



De-perimeterization

Dream or Nightmare for Network Security?

Cédric BLANCHER

`cedric.blancher@eads.net`
Computer Security Research Team Leader
EADS Innovation Works

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

Source Boston - March 12th-14th
<http://sourceboston.com/>

Why de-perimeterization...

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

- We defend our network creating boundaries
- We are still using firewalls
- We just added network authentication

All this is just about protecting our perimeter(s)

Breaking the model

De-perimeterization breaks that security model

- Network should be open
- Network should be considered as hostile
- Emphasis should be put on data protection

Surprising approach at first
Thus all the more interesting !

Agenda

- 1 De-perimeterization concept
- 2 Too beautiful to be true?
- 3 Thinking differently (again)
- 4 Final thoughts



Agenda

- 1 De-perimeterization concept
- 2 Too beautiful to be true?
- 3 Thinking differently (again)
- 4 Final thoughts



Perimeters are arming business

De-perimeterization fans state 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

Less effective, more annoying, why keep it ?



Perimeters weaknesses

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 ?

Perimeter as a vulnerability cause

When perimeter arms business, users tend to find "solutions"

- No webmail ? Forward corporate email to Gmail account
- No Blackberry ? Forward corporate email to private BB account
- No shared agenda ? Use Google Calendar
- Etc...

Information goes anywhere, but where you can control it !

Side effects are very difficult to predict and assess...

De-perimeterization as a solution

De-perimeterization fans advocate a big shift for security mindset

- Concentrate on data access
- Secure endpoints
- Consider network environment hostile
- Move security from network to protocols

See Jericho Forum 11 Commandments,
Business Case and other papers



Agenda

- 1 De-perimeterization concept
- 2 Too beautiful to be true?**
- 3 Thinking differently (again)
- 4 Final thoughts

What's behind the story

Looking at the 11 commandments

- The scope and level of protection should be specific & appropriate to the asset at risk
- Security mechanisms must be pervasive, simple, scalable & easy to manage
- Assume context at your peril
- Devices and applications must communicate using open, secure protocols
- All devices must be capable of maintaining their security policy on an untrusted network
- Etc.

Common sense, but not that incompatible with perimeters...



Examples of successful de-perimeterization

Some success stories mentioned during a presentation at Deepsec

- Speaker laptop built according to these principles
- BP to put 18k laptops outside LAN directly on Internet
- ICI to move its central Internet access to multiple DSL
- KLM to move from corporate laptops to user managed laptops

Is this really de-perimeterization ?

Facing reality

Technical reality is IPv4 Internet **is** fragmented

- IPv4 involves NAT
- NAT means perimeters

Consequence

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

De-perimeterization scope

Does de-perimeterization affect the whole IT system ?

- There's a change in how to deal with security
- But why should fixed resources should be affected ? !

De-perimeterization affects mobile ressources and their way to communicate with home network

Any solution so far ?

One efficient solution seems to be overlayed networking

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

Creating a (hopefully) secure network over the network to regain connectivity

Agenda

- 1 De-perimeterization concept
- 2 Too beautiful to be true?
- 3 Thinking differently (again)
- 4 Final thoughts

Global connectivity

Global connectivity is a key factor to de-perimeterization

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

De-perimeterization has more to do with reperimeterization

How to regain connectivity

The "I" word : IPv6

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

Global connectivity does not means no firewall !

Example of technological shift

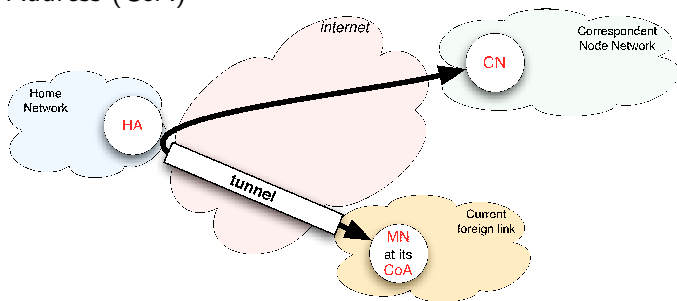
Mobile IPv6 is an IPv6 extension for mobility

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

Efficient, pervasive and secure solution for roaming...

MIPv6

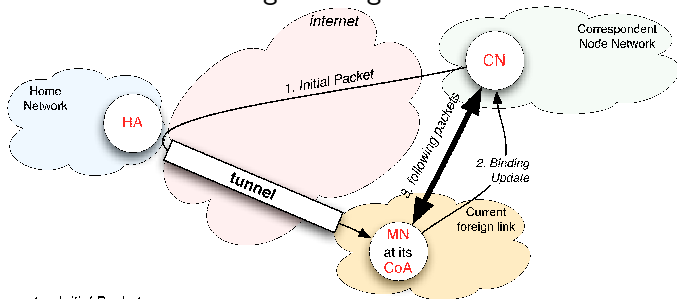
CN is a random IPv6 node
HA relays communications for MN to its Care-of Address (CoA)



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

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

Is it enough ?

This only addresses communication security vs. network environment

- Need to address data access
- Need to address virus/malware/spam problem

A lot to do on the system side

Systems need to be made more resilient to external threats as classical prevention/detection/response schemes are losing ground

Agenda

- 1 De-perimeterization concept
- 2 Too beautiful to be true?
- 3 Thinking differently (again)
- 4 Final thoughts**

Network security doomed ?

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

- Network security does not scale
- Segregation is more and more difficult to maintain
- In the end, we never get what we need

Is perimeter dead anyway ?

De-perimeterization or Re-perimeterization ?

It is more a question of rethinking the network, and the concept of perimeter...

- 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 ? :)