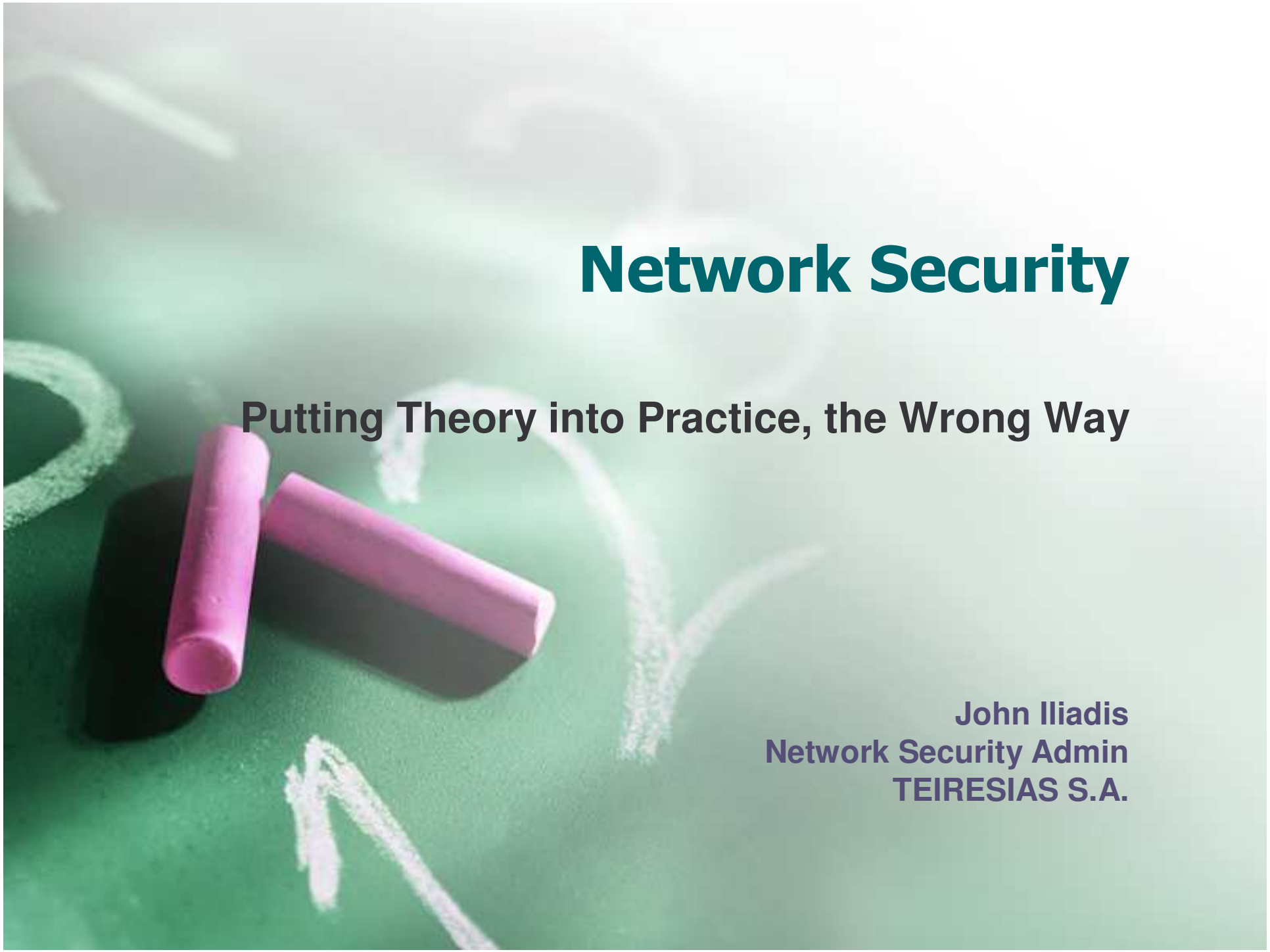


Network Security

Putting Theory into Practice, the Wrong Way

John Iliadis
Network Security Admin
TEIRESIAS S.A.

Why do implementations fail to address the issues?

- *Understand the theory*

  …sometimes even Engineers have to go back and (re)comprehend the theory, to get things done ☺

- *Understand the problem*

  Actually listen to the problem before providing a solution.

- *Provide an integrated solution*

  A security mechanism per se is not a solution; it is merely a tool (more about that later)

A simple example: failing to provide an integrated solution

Problem

I want to protect confidentiality of data exchanged between network A and network B

Network A

Network Service Provider

Network B

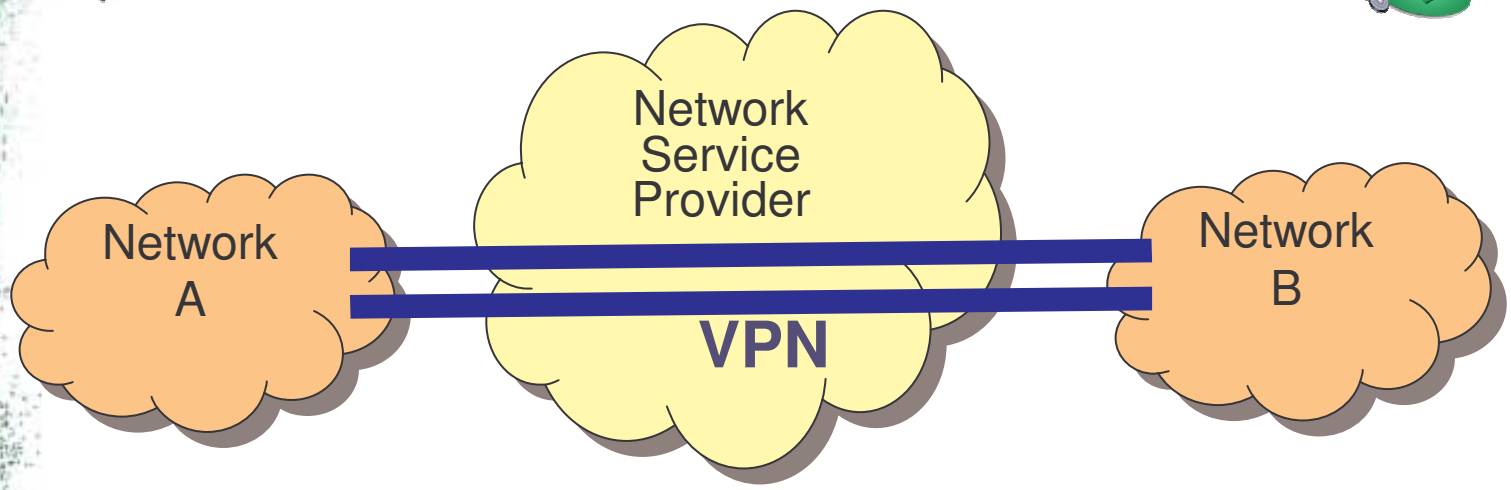
A simple example: failing to provide an integrated solution

Problem

I want to protect confidentiality of data exchanged between network A and network B

