Improving Resilience of Critical Information Infrastructures against Complex Threats - an Approach based on Operational Models

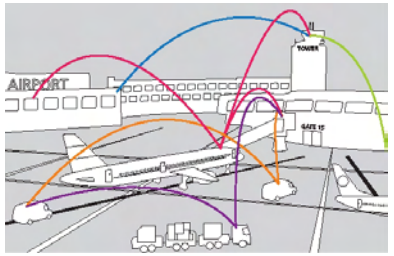
Roland Rieke[1]
rieke@sit.fraunhofer.de

Fraunhofer Institute for Secure Information Technology SIT,
Darmstadt, Germany
http://www.sit.fraunhofer.de/

IFIP WG 10.4, January 2007

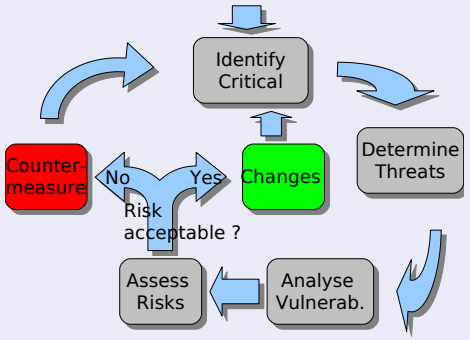
[1]Part of the work presented here was developed within the project SicAri being funded by the German Ministry of Education and Research.

Outline



Challenge: Protect Critical ICT Infrastructures

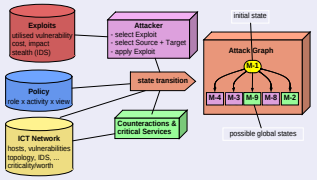
Process to guide the systematic protection

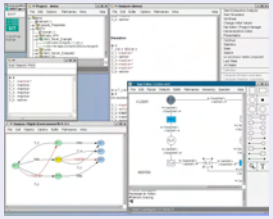


- *identify critical infrastructures*
- *determine the threats* - against those infrastructures
- *analyse the vulnerabilities* - of threatened infrastructures
- *assess the risks* - of degradation/loss
- *apply countermeasures* - where risk is unacceptable

Scope/Contributions of this work

Support this analytical CIIP process

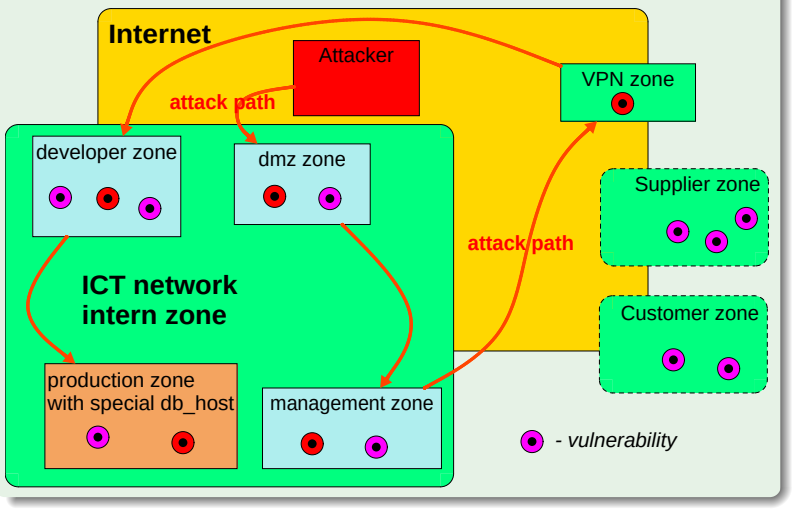




- supply a formal framework to specify critical (ICT) network infrastructures and threats against them
- provide tool based methods for a systematic evaluation
  ▸ tool
- assist with finally determining exactly what really needs protection & which strategy and means to apply

