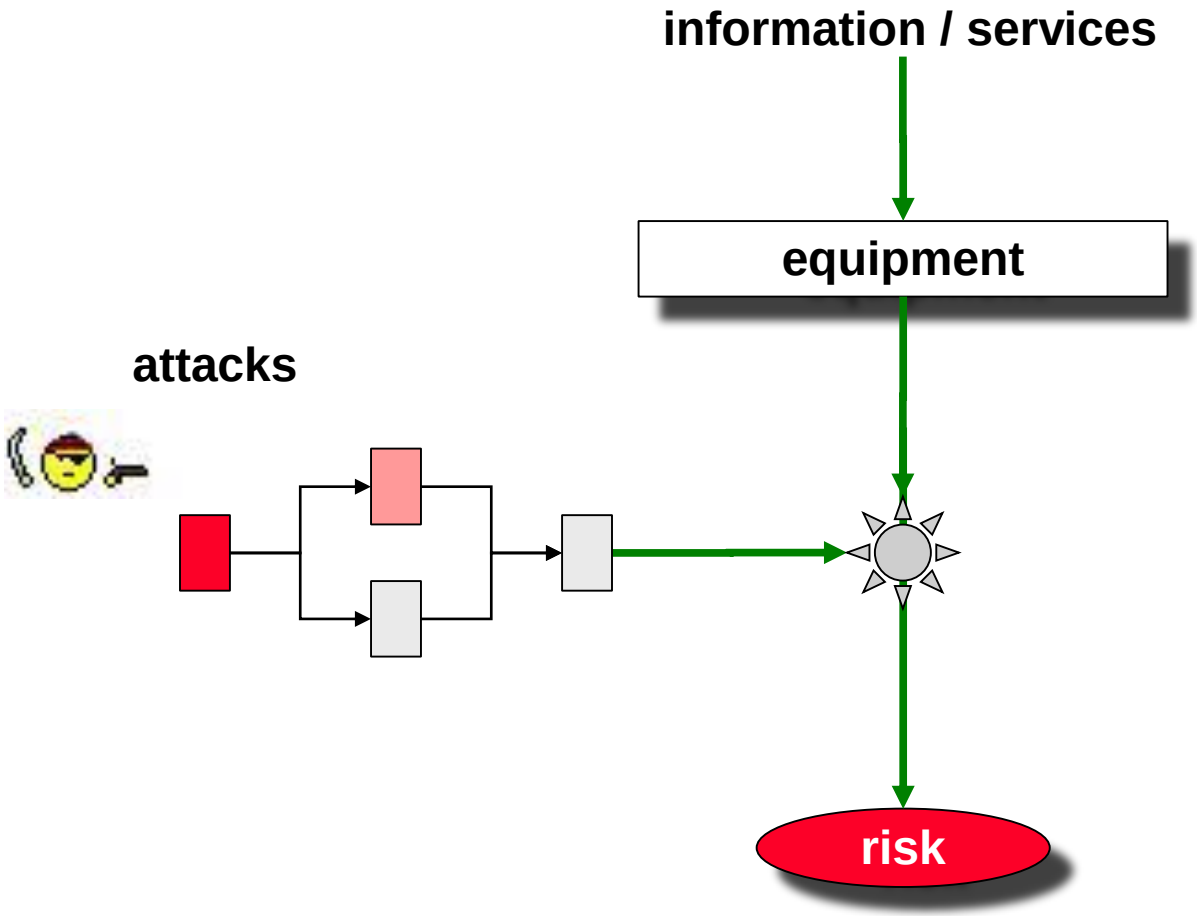
PILAR
External Attacks
Physical

José A. Mañas jmanas@pilar-tools.com

13.6.2016

