Network Security
Network design

Marcus Bendtsen, Andrei Gurtov
Institutionen för Datavetenskap (IDA)
Avdelningen för Databas- och Informationsteknik (ADIT)

LINKÖPING UNIVERSITY

Risk

Expanding the classical definition of risk:

$$\text{Risk} = \text{Threat} \times \text{Exposure} \times \text{Vulnerability} \times \text{Consequence}$$

- **Threat:** Probability of an attack (an attack could happen)
- **Exposure:** Probability a vulnerability is exposed to an attack
- **Vulnerability:** Probability of an exploitable vulnerability
- **Consequence:** Cost of a successful attack

Network security is about reducing risk, and is motivated by the fact that networked systems typically have greater exposure and greater threats than does non-networked systems.

Threats

- Networking changes the attacker's risk analysis.
  - Attackers also do risk analysis – Is the potential gain of the attack worth the cost and risk of being caught?
- **More** networked systems = more profitable targets.
  - The benefit of an attack increases.
- Networking makes the attacker **less visible**.
  - Reduced risk of capture.
- Networking **increases pool** of potential attackers.
  - Geographic location is of less importance.
  - Increases threat, e.g. as the pool increases the chance that a motivated attacker exists increases.
  - From hackers to government agencies

Exposure

- Non-networked systems becoming more networked.
  - Systems become accessible to more attackers
  - Check Shodan search tool
- Convergence on IP technology (i.e. more systems use the same protocols etc.).
  - Attackers have better understanding of the systems.
- Mobility and wireless technology increases:
  - Easier to access devices than before.
  - No need to have physical access to network, a good antenna and an amplifier may suffice.

Vulnerabilities

- Constant flow of vulnerabilities in TLS, RPC, etc protocols require patching hosts
  - Networking allows systems to grow more complex.
    - Complexity breeds vulnerabilities.
  - Non-networked systems becoming networked.
    - No security focus in these systems. Should have been analysed before networked, but not always the case.
    - Can also become networked by accident.
  - Security awareness *is* increasing.
    - Modern software is more secure than old software.
    - Standard components are being used (good, but also increases probability of wide spread vulnerabilities).

Consequence

- Networking becomes critical infrastructure, e.g. SmartGrid, transport control, water systems, payments
  - In 1996 a website being down for a few days was not much of a problem. Today, many businesses see their website as one of the top business critical resources.
  - Taking a website down has side consequences, **search engine rankings may drop**. Furthermore, putting ***bad*** **content** on a website may also negatively effect rankings.

- A networked system can also be taken over by an attacker and used to launch attacks on other networks. This can lead to legal repercussions.

Networks and Risk

- ***Keeping an attackers risk analysis in mind:*** Network security addresses threats by increasing the risk to the attacker.
  - Intrusion detection
- Network security is traditionally all about **reducing exposure**.
- Network security does not remove host vulnerabilities.
  - Instead we should look at secure programming techniques, good administration and practices.
  - Need to design secure communication protocols
- Network security can reduce consequences.
  - Self-healing, make data exfiltration difficult

Network security

- Network security is mostly about reducing exposure, and in doing so increasing risk for the attacker.
- **Network security goes hand-in-hand with system security:** even if your network security is great, you need to make sure that accounting, auditing, monitoring, access control, and all other parts of a system is working too.
- To understand network security it is important that you are *security aware*. This is what we will focus on in these lectures.
- ***Security awareness* is a mind-set, including an attitude of questioning parts that may have been overlooked.**

Designing for security

- Information Security - Network security

Designing for security

Designing for security == Ultimate prevention

- If security is not part of the design, then you will spend a lot of time patching systems that are fundamentally insecure.
- Prerequisites
  - Risk and security awareness
  - Accepted security policy – The goals of the design, widely accepted by all participants, including users.
    - If the users are not on-board then we will have major issues during implementation.

Furthermore, all systems should have been designed for security, not only the network.

Design for security

Three main points:

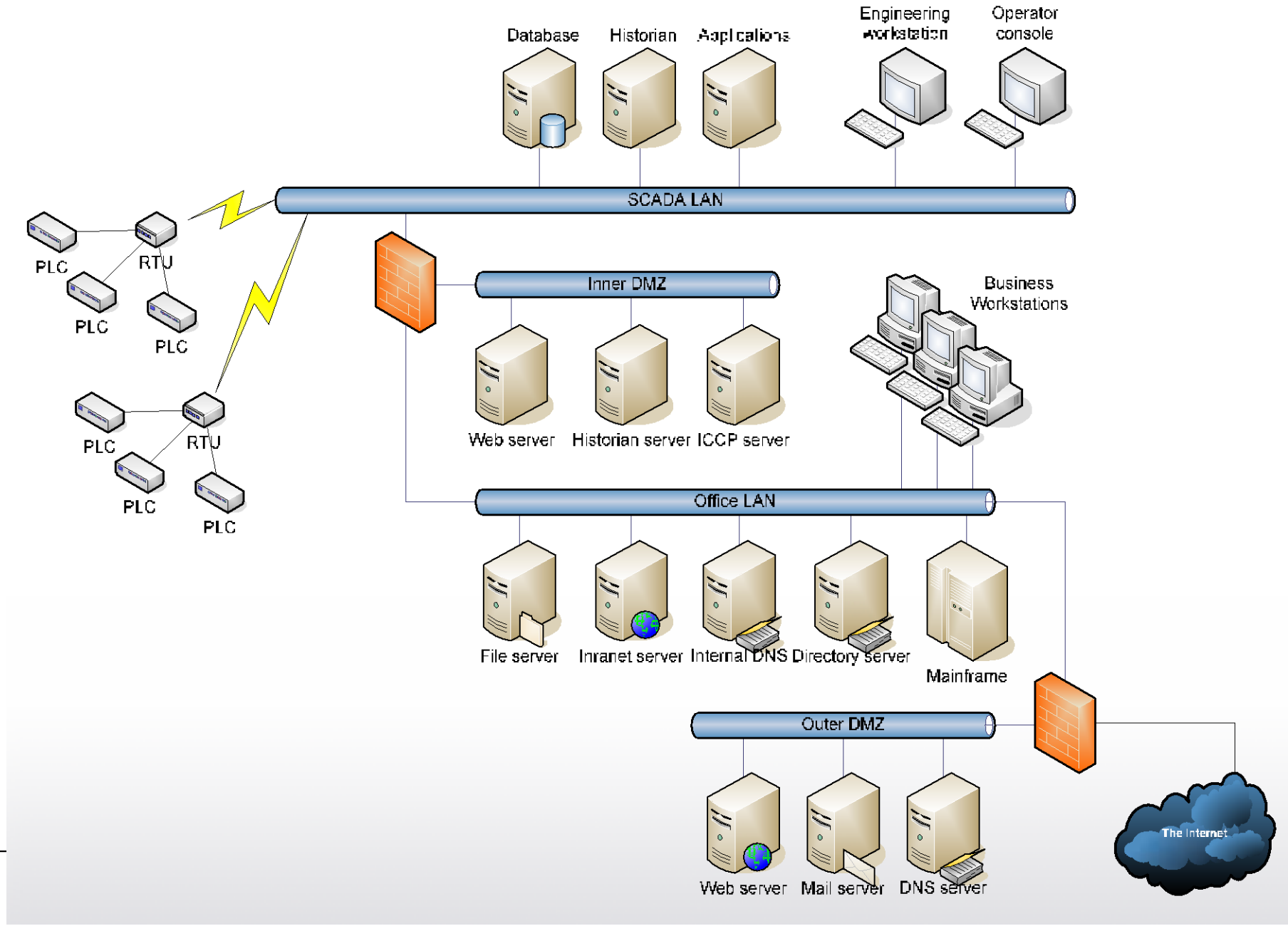
1. Network segmentation
2. Perimeter defence
3. Network containment

Designing secure networks

- **Network segmentation**
  - Multi-layered security architecture by dividing the network into different parts, with barriers between them.
    - Different zones for different functions
    - Contains threats to specific resources
    - With no segmentation then all users and all systems are connected, and everyone can access everything.

Designing secure networks

- **Perimeter defence**
  - Protects the borders between network segments. Protects against attackers from the outside.
  - Typically a ***firewall*** and a ***network intrusion detection*** system.
- **Network containment**
  - Limiting network to a known extent, *doubly hard with wireless networks*.


Database
Historian
Applications
Engineering workstation
Operator console
SCADA LAN
PLC
RTU
PLC
PLC
PLC
RTU
PLC
PLC
PLC
Inner DMZ
Web server
Historian server
ICCP server
Business Workstations
Office LAN
File server
Intranet server
Internal DNS
Directory server
Mainframe
Outer DMZ
Web server
Mail server
DNS server
The Internet

Separation mechanisms

Two approaches to separation:

- **Air-gaps**
  - Physically disconnected network segments
  - No integration between networks

- **Firewalls**
  - Essentially a router with rules for which traffic is allowed
  - Devices that can block disallowed traffic
  - Tuneable integration between networks

(If you take the lab, you will get cosy with these…)

Separation mechanisms

- **A word on *routers:***
  - Devices that forward traffic between networks
  - **Not** for segmenting networks for security
  - Routers and switches are built to connect, not to segment

  - But sometimes it is hard to distinguish, as the routers we use at home and in small offices do everything (routing, firewall, NAT, etc).

Air-gaps

- No physical connection
- No traffic can flow
- **Complete security!**

- **Maybe not…**
  - Temporary connections
  - Wireless devices
  - Insider threats
  - Misconfiguration
  - Unintentional bridges
  - Laptop computers
  - Physical access

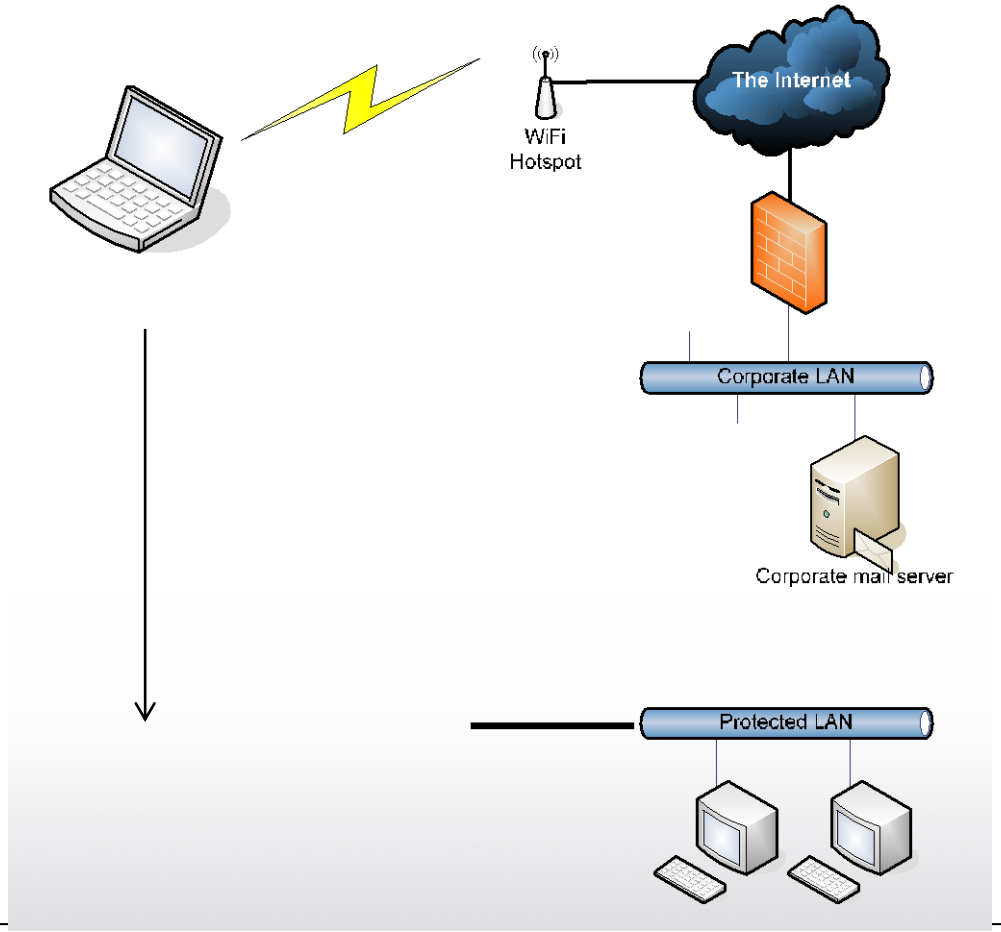
- The ideal separator is the air-gap. But in reality they do not work.
- The main reason is that we often need to transport data to and from the network, and when data can be transported then attacks can be staged.
- It may not be easy, but it can be done.
- If we transfer data frequently, then chances are that we have found a ***convenient way*** of doing so, making the attack easier.