Example Scenario

Attack paths

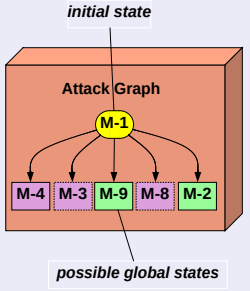


Attack Graphs and Blended Threats

Attack graphs

blended threat - a malware that uses a combination of different malware components (worm, trojan horse, virus) and uses multiple techniques to attack and propagate

attack graph - graph of all possible attack paths



Modelling critical (ICT) network infrastructures

Asset inventory

hosts
- products → vulnerabilities vulnerabilities
- services

trust relation between hosts

topology of network

IDS intrusion detection info

Asset prioritisation

criticality/worth of component

used for cost/benefit evaluations

Vulnerability Model

Vulnerability - weakness of a system to a threat

- identifier - Common Vulnerabilities and Exposures (CVE/CAN), MITRE Corporation
- preconditions - credentials, ...
- range - e.g locally/remotely exploitable
- impact type - e.g. get unauthorised/user/root access
  - National Institute of Standards and Technology (NIST) - classification and attribution to CVEs
- severity - reflects probability of exploitation
  - Common Vulnerability Scoring System (CVSS) - universal severity ratings for security vulnerabilities
  - US-CERT (Computer Emergency Response Team) - vulnerability metric

Vulnerability Template

E3: is target T vulnerable from source S by CAN_2003_0693 ?

V1: is target configured vulnerable ?
$(T, 'CAN\_2003\_0693') \in host\_vulnerability\_state$,

V2: is target currently running sshd ?
$(T, (('sshd', port), plvl\_service)) \in host\_service\_state$,

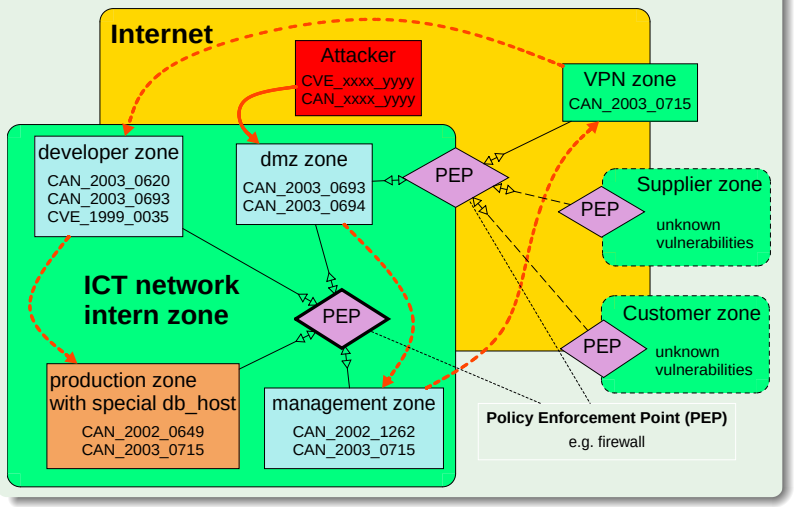
V3: is target reachable from source on port ssh (policy permission) ?
$PoI :=$
$reachable((S, T, port), role\_view\_activity\_seq(), role\_def\_seq())$,
$PoI \neq \emptyset$,

V4: effects for attacker (get sshd privileges on target)
$(T, plvl_T) \hookrightarrow Attacker\_plvl\_state$,
$(T, max\_access(plvl\_service, plvl_T)) \hookrightarrow Attacker\_plvl\_state$,

V5: direct impact (target is no longer running sshd)
$(T, (('sshd', port), plvl\_service)) \hookrightarrow host\_service\_state$

Security Policy Enforcement

Restrict possible attack paths



Network Security Policy Model

Policy definition

Organisation Based Access Control (Or-BAC) model

roles	represent	subjects (hosts)
activities	represent	actions (service, e.g. ssh)
views	represent	objects (target)

Permissions

organisation × role × activity × view × context

Organisation

structuring

Context

e.g. default, emergency

Exploit Model

Exploit - special type of threat (¬ accident/malfunc.)

