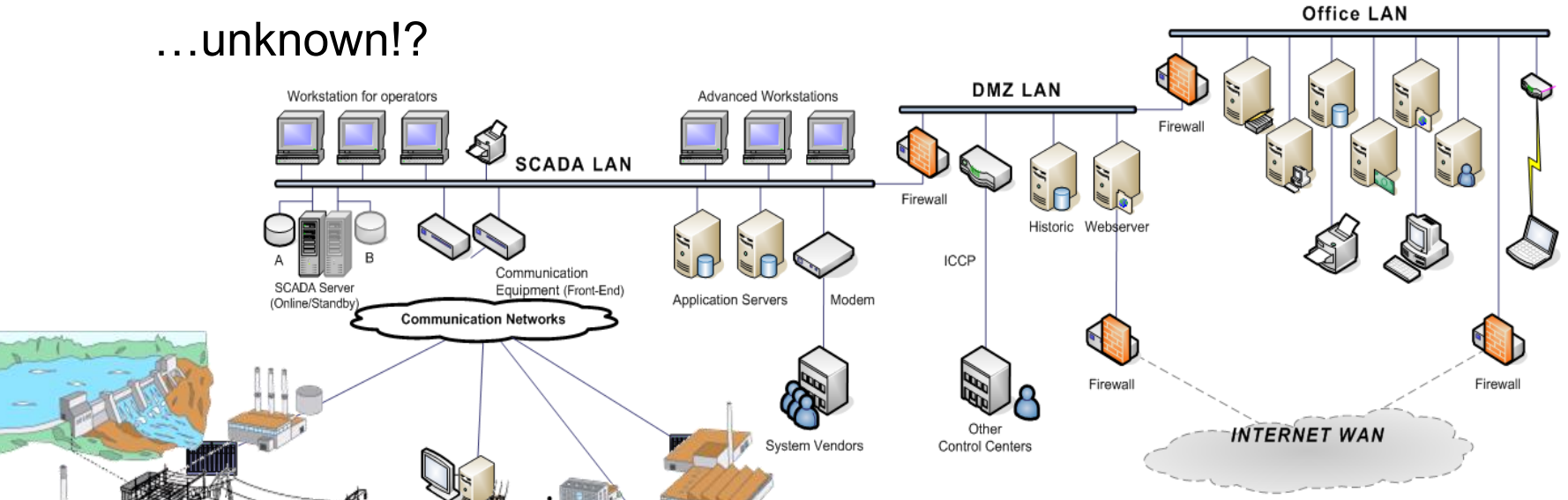
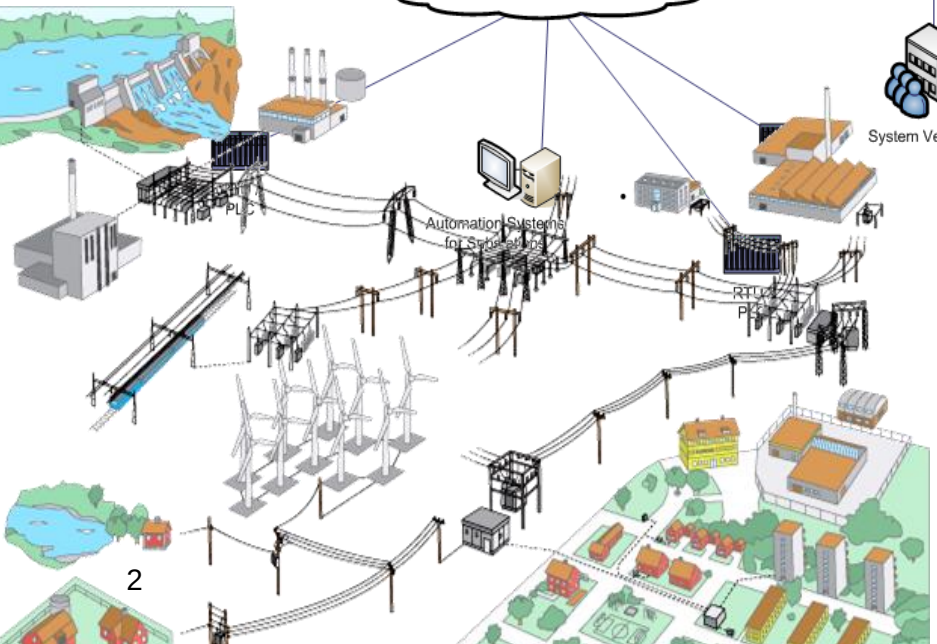
Vulnerability Assessment Using Attack Graphs (and securiCAD®) - A SEGRID Use Case Study

Alexandre Vernotte & Mathias Ekstedt
KTH Royal Institute of Technology
Sweden

Security managment challange

- ICT infrastructure:
  large, complex, heterogenous, legacy, modern
  …unknown!?