Solution

OK, we 'll implement an IPSec VPN, using preshared keys



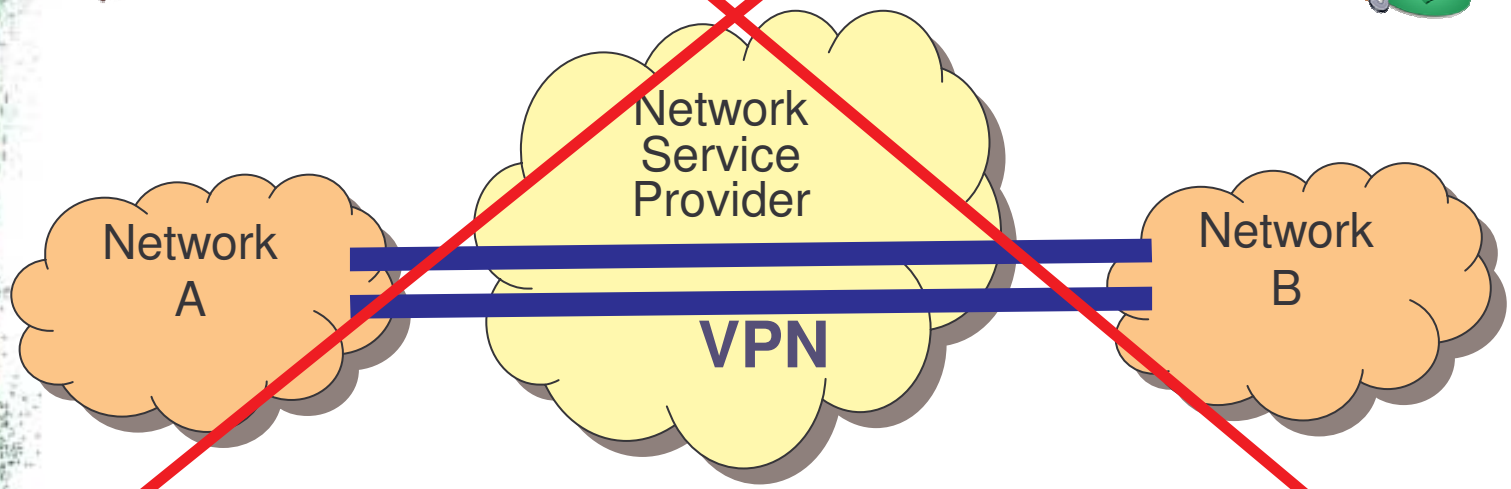
A simple example: failing to provide an integrated solution

Problem

I want to protect confidentiality of data exchanged between network A and network B

Solution

OK, we 'll implement an IPSec VPN using preshared keys



Providing an integrated solution

Problem

I want to protect confidentiality of data exchanged between network A and network B

Providing an integrated solution

Problem

I want to protect confidentiality of data exchanged between network A and network B

Solution

I trade your problem with another: that of managing symmetric encryption keys

Providing an integrated solution

Problem

I want to protect confidentiality of data exchanged between network A and network B

Solution

I trade your problem with another: that of managing symmetric encryption keys

Problem

How does it sound if I send a sealed envelope with the new symmetric key every week by courier to the network admin of network B?

Providing an integrated solution

Problem

I want to protect confidentiality of data exchanged between network A and network B

Solution

I trade your problem with another: that of managing symmetric encryption keys

Problem

How does it sound if I send a sealed envelope with the new symmetric key every week by courier to the network admin of network B?

Solution

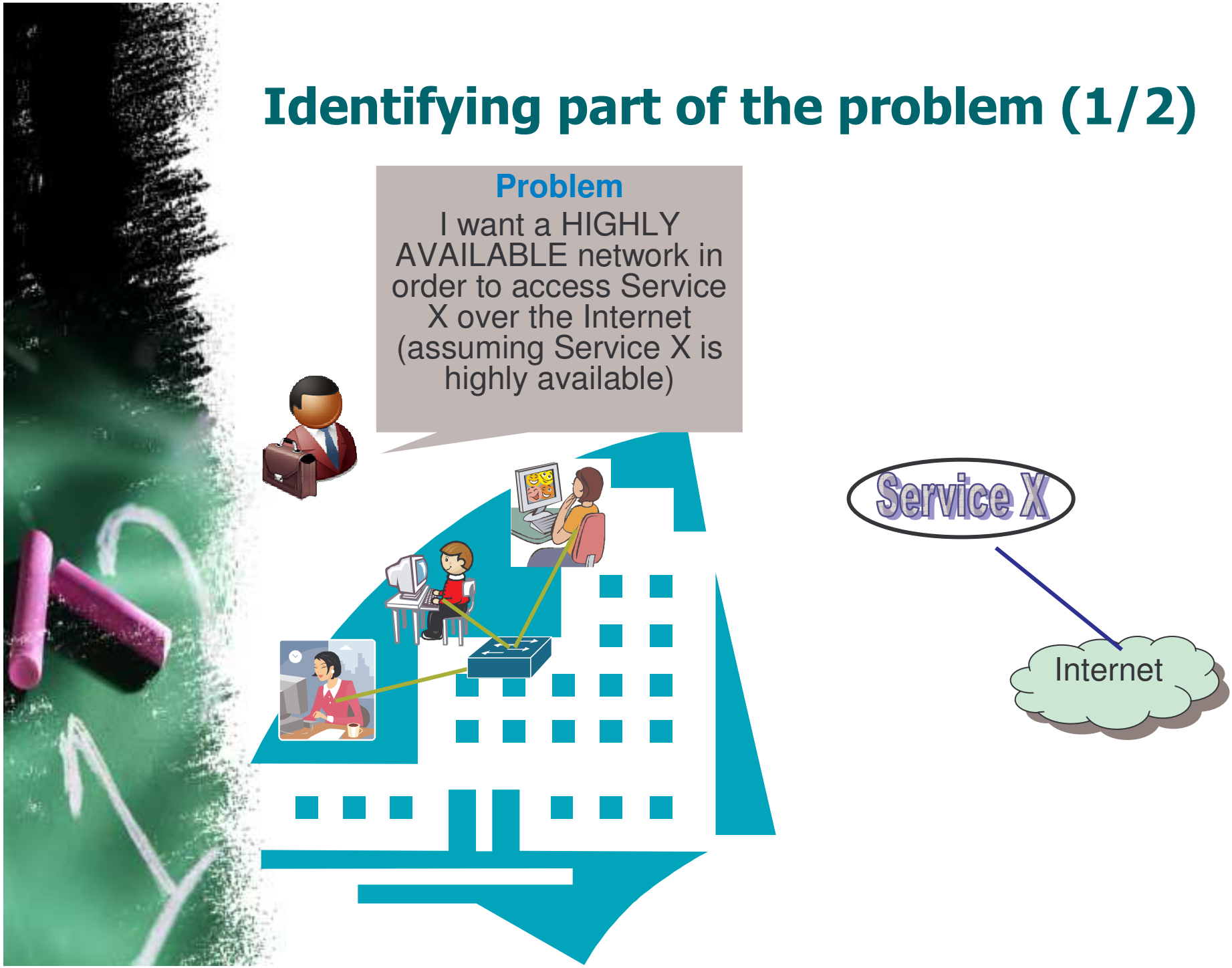
OK! I 'll implement the IPSec VPN and you are done!