Vulnerability

- exploits one or more vulnerabilities

Properties

- cost
- detectability

Additional impact

- on attacker (e.g. get confidential information)
- on host (e.g. shut down service)
- effects on network (e.g. disturbed connection)

Exploit Template

Exploit e.g. *CAN_2003_0693 ssh exploit*

Bind: attack from host S to host T $(S, T, plvl_S, plvl_T)$

E1: intruder knows exploit
$Exploit \in Attacker\_known\_exploits\_state$,

E2: selection of source and target host
$(S, plvl_S) \in Attacker\_plvl\_state$,
$rank(plvl_S) \geq rank('user')$,
$(T, plvl_T) \in Attacker\_plvl\_state$,

E3: is target vulnerable from source
$is\_vulnerable(S, T, Exploit, plvl_T)$,

E4: attacker gets all knowledge of host T
$get\_knowledge(T)$,

E5: intrusion detection check $ids\_check(Exploit, S, T)$,

E6: assign cost benefit values $cost\_benefit(Exploit, T, 'root')$

E7: no additional impact in this example

Attacker Model

Attacker - subject/entity executing an exploit

Attacker profile

- known exploits
  (e.g. assume the attacker uses only exploits for vulnerabilities with a severity above a given threshold)
- known hosts, credentials, ...

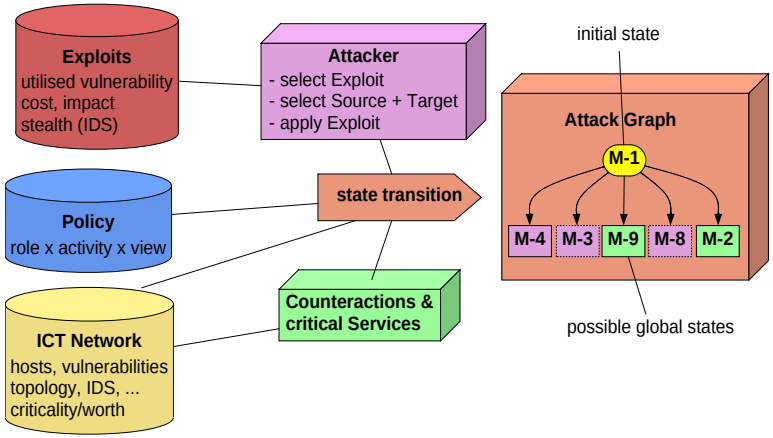
Attacker strategy

- select known exploit
- select source and target (monotonic benefit)
- apply exploit

Attacker collaboration

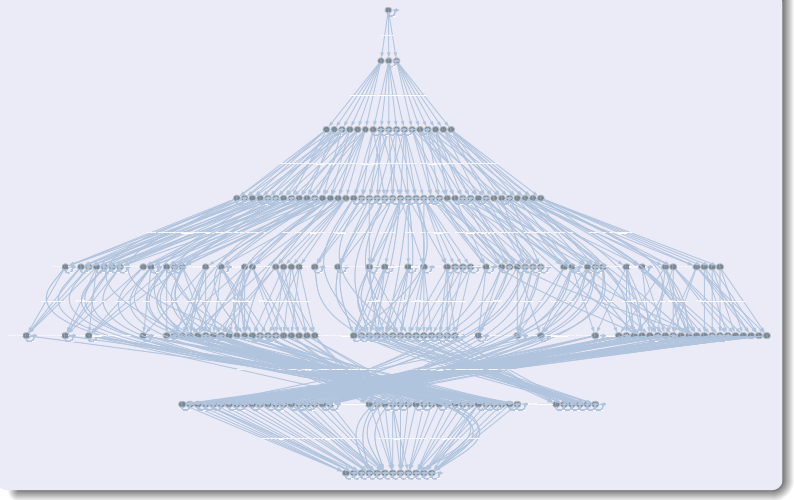
- the model allows multiple attackers (role based)

