rendez-vous

Qu'est-ce que la confiance ?

A. Bravo (Supélec)
- *Ouverture*

M. Sadler (HP Labs Bristol)
- *Trusted computing: objectives and roadmap*

G. Trouessin (OPPIDA Sud)
- *Quelle confidentialité, pour quelle confidence, et avec quelle confiance ?*

J-M. Seigneur (Univ. Genève)
- *Can computer security live with the human notion of trust ?*


Martin Sadler

Qu'est-ce que la confiance ?

La confiance n'est pas la sécurité
- On fait plutôt l'hypothèse du manque de confiance
- Principe de Kerckhoffs

La confiance est nécessaire à la sécurité
- Quis custodiet ipsos custodes?
- Systèmes de réputation

Avoir confiance ce serait…
- Croire qu'une entité réalisera correctement certaines actions dans certains contextes
- Croire qu'il existe une « police », un système de réaction proportionné

Où sont les problèmes ?

D. Boucart (DGA / CELAR)
- ***Multiniveau*** *: problématique, solutions et axes d'étude*

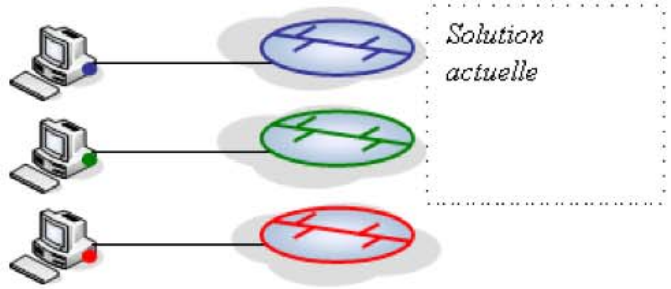
Y. Deswartes (LAAS)
- ***Multiniveau***

P. Wolf (SGDN / DCSSI)
- *Protection des infrastructures vitales*

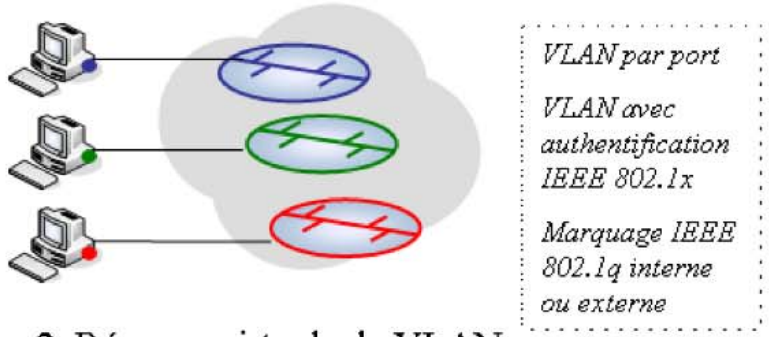
P. Chour (SGDN / DCSSI)
- *Assurance et sécurité : Interprétation du vla.4/van.5 dans le domaine du logiciel*