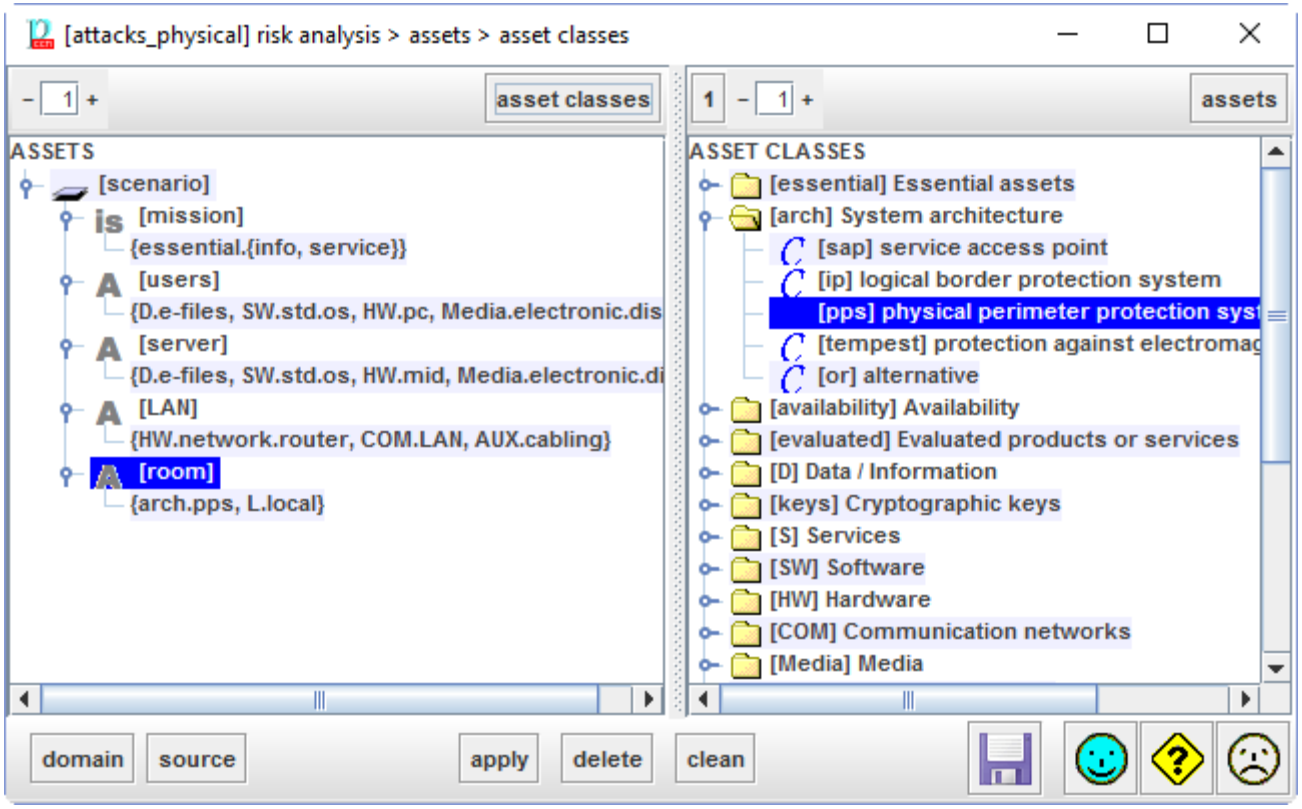
Attacks



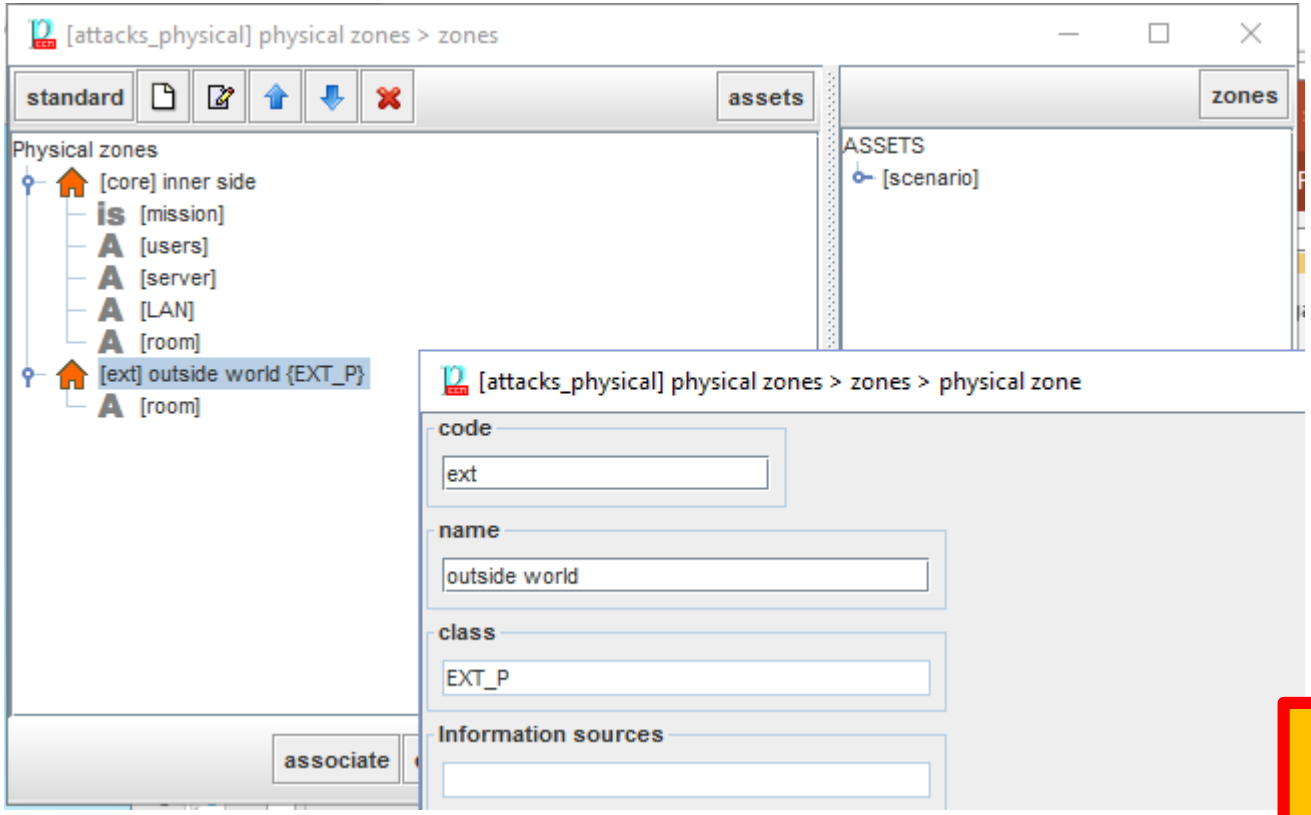
modelling

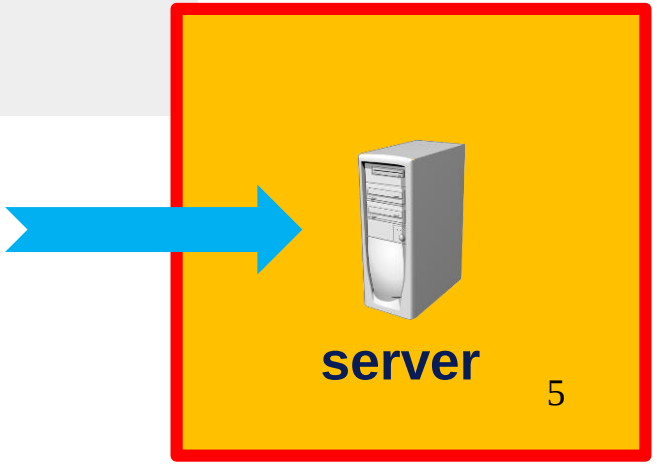
- **zones**
  identify zones & assets in zones
- **timing**
  compares attack & reaction times
- **paths**
  attack opportunities

