OSY.SSI[2019][4]

On the limitations of access control

As you probably noticed by now, AC is not a panacea:

- It is imperfect (and far from perfect)
- It is a complicated mechanism to setup and maintain and update

On the limitations of access control

As you probably noticed by now, AC is not a panacea:

- It is imperfect (and far from perfect)
- It is a complicated mechanism to setup and maintain and update

We argued during the first lecture that security is not about protecting things; we should now add that security is not about keeping the bad guys out.

On the limitations of access control

As you probably noticed by now, AC is not a panacea:

- It is imperfect (and far from perfect)
- It is a complicated mechanism to setup and maintain and update

We argued during the first lecture that security is not about protecting things; we should now add that security is not about keeping the bad guys out.

(you now the drill: these are only means to an end)

On the limitations of access control

As you probably noticed by now, AC is not a panacea:

- It is imperfect (and far from perfect)
- It is a complicated mechanism to setup and maintain and update

We argued during the first lecture that security is not about protecting things; we should now add that security is not about keeping the bad guys out.

(you now the drill: these are only means to an end)

Again, this should be a somewhat puzzling statement, so let's dig in.

Back to the future

To understand the last central element of the Classical Security Theory...

... let's look at how humans try to protect themselves from other humans.

Back to the future

To understand the last central element of the Classical Security Theory...

... let's look at how humans try to protect themselves from other humans.

Cultural point: first evidence of human/human organised conflict is Jebel Sahaba, Qadan culture (far northern Sudan) some 13,000 years ago. It seems we hadn't invented warfare before.

How do you protect yourself?

Question: someone wants to attack you, what do you do if you can't run?

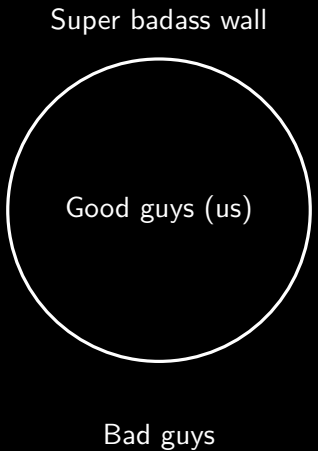
(cue obscure parody of a horror movie)

Let's build a wall!

It will look nice on photos with some pollution and filters!

Let's build a wall!

Conceptually:



Let's build a wall!

What are some assumptions of this approach?

Let's build a wall!

What are some assumptions of this approach?

- Assumption 1: Wall is "airtight" – it really separates the inside from the outside with no holes

Let's build a wall!

What are some assumptions of this approach?

- Assumption 1: Wall is "airtight" – it really separates the inside from the outside with no holes
- Assumption 2: Wall cannot be crossed – it is too high and too tough to break

Let's build a wall!

What are some assumptions of this approach?

- Assumption 1: Wall is "airtight" – it really separates the inside from the outside with no holes
- Assumption 2: Wall cannot be crossed – it is too high and too tough to break
- Assumption 3: Bad guys are only outside

Let's build a wall!

What are some assumptions of this approach?

- Assumption 1: Wall is "airtight" – it really separates the inside from the outside with no holes
- Assumption 2: Wall cannot be crossed – it is too high and too tough to break
- Assumption 3: Bad guys are only outside
- Assumption 4: Bad guys can only hurt us if they come inside

Let's build a wall!

What are some assumptions of this approach?

- Assumption 1: Wall is "airtight" – it really separates the inside from the outside with no holes
- Assumption 2: Wall cannot be crossed – it is too high and too tough to break
- Assumption 3: Bad guys are only outside
- Assumption 4: Bad guys can only hurt us if they come inside
- Assumption 5: Every single good guy would rather starve to death than make a deal with the bad guys and give up the other good guys in exchange for some froyo, i.e. good guys remain good.

Let's build a wall!

What are some assumptions of this approach?

- Assumption 1: Wall is "airtight" – it really separates the inside from the outside with no holes
- Assumption 2: Wall cannot be crossed – it is too high and too tough to break
- Assumption 3: Bad guys are only outside
- Assumption 4: Bad guys can only hurt us if they come inside
- Assumption 5: Every single good guy would rather starve to death than make a deal with the bad guys and give up the other good guys in exchange for some froyo, i.e. good guys remain good.

Now let's challenge these assumptions.

Let's build a wall!

Assumption 1: Wall is "airtight"

Let's build a wall!