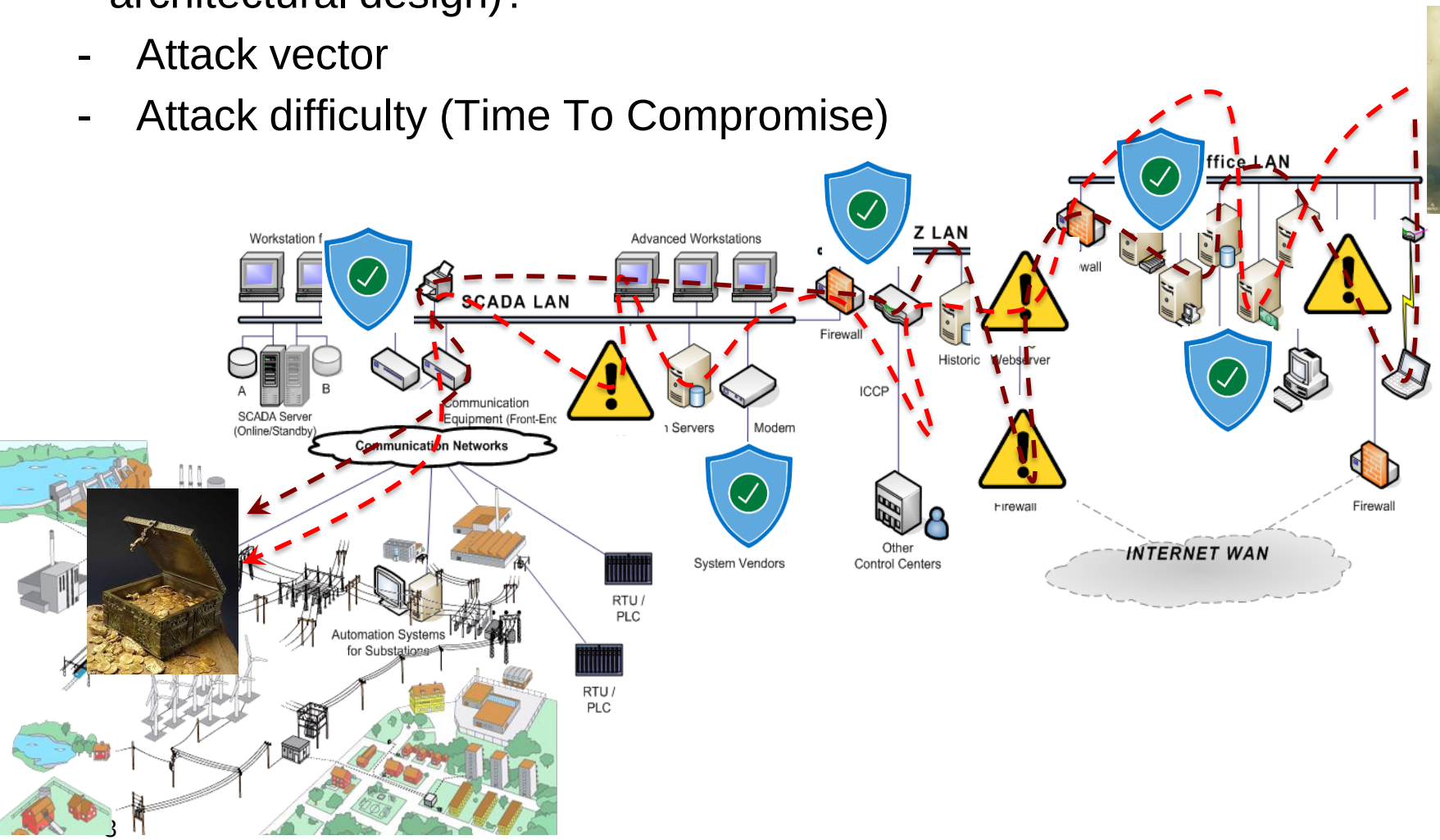




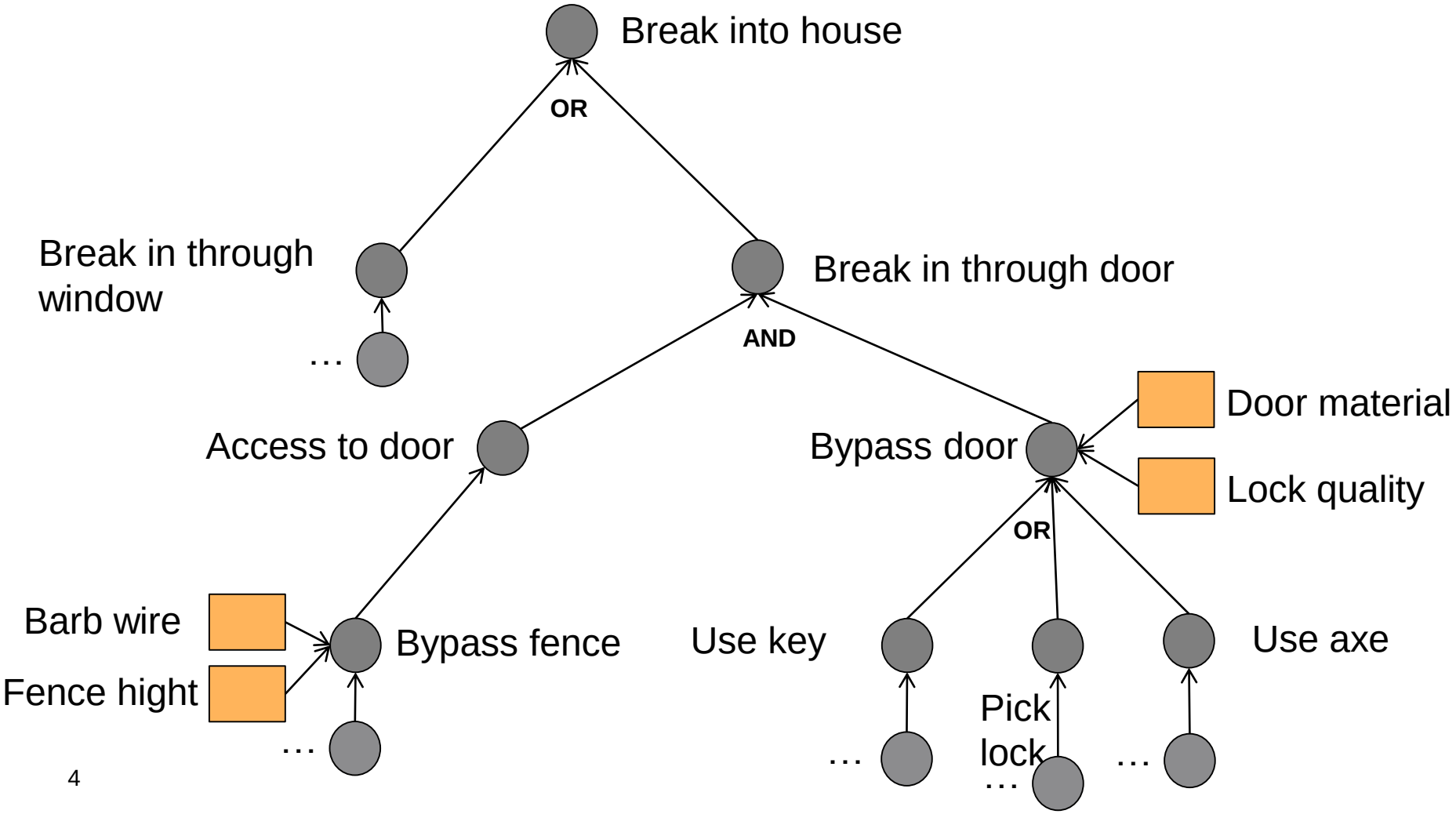
How secure / resilient is it..?