Yves Deswartes

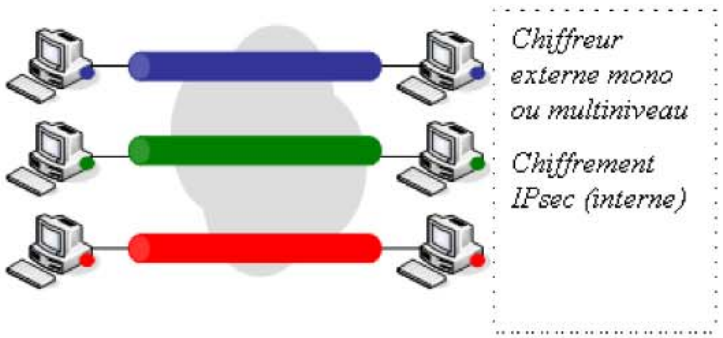
Zoom : multiniveau



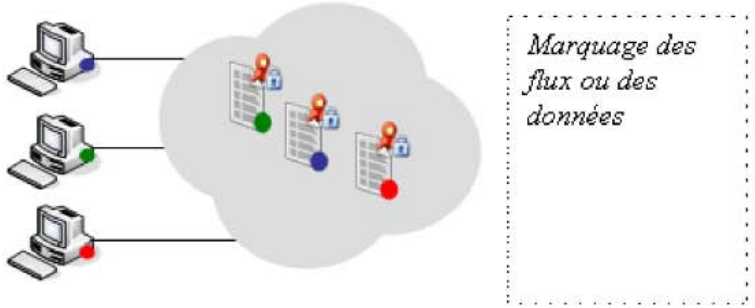
1. Réseaux physiques dédiés



2. Réseaux virtuels de VLAN

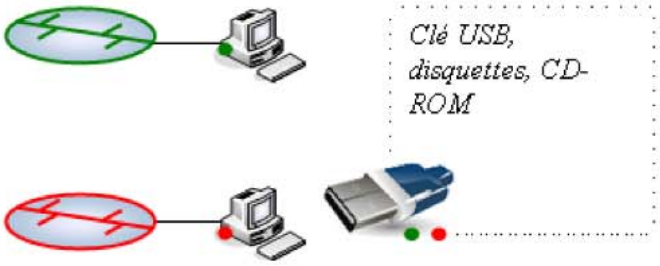


3. Réseaux virtuels VPN



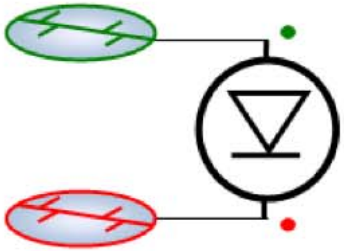
4. Réseau unique

Zoom : multiniveau



Clé USB, disquettes, CD-ROM

1. Echanges hors-ligne

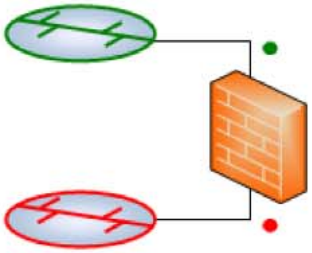


Diode

Anti-virus

Sas de dépollution

2. Echanges unidirectionnels

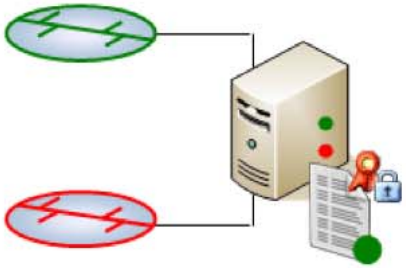


FOX,

Pare-feu avec DMZ

Pare-feu avec proxy

3. Echanges bidirectionnels avec contrôle des flux



Sas de dépollution,

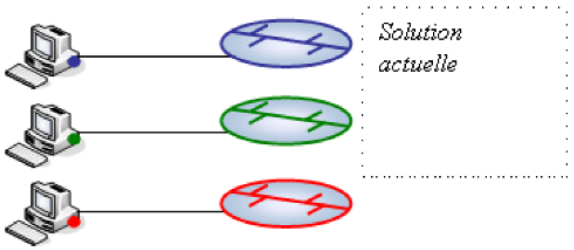
Labellisation

4. Echanges de données maîtrisés

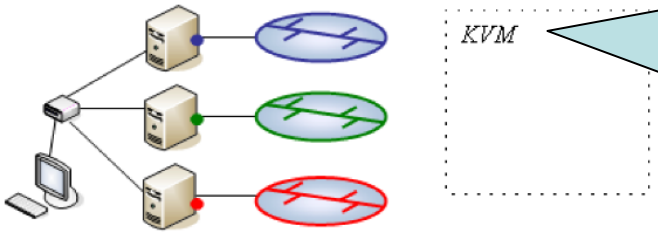
Zoom : multiniveau

Problèmes du multiniveau

- Accès à plusieurs niveaux depuis un/des postes
- Communications entre niveau

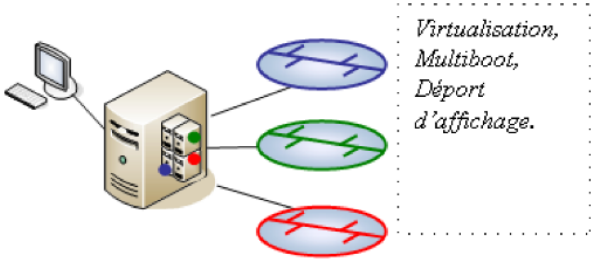


1. Pas de mutualisation

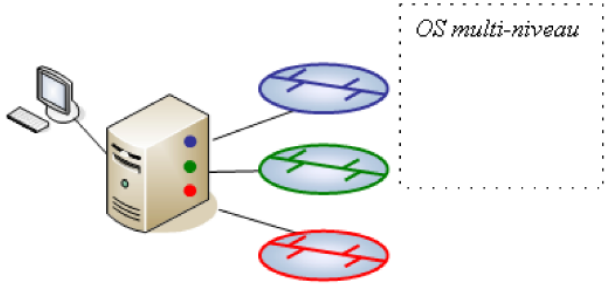


2. Mutualisation des périphériques

Quels canaux cachés dans un switch KVM ?



3. Mutualisation du hardware



4. Mutualisation de l'OS

Où sont les problèmes ?

Anonymat, santé et vie privé
- On choisit d'entrer, ou pas, dans un réseau social