Does the air-gap exist?

- Air-gaps do not always exist:
  - Temporary connections (for software updates and patches)
  - Misconfiguration of switches where “virtual” air-gaps are created by partitioning or using VLANs.

- Why?
  - Honest mistakes.
  - Poor understood policy.
  - Design does not support business needs.

Laptops defeat the air-gap



A technician brings his or her laptop to an internet café, connects to their Wi-Fi, gets infected by a worm.

Same laptop is then connected to the air-gapped corporate network.

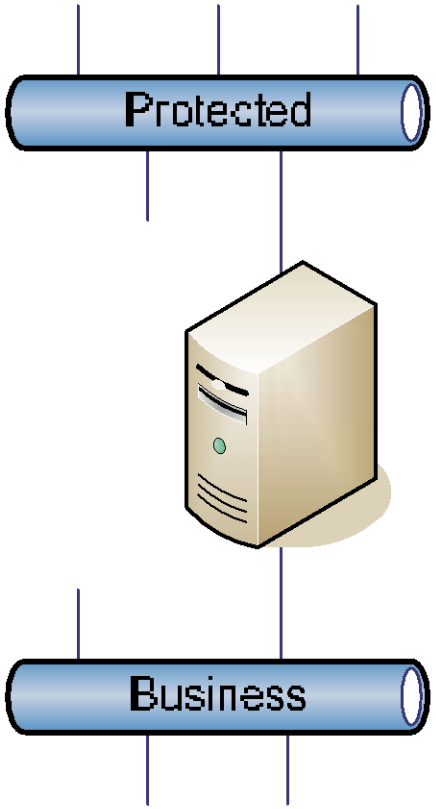
The laptop creates a time lapse network connection.

Dual-homed systems

If a system sits on more than one network, then access from one network can be gained from the other.

E.g. a protected network uses the same DNS server as a network that is accessible from the Internet. Then there is a connection from the Internet to the protected network.

Never forget that network equipment are themselves systems: a switch that manages two separate networks forms a connection (of sort) between these networks.



Database server
Directory server
Logging server
Intrusion detection system
Software deployment server
Authentication server
Storage server

Security aware – Even if the spec says it can not happen, do not trust. If there is a way, it will be found.

Good network management defeats air-gaps

- Network management usually like having the entire network at their fingertips, and often do so by using virtual LANs.
  - These VLANs are logically disconnected, but run on the same wires and hardware.
  - Network managers also like a **management LAN** from which they can reach all networked devices.
  - The management LAN is usually a VLAN that can be accessed from only a few places.
  - Nevertheless, this management LAN connects all other networks, and if any of the "air-gapped" networks use equipment from the management LAN then they are, in a way, connected to all other networks.

Air-gaps conclusion

- Yes, air-gaps offer excellent separation.
- But, they are often impractical:
  - Need very strict physical security around the entire network.
  - Can not transfer anything, including on a USB stick, between networks.
  - People tend to defeat air-gaps.

- **Conclusion:** Do not bother.
  - Assume that you do not have fully functioning air-gaps.
  - Design the rest of the network with that in mind.

Firewalls

A firewall is a computer that can act as a router, and can filter traffic passing through it based on a set of rules.

- It restricts traffic flows from the inside to the outside.
- It restricts traffic flows from the outside to the inside.

