# OSY.SSI[2015][6]

Topology

# Topology : discourse on places

**Key point:**

# Topology : discourse on places

**Key point:** “Jordan curve theorem”

# Topology : discourse on places

**Key point:** "Jordan curve theorem"

Theorem ("Jordan", 1887)

$f : S^1 \hookrightarrow \mathbb{R}^2 \Rightarrow \mathbb{R}^2 = A \cup B \cup C, A \cap B = \emptyset$, *$A$ and $B$ open and* $\partial A = \partial B = C = f(S^1)$.

# Topology : discourse on places

**Key point:** "Jordan curve theorem"

Theorem ("Jordan", 1887)

$f : S^1 \hookrightarrow \mathbb{R}^2 \Rightarrow \mathbb{R}^2 = A \cup B \cup C, A \cap B = \emptyset$, *A and B open and* $\partial A = \partial B = C = f(S^1)$.

Proof.

Using Bouwer's fixed-point theorem, see Maehara 1984. □

# Topology

# Topology

# Topology

Two interesting, dual angles:

# Topology

Two interesting, dual angles:

- **Zones** and their **boundaries**

# Topology

Two interesting, dual angles:

- **Zones** and their **boundaries**
- **Neighbourhoods** and the resulting **network**

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)
- Airgaps, firewalls, VLANs, encrypted networks, NIPS (network)

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)
- Airgaps, firewalls, VLANs, encrypted networks, NIPS (network)
- OS/software access control, A/V, encrypted disks, HIPS (host/application)

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)
- Airgaps, firewalls, VLANs, encrypted networks, NIPS (network)
- OS/software access control, A/V, encrypted disks, HIPS (host/application)
- People themselves (policy)

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)
- Airgaps, firewalls, VLANs, encrypted networks, NIPS (network)
- OS/software access control, A/V, encrypted disks, HIPS (host/application)
- People themselves (policy)

**Question 1:**

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)
- Airgaps, firewalls, VLANs, encrypted networks, NIPS (network)
- OS/software access control, A/V, encrypted disks, HIPS (host/application)
- People themselves (policy)

**Question 1:** how do we know a boundary was crossed?

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)
- Airgaps, firewalls, VLANs, encrypted networks, NIPS (network)
- OS/software access control, A/V, encrypted disks, HIPS (host/application)
- People themselves (policy)

**Question 1:** how do we know a boundary was crossed? **Detection**.

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)
- Airgaps, firewalls, VLANs, encrypted networks, NIPS (network)
- OS/software access control, A/V, encrypted disks, HIPS (host/application)
- People themselves (policy)

**Question 1:** how do we know a boundary was crossed? **Detection**.

**Question 2:**

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)
- Airgaps, firewalls, VLANs, encrypted networks, NIPS (network)
- OS/software access control, A/V, encrypted disks, HIPS (host/application)
- People themselves (policy)

**Question 1:** how do we know a boundary was crossed? **Detection**.

**Question 2:** what boundaries do we want?

# What constitutes a “boundary”?

## Beyond hack-and-slash

A *boundary* is anything performing NEAT *access control*.

Examples:

- Walls, giant crocodile-filled pools, locks and doors (physical)
- Airgaps, firewalls, VLANs, encrypted networks, NIPS (network)
- OS/software access control, A/V, encrypted disks, HIPS (host/application)
- People themselves (policy)

**Question 1:** how do we know a boundary was crossed? **Detection**.

**Question 2:** what boundaries do we want?

# Perimeter defence

## All-round protection

**Idea:**

# Perimeter defence

## All-round protection

**Idea:** The enemy is “outside”.

# Perimeter defence

## All-round protection

**Idea:** The enemy is “outside”. Keep her outside.

# Perimeter defence

## All-round protection

**Idea:** The enemy is “outside”. Keep her outside.

**Approach:**

# Perimeter defence

## All-round protection

**Idea:** The enemy is “outside”. Keep her outside.

**Approach:** Strong perimeter barriers (customs, walls, ...)
Aka the good ol’ way.

# Perimeter defence

## All-round protection

**Idea:** The enemy is “outside”. Keep her outside.

**Approach:** Strong perimeter barriers (customs, walls, ...)
Aka the good ol’ way.

**Examples:**

# Perimeter defence

## All-round protection

**Idea:** The enemy is “outside”. Keep her outside.

**Approach:** Strong perimeter barriers (customs, walls, ...)
Aka the good ol’ way.

**Examples:** Hadrian Wall, Berlin Wall, Great Wall, Bacterial cell wall

# Perimeter defence

## All-round protection

**Idea:** The enemy is “outside”. Keep her outside.

**Approach:** Strong perimeter barriers (customs, walls, ...)
Aka the good ol’ way.

**Examples:** Hadrian Wall, Berlin Wall, Great Wall, Bacterial cell wall

Bonus: keeps your people from emigrating.