Attack Graph Computation



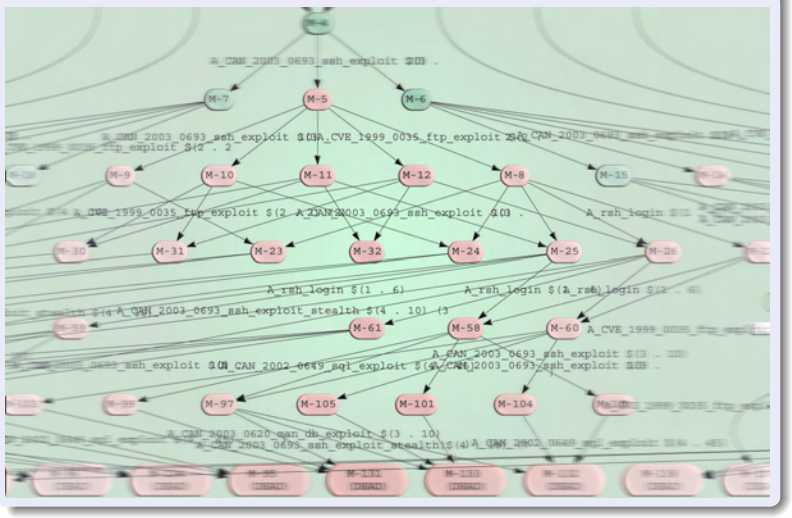
Motivating Analysis Methods

Attack graph of small scenario - so what ?

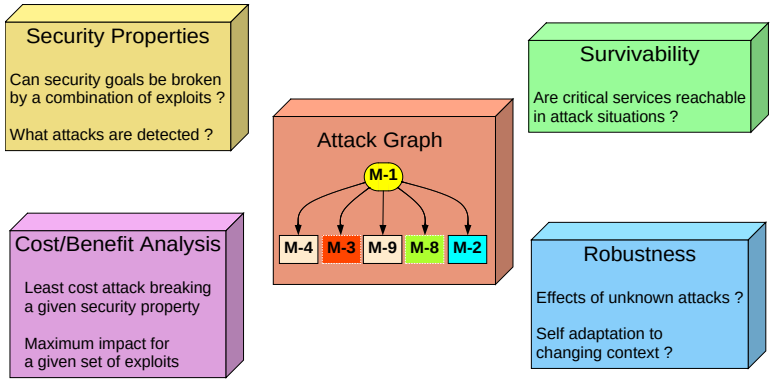


Motivating Analysis Methods

Attack graph magnification - zoom in $\neq$ focus ?

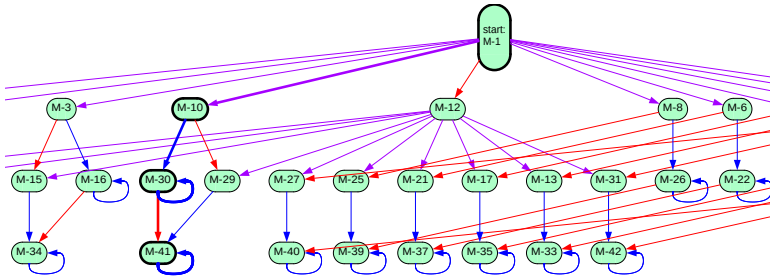


Security Risk Analysis

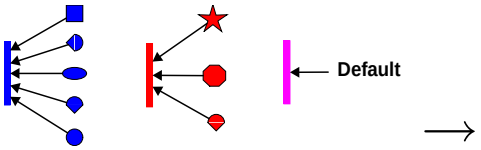


CIIP vs. Complex Threats
Roland Rieke
CIIP Process
Example Scenario
Modelling ICT Infrastructures
Network Security Policies
Modelling Threats
Attack Graph Computation
Assess Risks
Countermeasures
Problems
Related work
Outlook

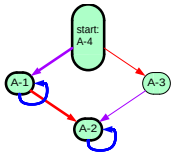
Abstract Representations (alphabetic lang. hom.)



Mapping (property preserving)

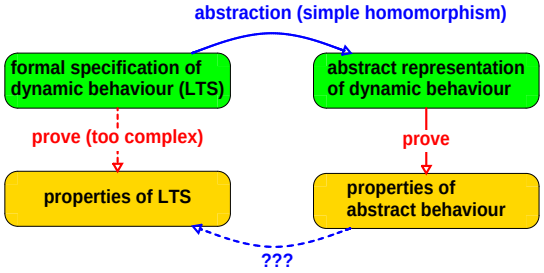


Minimal Automaton

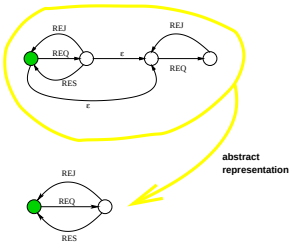


CIIP vs. Complex Threats
Roland Rieke
CIIP Process
Example Scenario
Modelling ICT Infrastructures
Network Security Policies
Modelling Threats
Attack Graph Computation
Assess Risks
Countermeasures
Problems
Related work
Outlook