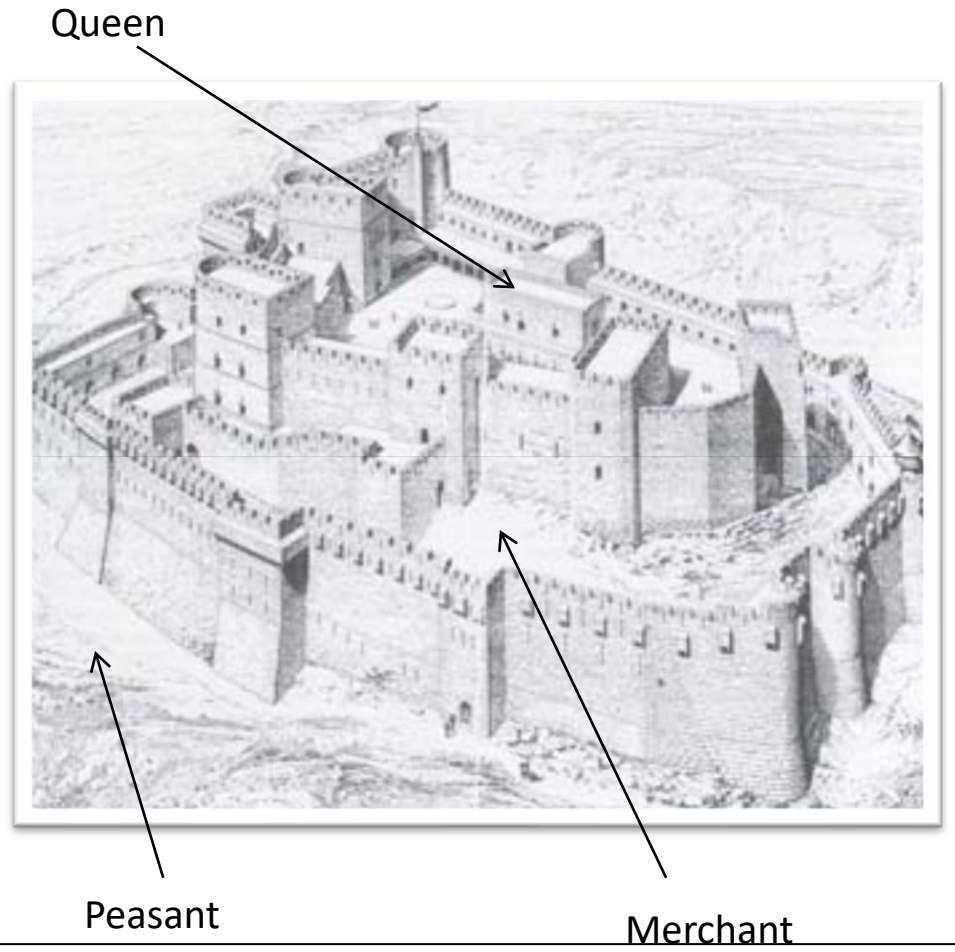
- **Used to:**
  - Enforce network security policy
  - Enforce network segmentation (partitioning)
- **Abused as:**
  - An excuse to not secure the inside

A policy is created based on the need of the business, e.g. “the inner LAN should not be accessible from the Internet”. The policy is then enforced with “mechanisms”, such as firewalls.

Really, really, bad idea….

Multi-level defence

- The way we think about networks today has a lot in common with the way we used to build castles.
- Multi-layering protects our resources with increasing importance as we go towards the centre.

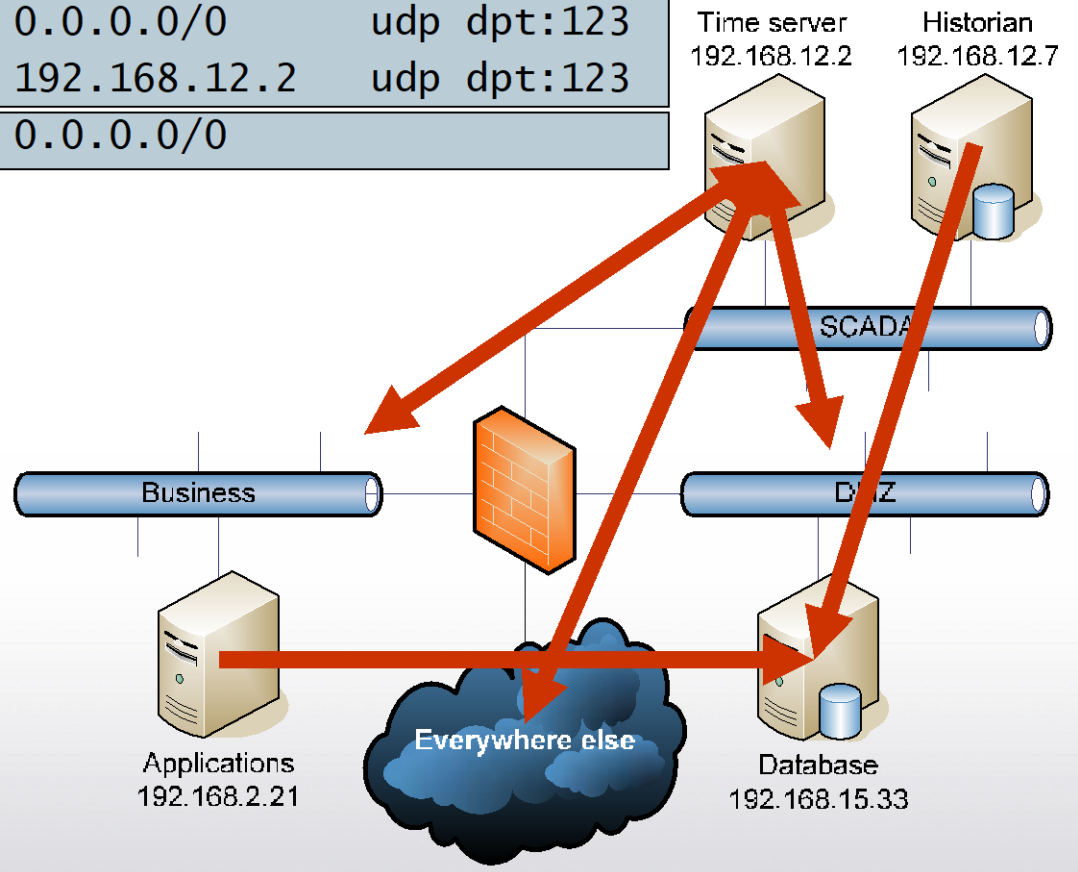


Firewall rules

Firewalls consists of rules that say what to do with traffic. A rule usually consists of a set of criteria and an action to take if the criteria match.