Vulnerability analysis of architectures

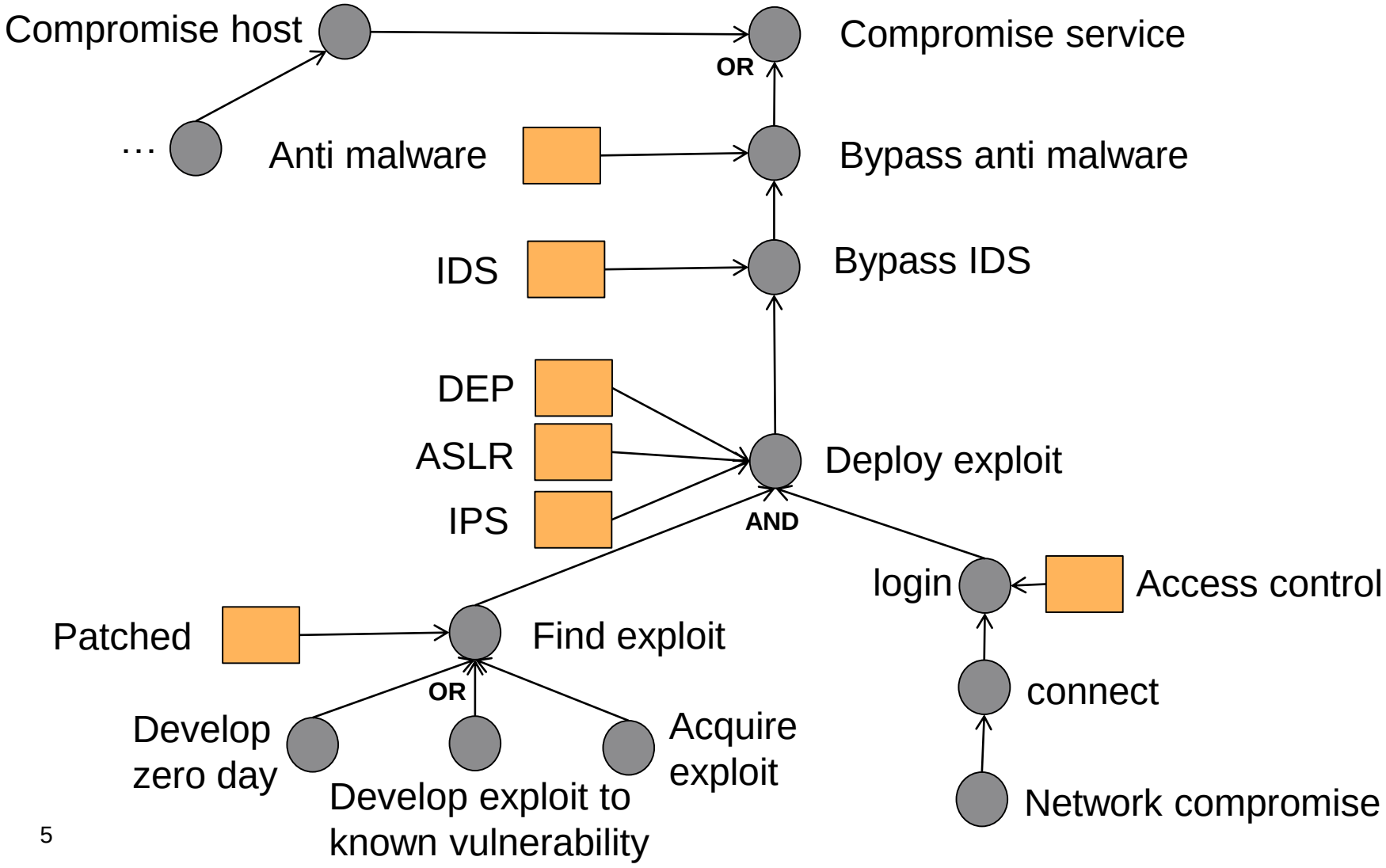
- How will attacks vary with vulnerabilities and defenses (and architectural design)?
  - Attack vector
  - Attack difficulty (Time To Compromise)



