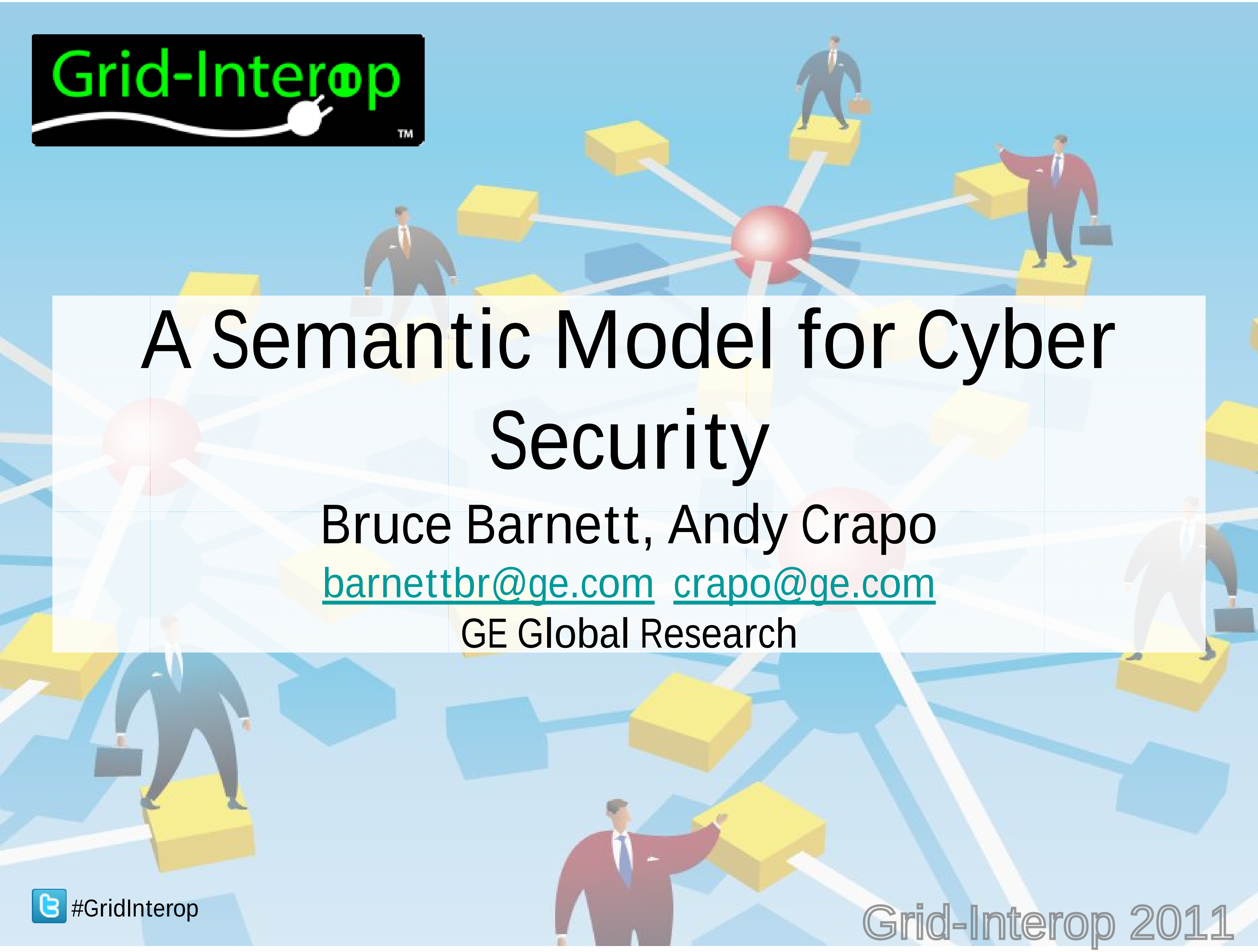


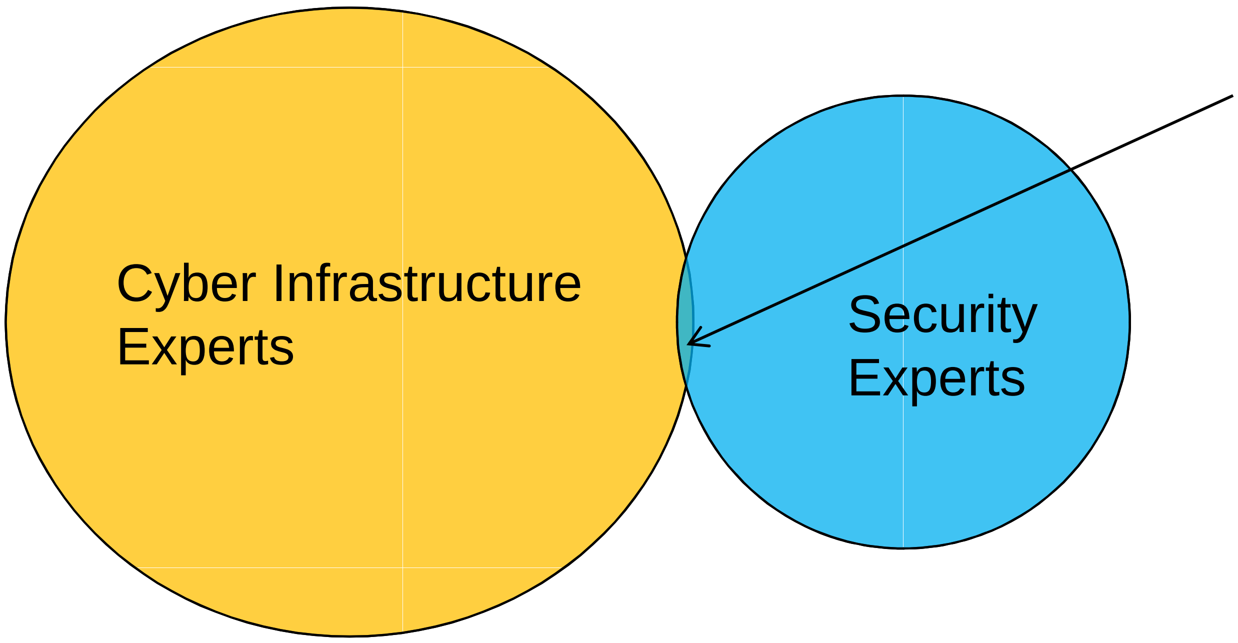
A Semantic Model for Cyber Security

Bruce Barnett, Andy Crapo

barnettbr@ge.com crapo@ge.com

GE Global Research

Problem #1 Lack of Cyber Security Experts



Cyber Infrastructure Experts