- Traffic criteria
  - Source and destination address, source and destination port, protocol, physical interface, rate…
  - Typically not application level information. (Although they exist)
- Action to take
  - Allow traffic to pass
  - Drop traffic without notification
  - Reject traffic with notification to source
- Policy
  - What to do with traffic that does not match any criteria?

target	prot	source	destination	criteria
ACCEPT	tcp	0.0.0.0/0	0.0.0.0/0	state ESTABLISHED
ACCEPT	tcp	192.168.12.7	192.168.15.33	tcp dpt:3306
ACCEPT	tcp	192.168.2.21	192.168.15.33	tcp dpt:3306
ACCEPT	udp	192.168.12.2	0.0.0.0/0	udp dpt:123
ACCEPT	udp	0.0.0.0/0	192.168.12.2	udp dpt:123
DROP	all	0.0.0.0/0	0.0.0.0/0	



Network Address Translation

- Rewrite addresses on packets going through the firewall/NAT box.
  - Address on the inside is re-written to an address on the outside
  - Allow hosts with private addresses to access outside networks
  - Prevents direct connection to NATed systems

- Abused as a security mechanism
  - The theory is that if the attacker can not connect to you then the attacker can not attack you
  - No protection against stuff requested from the inside (e.g. malware)

NAT penetration – Simple example

- You have a firewall, it does NAT for hosts behind it. An attacker cannot connect to the hosts. Furthermore, you only allow hosts to use HTTP to specific sites. You do not even allow DNS, that is done via a corporate proxy server. So if a host is compromised it is of no use, they can't connect to it, and it can't connect to them, right?
- Wrong – I can set up a DNS server for a domain, e.g. evil.example.com. An infected host on the inside could then be told to query for this domain, and I will return a TXT field with commands, e.g. "delete content". The corporate proxy server allows for data being sent to hosts from the outside.

Security aware – Be sceptical of all kind of traffic flows….

Some firewall concerns

- Only as good as its configuration
  - Studies have shown that many firewalls are misconfigured
  - Typical IT testing is not that thorough

- Firewall weaknesses
  - Firewalls give little or no protection from attackers on the inside
  - Firewall failure can lead to network failure
  - Firewalls may have vulnerabilities that attackers may exploit

Firewall, final concerns

- Firewalls are great when used right
  - They can implement security policy and allow for perimeter security.
  - They are a single component in a multi-faceted approach to security
  - It can help protect resources, but not on its own
- Some use firewalls as an excuse for bad (or no) security elsewhere
- Firewalls are not an easy solution, they may look easy, but they are not
  - They need to be monitored and managed, and they **place part of your overall security on a single device**

Trust relationships: bridging the gaps

trust *n*, **1.** reliance on the integrity, strength, ability, surety, etc., of a person or thing; confidence. **2.** confident expectation of something; hope

- When we segment networks we still need to allow some communication between them. Within a segment, systems needs to rely on each other or share sensitive information.
- Trust relationships bridge gaps in our systems
  - Trusted systems are given additional access and rights
  - Trusted systems may provide data that we rely on
- Trust relationships are potential vulnerabilities
  - What if trusted systems misbehaves?
  - A trusts B, but B misbehaves?