- On ne choisit pas d'entrer dans un fichier santé

(Re-)définir la sphère privée ?
- Anciennes lois, Soft-laws, réaction proportionnée
- Impudeur sur Internet (voir aussi « traces de soi »)

Certification
- On ne peut pas tout certifier, il faut des principes directeurs pour accepter, ou pas, une certification
- Difficulté d'harmoniser les certifications (ex. du VLA4)

C&ESAR 2008

Computer & Electronics Security Applications Rendez-vous

Jour 2 : technologies

(Para)virtualisation, Preuves, Architectures, Composants, et Attaques

C&ESAR 2008

Technologies

C. Burgod (XLIM)

- *Environnement matériel de confiance et sécurité des protocoles distribués*

S. Gay (DGA / CELAR)

- *Apports de la **virtualisation** pour une plate-forme informatique de confiance*

F. Pessaux et al. (LIP6, INRIA…)

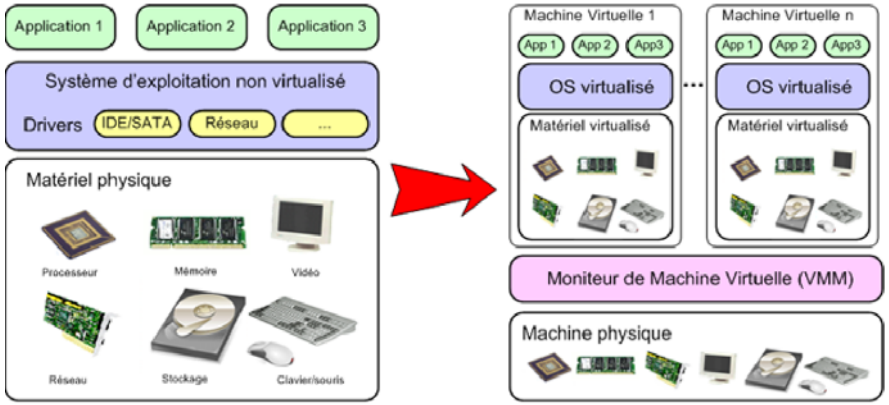
- *Trusted software within Focal*

Sébastien Gay

Zoom : virtualisation

Virtualisation et sécurité

- Plusieurs orateurs ont rappelé que l'objectif de la virtualisation d'OS *n'est pas* la sécurité
- Pourtant la virtualisation peut aider au cloisonnement et au contrôle d'accès



Paravirtualisation

- l'OS virtualisé coopère avec l'hyperviseur
- Il faut modifier l'OS (cf. XEN, Hyper-V) ou implémenter une API (paravirt-ops)

