Simulation in Cyber Security

Andres Ojamaa

Institute of Cybernetics at TUT, Estonia

28–29.10.2013, MBJSDT Project Seminar, Laulasmaa

Outline

Definitions

Applications

Ideas and Problems for Future Development

A *simulation* is the imitation of the operation of a real-world process or system (over time).

The behaviour of a system is studied by developing a simulation *model*.

Once the model is developed and *validated*, it can be used to investigate a wide variety of “what if” questions about the real-world system.

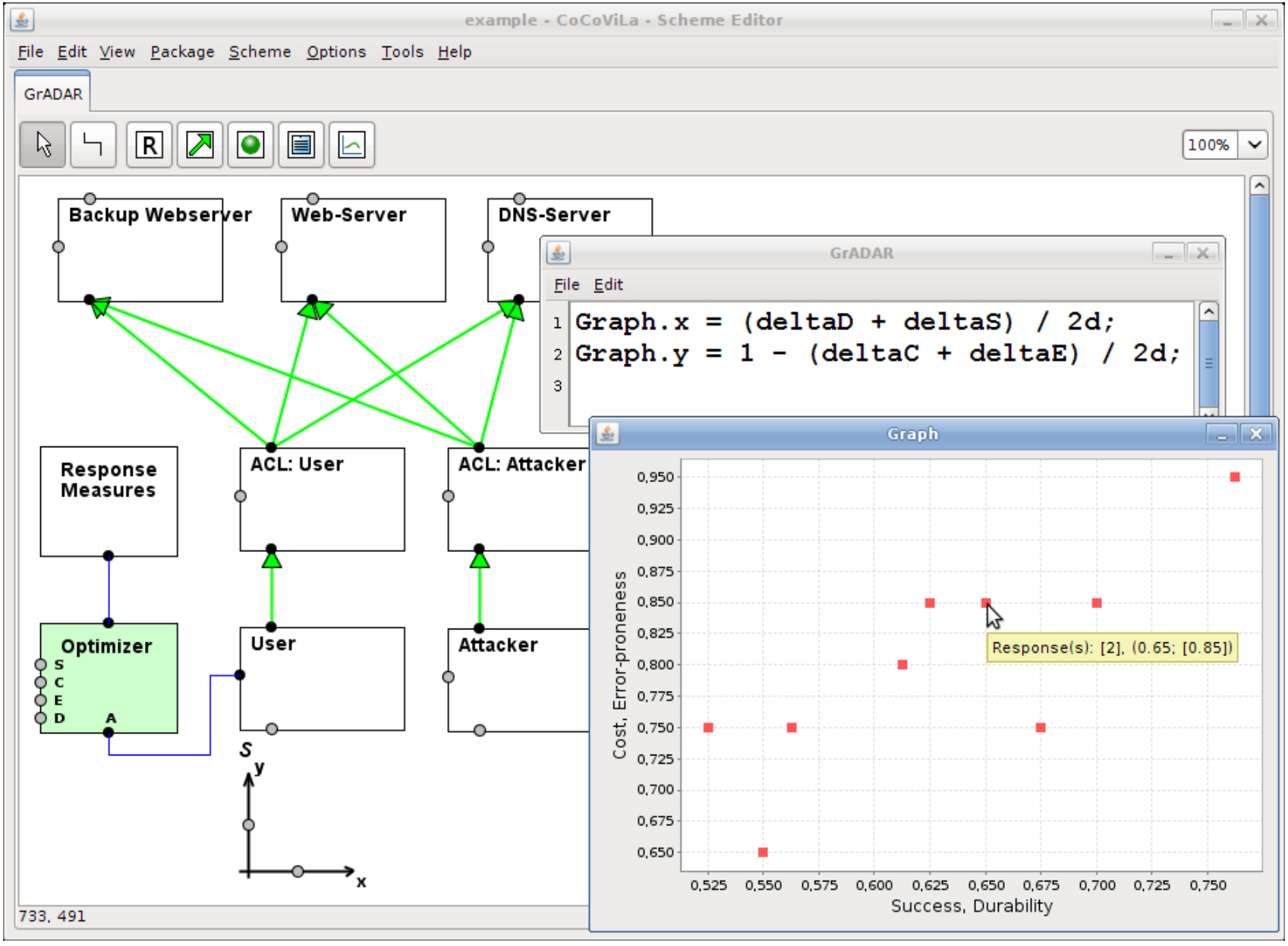
Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