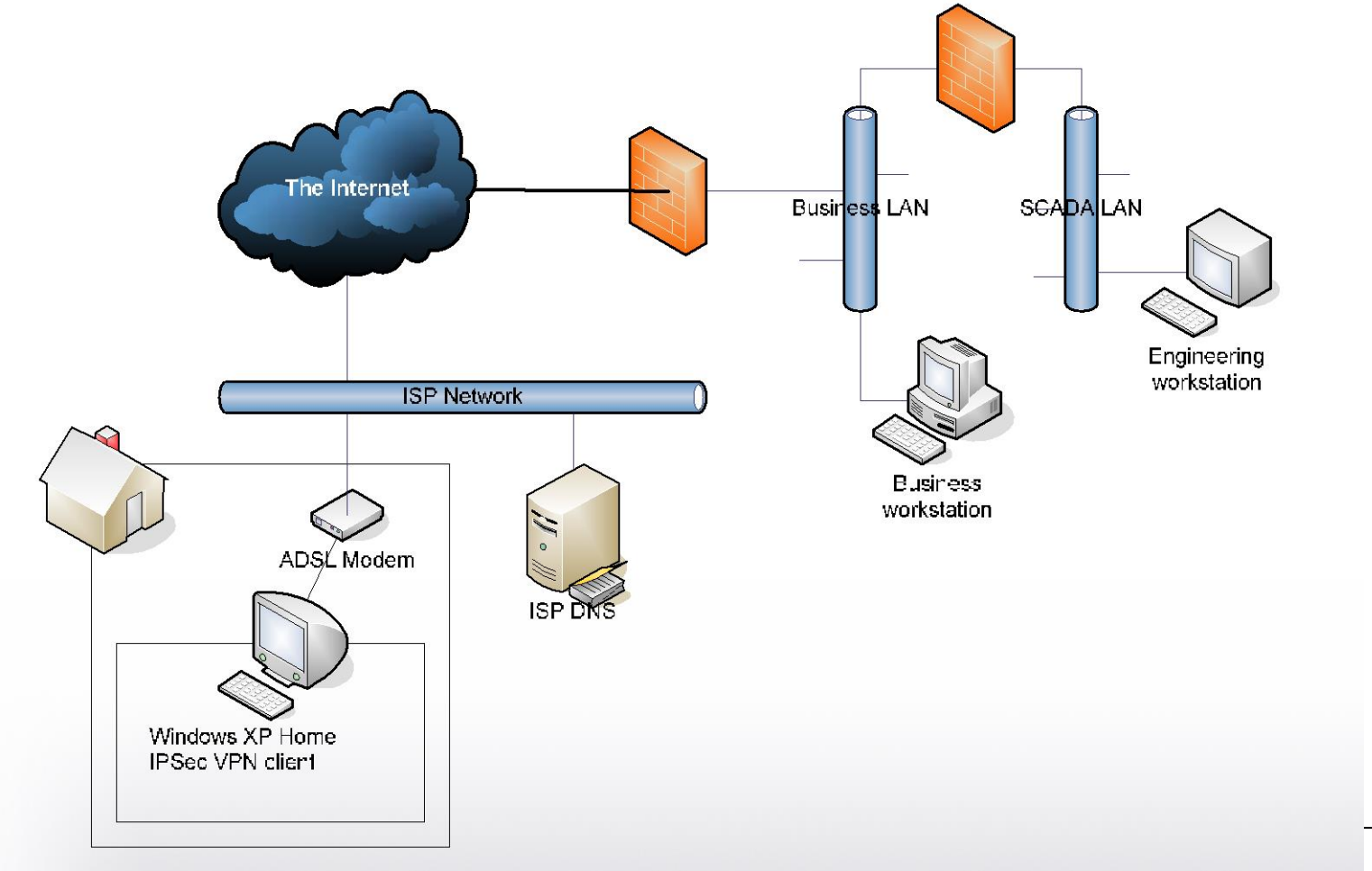
Examples of trust relationships

- Use of a DNS server
  - Trust the DNS server to convert the name to the correct address
  - Trust the DNS server **not** to send malformed data back
- Use of directory server for authentication
  - Trust directory server to provide correct authentication data

- Use of shared passwords
  - Trust others (systems or users) not to divulge the secret

- Firewall rules
  - Trusted systems may communicate with each other

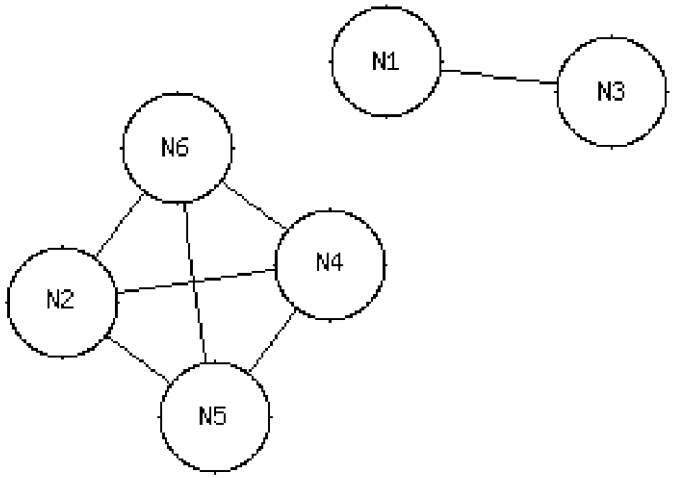
Trust relationships: remote access scenario



Modelling trust relationships

- Adjacency matrix M
  - A trusts B -> 1 in M_{AB}
  - If A is compromised, consider transitive closure from A to be compromised
  - Trust can be uni- or bi-directional
  - This allows us to create graphs over trust relationships

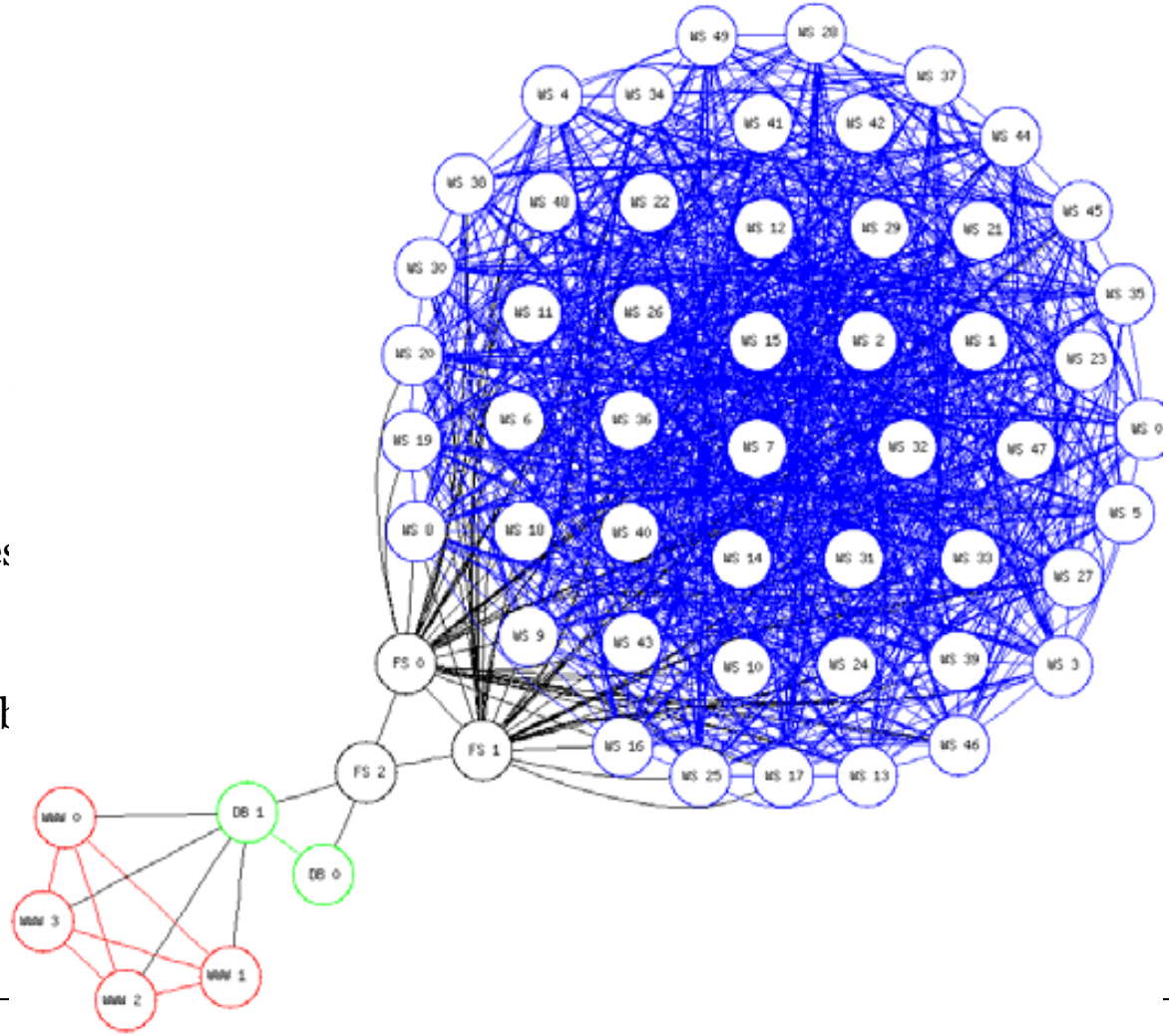
$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$