Zoom : virtualisation

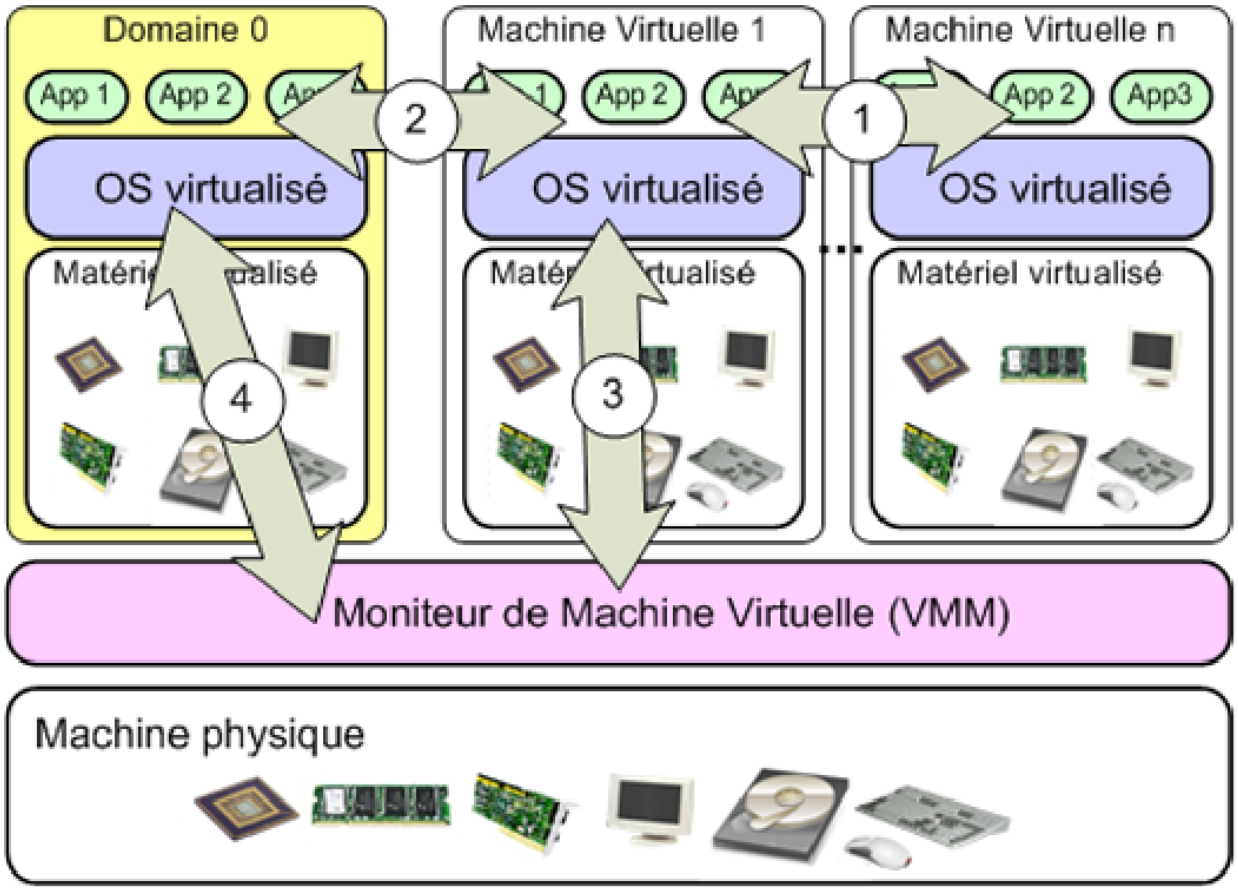
Détection de la virtualisation

- Possible en pratique. La détection de la para-virtualisation est même plus simple
- Plusieurs malwares utilisent des techniques de détection pour adopter un comportement bénin
- Remarque : pour éviter les malwares, virtualisez tout ;)

Mise en défaut du cloisonnement

- Comment se protéger d'une instance corrompue?
- Difficile : canaux de communication non documentés, quantité de code à vérifier…