Cryptographic mechanisms…

…exchanging one problem for another,

easier problem to solve

Identifying part of the problem (1/2)



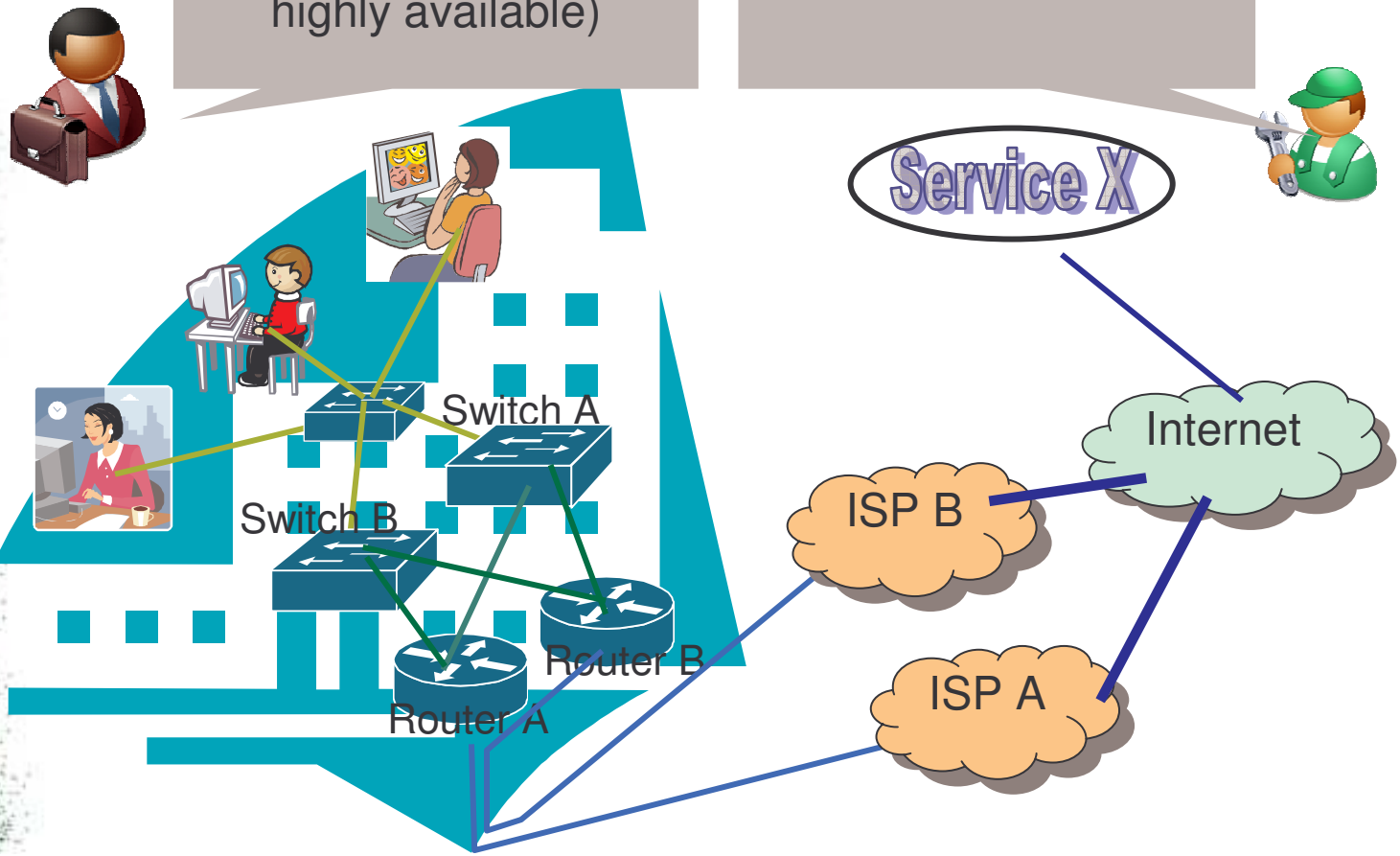
Identifying part of the problem (1/2)

Problem

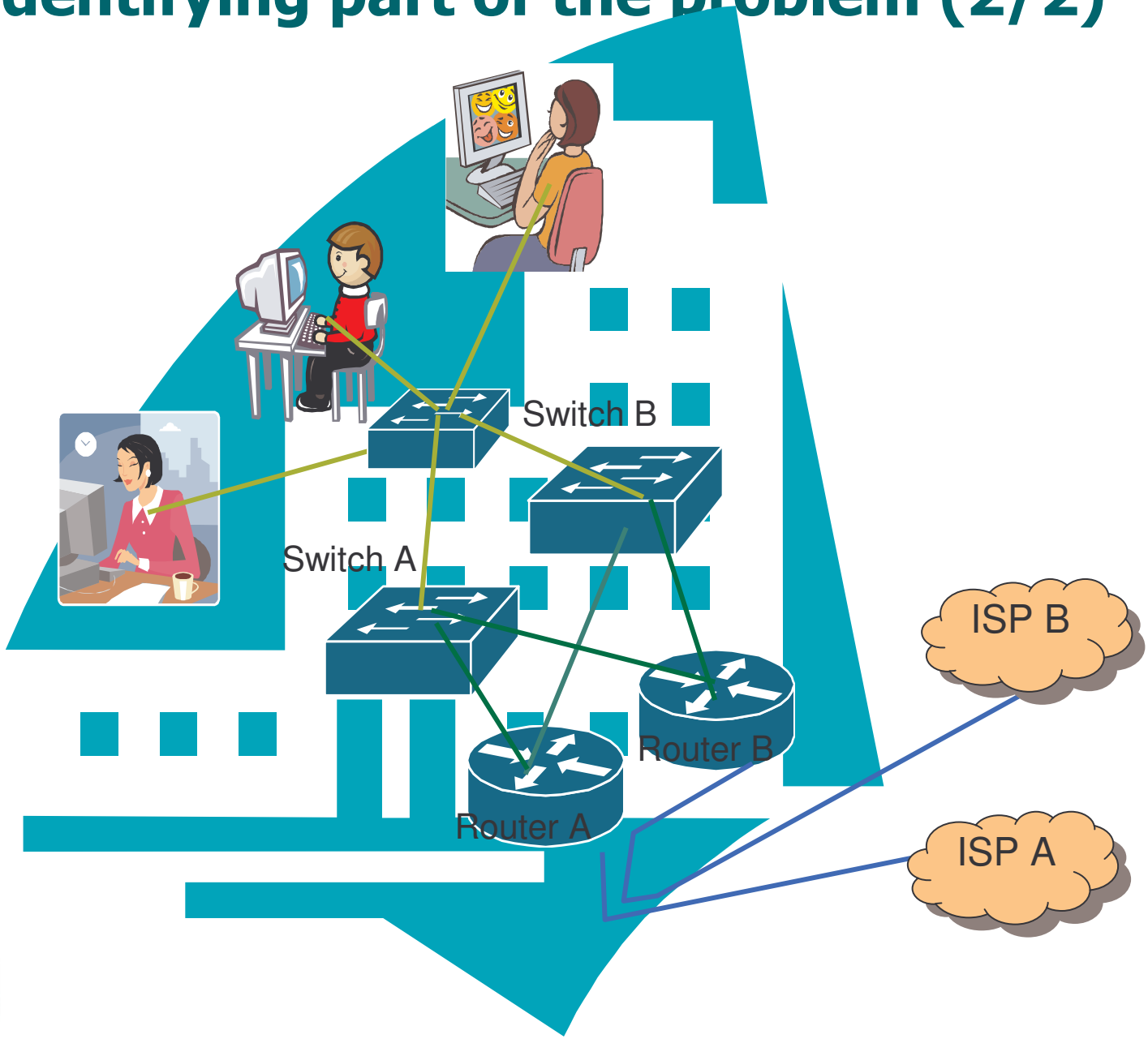
I want a HIGHLY AVAILABLE network in order to access Service X over the Internet (assuming Service X is highly available)