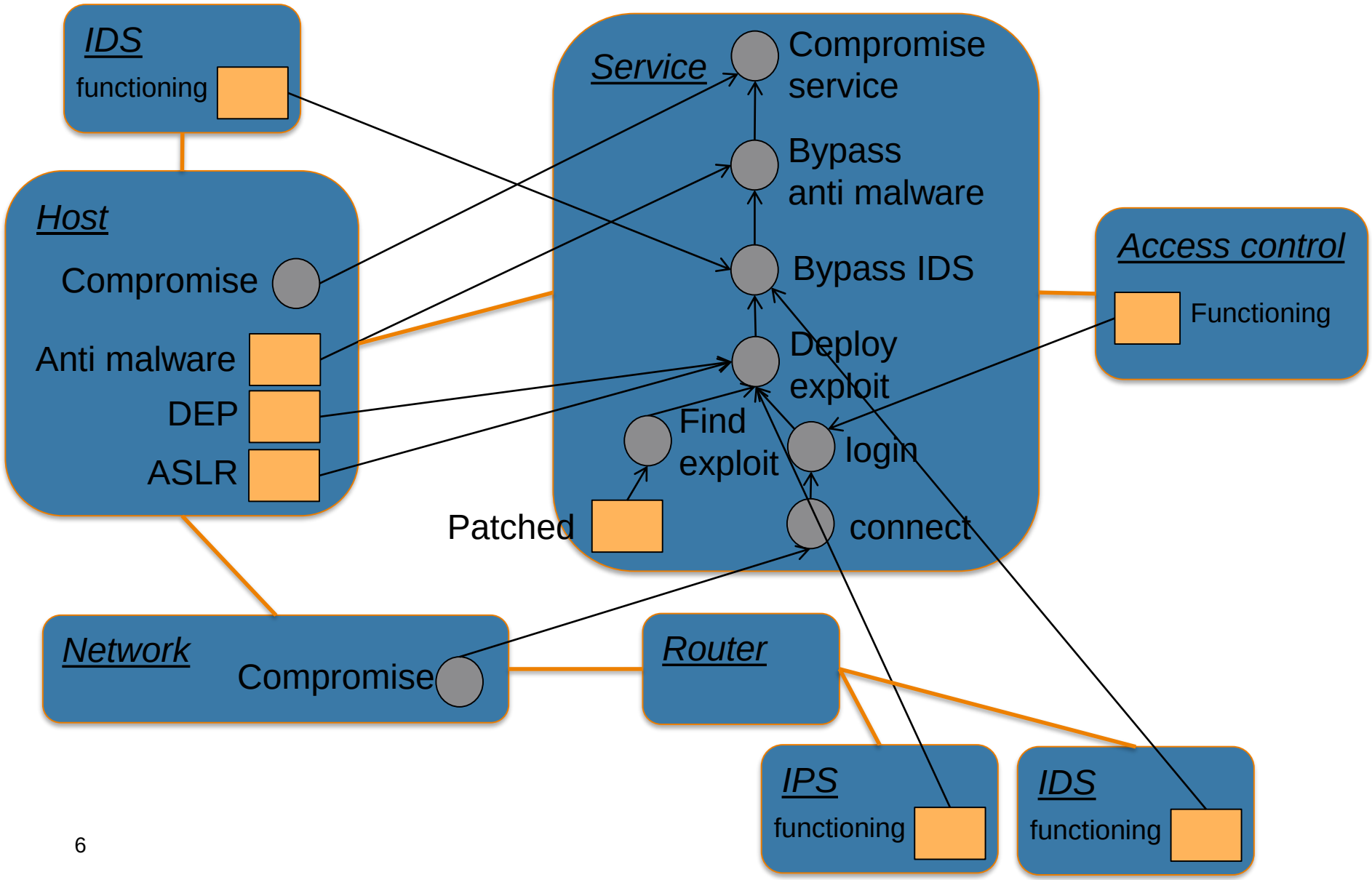
Attack/defense graphs – a simple example



Attack/defense graphs – securiCAD



Architecture-generated attack/defense graphs



securiCAD meta model – examples

Object

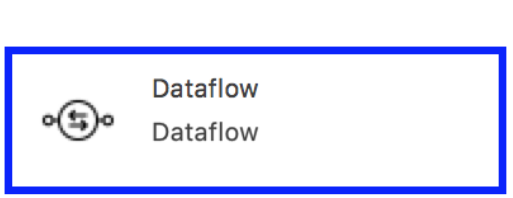
- Host
- Service
- Software product
- Dataflow
- User
- Physical zone
- …

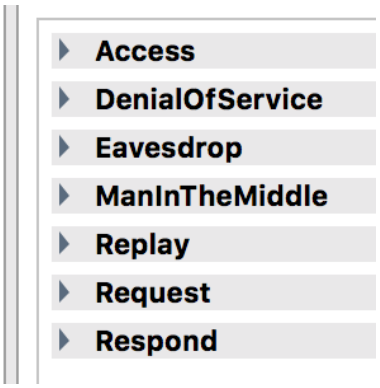
Attack step

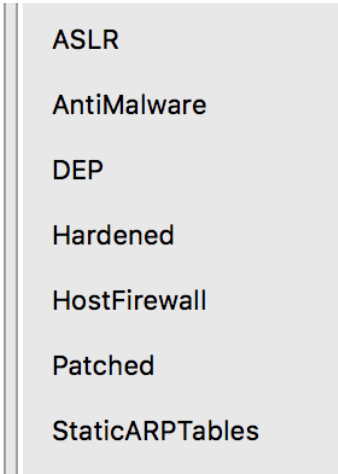
- MiTM
- DevelopZeroDay
- Exploit SQL injection
- Exploit XSS
- Guess password offline
- DenialOfService
- …

