



Reconsidering Network Defenses

Or not...

Cédric BLANCHER

cedric.blancher@eads.net

Computer Security Research Team Leader
EADS Innovation Works

Securitybyte

Delhi - November 17th-18th 2009



Who am I ?

- Senior Research Engineer at EADS Innovation Works
- Head of Computer Security research lab for 3 years
- Leading Security Evaluation activities



What is this presentation about ?

When you look at network security, things have not changed much

- We defend our network creating boundaries
- We heavily rely on multipurposes firewalls
- We just added network authentication

All this is just about protecting our perimeter(s)



Perimeter-wise approach issues

IT has changed a lot...

- Mobility
- Extended enterprise
- Cloud computing
- Etc.



Perimeter-wise approach issues

IT has changed a lot...

- Mobility
- Extended enterprise
- Cloud computing
- Etc.

Perimeters as we use to understand them have vanished



Breaking the model

Deperimeterization aims at breaking such a security model

- Network should be open
- Network should be not be trusted
- Emphasis should be put on data protection



Breaking the model

Deperimeterization aims at breaking such a security model

- Network should be open
- Network should be not be trusted
- Emphasis should be put on data protection

Surprising approach ?

That's what make it all the more interesting !



Agenda

- 1 Deperimeterization concept
- 2 Facing reality
- 3 Thinking differently (again)
- 4 Final thoughts



Agenda

- 1 Deperimeterization concept
- 2 Facing reality
- 3 Thinking differently (again)
- 4 Final thoughts

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...

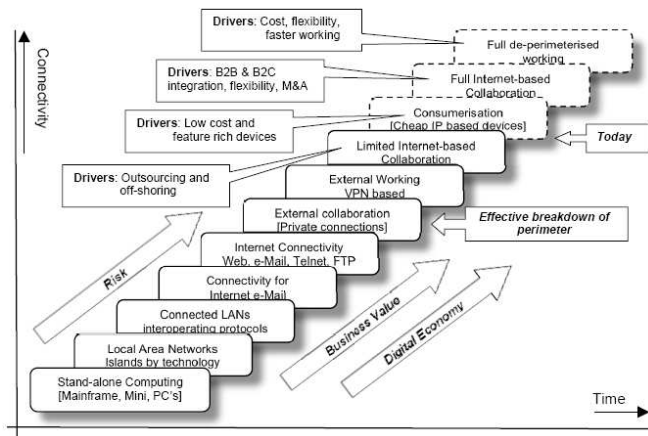
The Open Group is largely a federation of semi-autonomous forums that confront major barriers to enterprise integration, and enable their members to guide development and adoption of industry directives and standards. Covering a range of technical, business, legal and regulatory issues, each forum addresses 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 pushing deperimeterization

- 11 Commandments
- Business Case for Deperimeterisation
- Numerous White Papers
- Presentations, talks and examples



Rationals (1)





Perimeters are weak

Perimeters are facing major issues

- Overstacked protocols, especially over HTTP
- More and more complex protocols (SIP ?)
- Encryption, obfuscation, firewall piercing
- External users passing by

Not to mention perimeter sometimes arms security itself...



Perimeters are weak

Perimeters are facing major issues

- Overstacked protocols, especially over HTTP
- More and more complex protocols (SIP ?)
- Encryption, obfuscation, firewall piercing
- External users passing by

Solutions ?

- Bigger and bigger firewalls ?
- L2 based network security ?

Not to mention perimeter sometimes arms security itself...



Perimeters are arming business

Perimeters are bad for communication :

As connectivity and communication means grow,
perimeters are just blockers

- Users can't access resources they need
- B2B communication is difficult, when possible

In addition to that, they do not meet security
expectations

- Roaming makes perimeter less clear and more vulnerable
- Perimeter does not address data security



Perimeters are arming business

Perimeters are bad for communication :

As connectivity and communication means grow,
perimeters are just blockers

- Users can't access resources they need
- B2B communication is difficult, when possible

In addition to that, they do not meet security
expectations

- Roaming makes perimeter less clear and more vulnerable
- Perimeter does not address data security

Point

Less effective, more annoying, why keep them ?



Deperimeterization as a solution

Deperimeterization proposes a big shift for security mindset

- Concentrate on data access
- Secure endpoints
- Consider network environment hostile
- Put security in the application protocols

In other words...

Move security from network to endpoints



Agenda

- 1 Deperimeterization concept
- 2 Facing reality**
- 3 Thinking differently (again)
- 4 Final thoughts



Is deperimeterization possible today ?

Technical reality is IPv4 Internet **is** fragmented

- IPv4 involves NAT
- NAT leads to perimeters



Is deperimeterization possible today ?

Technical reality is IPv4 Internet **is** fragmented

- IPv4 involves NAT
- NAT leads to perimeters

Consequence

As a matter of fact, whether you live with perimeters, whether you quit IPv4...



Deperimeterization scope

Does deperimeterization affect the whole IT system ?