Solution

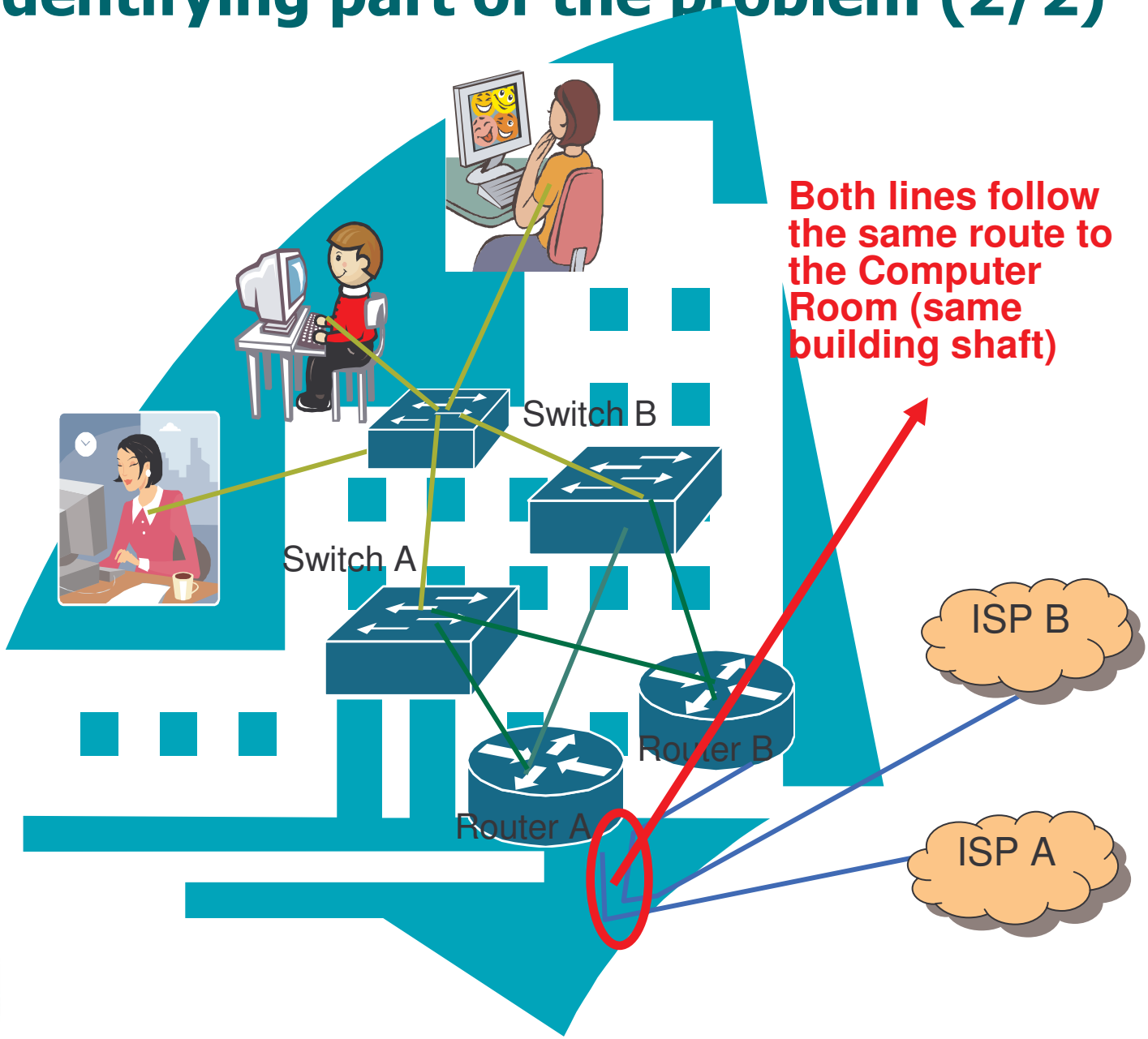
…just another day at the office…



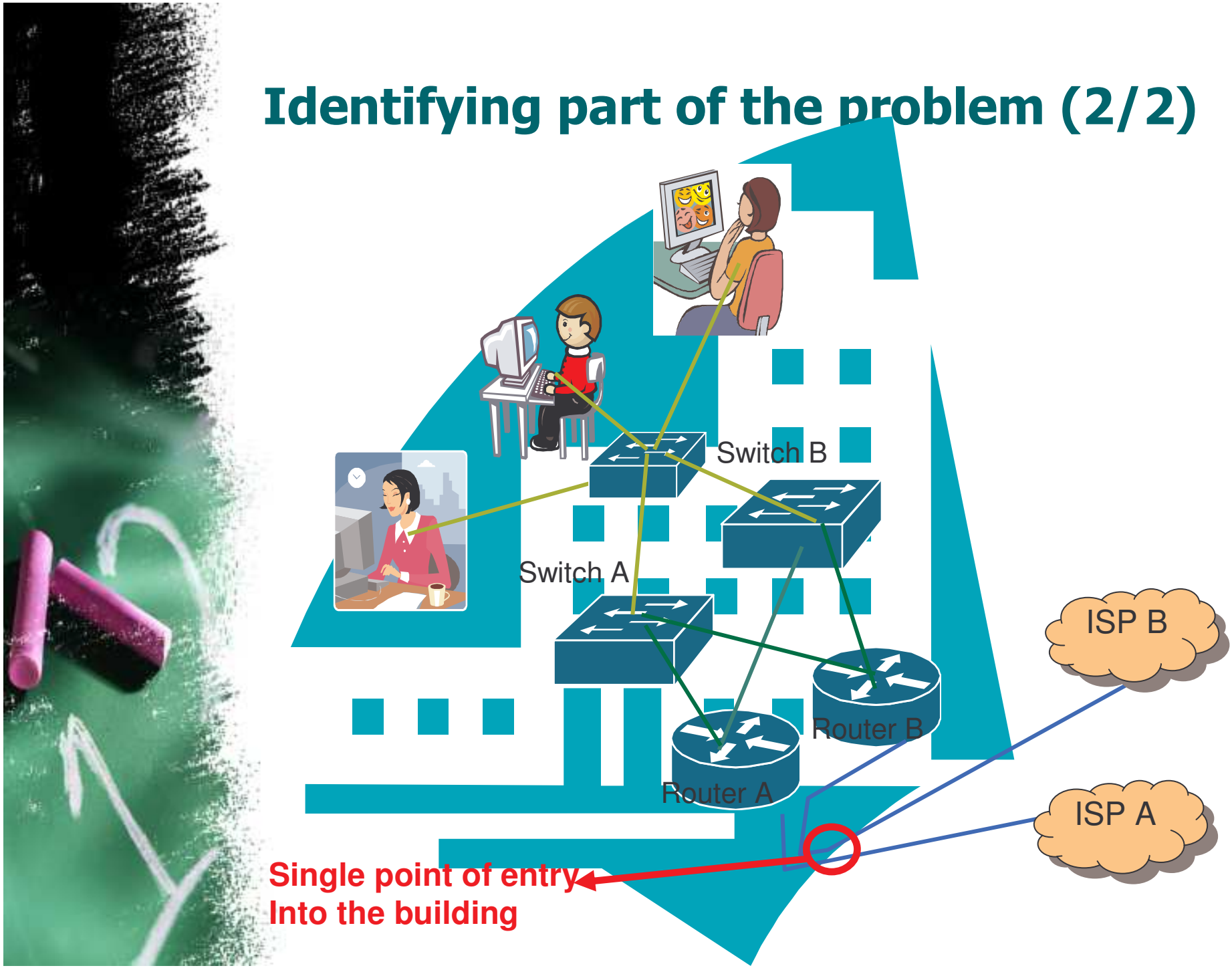
Identifying part of the problem (2/2)



