



# Dépérimétrisation

Futur de la sécurité réseau ou pis aller passager ?

Cédric BLANCHER

cedric.blancher@eads.net  
EADS Innovation Works  
Computer Security Research Lab

sid@rstack.org  
Rstack Team  
<http://sid.rstack.org/>

Symposium sur la Sécurité des Technologies de l'Information et de la  
Communication  
Rennes - 4-6 juin 2008

## La dépérimétrisation...

Sujet un poil polémique en vogue en ce moment

- Suppression (ou presque) des firewalls
- Ouverture des périmètres
- Concentration sur la sécurité des données

Vision quelque peu surprenante, mais néanmoins intéressante



## Agenda

- 1 La dépérimétrisation
- 2 Différents niveaux
- 3 Conclusion



## Agenda

- 1 La dépérimétrisation
- 2 Différents niveaux
- 3 Conclusion

## Jericho Forum



THE *Open* GROUP  
Making standards work®

HOME | SITE MAP | SEARCH

Sponsor an Event | Become a Member | Member Area

About | **Forums** | Certification | Services | Government | Events | Bookstore & Downloads | Newsroom | Contact

You are here: [Home](#) > [Forums](#)

**Forums**

- Architecture
- Enterprise Management
- Identity Management
- Platform
- Real-Time & Embedded Systems
- Security

**Customer Council**

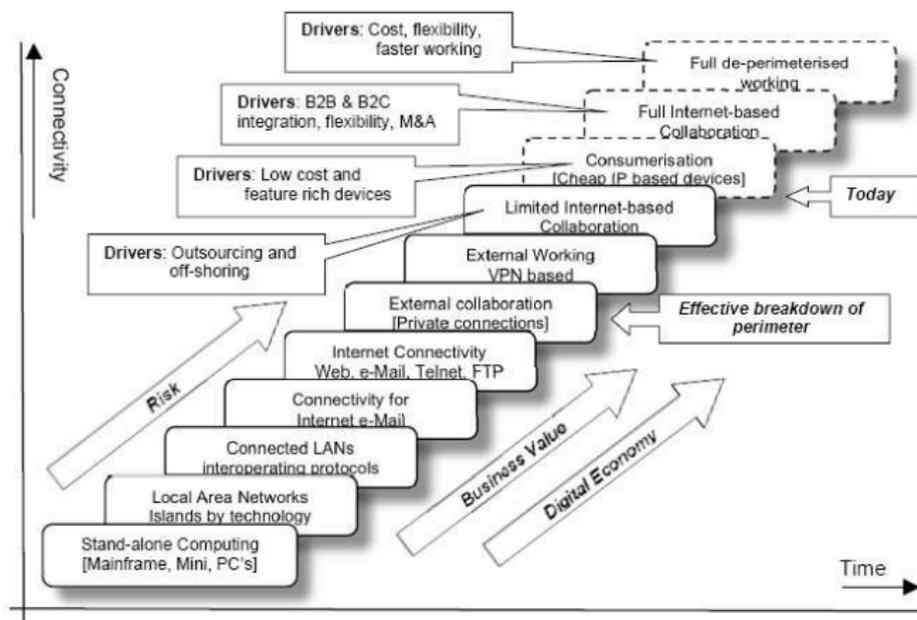
**What Forums are...**

The Open Group is largely a federation of semi-autonomous forums that confront major barriers to enterprise integration, and enable their members to guide development and adoption of industry directives and standards. Covering a range of technical, business, legal and regulatory issues, each forum addresses a specific functional area, and provides a neutral platform to meet others with similar issues and work together on best practices. Each Forum is lead by a Forum Director, a specialist with thorough knowledge of their subject, and access to the vendor and user community.

### Think Tank poussant la dépérimétrisation

- Les 11 commandements
- Business Case for Deperimeterisation
- Nombreux White Papers
- Présentations et exemples

## Arguments (1)



## Arguments (2)

### En résumé

- Les mécanismes de sécurité réseau sont vieux
- Ils ne préviennent pas la plupart des attaques
- Ils sont contre-productifs

### Solution

- Ouvrir le réseau pour rétablir de la connectivité
- Remonter la sécurité vers les applications

## Problèmes ?

Une jolie collection de Yakafokons© qui apportent plus de questions que de réponses

- Envisageable techniquement ?
- Quels sont les bénéfices ?
- Quelle est leur portée ?
- Tout le monde peut-il en profiter ?
- Quelles sont les limites, les risques ?
- Etc.

# Agenda

- 1 La dépérimétrisation
- 2 Différents niveaux
- 3 Conclusion

## Point de vue du réseau...

### Migration vers un réseau plus plat

- Moins de firewalls
- Plus de connectivité (cf. modèle IPv6)
- Sécurité de bout en bout
- Fonctionnalités : overlay, mobilité, etc.

Globalement, on sait gérer à ce niveau

## Repérimétrisation

On ne supprime pas le périmètre, on le reconstruit...

- Périmètre " physique" plus ouvert
- Construction d'un domaine logique (ou plus)
- Fonctionnement au sein de ce(s) nouveau(x) périmètre(s)

La dépérimétrisation transforme le périmètre physique en périmètre logique par l'utilisation de liens chiffrés (VPN, SSL/TLS, etc.)

## Point de vue système...

La situation n'évolue pas trop

- Mêmes moyens de sécurité
- Menaces client-side
- Problématiques de confinement

La question reste de savoir comment gérer l'exposition des systèmes en terme de résilience, en particulier par rapport au reste du périmètre...

## L'accès aux données

Problématique strictement identique

- Mêmes services
- Mêmes données
- Mêmes accès

Le problème essentiel est de gérer l'impact de l'exposition accrue des clients



## Agenda

- 1 La déprimétrisation
- 2 Différents niveaux
- 3 Conclusion**

## L'accès aux données

Le fond du problème réside dans la gestion des données

- La valeur réside dans les données
- Comment protéger efficacement les données ?

Problématique accrue par le fait que de nombreuses données ne transitent pas sur le réseau !

## Une solution ?

La dépérimétrisation c'est peut-être sexy, mais...

- Comment gérer l'explosion des clients avec des moyens dépassés
- Comment gérer la protection des données dans ces conditions
- Quelle est la résilience d'un tel réseau face à un hôte compromis ?

De bons sentiments, mais qui demandent encore beaucoup de travail...



That's all folks !

Merci pour votre patience...

Questions ?