# Perimeter defence

## All-round protection

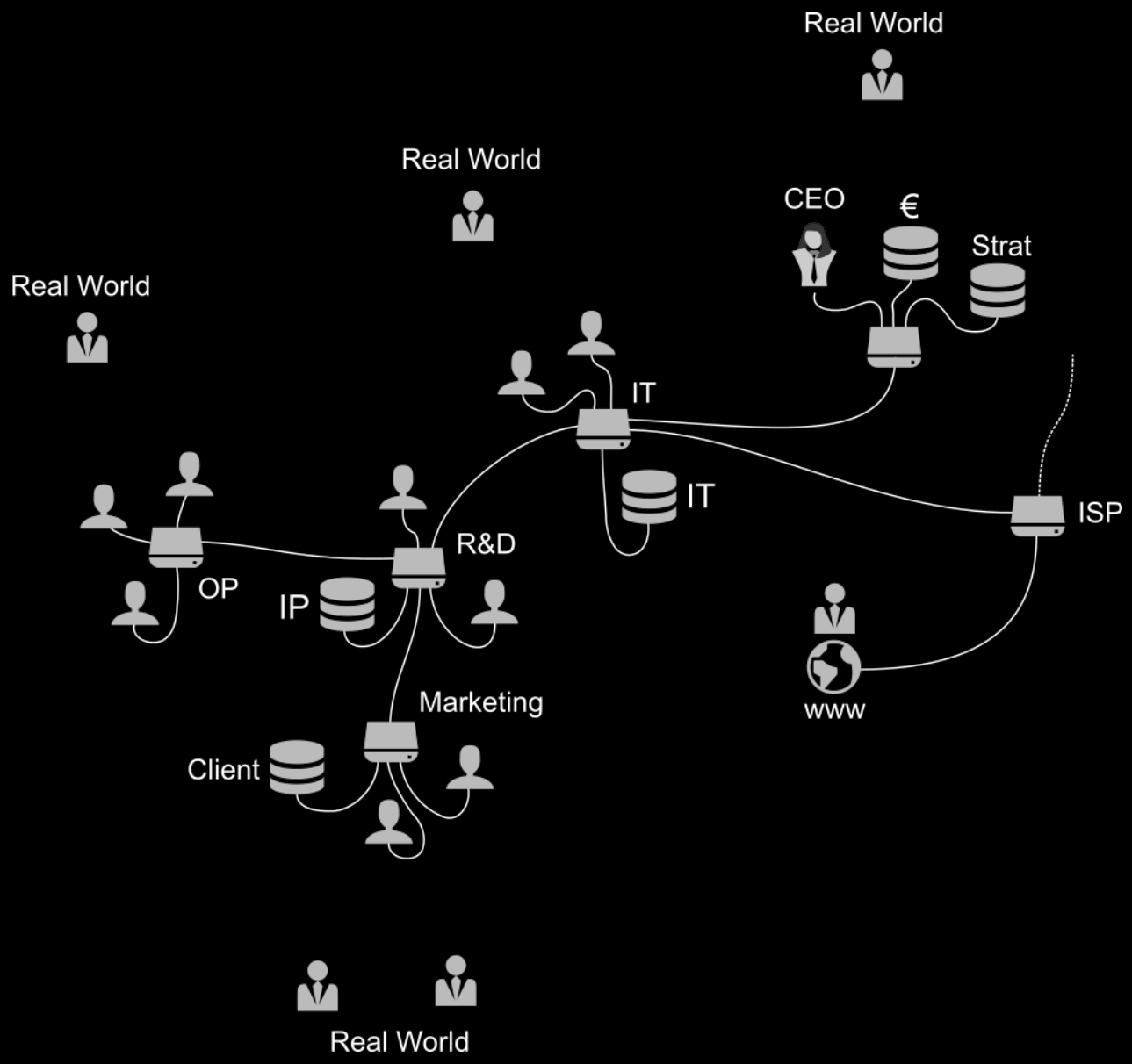
**Idea:** The enemy is “outside”. Keep her outside.

**Approach:** Strong perimeter barriers (customs, walls, ...)
Aka the good ol’ way.

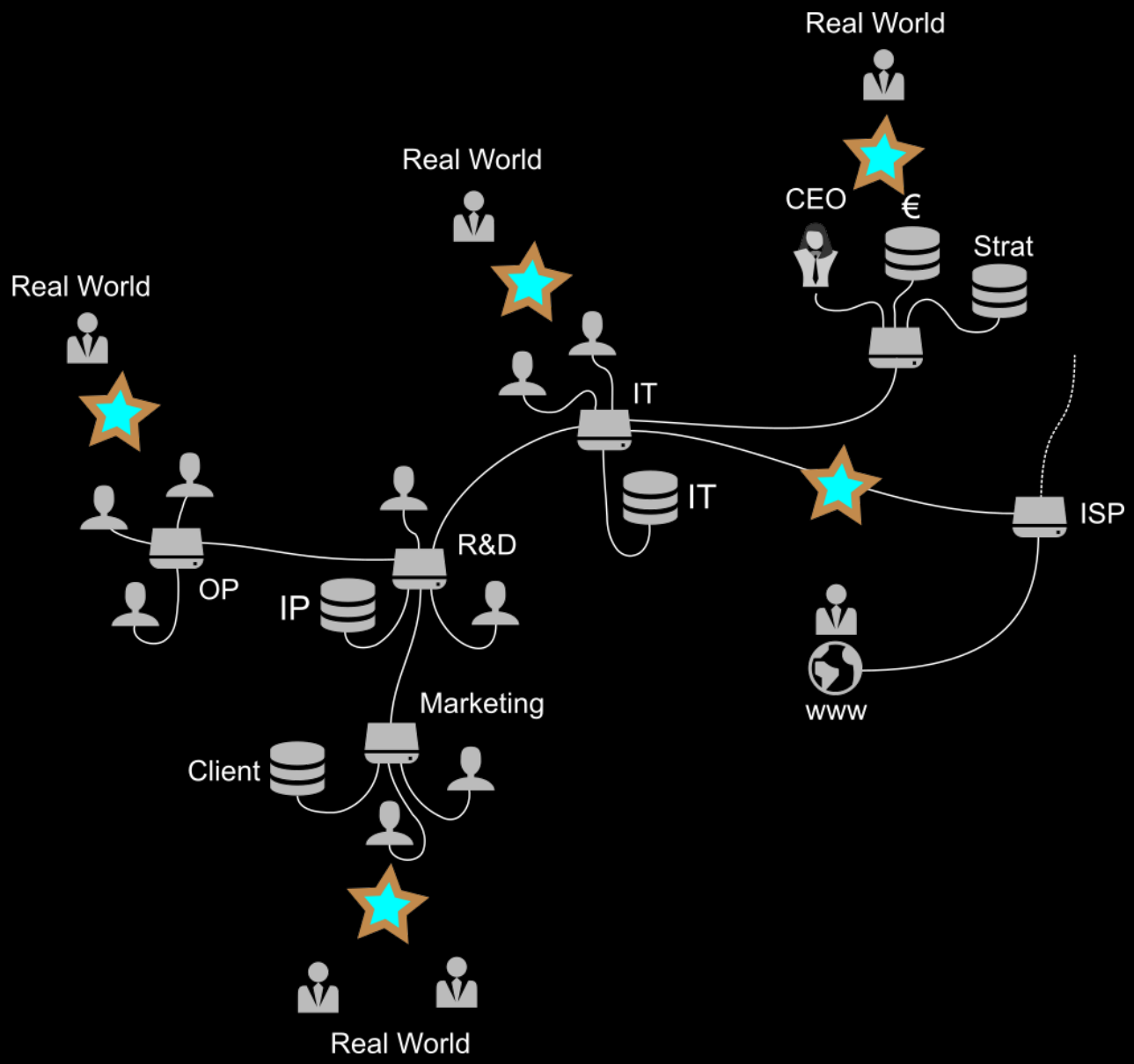
**Examples:** Hadrian Wall, Berlin Wall, Great Wall, Bacterial cell wall

Bonus: keeps your people from emigrating.
Hypotheses, weaknesses? Limitations?