Property Preserving Abstractions



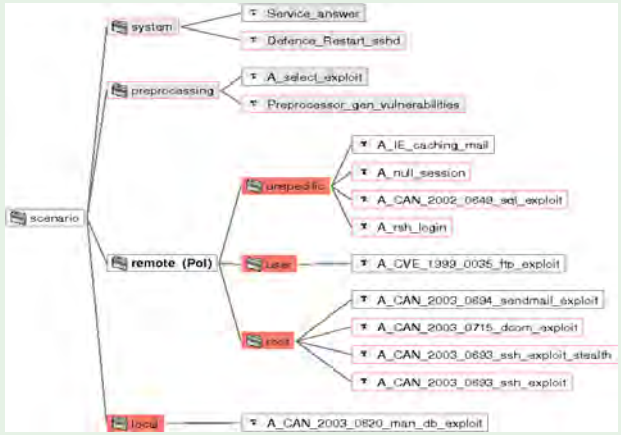
Abstract representation may hide restricted behaviour



CIIP vs. Complex Threats
Roland Rieke
CIIP Process
Example Scenario
Modelling ICT Infrastructures
Network Security Policies
Modelling Threats
Attack Graph Computation
Assess Risks
Countermeasures
Problems
Related work
Outlook

Example Scenario: Risk Visualisation

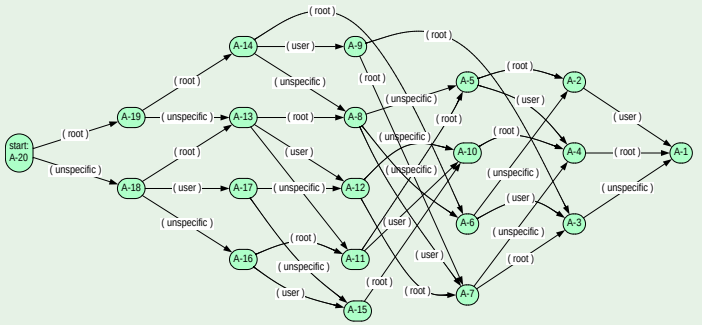
Step 1 - Define an abstract representation



exploit → range + impact

Example Scenario: Risk Visualisation

Step 2 - Compute the abstract representation

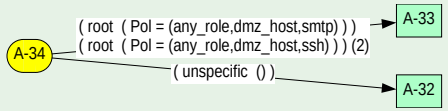


178 states and 1309 edges → 20 states and 37 edges

Example Scenario: Risk Visualisation

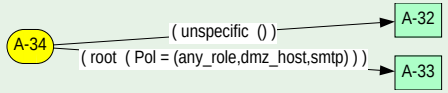
Step 3 - Optionally refine the mapping

now details about related policies are visible



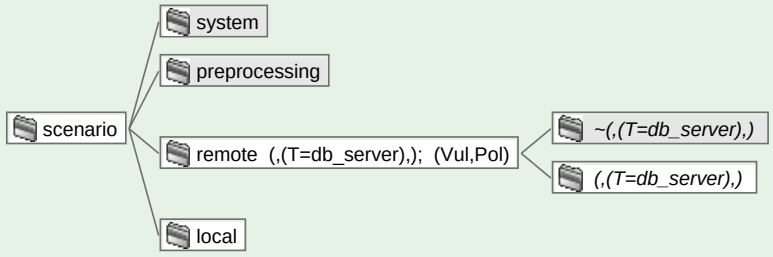
Step 4 - Adapt/Optimise the system configuration

visualise impact of policy changes in the abstract representation



Using Predicates to define Abstractions

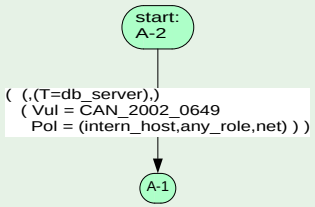
Step 1 - Define a mapping



- the mapping $(T = db\_server)$ matches only those transitions that model direct attacks to the target host *db_server*