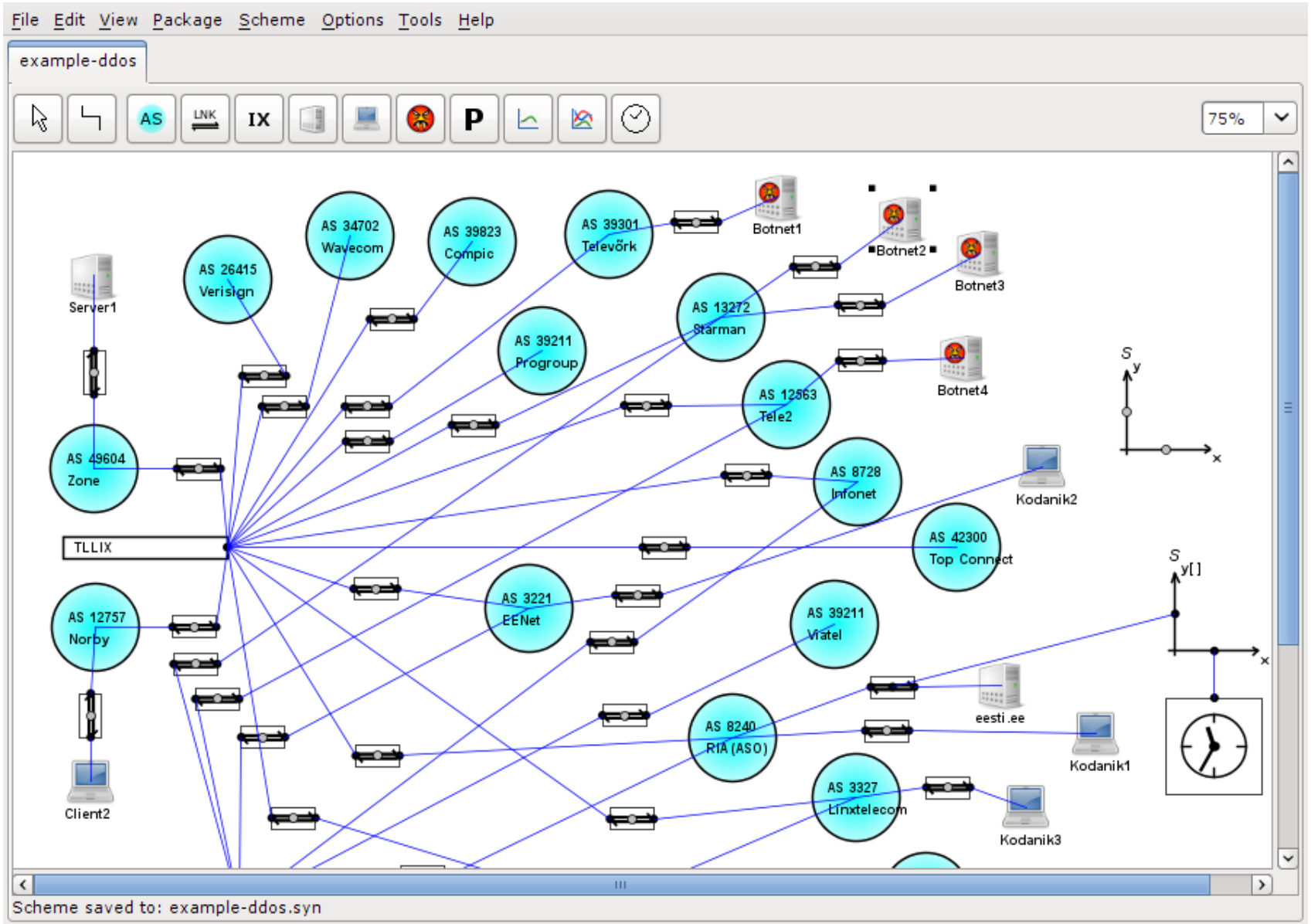
Information Technology (IT) security

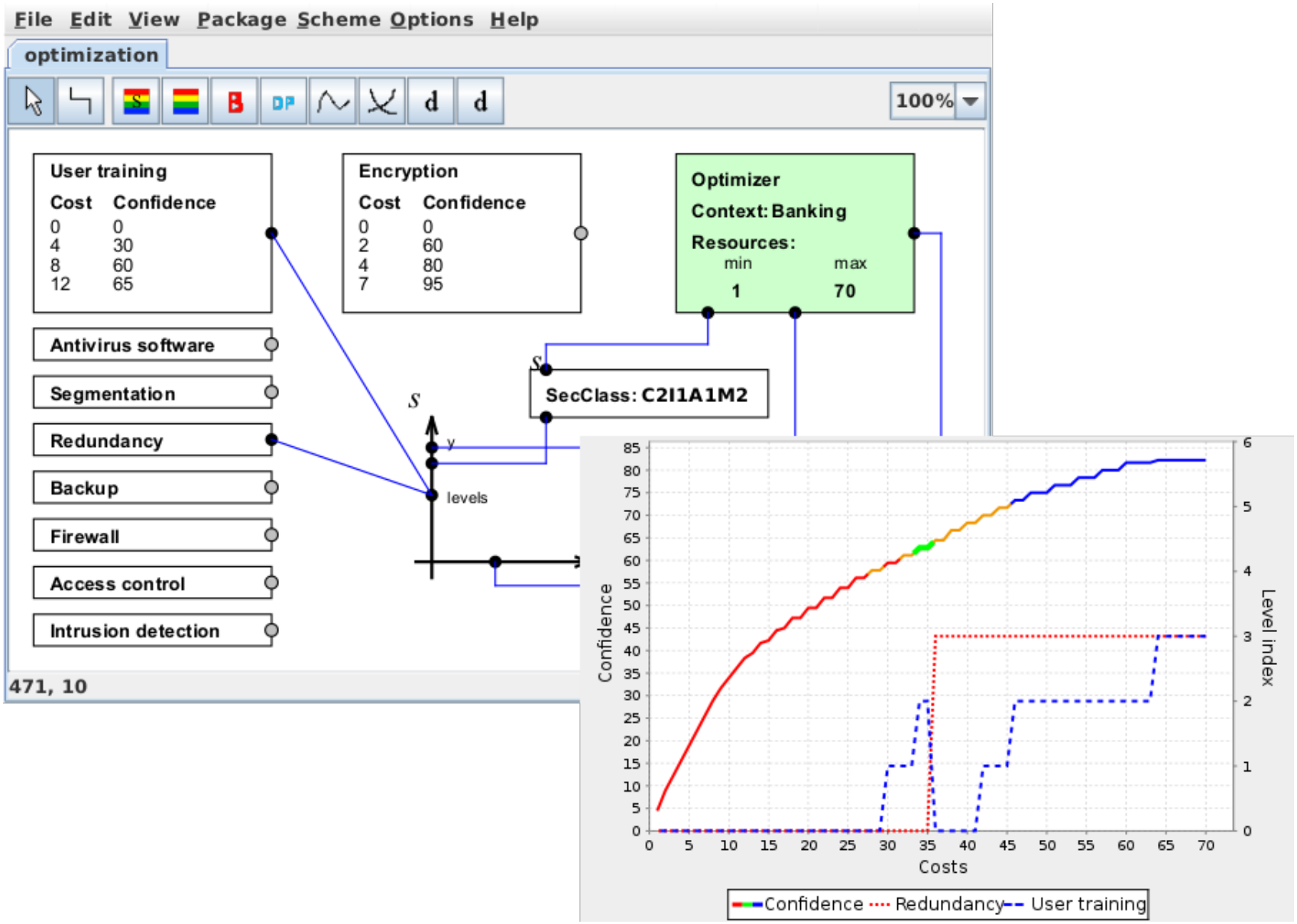
Cyber security?