Security Experts

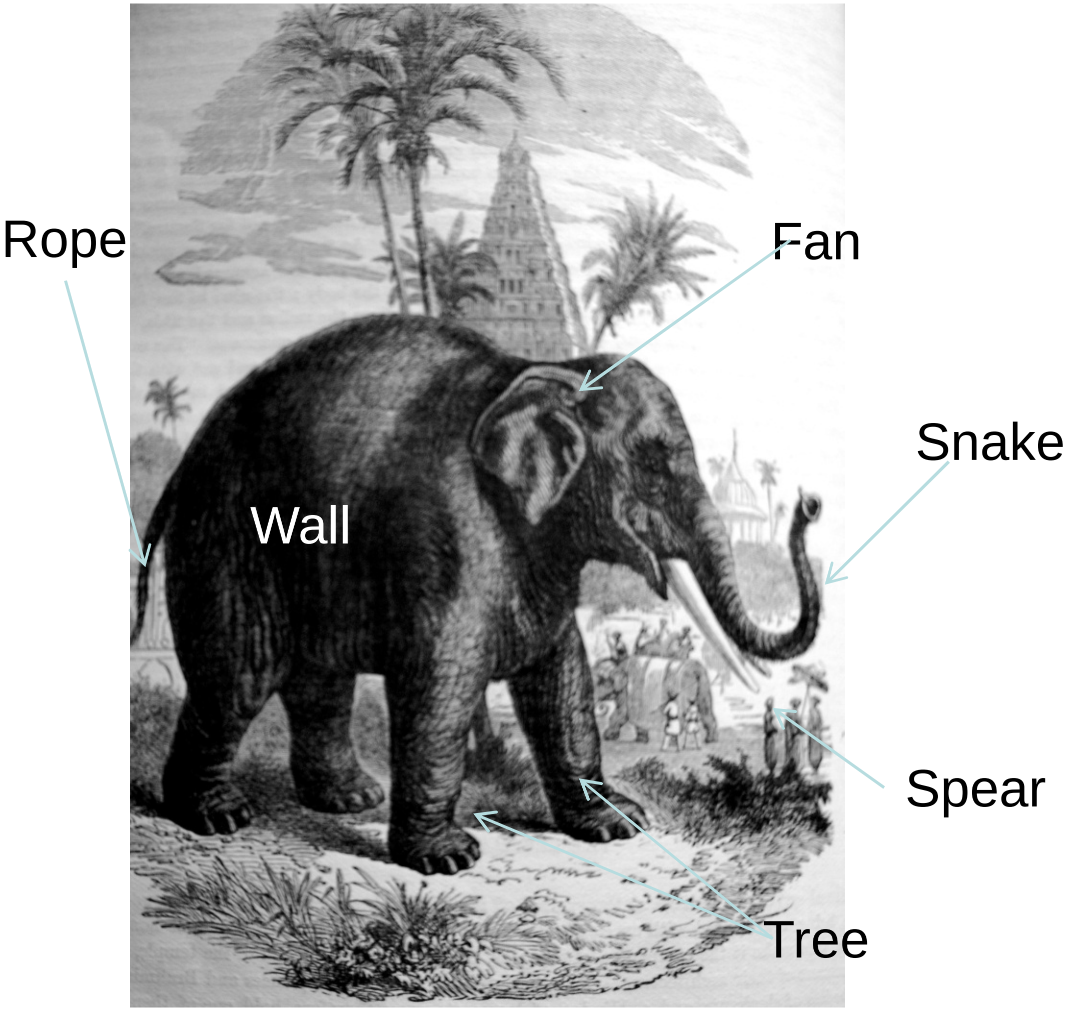
Intersection of Security Experts and Cyber Experts

We need more people!

We need more tools!

Problem #2: Capture security knowledge from multiple Subject Matter Experts

- – Physical Security
- – Application Security
- – Protocol Security
- – Device Security
- – Cryptographic Security
- – Network Security
- – Reverse Engineering
- – Web Security



"Blind Men" arguing over security requirements

Image courtesy of http://www.flickr.com/photos/feargal/

Answer: Semantics

Rigorously defined “Nouns”