- Our way to deal with security must change
- But do we need to throw in-depth network security ?
- But why should fixed ressources should be affected ? !

Deperimeterization scope

Does deperimeterization affect the whole IT system ?

- Our way to deal with security must change
- But do we need to throw in-depth network security ?
- But why should fixed resources should be affected ? !

Scope

Deperimeterization affects first and foremost mobile resources



Is it enough ?

Network security issue can be addresses easily but...

- What about system security ?
- What about controlling data access ?
- How to ensure applications can be trusted ?

Is it enough ?

Network security issue can be addresses easily but...

- What about system security ?
- What about controlling data access ?
- How to ensure applications can be trusted ?

Survival...

Can we trust workstations ability to evolve alone in a malicious network environment ?



Agenda

- 1 Deperimeterization concept
- 2 Facing reality
- 3 Thinking differently (again)**
- 4 Final thoughts



Any working solution so far ?

One possible solution might be overlaid networking

- Find connectivity
- Establish link with a central point or a P2P community
- Pass your communication through that link



Any working solution so far ?

One possible solution might be overlaid networking

- Find connectivity
- Establish link with a central point or a P2P community
- Pass your communication through that link

Network communities ?

Creating a secure, overlaid perimeter over a perimeterless network



Back to global connectivity

Global connectivity is a key factor to deperimeterization

- Communication becomes possible
- We can build security features on top of it
- Including overlaid network clouds

Deperimeterization has more to do with reperimeterization



How to regain connectivity

The "I" word : IPv6

- Huge address space
- No more need for NAT
- Global connectivity



How to regain connectivity

The "I" word : IPv6

- Huge address space
- No more need for NAT
- Global connectivity

However !

Global connectivity does not means no firewall...



Example of technological shift

Mobile IPv6 is an IPv6 extension for mobility

- Ressource is always reachable on one fixed address
- Medium changes are transparent for applications
- Security is handled the same way wherever ressource is located

Example of technological shift

Mobile IPv6 is an IPv6 extension for mobility

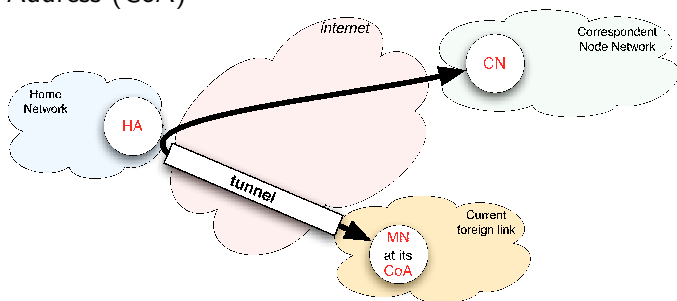
- Ressource is always reachable on one fixed address
- Medium changes are transparent for applications
- Security is handled the same way wherever ressource is located

GSM-like communication model ?

Efficient, pervasive and secure solution for roaming...

MIPv6 simple case

CN is a random IPv6 node
 HA relays communications for MN to its Care-of Address (CoA)

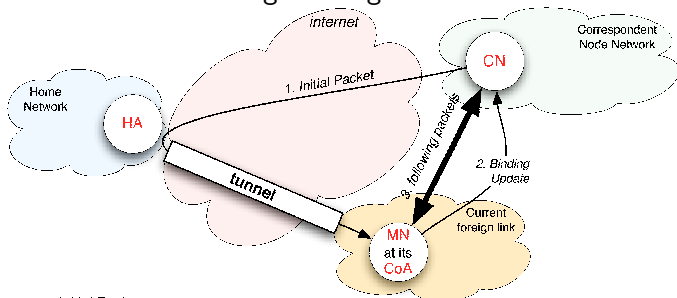


MN updates its status (CoA) to HA whenever changes occur

MN can also be a Mobile Router (MR), providing mobility for a whole IPv6 prefix

MIPv6 optimizations

Prevent all traffic to go through HA



1. *Initial Packet*
2. *Binding Update (BU)* : src = CoA, dst = CN, HAO, RH type 2 (HoA)
- 3a. *Traffic towards CN* : src = CoA, dst = CN, HAO
- 3b. *Traffic from CN* : src = CN, dst = CoA, RH Type 2 (HoA)

MN can decide to communicate directly with CN
 MN updates its CoA to CN during communication



Agenda

- 1 Deperimeterization concept
- 2 Facing reality
- 3 Thinking differently (again)
- 4 Final thoughts**



Network security doomed ?

Is today network security model able to deliver what we need ?

- Traditional network security scales with difficulties
- Segregation is more and more difficult to maintain
- In the end, we never get what we need

Is perimeter dead anyway ?



Deperimeterization or Reperimeterization ?

It is more a question of rethinking the network, and the concept of perimeter than just trashing the idea

- Let the network do its job !
- Re-establish global connectivity
- Use network agnostic security means
- Enjoy nice features

OK, and there still will be a lot of work to come
But who said security was easy ? :)



End...

Thank you for your attention

Questions ?