Assumption 1: Wall is "airtight"

Wall built under the Qing dynasty (blue territory) to fend off Han invaders

Let's build a wall!

Assumption 2: Wall cannot be crossed

Let's build a wall!

Assumption 2: Wall cannot be crossed

Wall built under the USSR to fend off Capitalist migrants (pictured)

Let's build a wall!

Assumption 3: Bad guys are only outside
Assumption 5: Every single good guy would rather starve to death

Let's build a wall!

Assumption 3: Bad guys are only outside
Assumption 5: Every single good guy would rather starve to death

Ephialtes (lit. "nightmare") of Trachis, Onetas or Carystus, Corydallus of Anticyra were instrumental in the victory of the Persian armies (pictured) at the Battle of Thermopylae against 300 rebel Spartans.

Let's build a wall!

Assumption 4: Bad guys can only hurt us if they come inside

Wait! How is that related to information security?

(This is the question you should be asking yourselves)

- "Walls" are a form of perimeter defence
- Mutatis mutandis, the same assumptions (and limitations) hold for all such defences

We can (and many people still) use access control to separate

- The "inside" == good guys from
- The "outside" == bad guys

but you should by now realise this is a flawed idea.

Let's bash some walls!

What are some other issues with walls?

Let's bash some walls!

What are some other issues with walls?

- Cost increases with perimeter + Maintenance cost
- Hard to move (without creating holes!)
- Absolutely inefficient against airborne weaponry
- May turn to the defender's disadvantage
- Adversary needs only one success to win

Fundamentally, at best, wall give us time: they are dilatory devices.

In the olden days, besieging was tiring and boring, so eventually attackers stopped.
But in the modern world, attackers are not going away and they are not going to stop.
Also they're robots.

Perimeter defence is not adapted

Perimeter defence:

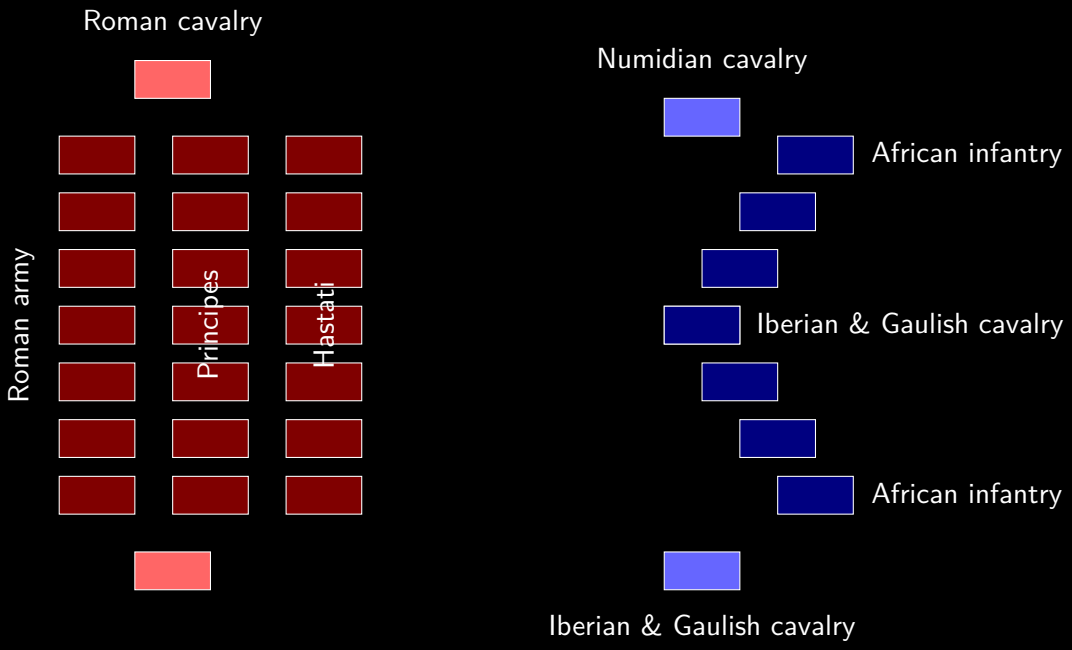
- Good points: easy to understand, good ol' method. May work in actual siege.
- Bad points: pretty much all the rest. Fails miserably in infosec.

Bottom line: we need a better strategy.