Defense

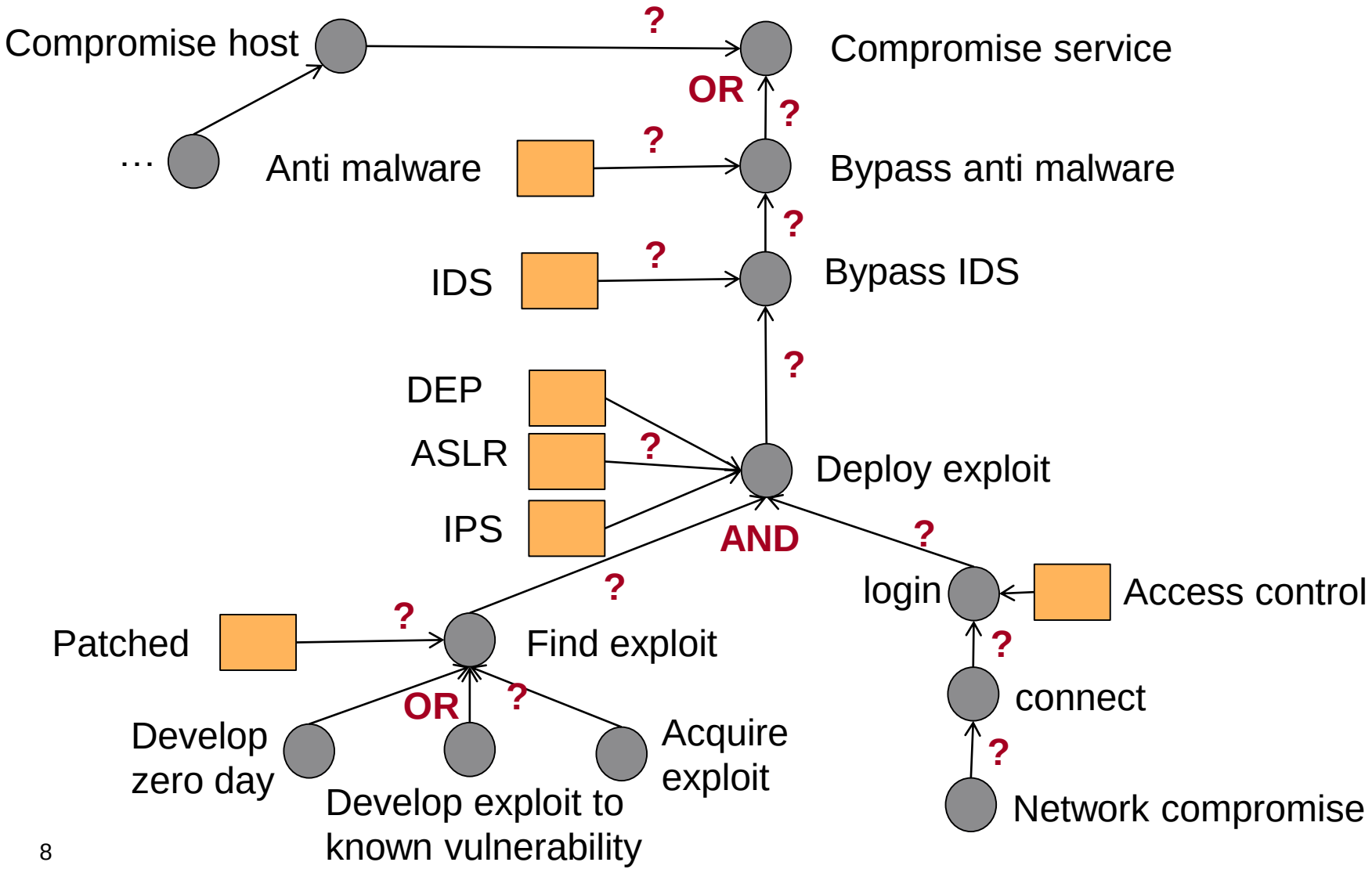
- Patch level
- DNS Security
- Static ARP tables
- ASLR
- DeveloperSecurityAware
- Hardened
- …



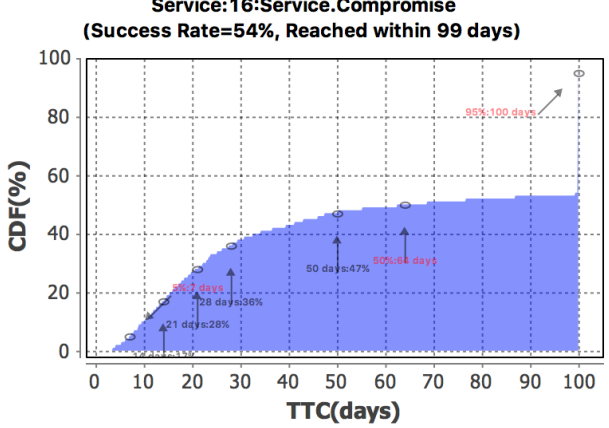




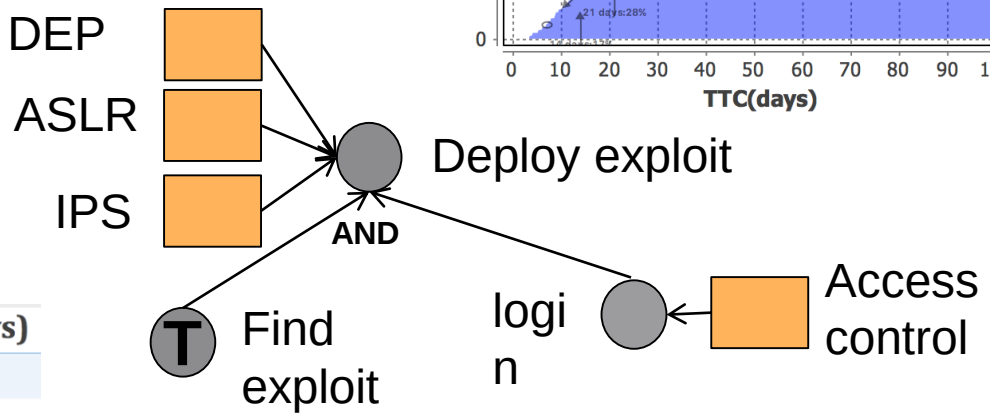
Attack and defense graphs – calculations