Identifying part of the problem (2/2)

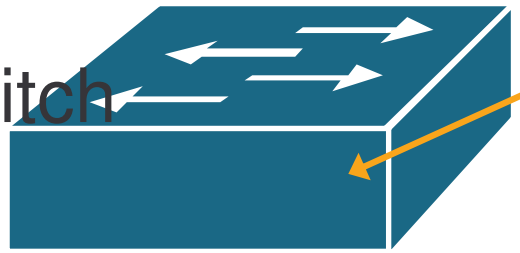


Identifying part of the problem (2/2)



Getting carried away by trends…

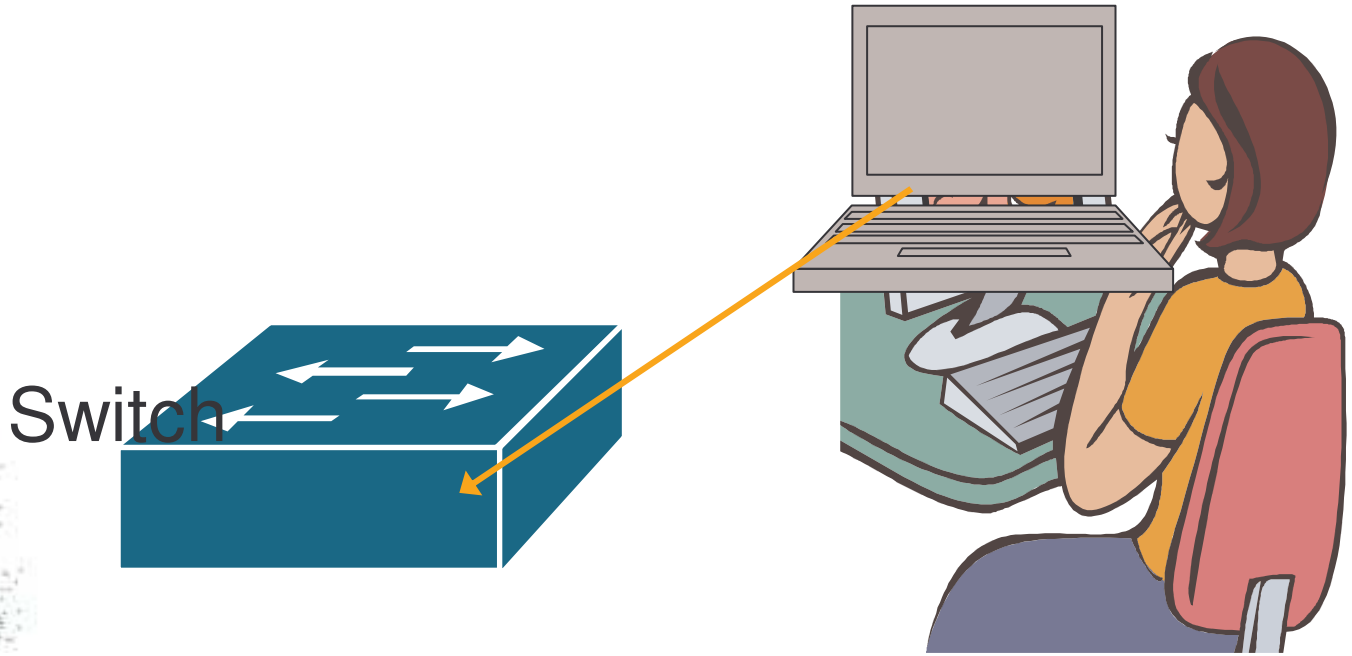
- User workstations should be equipped with centrally managed software:
  - *Antivirus*
  - *Antispyware*
  - *Firewall*
  - *Intrusion detection*
  - *Log consolidation*
  - *SW/HW Inventory*
  - *etc…*