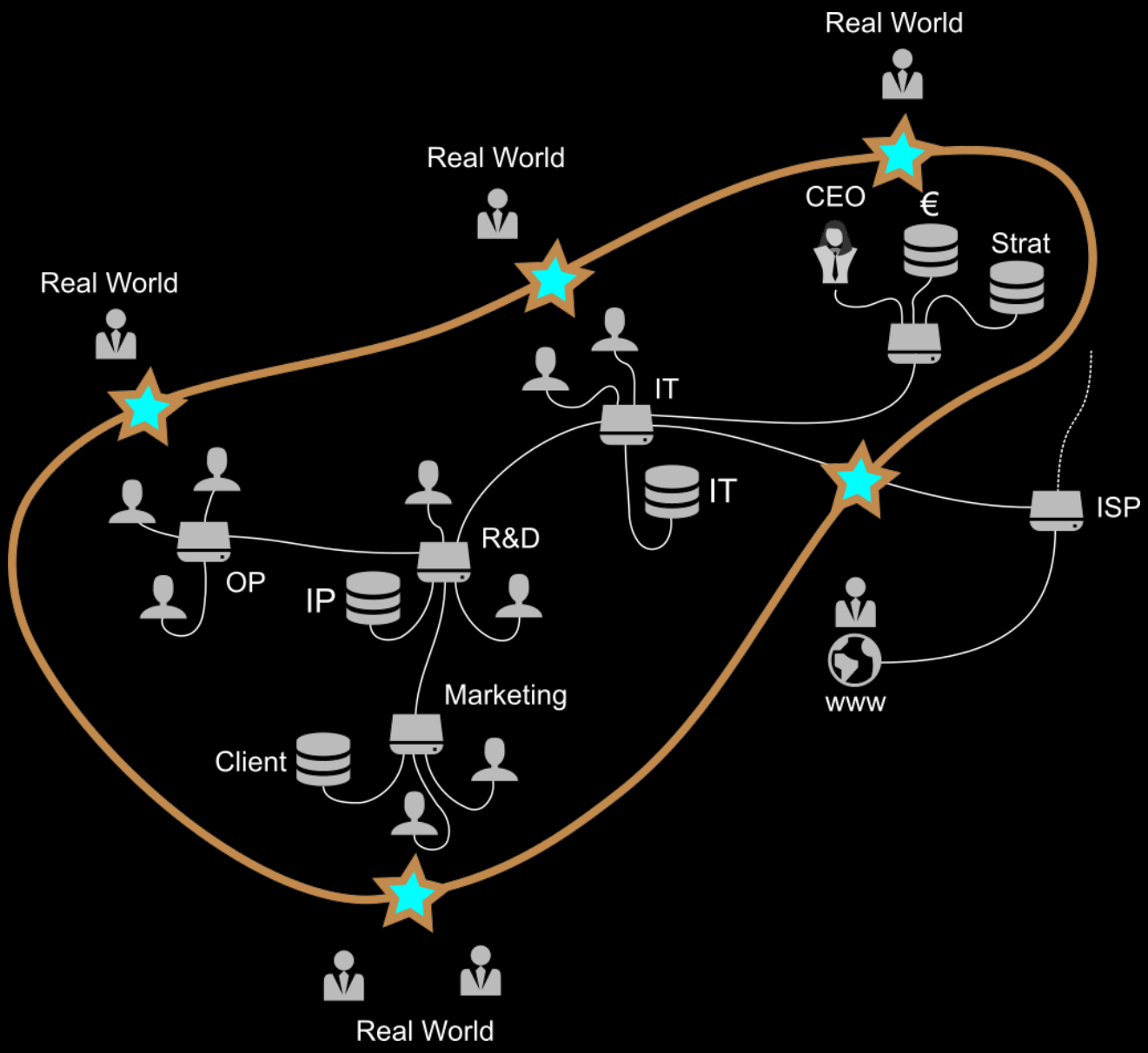
# An example


Real World
Real World
Real World
CEO
€
Strat
IT
IT
ISP
R&D
OP
IP
Marketing
Client
www
Real World

# An example


Real World
Real World
CEO
€
Strat
Real World
IT
IT
ISP
R&D
OP
IP
www
Marketing
Client
Real World

# An example


Real World
Real World
Real World
Real World
CEO
€
Strat
IT
IT
R&D
OP
IP
ISP
www
Marketing
Client

# Perimeter defence

## Flexibility

**Questions:**

# Perimeter defence

## Flexibility

**Questions:**

# Perimeter defence

## Flexibility

**Questions:**

- What if Marketing wants Financial data?

# Perimeter defence

## Flexibility

**Questions:**

- What if Marketing wants Financial data?
- BYOD? USB sticks?

# Perimeter defence

## Flexibility

**Questions:**

- What if Marketing wants Financial data?
- BYOD? USB sticks?Not everything flows through your network.

# Perimeter defence

## Flexibility

**Questions:**

- What if Marketing wants Financial data?
- BYOD? USB sticks?Not everything flows through your network.
- Bluetouff/Robots?

# Perimeter defence

## Flexibility

**Questions:**

- What if Marketing wants Financial data?
- BYOD? USB sticks?Not everything flows through your network.
- Bluetouff/Robots?No access control means no boundary.

# Perimeter defence

## Flexibility

**Questions:**

- What if Marketing wants Financial data?
- BYOD? USB sticks?Not everything flows through your network.
- Bluetouff/Robots?No access control means no boundary.
- Smart grids and side-channels?

# Perimeter defence

## Flexibility

**Questions:**

- What if Marketing wants Financial data?
- BYOD? USB sticks?Not everything flows through your network.
- Bluetouff/Robots?No access control means no boundary.
- Smart grids and side-channels?Not everything flows through your network (bis).

# Perimeter defence

## Flexibility

**Questions:**

- What if Marketing wants Financial data?
- BYOD? USB sticks?Not everything flows through your network.
- Bluetouff/Robots?No access control means no boundary.
- Smart grids and side-channels?Not everything flows through your network (bis).

# Perimeter defence

## Crossing number

# Perimeter defence

## Crossing number

The *crossing number* $\kappa(x, y)$ is

# Perimeter defence

## Crossing number

The *crossing number* $\kappa(x, y)$ is the *minimum* number of times one has to cross a boundary to get from $x$ to $y$.

# Perimeter defence

## Crossing number

The *crossing number* $\kappa(x, y)$ is the *minimum* number of times one has to cross a boundary to get from $x$ to $y$.

In perimeter defence,

# Perimeter defence

## Crossing number

The *crossing number* $\kappa(x, y)$ is the *minimum* number of times one has to cross a boundary to get from $x$ to $y$.