assets

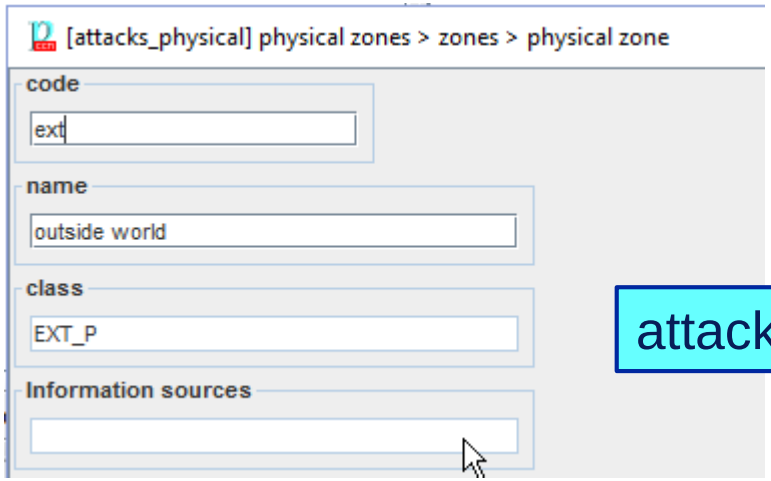

[attacks_physical] risk analysis > assets > asset classes
asset classes
assets
ASSETS
[scenario]
[mission]
{essential.{info, service}}
[users]
{D.e-files, SW.std.os, HW.pc, Media.electronic.dis
[server]
{D.e-files, SW.std.os, HW.mid, Media.electronic.di
[LAN]
{HW.network.router, COM.LAN, AUX.cabling}
[room]
{arch.pps, L.local}
ASSET CLASSES
[essential] Essential assets
[arch] System architecture
[sap] service access point
[ip] logical border protection system
[pps] physical perimeter protection syst
[tempest] protection against electromag
[or] alternative
[availability] Availability
[evaluated] Evaluated products or services
[D] Data / Information
[keys] Cryptographic keys
[S] Services
[SW] Software
[HW] Hardware
[COM] Communication networks
[Media] Media
domain
source
apply
delete
clean

zones


[attacks_physical] physical zones > zones
standard
assets
zones
Physical zones
[core] inner side
[mission]
[users]
[server]
[LAN]
[room]
[ext] outside world {EXT_P}
[room]
ASSETS
[scenario]
[attacks_physical] physical zones > zones > physical zone
code
ext
name
outside world
class
EXT_P
Information sources
associate