"it is possible to fly from x to y in one or more flights."

Example

- 40 workstations
  - same admin password, blue cluster
- 3 file servers
  - 2 are connected to the workstations,
- 2 database servers
  - The third file server is trusted by thes
- 4 web servers
  - One database is connected to the wel



All are connected, compromising any … compromises all

Trust relationships

- A necessary risk
  - Trust relationships are necessary for businesses to run
  - Trust relationships lead to exposure
  - **The question is:**
    - Is the added exposure motivated by business needs or not?

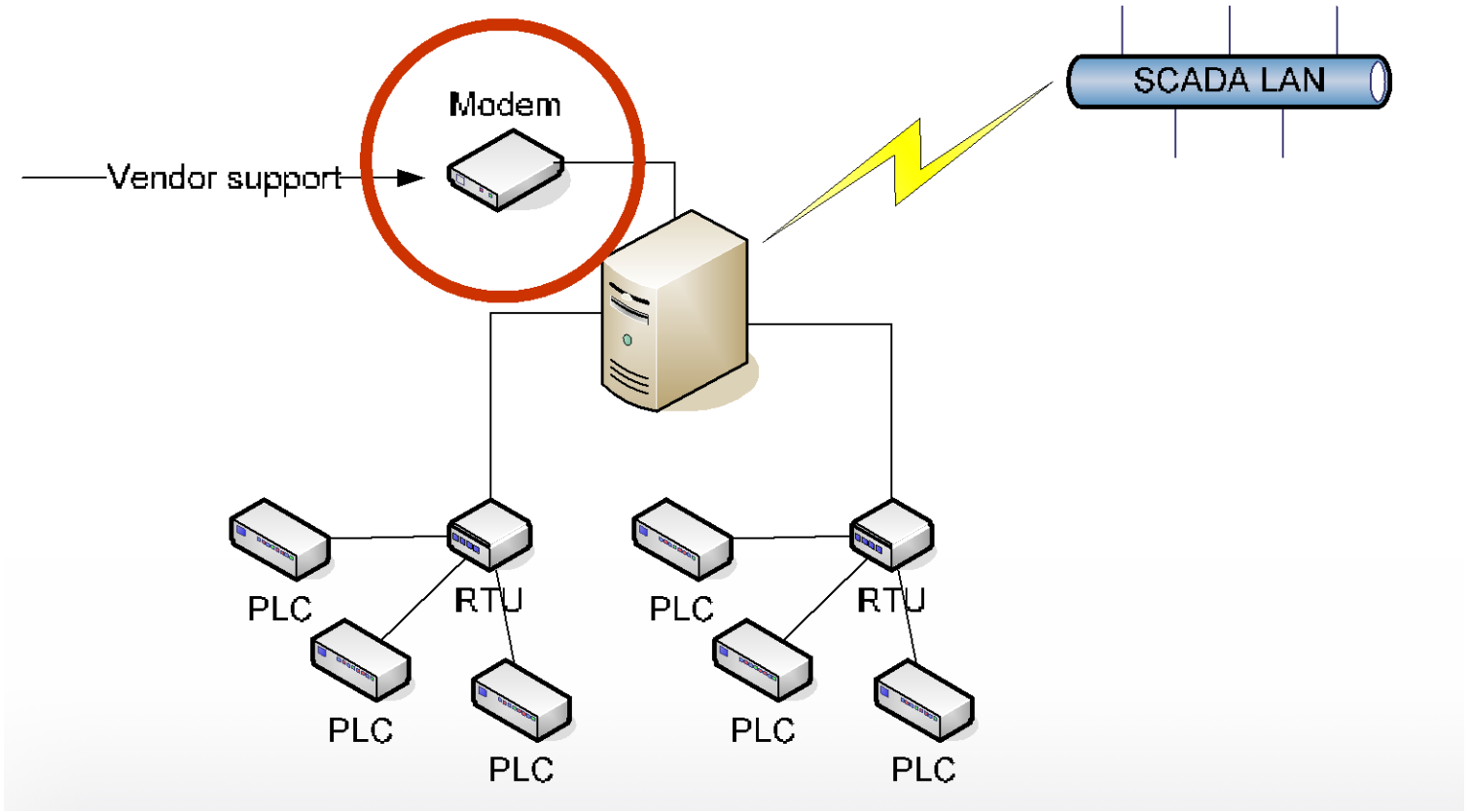
- What to do
  - Map existing trust relationships
  - Eliminate trust relationships that do not meet business needs
  - Evaluate exposures caused by trust relationships
  - Mitigate those leading to unacceptable exposure