Zoom : virtualisation



1: Entre deux instances invitées
2: Entre une instance invitée et le domaine de contrôle

3: Entre une instance invitée et l'hyperviseur
4: Entre le domaine de contrôle et l'hyperviseur

Technologies

G. Duc, R. Keryel (ENST Bretagne)

- *Un Panorama des architectures informatiques sécurisées et de confiance*

V. Kolesnikov (Bell Labs, Alcatel-Lucent)

- *Efficient techniques for securing off-chip memory*

F. Rémi, G. Guiheux (AMOSSYS)

- *Composant cryptographique TPM : retours d'expérience et perspectives*

Technologies : attaques

F. Vacherand et al. (CEA-LETI MINATEC)
- *Panorama of secure contactless communications*

L. Duflot (SGDN / DCSSI)
- *Quelle confiance dans les composants matériels ?*

J-L. Lanet et al. (Univ. Limoges)
- ***EMAN** : Un cheval de Troie dans une carte à puce*

J-M. Fraygefond (DGA / CELAR)
- *Un panorama des techniques de furtivité et de leur détection*

Technologies : attaques

Confiance dans les composants matériels (L. Duflot)

- Plusieurs facteurs d'insécurité sont explorés : absence de modèle de sécurité matériel, augmentation du nombre de fonctions, possibilités de piégeage du processeur

Contactless communications (F. Vacherand et al.)

- Contremesures intéressantes : noisy readers, stream ciphers, Contactless Privacy Manager (RF field sensing, black-lists, monitoring…)
- Une piste pour une contremesure à la relay attack

Zoom : EMAN

EMAN : Un cheval de Troie dans une carte à puce

- EMAN permet à une application de passer outre le firewall intégré à une Javacard
- Heureusement, les conditions de l'attaque sont rarement réunies en pratique : possession des clés de chargement, pas de vérification poussée du byte code, pas de code signé, cartes relativement anciennes
- Néanmoins, la violation du modèle de sécurité permet de récupérer, puis d'interpréter, la mémoire de la carte (là où une attaque matérielle se heurterait à du chiffrement)