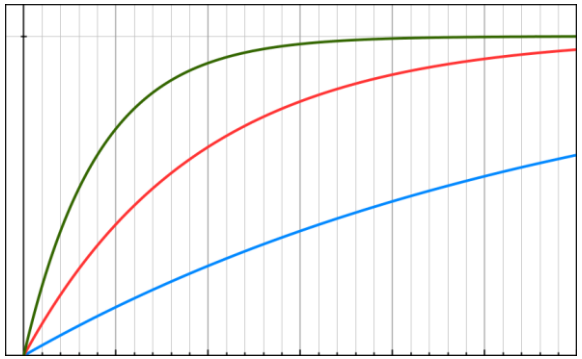
Deploy exploit - Attack success statistic



P (Deploy exploit.Time To Compromise (TTC)) = 1-exp(-lambda*TTC)



AC	DEP	ASLR	IPS	Lambda	TTC Median (days)
0	0	0	0	0.248	2.8
0	0	0	1	0.210	3.3
0	0	1	0	0.156	4.4
0	0	1	1	0.128	5.4
0	1	0	0	0.140	5.0
0	1	0	1	0.118	5.9
0	1	1	0	0.131	5.3
0	1	1	1	0.106	6.5
1	0	0	0	0.112	6.2
1	0	0	1	0.077	9.0
1	0	1	0	0.080	8.7
1	0	1	1	0.055	12.6
1	1	0	0	0.067	10.3
1	1	0	1	0.045	15.4
1	1	1	0	0.055	12.6
1	1	1	1	0.033	21.0



f(x)= 1-exp(-0.033*x)

f(x)= 1-exp(-0.106*x)

f(x)= 1-exp(-0.248*x)

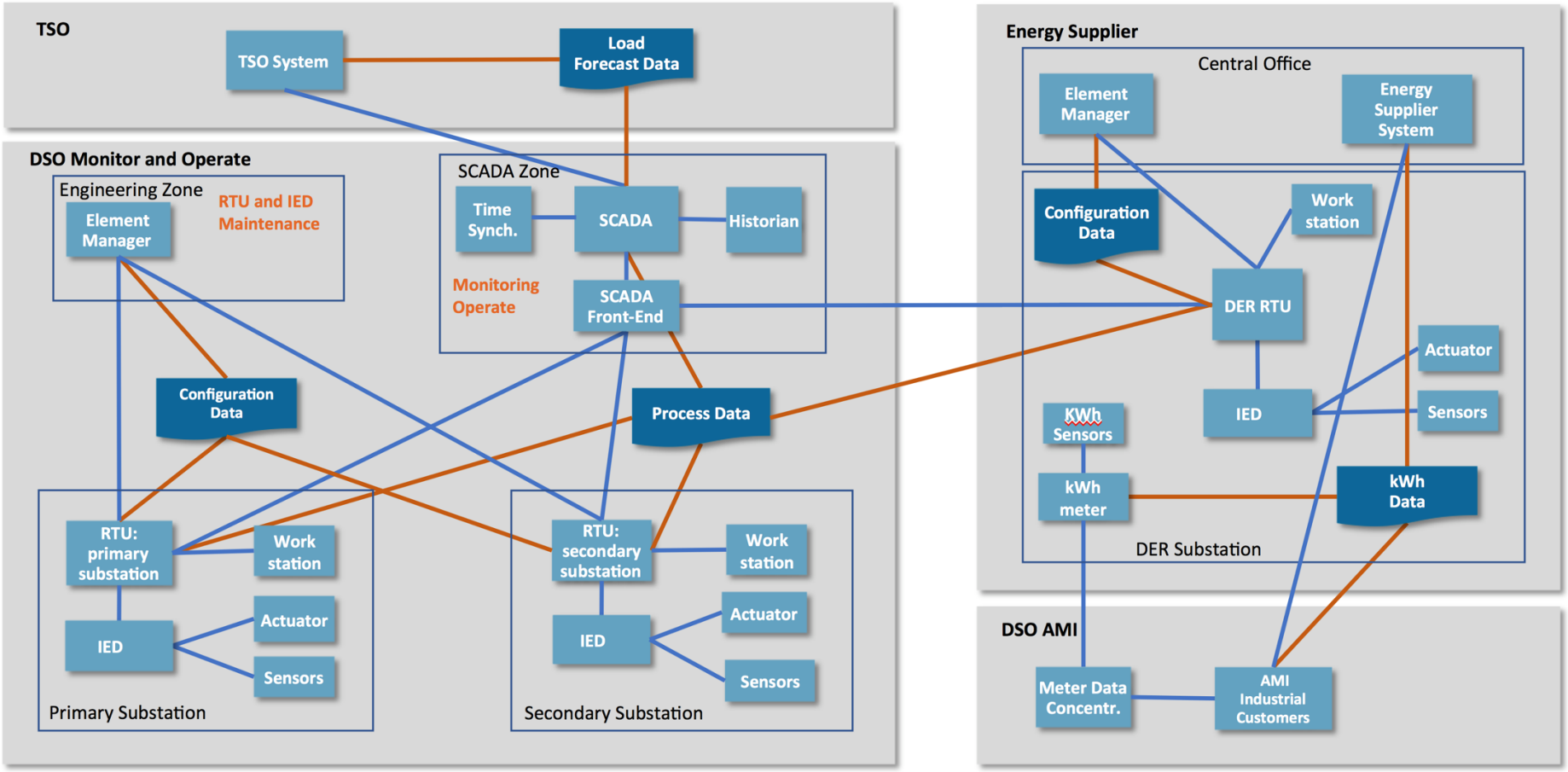
Sources - statistics

- **Logical necessities**, e.g. if the firewall allow you to connect to A from B and you have access to B, then you can connect to A.