In perimeter defence,

$$\kappa(x, y) = \begin{cases} 0 & \text{if } x, y \text{ on the same side} \\ 1 & \text{otherwise} \end{cases}$$

# Perimeter defence

## Crossing number

The *crossing number* $\kappa(x, y)$ is the *minimum* number of times one has to cross a boundary to get from $x$ to $y$.

In perimeter defence,

$$\kappa(x, y) = \begin{cases} 0 & \text{if } x, y \text{ on the same side} \\ 1 & \text{otherwise} \end{cases}$$

An attacker only has to be right once...

# Perimeter defence

## Crossing number

The *crossing number* $\kappa(x, y)$ is the *minimum* number of times one has to cross a boundary to get from $x$ to $y$.

In perimeter defence,

$$\kappa(x, y) = \begin{cases} 0 & \text{if } x, y \text{ on the same side} \\ 1 & \text{otherwise} \end{cases}$$

An attacker only has to be right once...
Once in a **trusted zone** she can do as she wishes.

# Perimeter defence

## Size matters

A large perimeter

# Perimeter defence

## Size matters

A large perimeter is hard to defend (France, WWII) and scale (China, Qing dynasty).

# Perimeter defence

## Size matters

A large perimeter is hard to defend (France, WWII) and scale (China, Qing dynasty).

A small perimeter

# Perimeter defence

## Size matters

A large perimeter is hard to defend (France, WWII) and scale (China, Qing dynasty).

A small perimeter is easy to besiege (Leningrad, WWII).

# Perimeter defence

## Size matters

A large perimeter is hard to defend (France, WWII) and scale (China, Qing dynasty).

A small perimeter is easy to besiege (Leningrad, WWII).

Sometimes, two dimensions aren't enough (London, WWII).

# Multi-perimeter defence

What if we have *several disjoint zones* ?

# Multi-perimeter defence

What if we have *several disjoint zones* ?
Same problem: attackers can simply target the most interesting one.

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

**Key ideas:**

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

**Key ideas:**

- *encapsulate*

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

**Key ideas:**

- *encapsulate*
- *multiple* boundaries

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

**Key ideas:**

- *encapsulate*
- *multiple* boundaries
- so as to *maximize* the crossing number

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

**Key ideas:**

- *encapsulate*
- *multiple* boundaries
- so as to *maximize* the crossing number
  - from untrusted zones to critical zones ("vertical" movement)

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

**Key ideas:**

- *encapsulate*
- *multiple* boundaries
- so as to *maximize* the crossing number
  - from untrusted zones to critical zones ("vertical" movement)
  - from one critical zone to another critical zone ("horizontal" movement)

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

**Key ideas:**

- *encapsulate*
- *multiple* boundaries
- so as to *maximize* the crossing number
  - from untrusted zones to critical zones ("vertical" movement)
  - from one critical zone to another critical zone ("horizontal" movement)
- "best practice"

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

**Key ideas:**

- *encapsulate*
- *multiple* boundaries
- so as to *maximize* the crossing number
  - from untrusted zones to critical zones ("vertical" movement)
  - from one critical zone to another critical zone ("horizontal" movement)
- "best practice"

Sounds hard...

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

**Key ideas:**

- *encapsulate*
- *multiple* boundaries
- so as to *maximize* the crossing number
  - from untrusted zones to critical zones ("vertical" movement)
  - from one critical zone to another critical zone ("horizontal" movement)
- "best practice"

Sounds hard...

**Hint:**

# Defence in depth

*Hannibal, battle of Cannae, 216 BCE

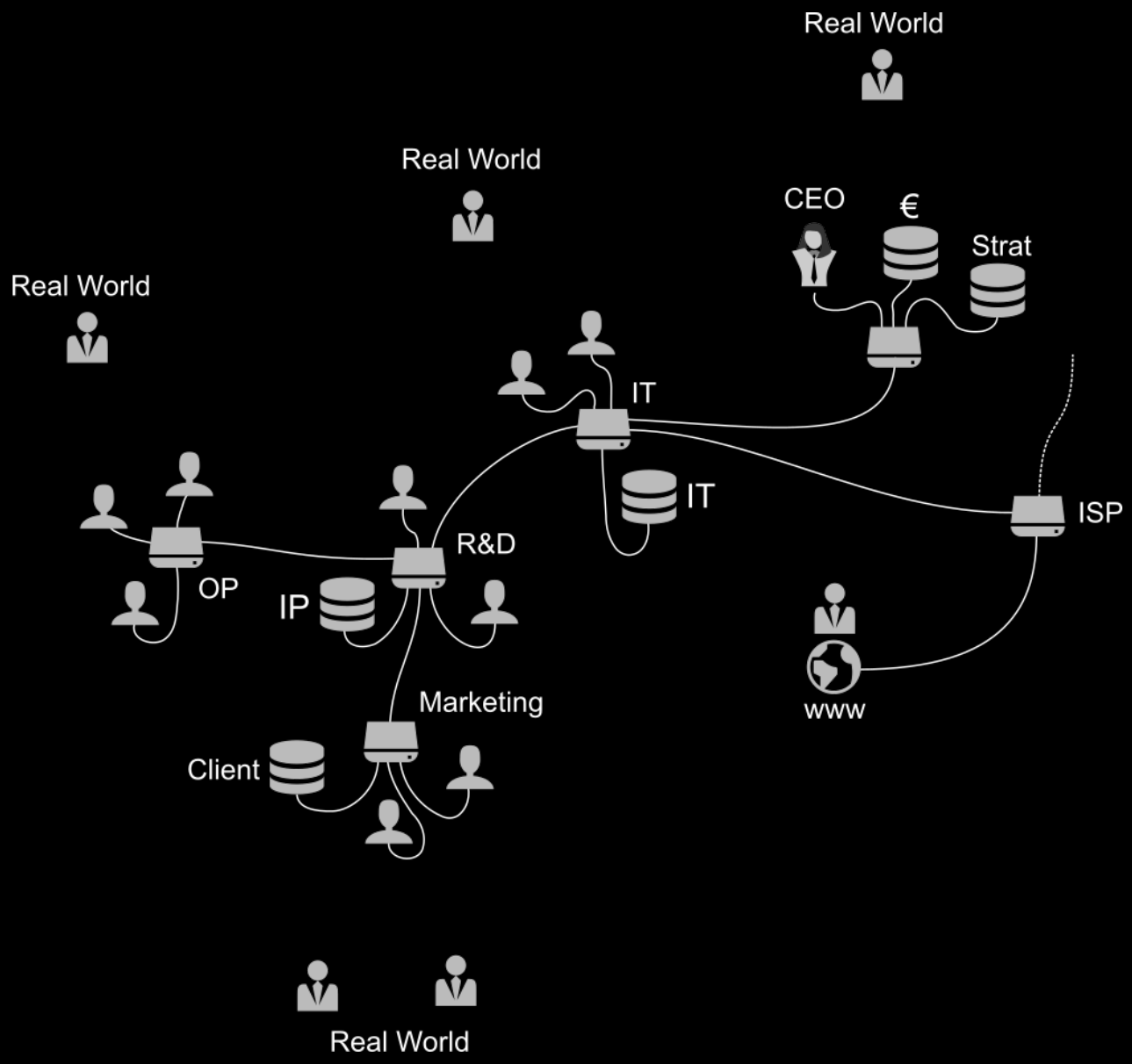
**Key ideas:**

- *encapsulate*
- *multiple* boundaries
- so as to *maximize* the crossing number
  - from untrusted zones to critical zones ("vertical" movement)
  - from one critical zone to another critical zone ("horizontal" movement)
- "best practice"