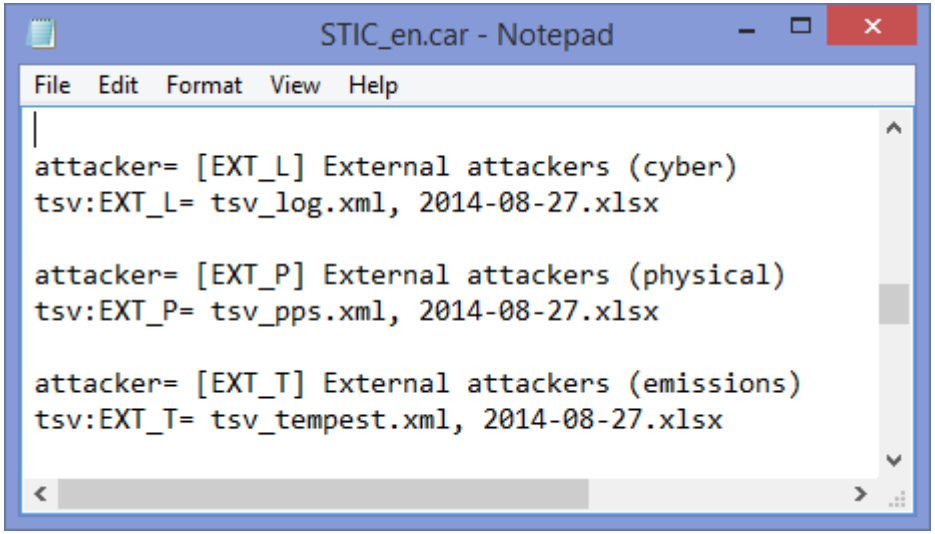

room
server

attacker



attackers

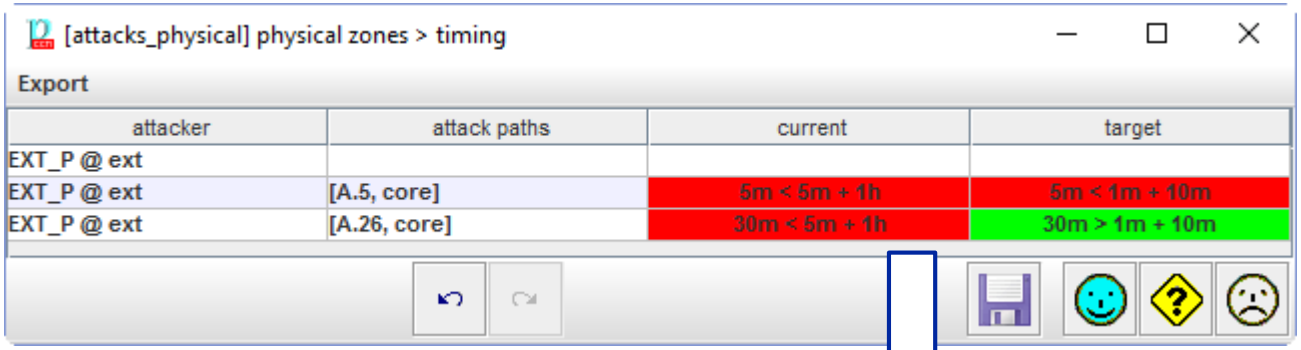
specified in configuration

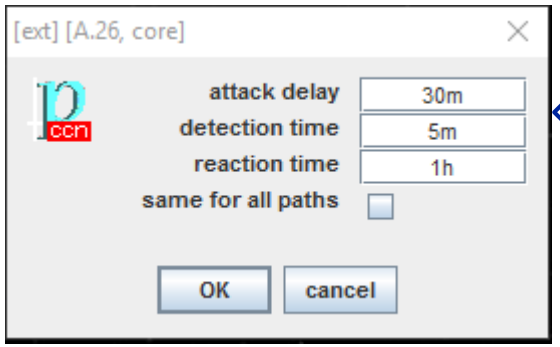


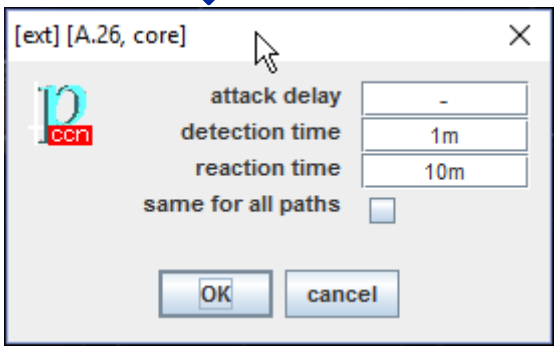
timing

feasible attack

averted attack



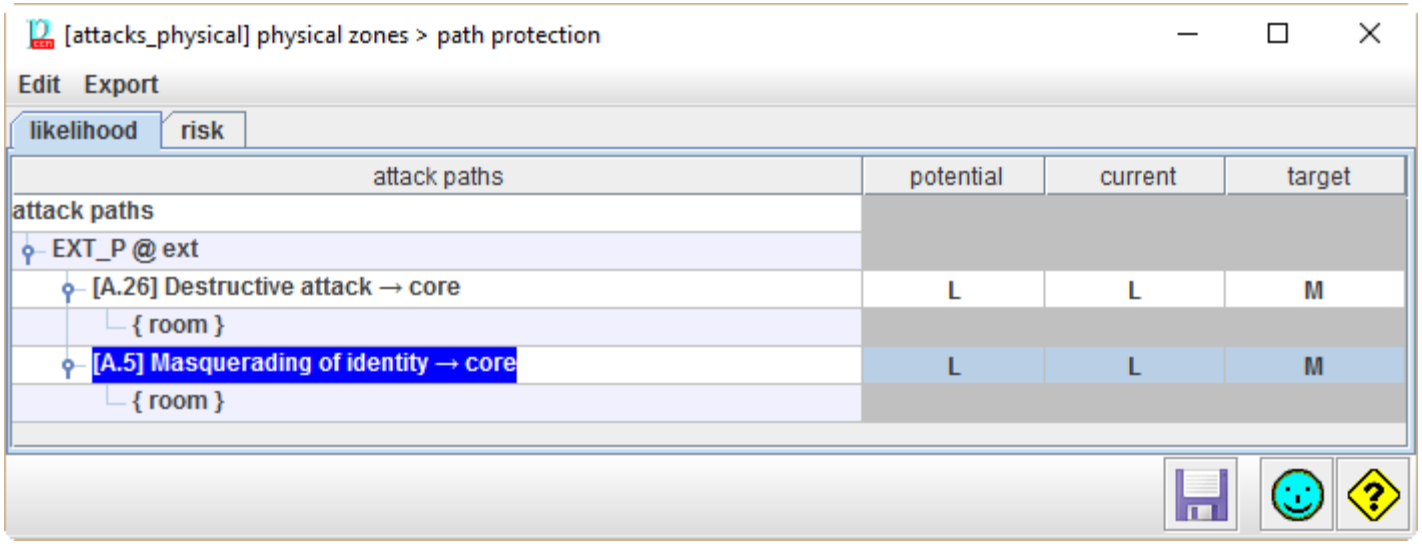




physical attacks

paths

1. The attacker (EXT_P) is at her domain (ext)
   - she may get into the room
   - Now, she may attack valuable assets



paths

[attacks_physical] physical zones > path protection

Edit Export

likelihood | risk

attack paths	potential	current	target
attack paths			
EXT_P @ ext			
[A.26] Destructive attack → core	{5.4}	{2.9}	{0.81}
server (D) [A.11] Unauthorised access	{4.2}	{1.6}	{0.52}
LAN (D) [A.11] Unauthorised access	{4.2}	{1.4}	{0.49}
LAN (C) [A.11] Unauthorised access	{5.4}	{2.7}	{0.75}