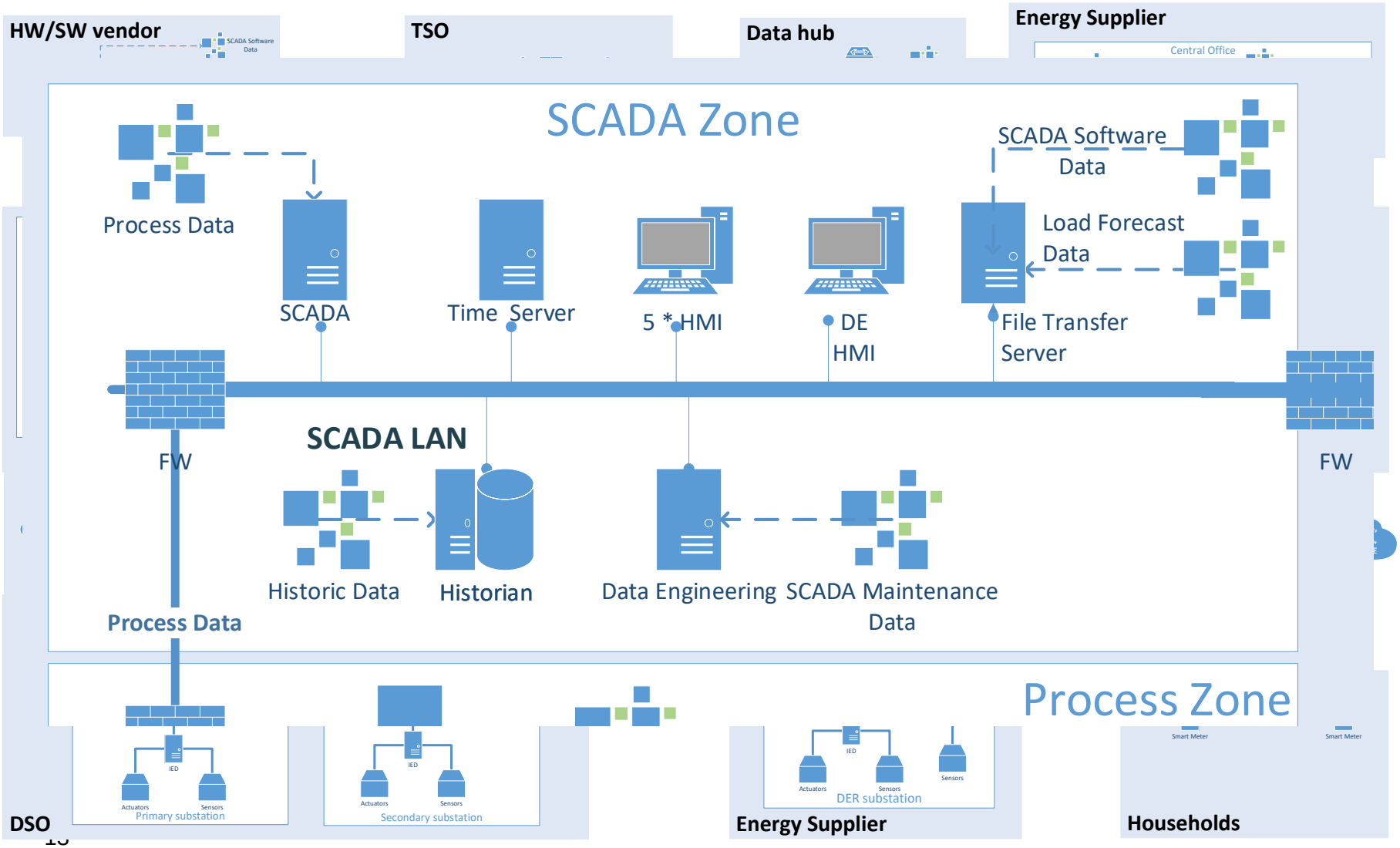
- **Scientific studies**
  - Research from KTH.
  - Other’s research studies.

Demo time

High-level logical view of UC2:S2 architecture



Physical view of UC2:S2 architecture



Data flows of UC2:S2 architecture (approx. 50)

No	Name	From	To	Initiator	Protocols	Auth
…						
5	Remote substation login	Office Station	Substation workstation	DSO Office Station, Engineering zone	CITRIX format for remote desktop or RDP	yes
6	Process data (bidirectional)	Primary RTU	SCADA Front End	SCADA Front End	IEC 60870-5-101/104 DNP 3.0, Modbus, Proprietary protocols	
…						
20	SCADA Software updates	Vendor Server	File transfer server (DMZ)	File transfer server (DMZ)	Protocol unknown, over Internet	yes
…						
34	Load Forecast Data	TSO	File Transfer server, DMZ	TSO	FTP format over Internet	
…						
40	Remote Login: Process Data (commands)	Office Station	SCADA HMI	Office Station	Internal format	

Additional parameters

Parameter	IT	OT
Host		
ASLR	On	On
Anti malware	On	Off
DEP	On	On
Hardened	Off	On
Host firewall	On	Off
Patched	75%	25%
Static ARP tabels	On	On
Access control		
Back-off	50%	Off
…	…	..