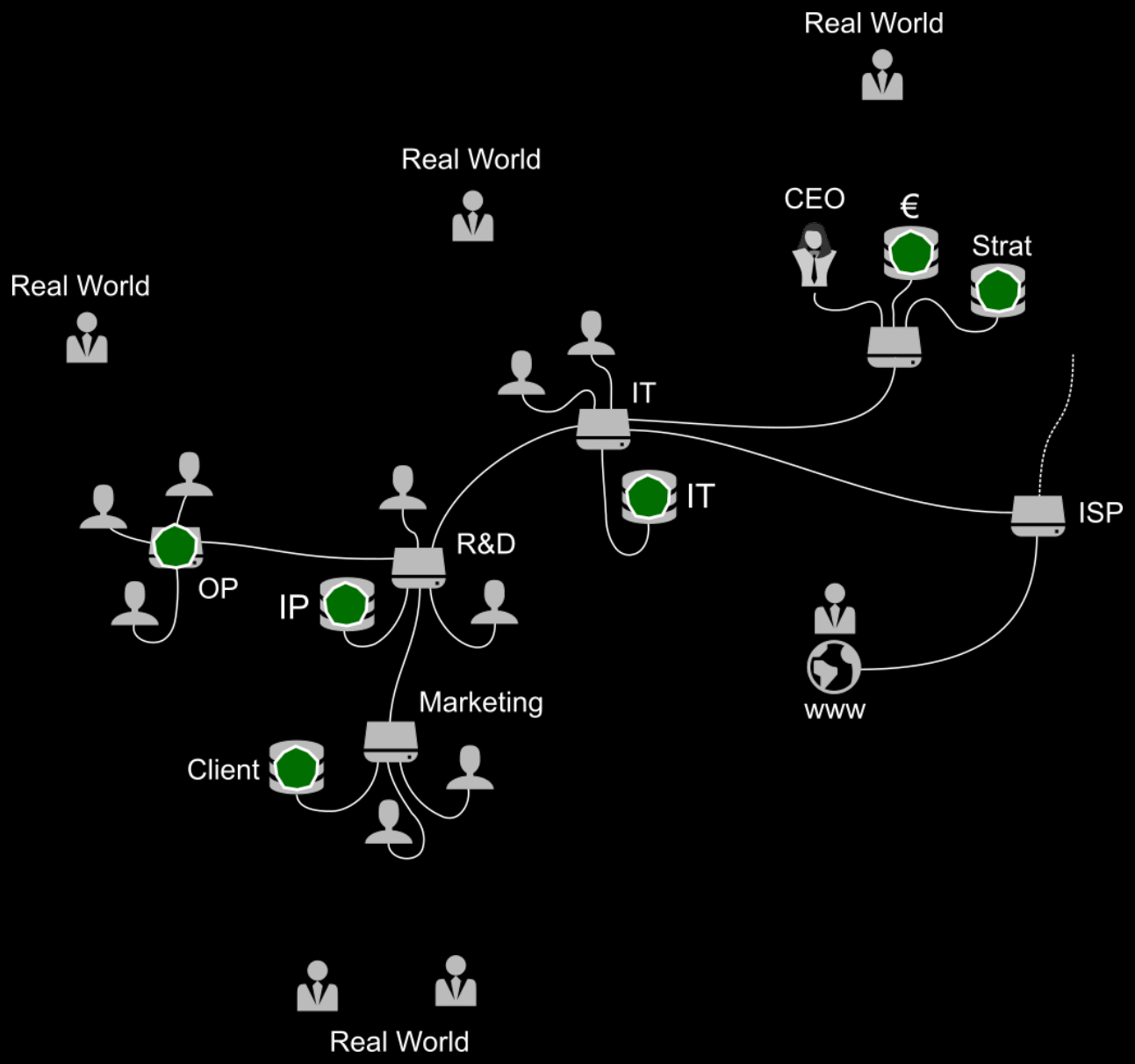
Sounds hard...