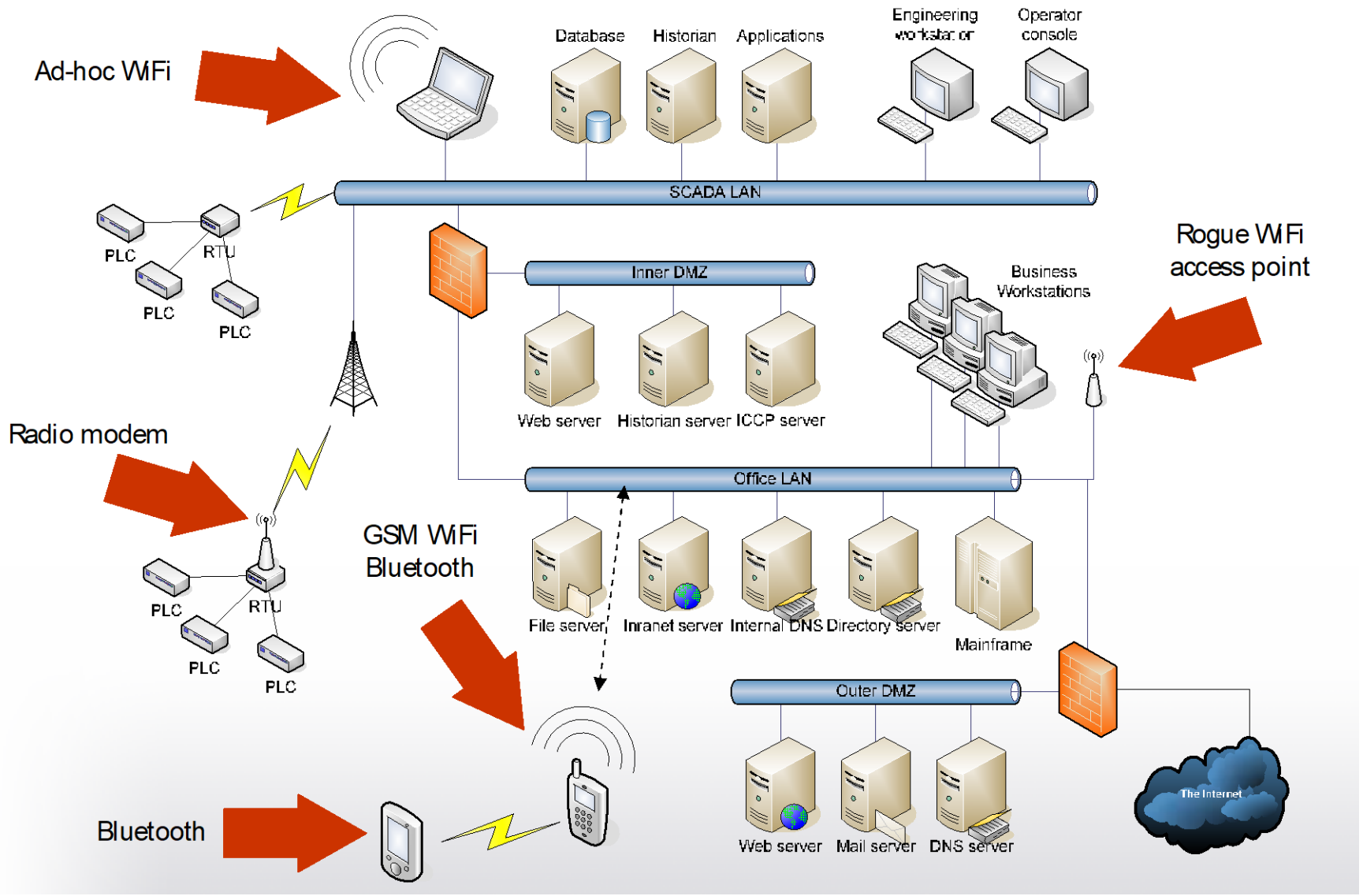
Backdoors – Bypassing the gaps

back door *n*. 1. a hardware or software based entrance into a computer system that bypasses security controls

- Backdoors allow intruders to bypass perimeter security
  - The firewall will not help – it has been bypassed
  - The network's intrusion detection system may **not** notice, it is designed to examine traffic coming through the front door (*more on these later in the course*)
  - Back doors may bypass access control and application security

Not so secret backdoor




Ad-hoc WiFi
Database
Historian
Applications
Engineering workstation
Operator console
SCADA LAN
PLC
RTU
PLC
PLC
Inner DMZ
Business Workstations
Rogue WiFi access point
Web server
Historian server
ICCP server
Radio modem
Office LAN
GSM WiFi Bluetooth
File server
Intranet server
Internal DNS
Directory server
Mainframe
PLC
RTU
PLC
PLC
Outer DMZ
The Internet
Bluetooth
Web server
Mail server
DNS server

Backdoor conclusions

- Backdoors are very common in complex systems
  - Things are forgotten, misplaced or mistakes are made
- Backdoors are *very* dangerous
  - They break the assumption that security is based upon
- Sometimes you do need them
  - But be aware of the risk they pose

Other Security Techniques

- Central orchestration with GUI
- ACL – Access Control Lists
- VPLS – Virtual Private LAN Service
  - Secure LAN interconnection
- Device cloaking
  - Reduce attack surface
- Software Defined Networking
  - OpenFlow, controller channel security
- Identity Defined Networking
  - Cryptographic Host Identities instead of IP and MAC addresses
  - Host Identity Protocol (HIPv2)

Marcus Bendtsen, Andrei Gurtov
Institutionen för Datavetenskap (IDA)
Avdelningen för Databas- och Informationsteknik (ADIT)

LINKÖPING UNIVERSITY