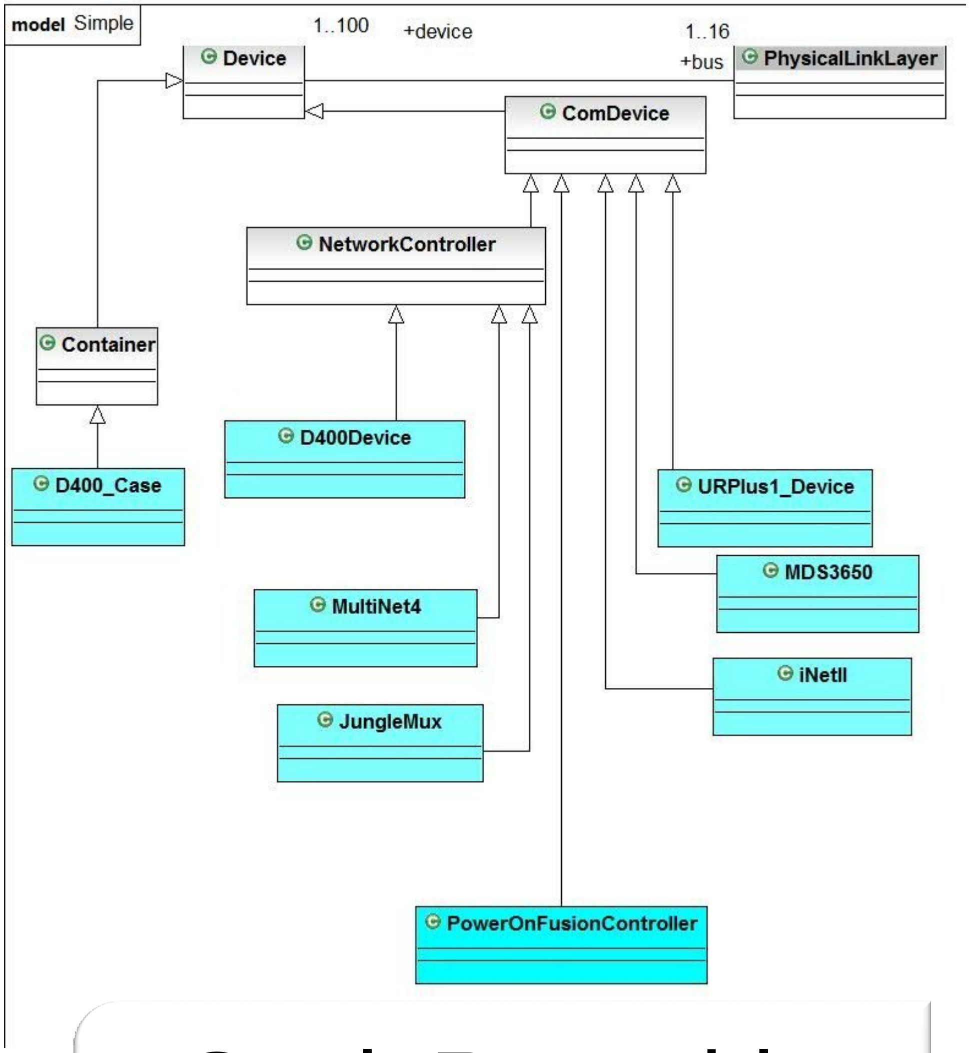
- Device, Container, NetworkController, PhysicalLinkLayer
- Vulnerability

Rigorously defined attributes

- Switch/hub/bridge/ router
- Number of homes Servicing

Rigorously defined relationships

- controlOf
- attachedTo



Goal: Reusable Components

Physical Security

- Probability of Detection:

  $SDP = 1 - (1\text{-}DP(\text{Layer}_1) * (1\text{-}DP(\text{Layer}_2)) \ldots * (1\text{-}DP(\text{Layer}_n))$

  - e.g. 1- (1-.90)*(1-.80)= .98 (98%)

- Likelihood:

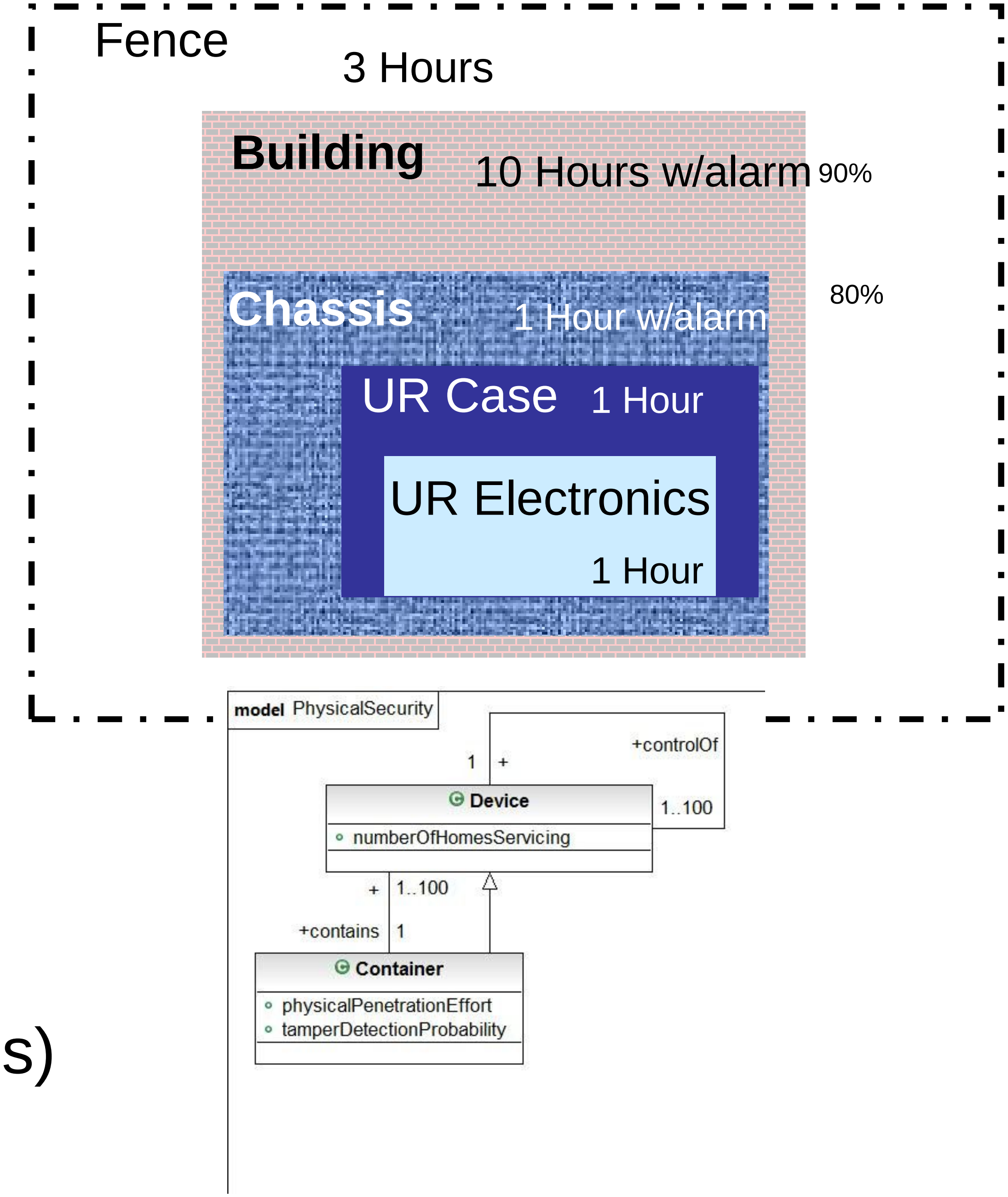
  S(Hours)*AttackerSkill

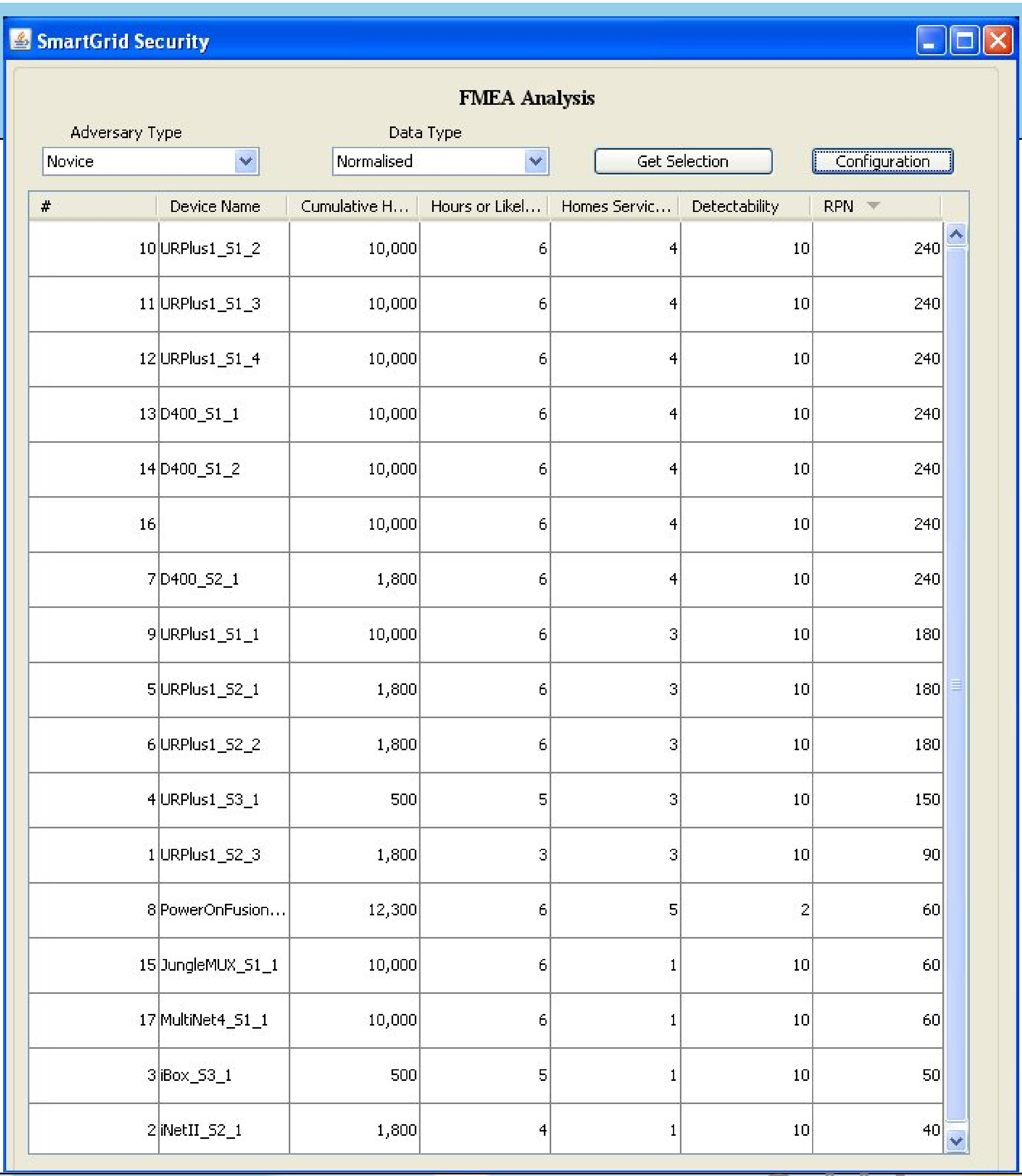
  e.g. 15 hours for Standard Expert

- Severity:

  S(NumberOfHomesServicing)

FMEA
(Failure Mode Effects Analysis)