server (I) [A.11] Unauthorised access	{2.4}	{0.76}	{0.16}
server (C) [A.11] Unauthorised access	{5.4}	{2.9}	{0.81}
users (I) [A.11] Unauthorised access	{2.4}	{0.76}	{0.16}
LAN (I) [A.11] Unauthorised access	{4.2}	{1.4}	{0.48}
users (D) [A.11] Unauthorised access	{4.2}	{1.6}	{0.52}
users (C) [A.11] Unauthorised access	{5.4}	{2.9}	{0.81}
[A.5] Masquerading of identity → core	{5.4}	{2.9}	{0.73}
LAN (C) [A.11] Unauthorised access	{5.4}	{2.7}	{0.67}
LAN (D) [A.11] Unauthorised access	{4.2}	{1.4}	{0.41}
LAN (I) [A.11] Unauthorised access	{4.2}	{1.4}	{0.40}
users (D) [A.11] Unauthorised access	{4.2}	{1.6}	{0.44}
server (I) [A.11] Unauthorised access	{2.4}	{0.76}	{0.08}
server (D) [A.11] Unauthorised access	{4.2}	{1.6}	{0.44}
users (C) [A.11] Unauthorised access	{5.4}	{2.9}	{0.73}
server (C) [A.11] Unauthorised access	{5.4}	{2.9}	{0.73}
users (I) [A.11] Unauthorised access	{2.4}	{0.76}	{0.08}