**Hint:** follow the abstraction layers from assets all the way up to turtles!

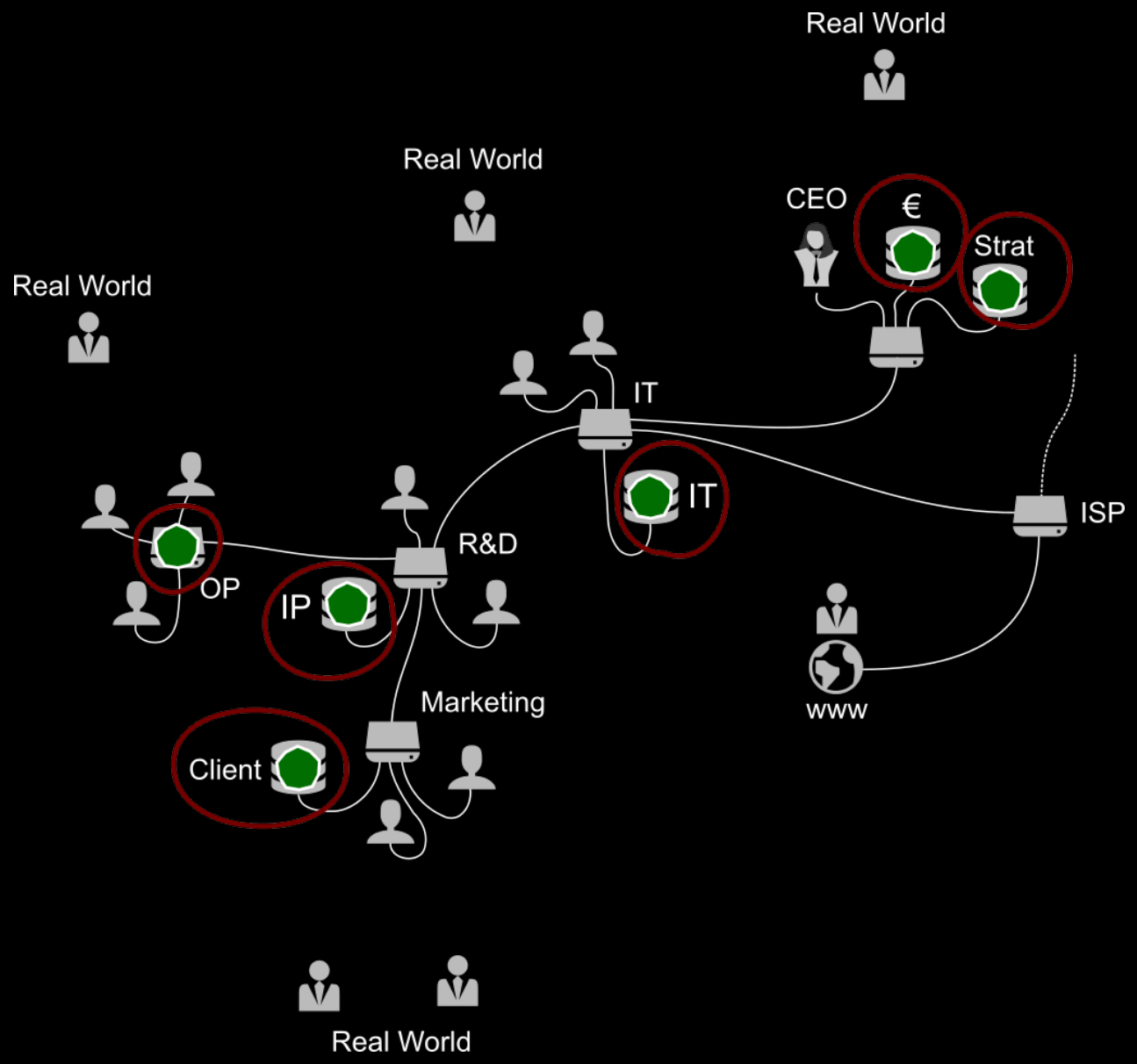
# An example


Real World
Real World
Real World
CEO
€
Strat
IT
IT
ISP
R&D
OP
IP
Marketing
Client
www
Real World

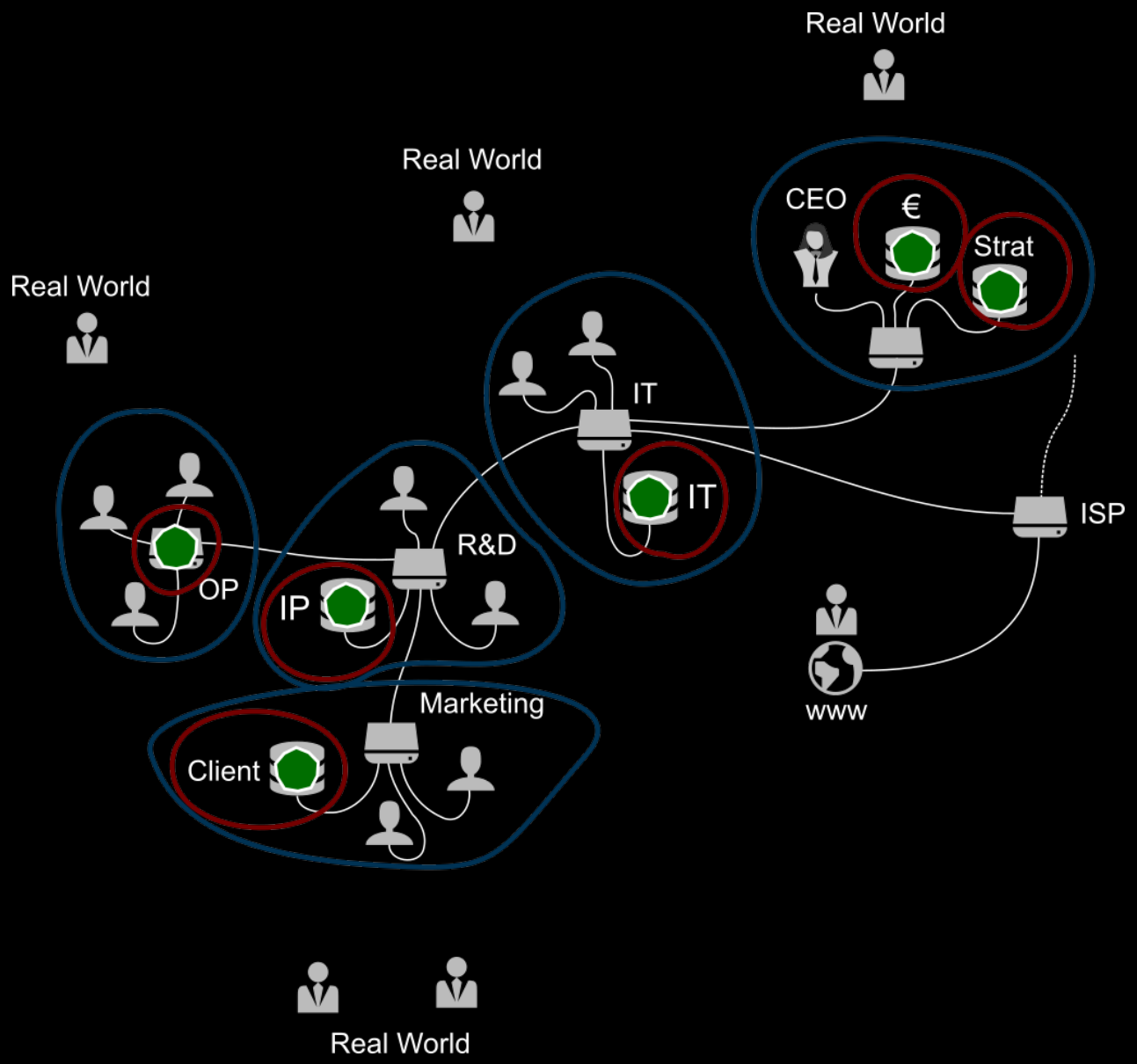
# An example


Real World
Real World
CEO
€
Strat
Real World
IT
IT
ISP
R&D
OP
IP
Marketing
Client
www
Real World