FMEA Analysis

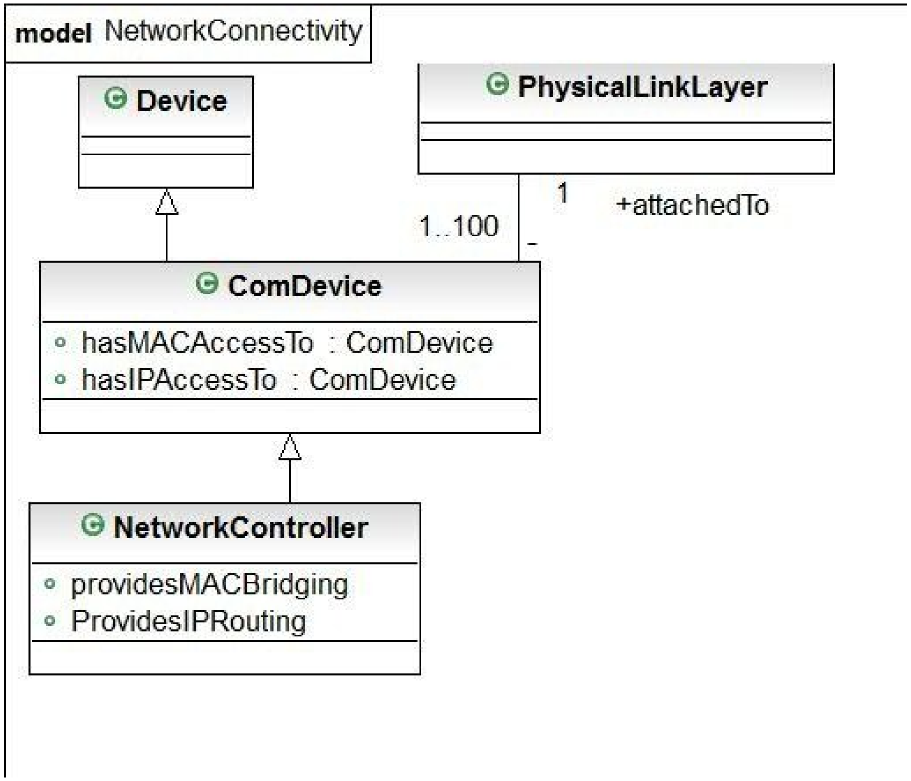
Adversary Type: Novice

Data Type: Normalised

#	Device Name	Cumulative H...	Hours or Likel...	Homes Servic...	Detectability	RPN
10	URPlus1_S1_2	10,000	6	4	10	240
11	URPlus1_S1_3	10,000	6	4	10	240
12	URPlus1_S1_4	10,000	6	4	10	240
13	D400_S1_1	10,000	6	4	10	240
14	D400_S1_2	10,000	6	4	10	240
16		10,000	6	4	10	240
7	D400_S2_1	1,800	6	4	10	240
9	URPlus1_S1_1	10,000	6	3	10	180
5	URPlus1_S2_1	1,800	6	3	10	180
6	URPlus1_S2_2	1,800	6	3	10	180
4	URPlus1_S3_1	500	5	3	10	150
1	URPlus1_S2_3	1,800	3	3	10	90
8	PowerOnFusion...	12,300	6	5	2	60
15	JungleMUX_S1_1	10,000	6	1	10	60
17	MultiNet4_S1_1	10,000	6	1	10	60
3	iBox_S3_1	500	5	1	10	50
2	iNetII_S2_1	1,800	4	1	10	40

Network Connectivity

- Given:
  - – Physical Connections
  - – Ethernet Switches
  - – IP Routers
  - – Firewalls
  - – …and their attributes
- Can deduce Layer 2/3 network connectivity