- **Attacker location → Internet**

First assessment

- From the SEGRID risk assessment – sensitive components:
  - SCADA master
  - substation RTUs (primary, secondary, DER)

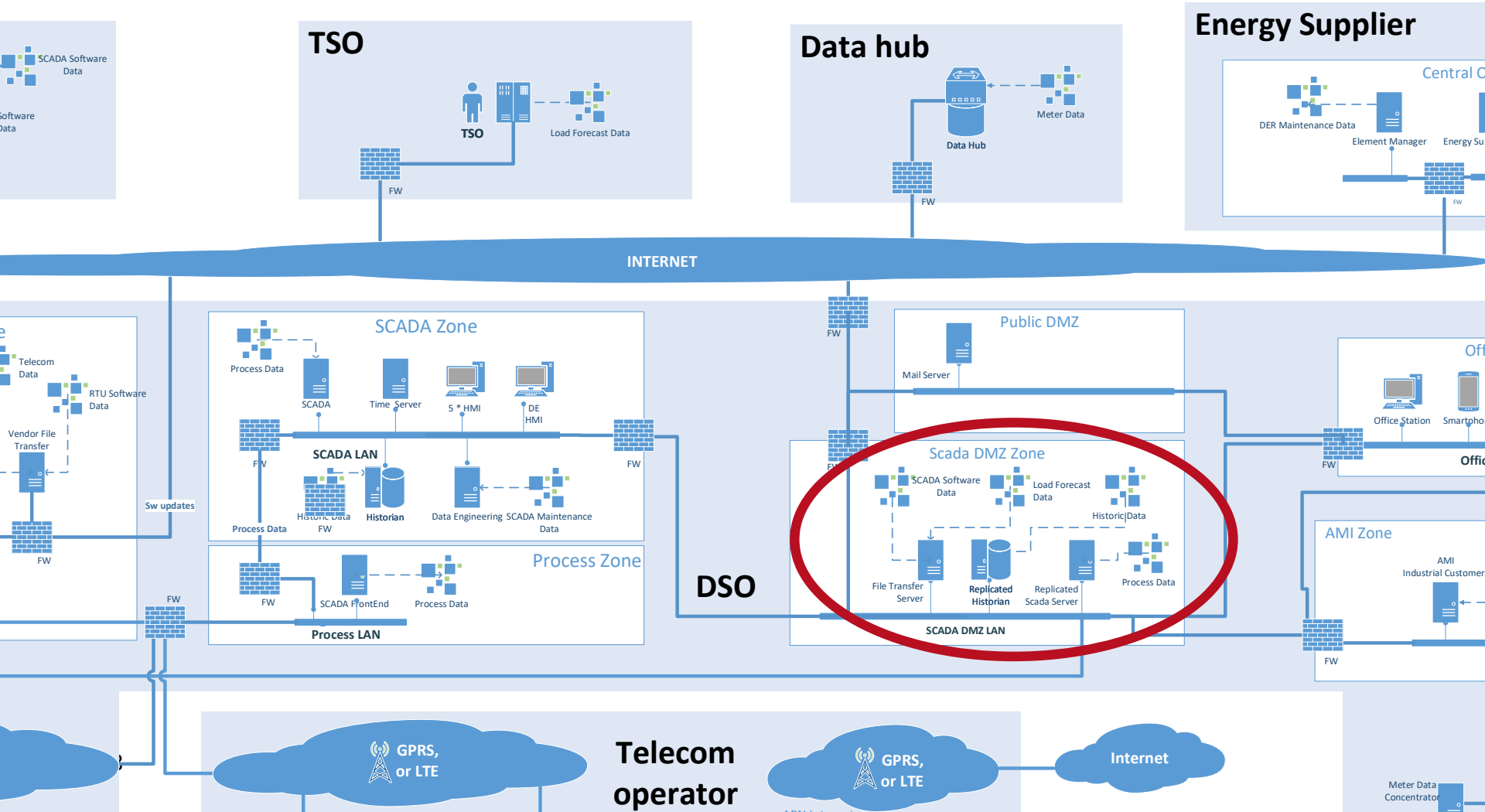
→ We choose these as evaluation points.

What happened?

- Inspect critical attack vector

What can be done?

- State-of-the-art propose the use of a SCADA DMZ



Are we securer?

- What happened this time?

Results from some simulations

	RTU - prim	RTU - 2nd	RTU - DER	SCADA
No HMI browsing (Base case)	22 days	22 days	23 days	20 days
HMI browsing allowed	12 days	12 days	14 days	12 days
No HMI browsing, good (/reasonable) patching	54 days	54 days	55 days	49 days
HMI replica placed in DMZ (shown improvement)	71 days	71 days	74 days	66 days
HMI replica placed in DMZ, good (/reasonable) patching	155 days	155 days	155 days	119 days
Add a diode from SCADA zone to DMZ	200 days (18%)	200 days (18%)	200 days (18%)	200 days (18%)

Other threat scenarions

- Can an attacker compromise the SCADA master from the smart meter?
  - Yes.

- …

Conclusion
&
Wrap-up

No silver bullet security solution…

- Security depends on a large number of details…
  - Details that differ with SCADA system installation
- What assets are you interested in?
- What attacks are you interested in?
- Reference model helps to get started with a specific analysis

- General observations
  - The best protection is close to the internet and other attacker entry points.
  - There are no isolated, completely secure) segments
  - Forcing the attacker to deploy zero days is a generally reasonable strategy.

How do I get to know my infrastructure?

- Manual modeling is extremely costly (sometimes necessary though)
- Automatic import of “ICT infrastructure raw data”
  - Nmap
  - Vulnerability scanners
  - Firewall rule config files
  - …
- Overlapping and seldomly 100% accurate

→ Poster on automatic modeling of inconsistent data

Thank you for listening!

-

(More) questions?