Switch

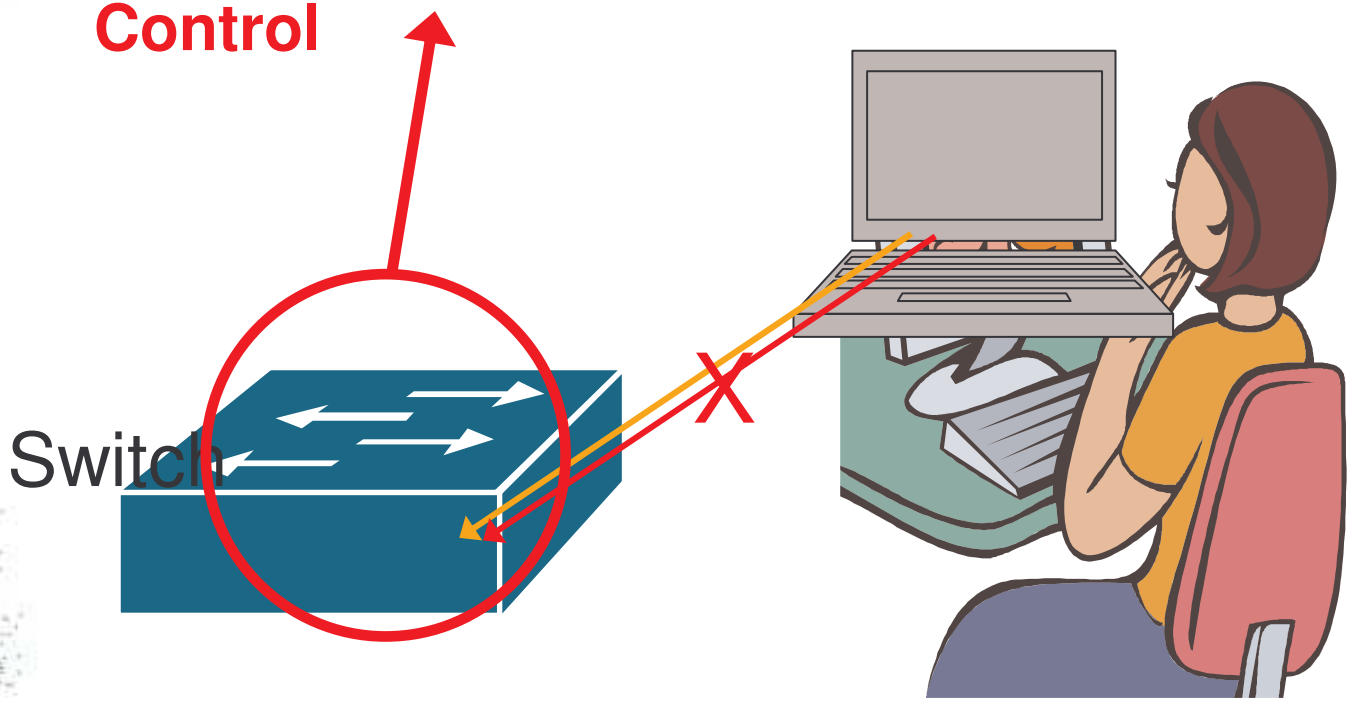
…and forgetting about the basics

- No Layer 2 authentication
- The user brings his own, personal laptop
  - to work without being “disrupted” by all this annoying software
  - to try some things he couldn’t do on the network due to this annoying software



...and forgetting about the basics

- Enforce 802.1x authentication
- Implement Port Security
- Trendy add-on: Network Admission Control



What is (not) an IDS

1. A turnkey security solution
2. Automatic identification/notification of attacks
3. THE new security panacea (UTMs)

The need for Network/Host IDS

Being given a chance to:

1. *identify potential attacks in traffic*
2. *review related host logs*
3. *decide if this is indeed a security issue*
4. *take action*

Network/Host IDS: Conclusions

- IDSs give us *a chance* to identify attacks and react

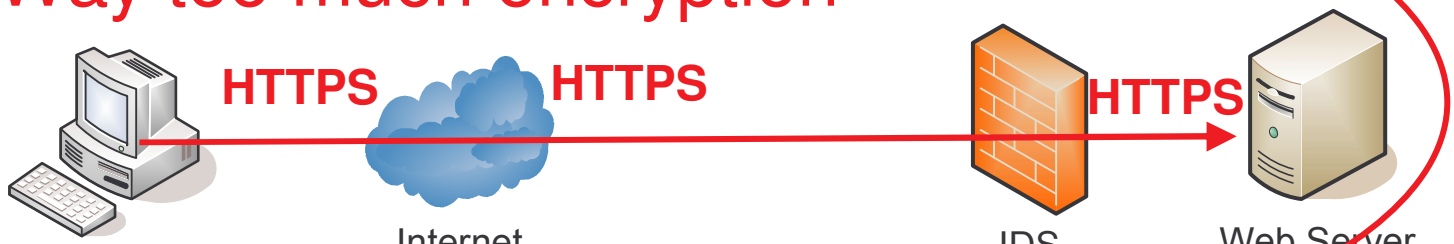
- Not much of a use if
  - *network traffic is not captured*
  - *there is no experienced security personnel*
  - *security personnel is not reviewing IDS logs*

not much of a *turnkey* solution…

Encryption overdose

No Encryption

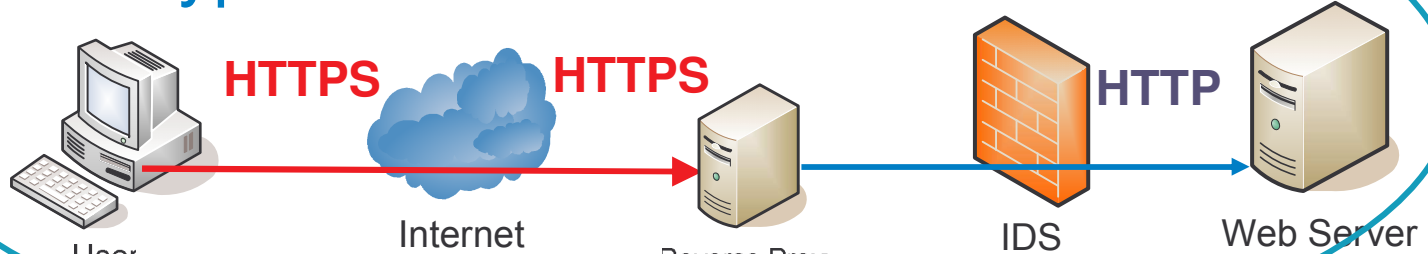
Way too much encryption



Encryption overdose

No Encryption

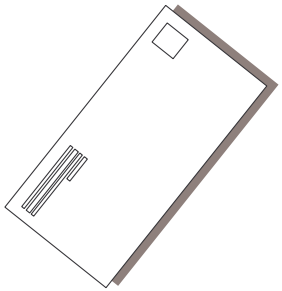
Encryption/IDS Balance



PKI Boom

Problem

Alice needs to send a HIGHLY confidential mail to Bob once a month



PKI Boom

Problem

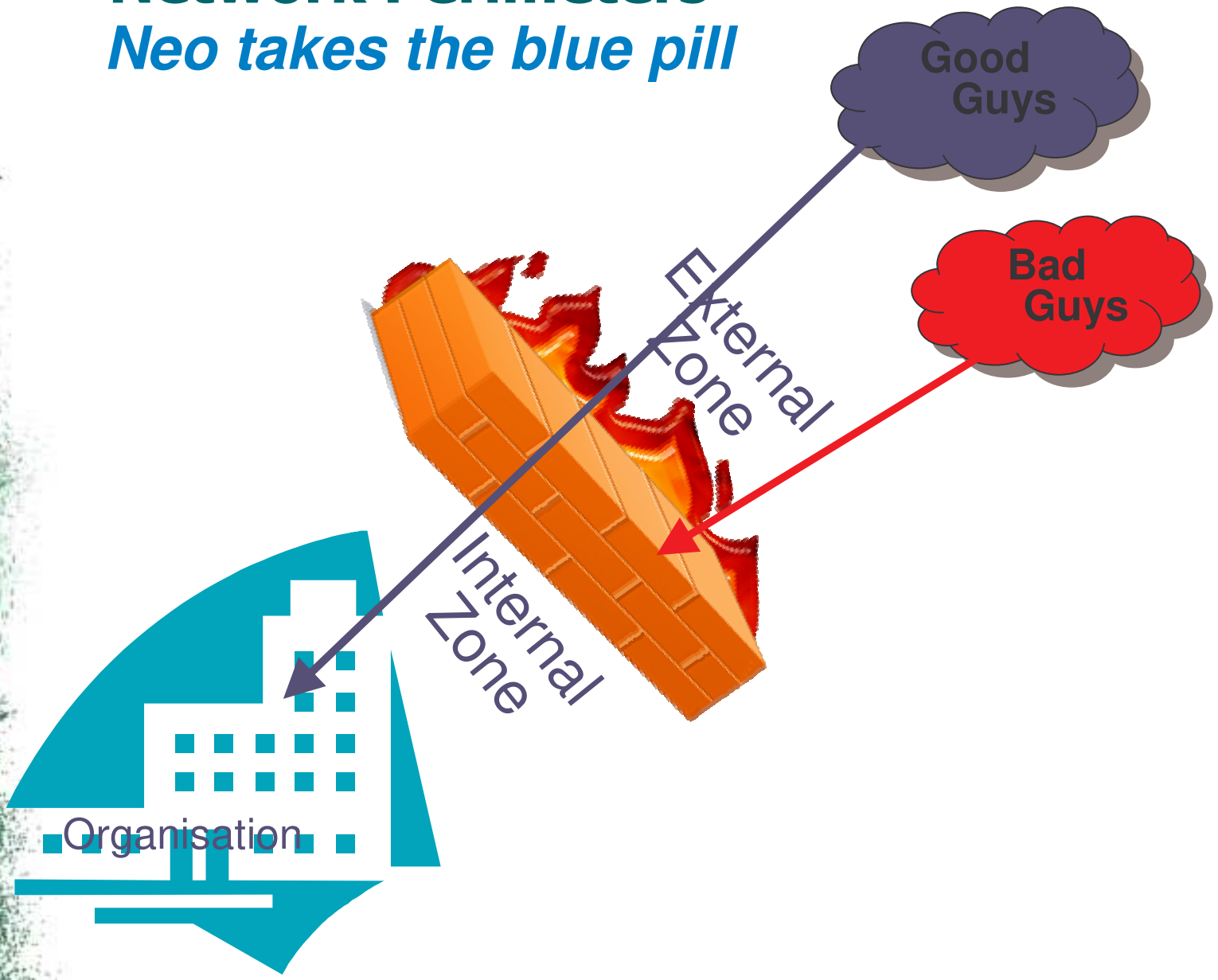
Alice needs to send a HIGHLY confidential mail to Bob once a month