C&ESAR 2008

Computer & Electronics Security Applications Rendez-vous

Jour 3 : applications

Transactions mobiles,
Interopérabilité,
DRM, vote

C&ESAR 2008

Applications

J-C. Paillès (Orange Labs)
- *Mobile transactions: trust and privacy aspects*

E. Diehl (Thomson R&D)
- *Digital Rights Management and Trust*

C. Enguehard (Univ. de Nantes / LINA)
- ***Vote électronique**: constats, questions, et certitudes*

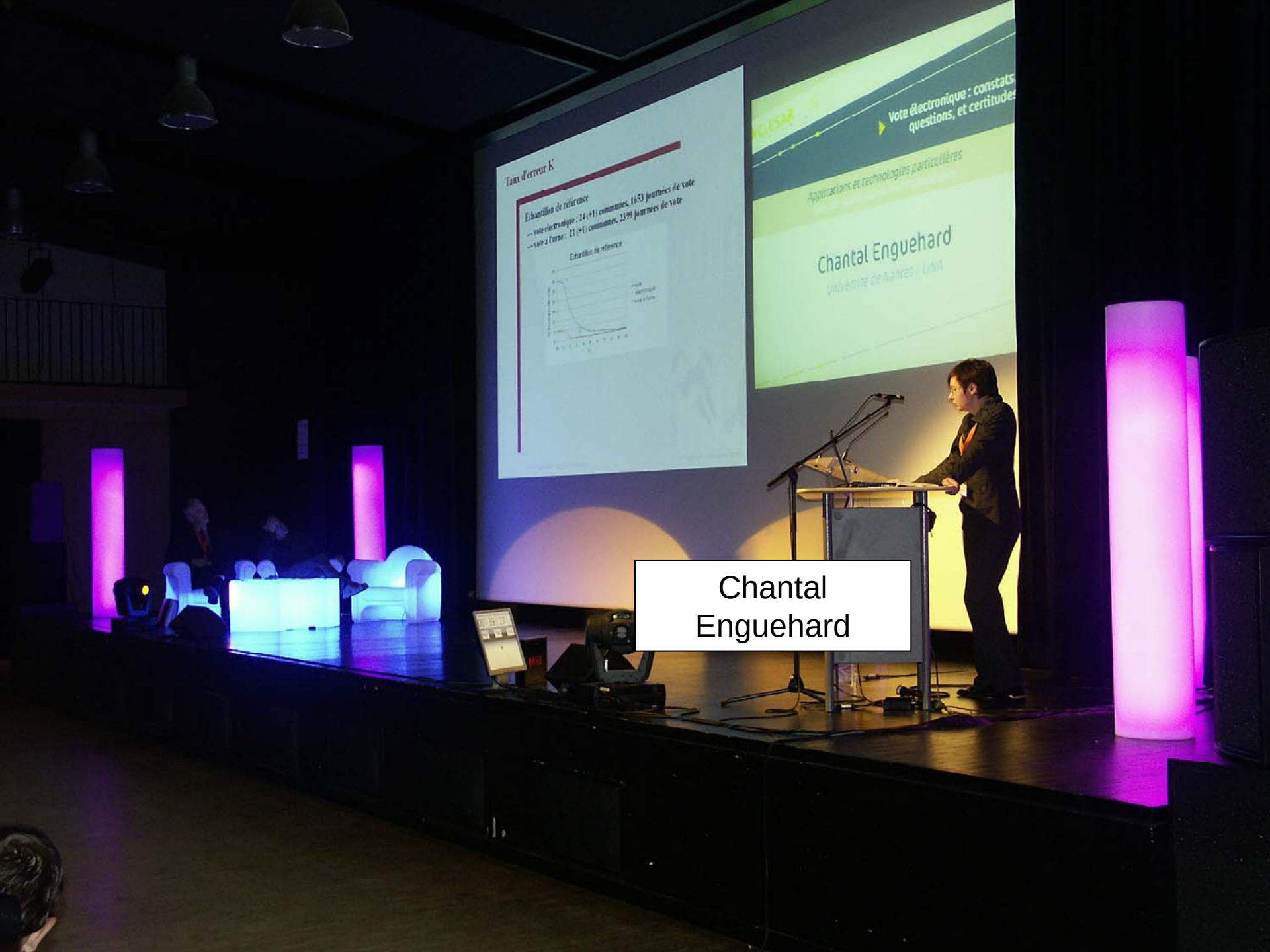
F. Chabaud et al. (SGDN / DCSSI)
- *Secured and practical **voting machines***

F. Fayard (DGA)
- *Clôture des journées SSI / Closing speech*

Zoom : vote électronique

Le débat s'est placé sur un terrain plus riche que le « POUR ! » vs. « CONTRE ! »

Tout d'abord, C. Enguehard montre sous un angle statistique rigoureux que les systèmes déployés ne sont pas satisfaisant


Taux d'erreur K'
Échantillon de référence
— vote électronique : 24 (+1) communes, 1653 journées de vote
— vote à l'urne : 21 (+1) communes, 2399 journées de vote
Échantillon de référence
Vote électronique : constats, questions, et certitudes
Applications et technologies particulières
Chantal Enguehard
Université de Nantes - LINA
Chantal Enguehard

Zoom : vote électronique

F. Chabaud indique que la sécurité est un préalable non négociable au déploiement d'une nouvelle solution, puis il présente les pistes d'une telle solution

Les bases de cette solution sont

- Séparer le processus de configuration du scrutin et le processus du vote proprement dit
- Publier et prouver formellement le processus du vote

En espérant vous voir à C&ESAR 2009…

Les figures reproduites ici sont extraites ou adaptées des actes et des supports de la conférence. Les photos des orateurs reproduites ici ont été prises pendant la conférence. Les nuages de mots sont réalisés sur www.wordle.net en Creative Commons. Pour toute question sur cette présentation contacter olivier(.)heen(@)inria(.)fr. Pour toute information sur la conférence, consulter le site officiel www.cesar-conference.fr