protecting paths

[attacks_physical] risk analysis > safeguards > Safeguard effectiveness

Edit Expand Export Import Statistics

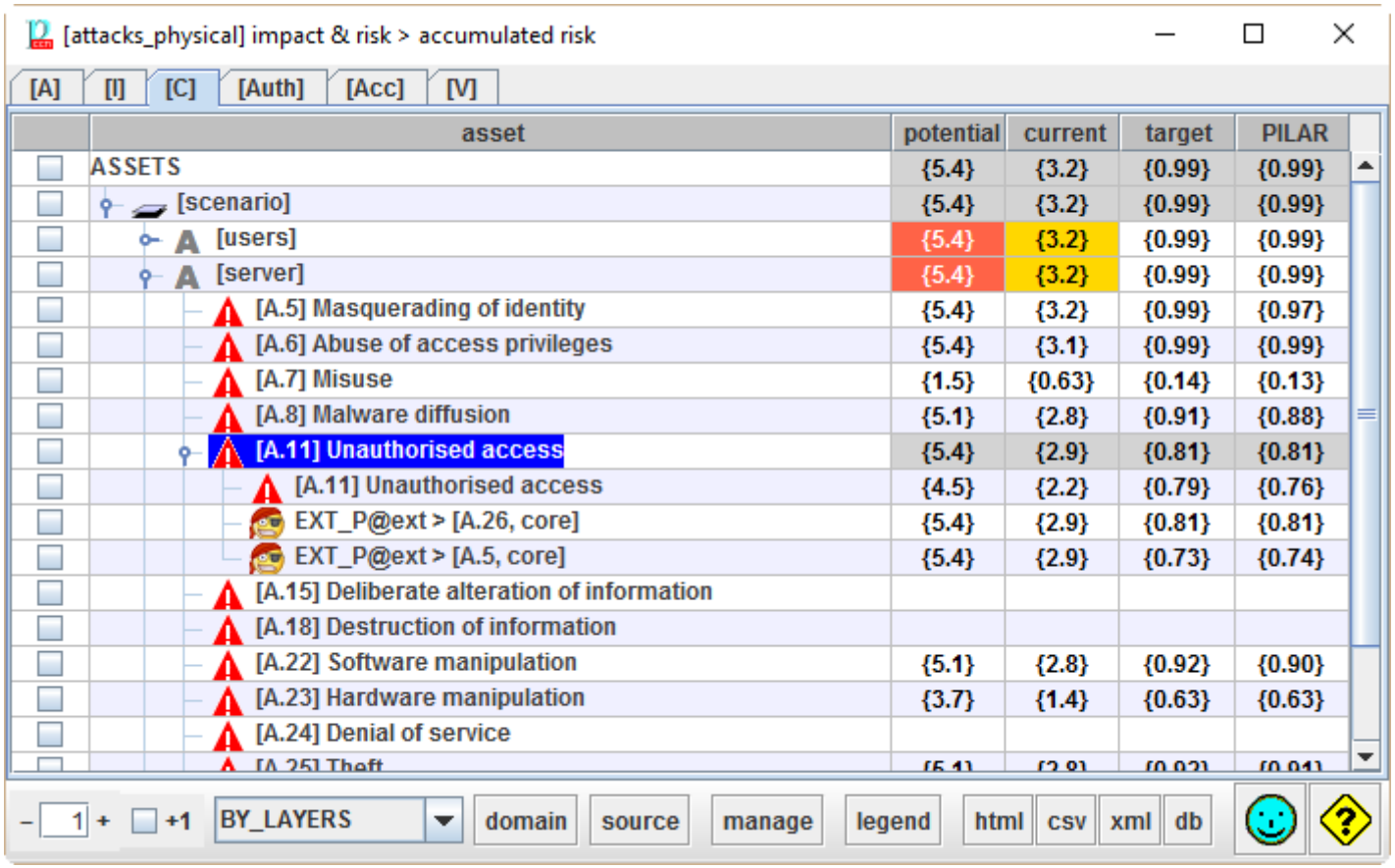
[base] Base | Information sources

as...	top	safeguard	do...	so...	co...	re...		cu...	tar...	Pl...
PHY	EL	[PPS] Perimeter protection				7		L2	L3	L2-...
PHY	EL	[L.depth] Defence in depth				5		L2	L3	L3
PHY	EL	[PPS.2] Design				7		L2	L3	L3-...
PHY	EL	[PPS.3] Doors				5		L2	L3	L3
PHY	EL	[PPS.4] Windows				5		L2	L3	L3
PHY	EL	[PPS.5] Grilles				4		L2	L3	L3
PHY	EL	[PPS.6] External walls				6		L2	L3	L3-...
PHY	EL	[PPS.7] Access doors				4		L2	L3	L2-...
PHY	EL	[PPS.8] Control of keys, combinations and security devices				4		L2	L3	L2-...
T	EL	[L.IA] {xor} Authentication mechanism				5		L2	L3	L3
PHY	EL	[L.AC] Physical access control				7		L2	L3	L2-...
PHY	DC	[PPS.b] Perimeter intrusion detection system				4		L2	L3	L3
PHY	DC	[PPS.c] There is a video monitoring system (CCTV)				4		L2	L3	L3
PHY	AW	[PPS.d] Personnel are aware and receive training regarding detection and response to suspicious activity nearby the premises				2		L2	L3	L2
PHY	PR	[PPS.e] Security lighting				4		L2	L3	L3
PHY	EL	[PPS.f] Surveillance				4		L2	L3	L2-...
PHY	EL	[PPS.g] Site security is not the responsibility of a single guard				7		L2	L3	L4
PHY	MN	[PPS.h] Recording of events				4		L2	L3	L2-...

– 1 + sources | operation | suggest | find >>

physical attacks

risk mitigation



threat profiles

A.5 masquerading of identity
A.11 unauthorized access
A.25 theft
A.26 destructive attack
A.27 enemy over-run
A.29 extortion
A.30 social engineering
A.31 distraction

```
<threat-standard-values>
  <filter>
    <families>
       arch.pps HW Media AUX L P other
    </families>
    <threats>
       A.5 A.11 A.29 A.30 A.31
    </threats>
  </filter>

  <family F="arch.pps">
    <threat Z="A.5" f="10" />
    <threat Z="A.26" f="10" />
  </family>

  <family F="P">
    <threat Z="A.26" >
      <set D="V" deg="1.0" />
    </threat>
  </family>

  <family F="other">
    <threat Z="A.25" >
      <set D="V" deg="0.9" />
    </threat>
    <threat Z="A.26" >
      <set D="V" deg="1.0" />
    </threat>
  </family>

</threat-standard-values>
```

physical attacks

current status

- beta
- getting experience
  - fast for simple (standard) scenarios
  - balance between complexity and actionability
- to be adjusted
  - threat profiles
  - safeguards
  - recommendations