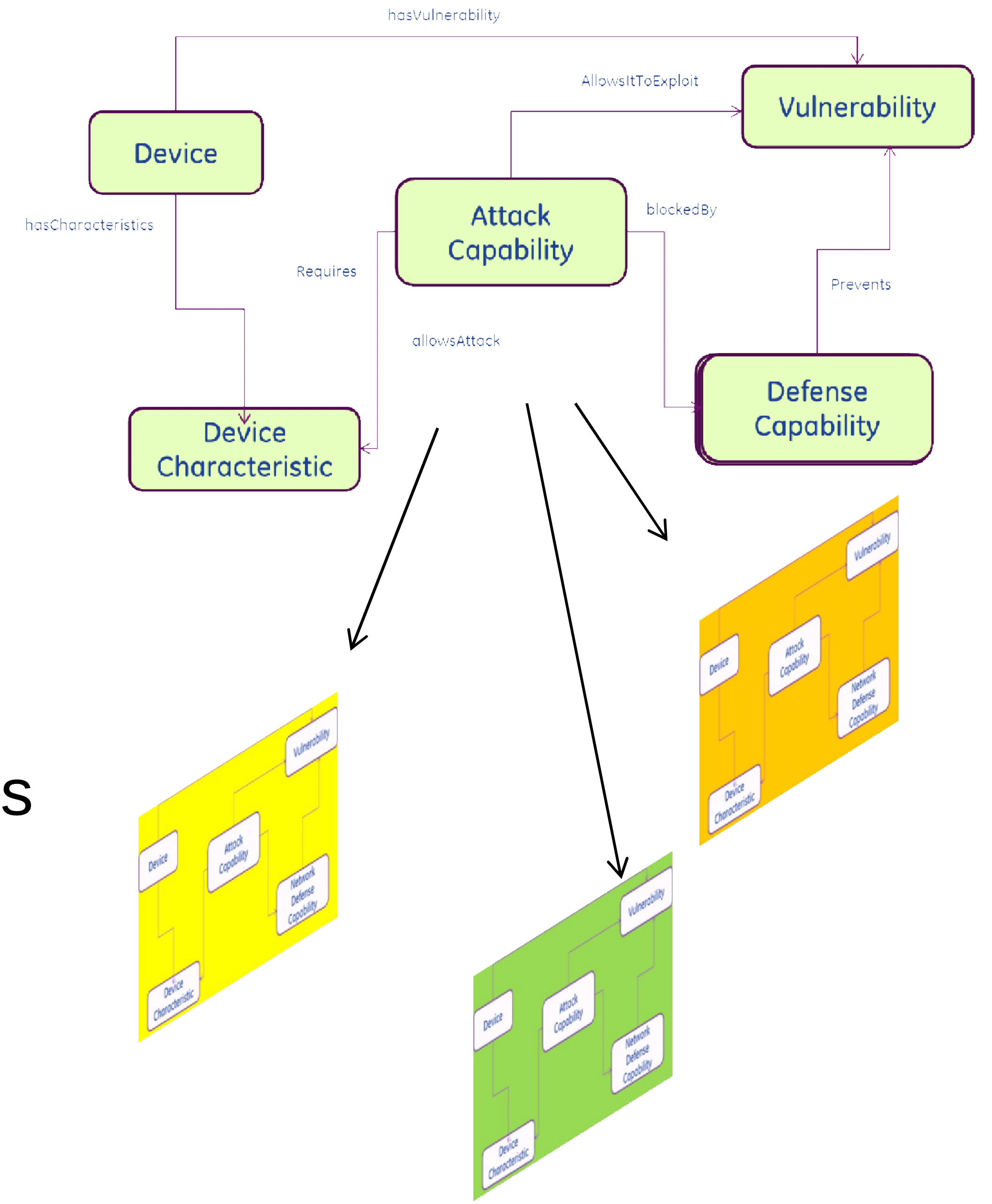


The Problem: Rule-based Vulnerabilities

- Required Semantic/Security/SADL expert
- Took days-weeks to add single attack
- Complex rules had to be added/modified
- Also addition of several unique attributes
- Rules interacted with existing rules
  - Incompatible
  - Adding attributes caused complexity

Solution: Model-based Vulnerability

- One reusable attack/defense model
- Rules are reusable
- Network Defense & Host Defense
- End users can add a new vulnerabilities
    - SADL/Semantic Experts no longer needed



Results

- Semantic Web technology can be used to
  - Provide measurable security w/automatic calculation
  - Measure physical & network-based protection
  - Combine several domains of knowledge
  - Perform what-if (defense-In-depth) analysis
  - Provide reusable rules for security independent of specific configuration and device characteristics

Conclusions

- A suitable ontology for security provides
  - A way to automatically calculate security metrics
  - A framework to combine knowledge from multiple security experts
  - A foundation for security tool interoperability by use of the Semantic Web

- Questions?