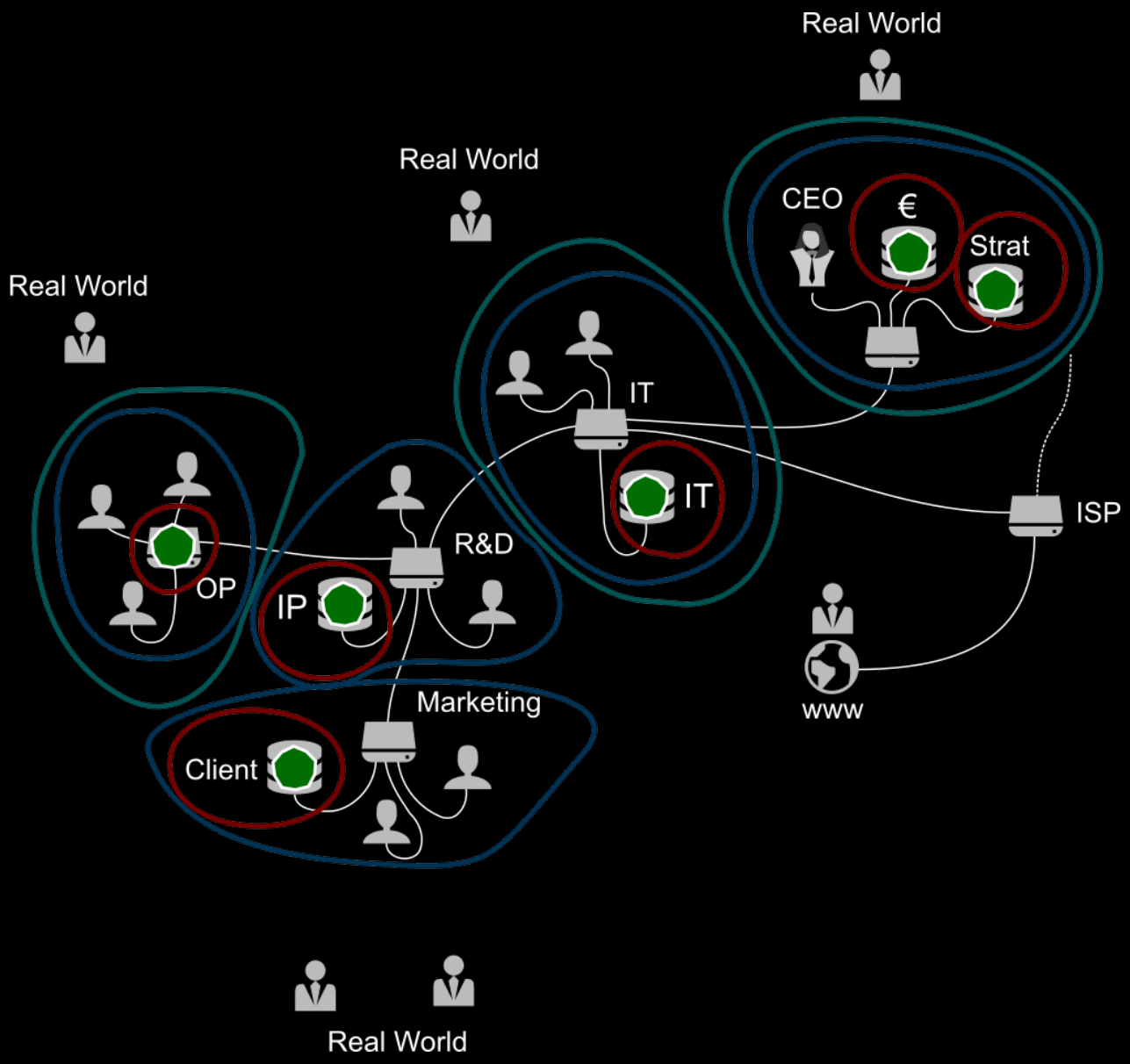
# An example


Real World
Real World
Real World
CEO
€
Strat
IT
IT
ISP
R&D
OP
IP
Marketing
Client
www
Real World