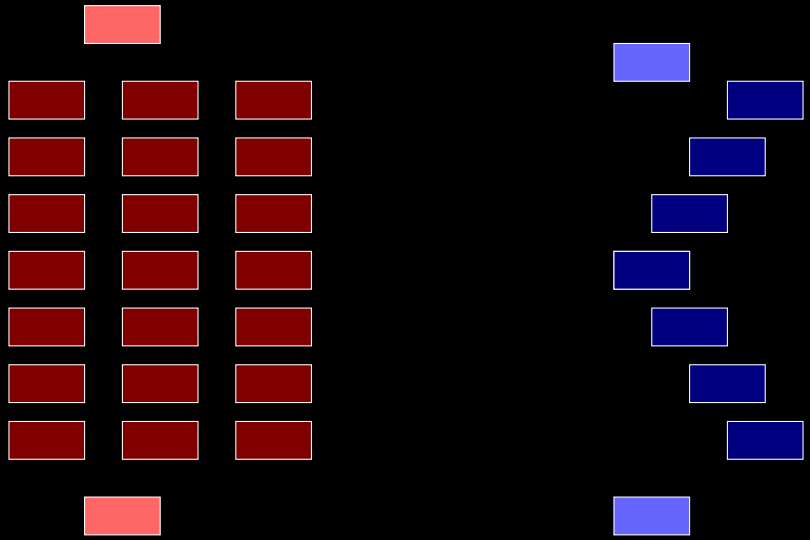
Table of Contents

Firts noteworthy example: Hannibal, battle of Cannae (216 BCE, modern-day Apulia in southeast Italy).