Solution

PKI !

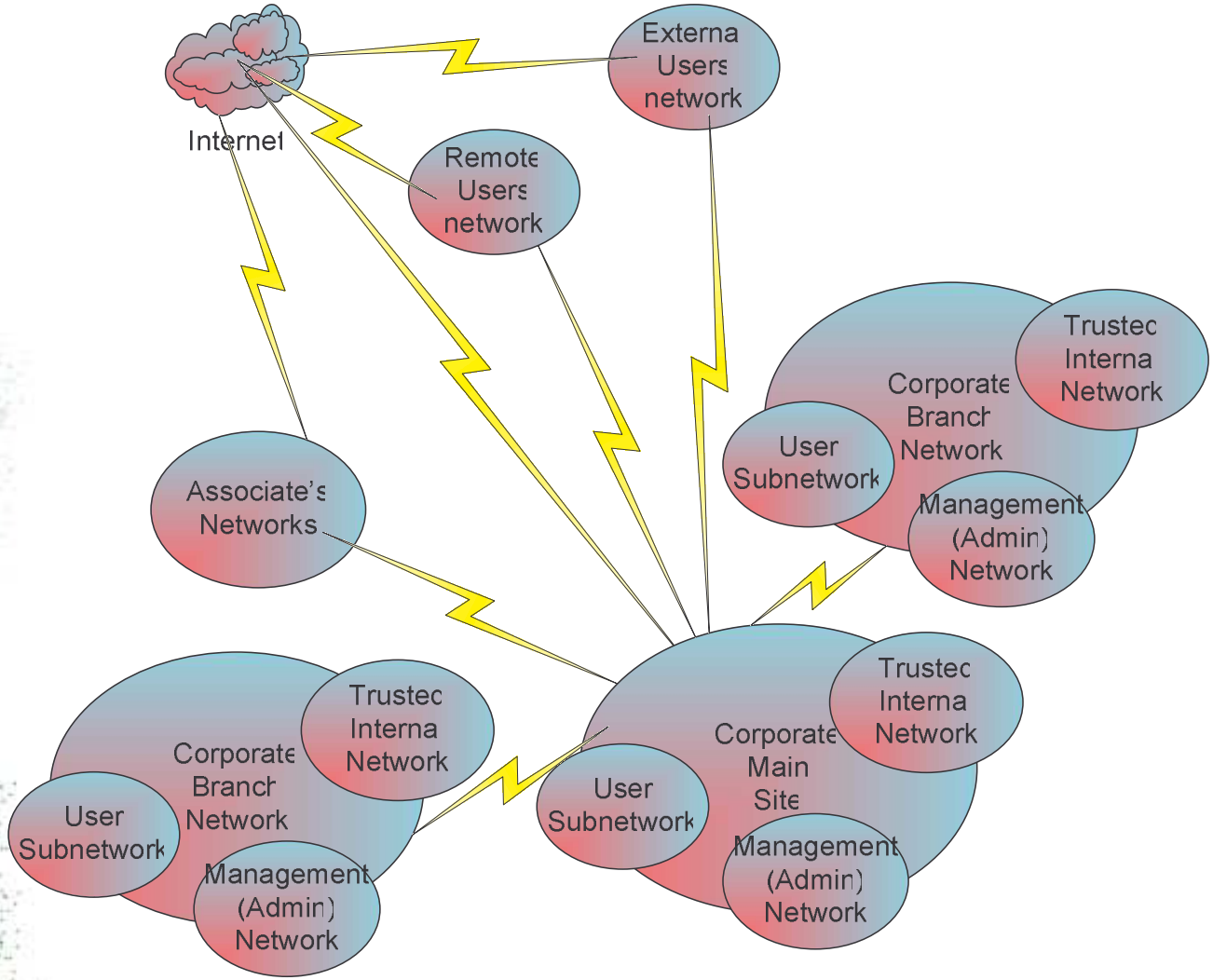
Network Perimeters

Neo takes the blue pill



Network Perimeters

Neo takes the red pill



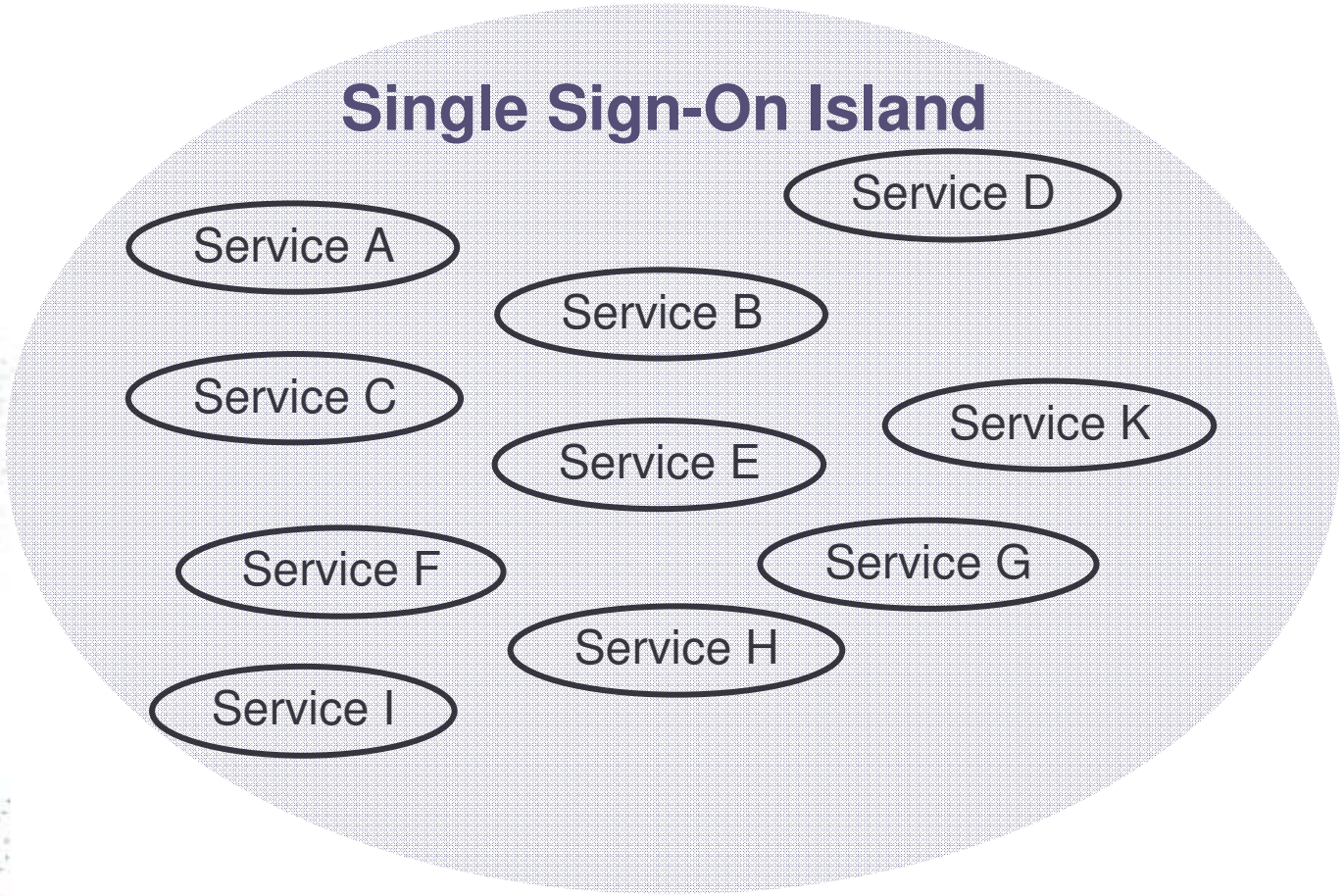
Quality of Service

All services & users are born equal.

Some are more equal than others

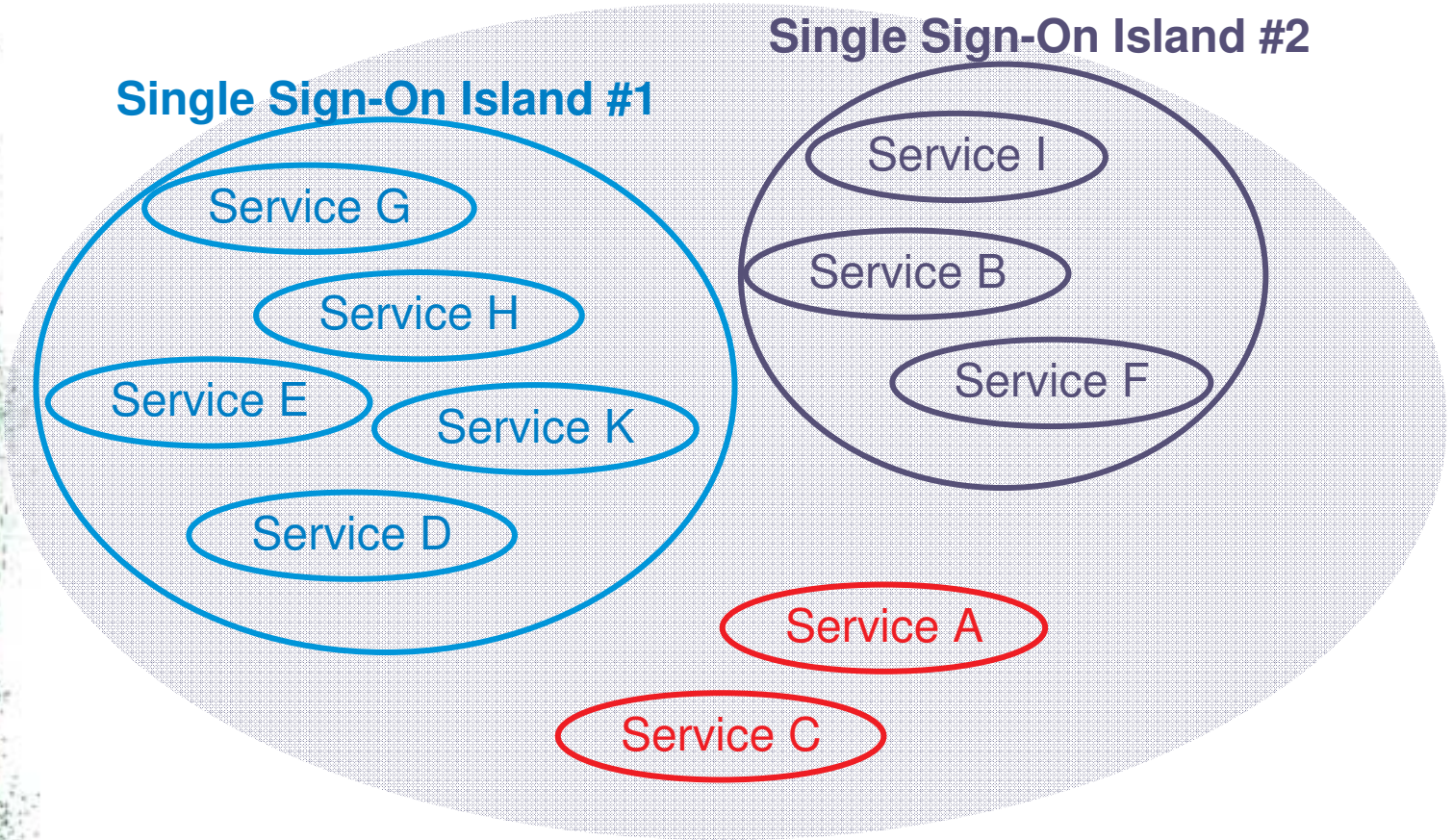
- *Expected user experience*
- *Prerequisite (e.g. VoIP, NMS)*
- *QoS as a security mechanism (DoS, packet filtering alternative, …)*

Single Sign-On: The Trendy (a.k.a. Wrong) Way



Single Sign-On: The Right Way

(Grouping by… impact factor, risk etc)



Threat: unauthorised access

- Impact factor: 1/5
- Impact factor: 3/5
- Impact factor: 5/5

…a side note about management (1/3)

- **Effect:** Managers taking the wrong (security-wise) strategic decisions
- **(Probable) Cause:** YOU did not educate them regarding security matters

…a side note about management (2/3)

- **Effect:** Users not being security-conscious enough
- **(Probable) Cause:** YOU did not educate them in security matters and the HIGHER MANAGEMENT did not provide incentives and show commitment

…a side note about management (3/3)

- **Effect:** Stakeholders perceive Security as an obstacle to business
- **(Probable) Cause:** Security is not a goal in itself. YOU must treat it as a business enabler, before anyone else can

Q&A