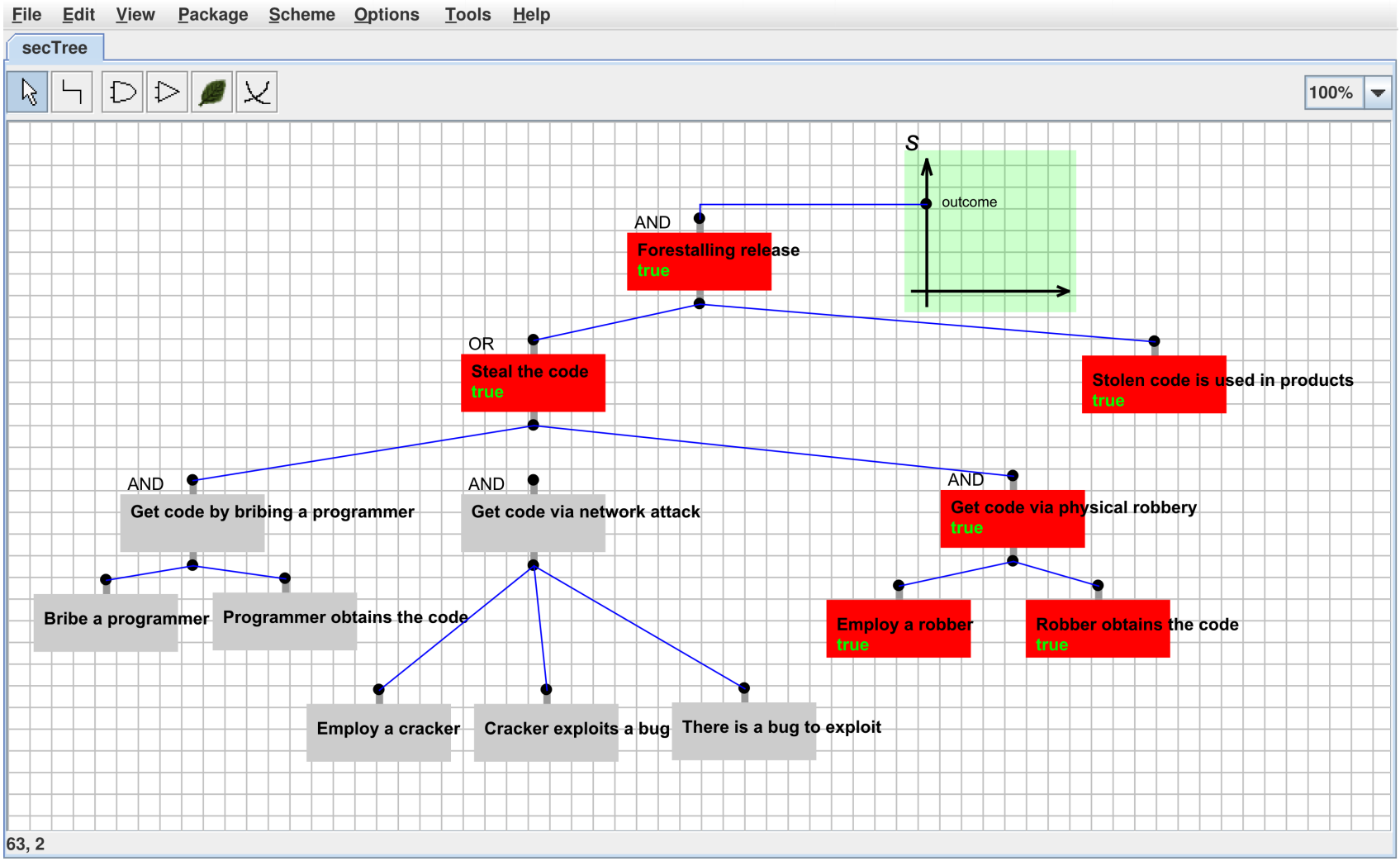
Properties of Cyber Security Field

- Many very different aspects (technical, social, . . .) are involved.
- Fast and invisible processes, large amounts of data
- Motivation of adversaries: economical, political, irrational
- Intelligent attackers, asymmetric attacks
- Overall security determined by the weakest link
- Running experiments on real systems sometimes impossible
- Artificial environment may be easier to simulate.


example - CoCoViLa - Scheme Editor
File Edit View Package Scheme Options Tools Help
GrADAR
100%
Backup Webserver
Web-Server
DNS-Server
GrADAR
File Edit
1 Graph.x = (deltaD + deltaS) / 2d;
2 Graph.y = 1 - (deltaC + deltaE) / 2d;
3
Response Measures
ACL: User
ACL: Attacker
Optimizer
S
C
E
D
A
User
Attacker
S
y
x
733, 491
Graph
Cost, Error-proneness
0,950
0,925
0,900
0,875
0,850
0,825
0,800
0,775
0,750
0,725
0,700
0,675
0,650
0,525
0,550
0,575
0,600
0,625
0,650
0,675
0,700
0,725
0,750
Success, Durability
Response(s): [2], (0.65; [0.85])


File Edit View Package Scheme Options Tools Help
example-ddos
AS
LNK
IX
P
75%
AS 34702
Wavecom
AS 39823
Compic
AS 39301
Televörk
Botnet1
Botnet2
Botnet3
AS 26415
Verisign
Server1
AS 13272
Starman
AS 39211
Progroup
Botnet4
AS 12563
Tele2
AS 49604
Zone
AS 8728
Infonet
Kodanik2
TLLIX
AS 42300
Top Connect
AS 3221
EENet
AS 12757
Norby
AS 39211
Viatel
eesti.ee
AS 8240
RIA (ASO)
Kodanik1
AS 3327
Linxtelecom
Kodanik3
Client2
S
y
x
S
y[]
x
Scheme saved to: example-ddos.syn


File Edit View Package Scheme Options Help
optimization
100%
User training
Cost Confidence
0 0
4 30
8 60
12 65
Encryption
Cost Confidence
0 0
2 60
4 80
7 95
Optimizer
Context: Banking
Resources:
min max
1 70
Antivirus software
Segmentation
Redundancy
Backup
Firewall
Access control
Intrusion detection
SecClass: C2I1A1M2
levels
471, 10
Confidence
Level index
Costs
Confidence
Redundancy
User training


File Edit View Package Scheme Options Tools Help
secTree
100%
S
outcome
AND
Forestalling release
true
OR
Steal the code
true
Stolen code is used in products
true
AND
Get code by bribing a programmer
AND
Get code via network attack
AND
Get code via physical robbery
true
Bribe a programmer
Programmer obtains the code
Employ a robber
true
Robber obtains the code
true
Employ a cracker
Cracker exploits a bug
There is a bug to exploit
63, 2

Ideas and Problems for Future Development

- Iterative MBST for research applications
- Version control of concept libraries, applications, results
- Scripting for users available from the GUI
- Guidelines for developing visual DSLs