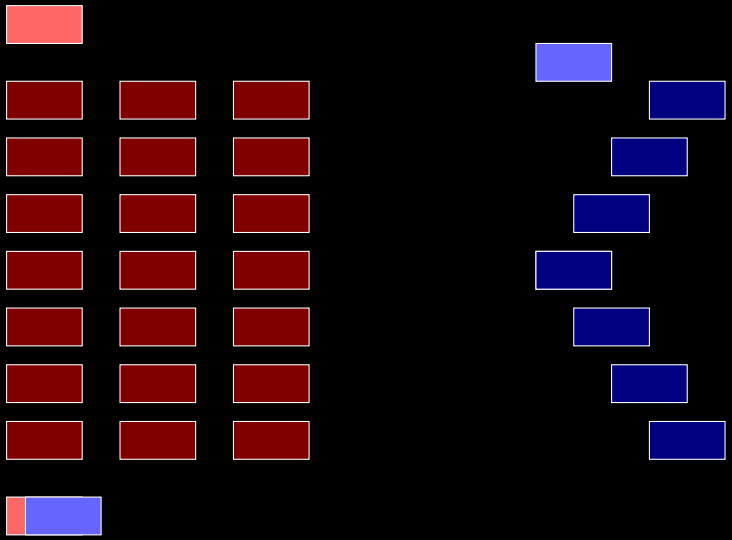
Defence in depth, the original version



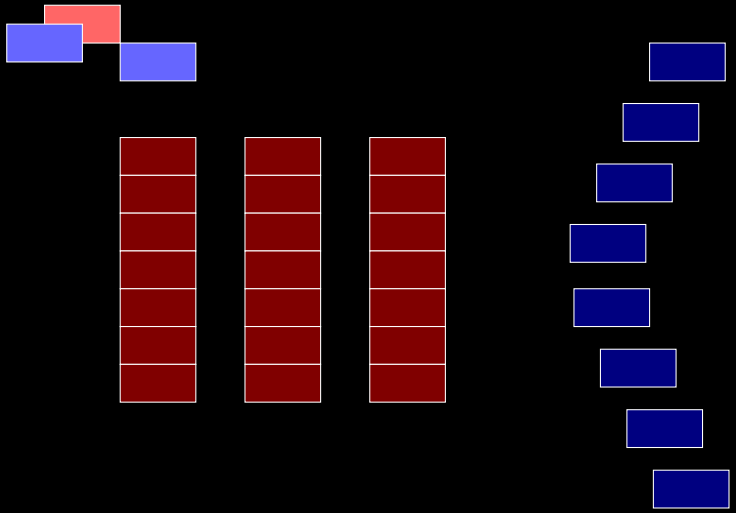
Defence in depth, the original version



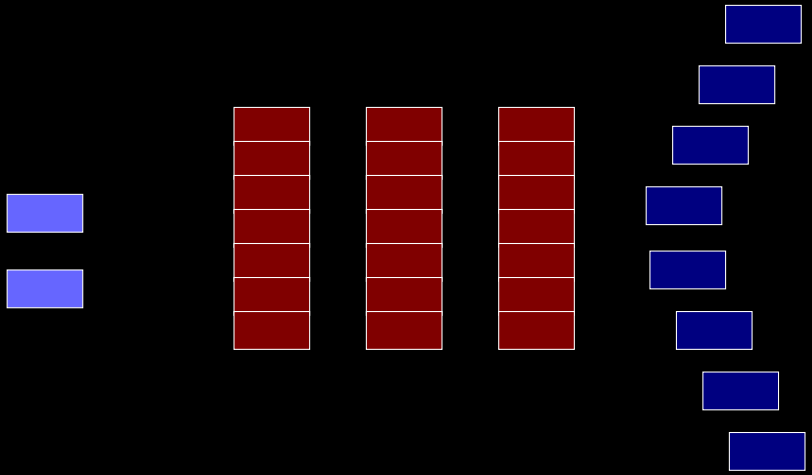
Defence in depth, the original version



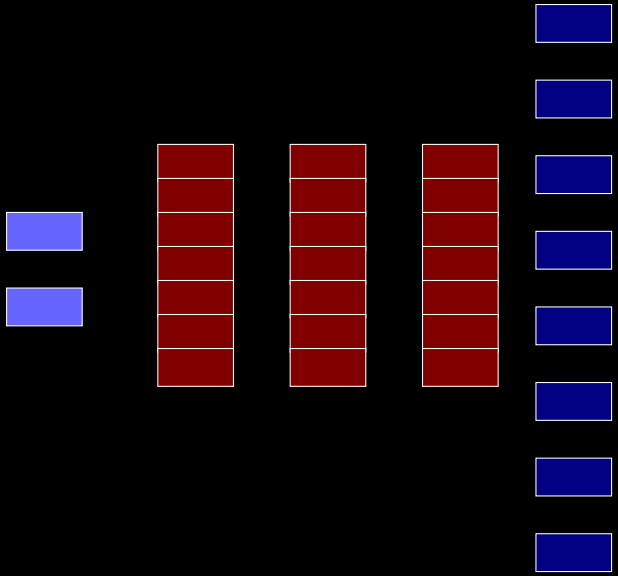
Defence in depth, the original version



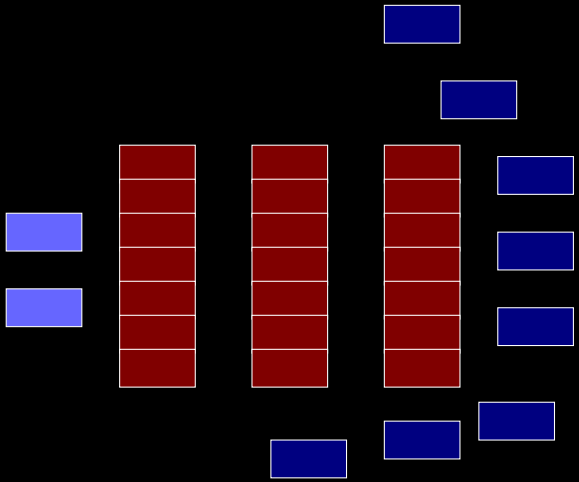
Defence in depth, the original version



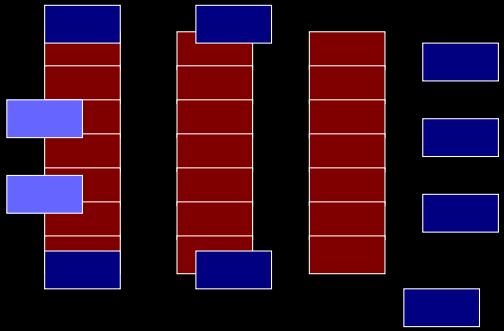
Defence in depth, the original version



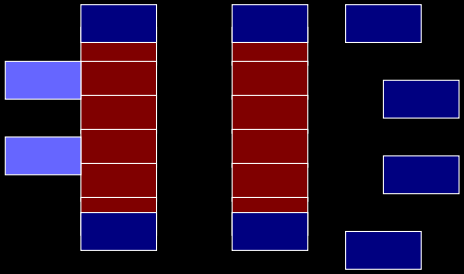
Defence in depth, the original version



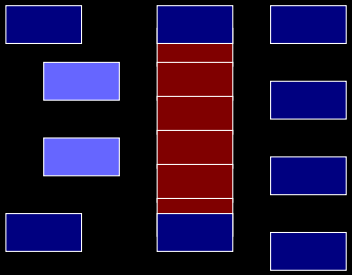
Defence in depth, the original version



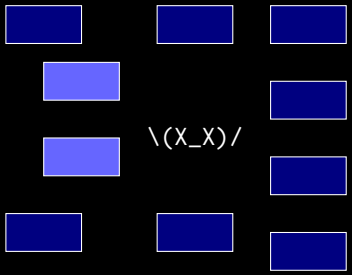
Defence in depth, the original version



Defence in depth, the original version



Defence in depth, the original version



Defence in depth

Ok so what did they do?