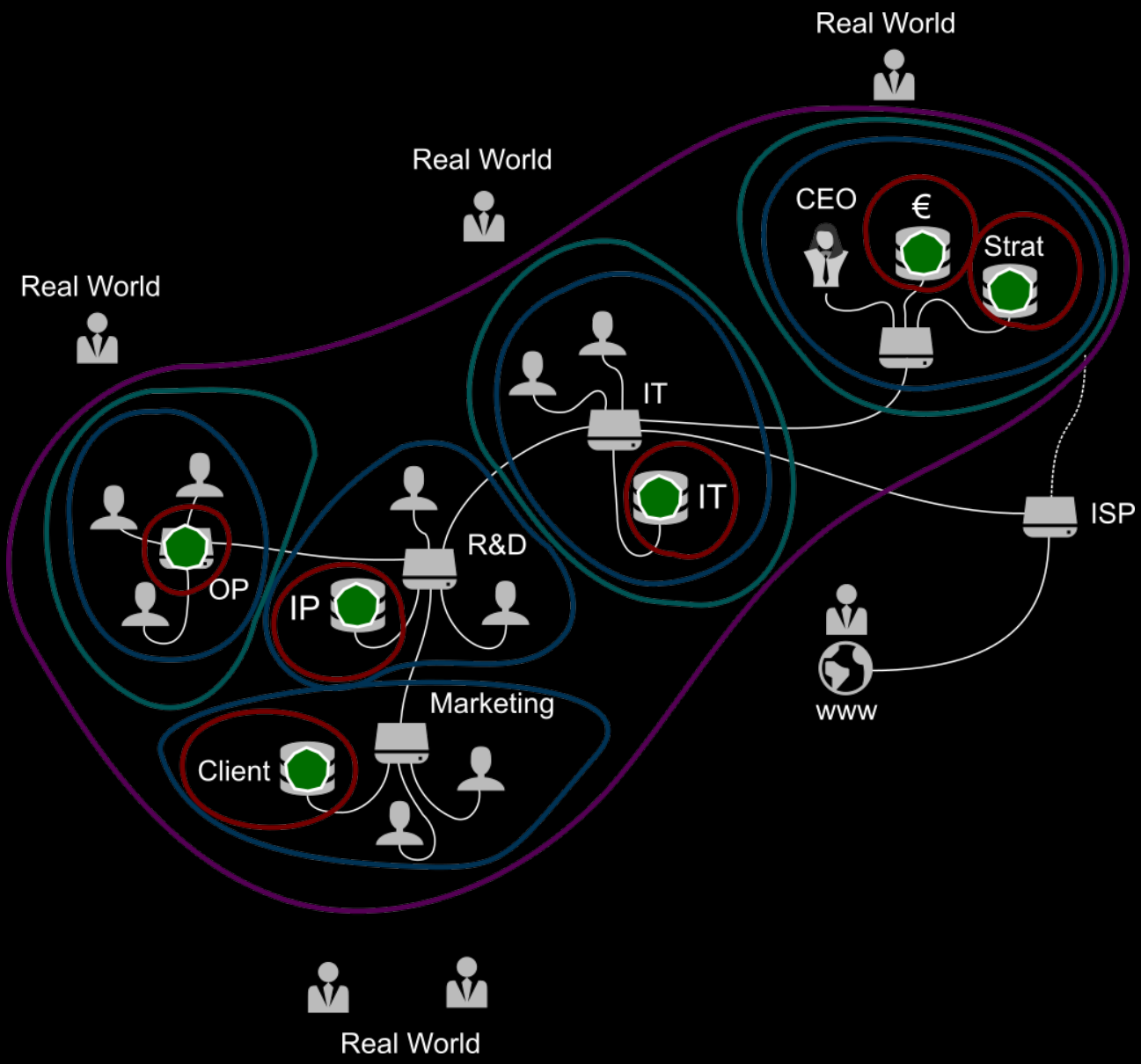
# An example


Real World
Real World
CEO
€
Strat
Real World
IT
IT
ISP
OP
R&D
IP
Marketing
Client
www
Real World

# An example


Real World
Real World
Real World
CEO
€
Strat
IT
IT
ISP
R&D
OP
IP
Marketing
Client
www
Real World

# An example


Real World
Real World
Real World
CEO
€
Strat
IT
IT
ISP
R&D
OP
IP
Marketing
Client
www
Real World

# Defence in depth

## A critical view

# Defence in depth

## A critical view

- Inspired by military operations (kinetic LSG)

# Defence in depth

## A critical view

- Inspired by military operations (kinetic LSG)
- But...the further the enemy, the less risk for her

# Defence in depth

## A critical view

- Inspired by military operations (kinetic LSG)
- But...the further the enemy, the less risk for her
- In particular: no *counter-attack* capability

# Defence in depth

## A critical view

- Inspired by military operations (kinetic LSG)
- But...the further the enemy, the less risk for her
- In particular: no *counter-attack* capability
- High entry-level cost; many directions to cover

# Defence in depth

## A critical view

- Inspired by military operations (kinetic LSG)
- But...the further the enemy, the less risk for her
- In particular: no *counter-attack* capability
- High entry-level cost; many directions to cover

"Attackers provoke the maintenance of a massive, difficult to manage, costly, expert-driven posture...

# Defence in depth

## They DiD it ;)

> ...and still abuse it." (Small, 2012)

# Defence in depth

## They DiD it ;)

...and still abuse it." (Small, 2012)

- Sony, loss $343 750 000 in one month (Peckham 2011)

# Defence in depth

## They DiD it ;)

...and still abuse it." (Small, 2012)

- Sony, loss $343 750 000 in one month (Peckham 2011)
- RSA SecurID, loss $66 000 000 (Tsukuyama 2011)

# Defence in depth

## They DiD it ;)

...and still abuse it." (Small, 2012)

- Sony, loss $343 750 000 in one month (Peckham 2011)
- RSA SecurID, loss $66 000 000 (Tsukuyama 2011)
- Citigroup, financial data of more than 360 000 users (Zetter, 2011)

# Defence in depth

## They DiD it ;)

...and still abuse it." (Small, 2012)

- Sony, loss $343 750 000 in one month (Peckham 2011)
- RSA SecurID, loss $66 000 000 (Tsukuyama 2011)
- Citigroup, financial data of more than 360 000 users (Zetter, 2011)
- US Army "Predator" drone keylogger (The Australian, 2011)

# Defence in depth

## They DiD it ;)

...and still abuse it." (Small, 2012)

- Sony, loss $343 750 000 in one month (Peckham 2011)
- RSA SecurID, loss $66 000 000 (Tsukuyama 2011)
- Citigroup, financial data of more than 360 000 users (Zetter, 2011)
- US Army "Predator" drone keylogger (The Australian, 2011)

**Key issue:**

# Defence in depth

## They DiD it ;)

...and still abuse it." (Small, 2012)

- Sony, loss $343 750 000 in one month (Peckham 2011)
- RSA SecurID, loss $66 000 000 (Tsukuyama 2011)
- Citigroup, financial data of more than 360 000 users (Zetter, 2011)
- US Army "Predator" drone keylogger (The Australian, 2011)

**Key issue:** the "ennemy" is never "killed".

# Defence in depth

**Open Question**:

# Defence in depth

**Open Question**: what could be an efficient, flexible, reasonably unexpensive strategy against *sustained cyber-siege*?

# Homework

Watch *Ocean's Eleven*.

# Homework

Watch *Ocean's Eleven*.

- Identify key assets

# Homework

Watch *Ocean's Eleven*.

- Identify key assets
- List all boundaries

# Homework

Watch *Ocean's Eleven*.

- Identify key assets
- List all boundaries
- Identify how the attackers can get past them

# Homework

Watch *Ocean's Eleven*.

- Identify key assets
- List all boundaries
- Identify how the attackers can get past them

# Challenged boundaries

From trench wars to guerrilla

# Challenged boundaries

## From trench wars to guerrilla

- Network boundaries traditionally embody defensive lines (trenches)

# Challenged boundaries

## From trench wars to guerrilla

- Network boundaries traditionally embody defensive lines (trenches)
- But this is changing:

# Challenged boundaries

## From trench wars to guerrilla

- Network boundaries traditionally embody defensive lines (trenches)
- But this is changing: Content delivery, Privacy concerns, Legal concerns

# Challenged boundaries

## From trench wars to guerrilla

- Network boundaries traditionally embody defensive lines (trenches)
- But this is changing: Content delivery, Privacy concerns, Legal concerns
- Political stakes:

# Challenged boundaries

## From trench wars to guerrilla

- Network boundaries traditionally embody defensive lines (trenches)
- But this is changing: Content delivery, Privacy concerns, Legal concerns
- Political stakes: Wikileaks, Arab Spring, Snowden's files, ...

# Challenged boundaries

## From trench wars to guerrilla

- Network boundaries traditionally embody defensive lines (trenches)
- But this is changing: Content delivery, Privacy concerns, Legal concerns
- Political stakes: Wikileaks, Arab Spring, Snowden's files, ...

As a result, distributed, pseudonymous or anonymous networks are on the rise, challenging boundaries *in the name of security*.

# The anonymous Internet

**Daily Tor users per 100,000 Internet users**

- > 200
- 100 - 200
- 50 - 100
- 25 - 50
- 10 - 25
- 5 - 10
- < 5
- no information

Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk

Oxford Internet Institute
University of Oxford