Defence in depth

Ok so what did they do?

- Yield space to force enemy force dispersion == let them in
- Retreat to force enemy advance in controlled territory == prepare battlefield
- Outflanking to force the enemy into perimeteric defensive position
- Cut out escape route
- Target highest-value, commanding officers first
- Use the limited information available to attackers (e.g. front line)

Can we perhaps learn some lessons relevant to our defence needs?

“Cyber”-defence in depth

From an information security perspective, we would need to clarify:

1. What “space” can we yield? What is “controlled territory”?
2. How to fend off attacks, and eventually “cut the head” of the attacker?
3. “Where” is the attacker? And how do we know?

To do that, we will

- Set-up zones with access control == boundaries
- Design the security battlefield == architecture
- Try to learn a maximum about the attacker while she’s here == surveillance

Table of Contents

"Cyber"-defence in depth I: Topologisation

An area is a portion of space delimited by a boundary.

E.g. continuous injection $\mathbb{S}^1 \hookrightarrow \mathbb{R}^2$ (Jordan's theorem).

General rule: locating something = finding the smallest area to which it belongs.
Consequences:

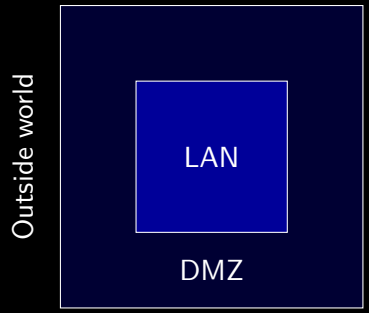
- Large single area $\Rightarrow$ coarse location — Costs less
- Many small areas $\Rightarrow$ precise location — Costs more

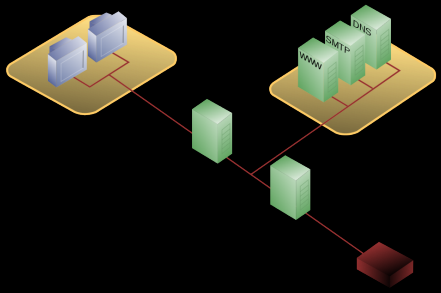
(nice mathematics to be done about formalising this, if you're interested)

So a starting point for us is to define areas. This seems to be a completely arbitrary process, although in practice we tend to follow natural boundaries (more about that later).

“Cyber”-defence in depth I: Topologisation

As an exemple, the notion of DMZ is increasingly common in organisational networks





In the DMZ: services such as e-mails, DNS, etc. + honeypot.

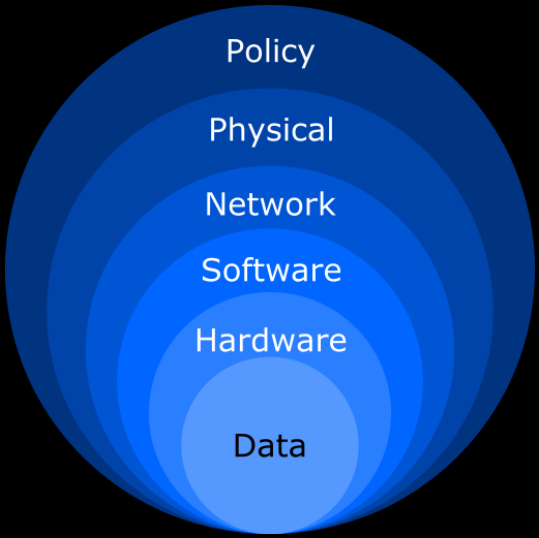
The original DMZ

“Cyber”-defence in depth I: Topologisation

General philosophy:

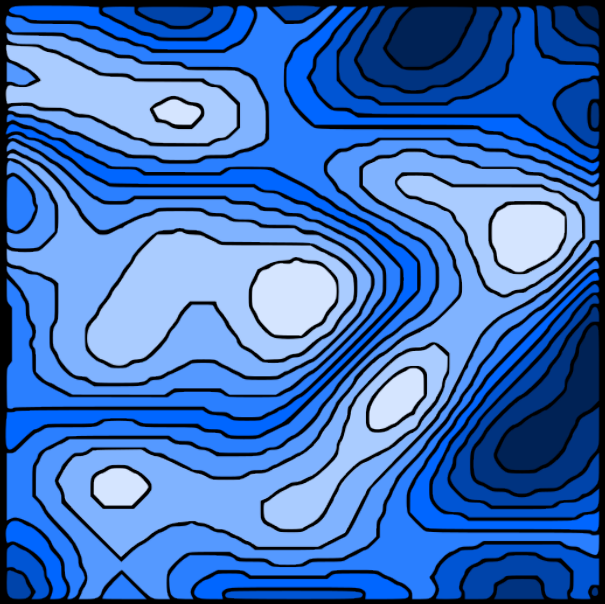
- Create boundaries around key assets
- Create boundaries between key assets (principle of least priviledge, why?)
- Leverage natural boundaries (walls, existing AC, ...)

Natural or “Vertical” boundaries (start at the bottom)

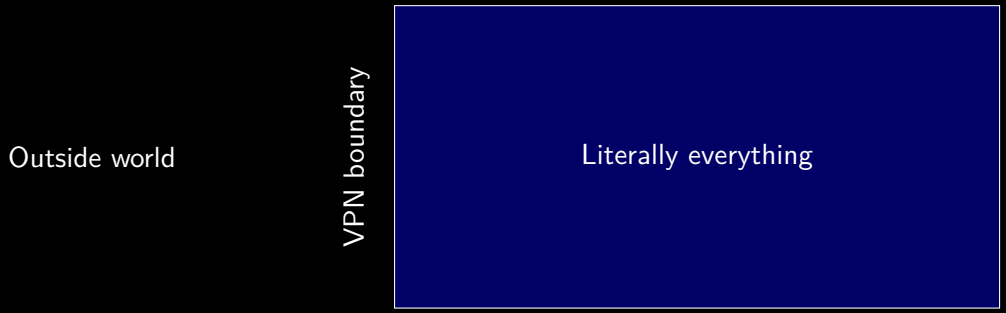


Natural or “Vertical” boundaries (topographic view)

Force them to climb!



What not to do: Target 2013



We'll see the consequences next time

Defence in Depth is really palliative

But its merits are that we can now

1. Prevent intrusion by setting up boundaries (AC)
2. Resist crossing to delay the adversary and force them inside one area
3. Limit the impact of area intrusion (PLP)

Defence in Depth is really palliative

But its merits are that we can now

1. Prevent intrusion by setting up boundaries (AC)
2. Resist crossing to delay the adversary and force them inside one area
3. Limit the impact of area intrusion (PLP)
4. Detect area intrusion (honeypots, IDS)
5. Log area intrusions (why?)

Defence in Depth is really palliative

But its merits are that we can now

1. Prevent intrusion by setting up boundaries (AC)
2. Resist crossing to delay the adversary and force them inside one area
3. Limit the impact of area intrusion (PLP)
4. Detect area intrusion (honeypots, IDS)
5. Log area intrusions (why?)

Is that enough?

Defence in Depth is really palliative

But its merits are that we can now

1. Prevent intrusion by setting up boundaries (AC)
2. Resist crossing to delay the adversary and force them inside one area
3. Limit the impact of area intrusion (PLP)
4. Detect area intrusion (honeypots, IDS)
5. Log area intrusions (why?)

Is that enough? We must also audit and pentest!

Table of Contents

Conclusion

- Layered defence mechanism to enable action and gather information
- Replace perimeter control by area control, with no trust zone
- Check and test everything regularly, and if necessary update
- Favour freedom of movement over firepower
- Beware of all the bullshit you can find on the Internet (or worse: elsewhere)

Good now we're as secure as can be we can list a number of cute vulnerabilities and go to bed.

Conclusion

- Layered defence mechanism to enable action and gather information
- Replace perimeter control by area control, with no trust zone
- Check and test everything regularly, and if necessary update
- Favour freedom of movement over firepower
- Beware of all the bullshit you can find on the Internet (or worse: elsewhere)

Good now we're as secure as can be we can list a number of cute vulnerabilities and go to bed.

OR CAN WE?!

See you next time! Bring your laptops!
xoxo