Results

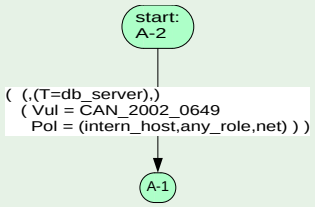
Step 2 - Compute the Abstract Representation



- In the current policy configuration attacks to the *db_server* are possible.
- Those attacks are based on exploits of the vulnerability *CAN*_2002_0649.
- They are utilising the policy rule (*intern_hosts*, *any_role*, *net*).

Countermeasures

Step 4 - Adapt/Optimise the System Configuration

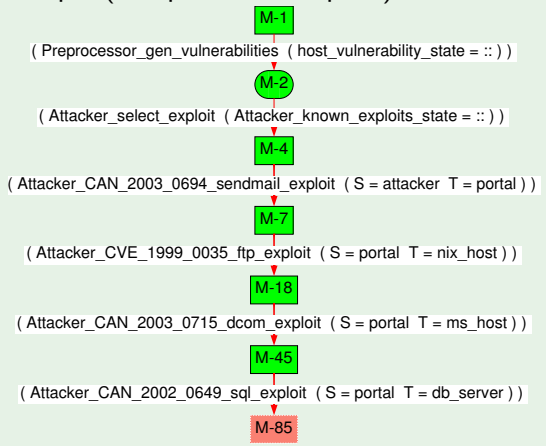


- uninstall the product that is hurt by the vulnerability *CAN*_2002_0649, or,
- restrict the internal hosts in their possible actions by replacing the policy (*intern_hosts*, *any_role*, *net*) with a more restrictive one.

Analysis: Check Security Properties

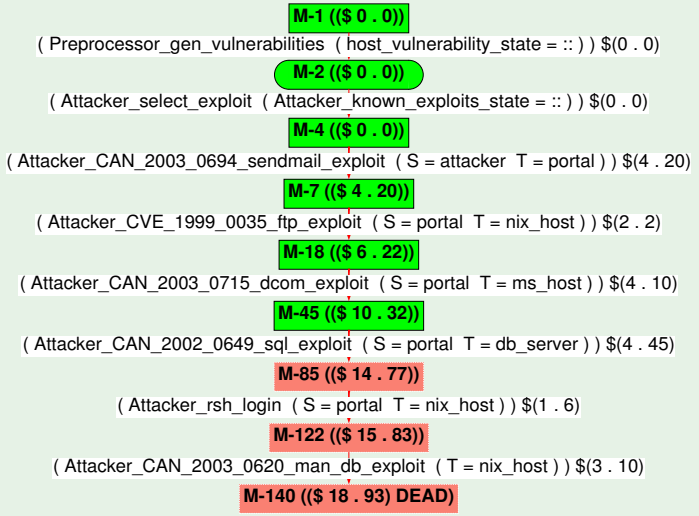
Security property: Attacker can not access *db_server*

- Counterexample (complete attack path)



Cost-Benefit Evaluation

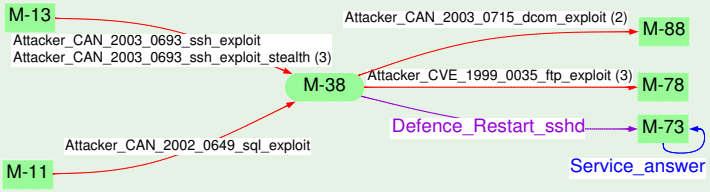
Find max. attacker impact for a given set of exploits !



Survivability: Service Continuity and System's Countermeasures

Can client get answers from server if network is attacked ?

- add formal models of e-service and countermeasures
- example: *db_server* always tries to answer queries from host *teleworker*; assume *sshd* is running the *portal* ("ssh-tunnel")
- add system countermeasure, e.g. restart *sshd* on *portal*



State Space Explosion ? YES !!!

Solution concepts

- model only critical aspects of the system
- operate on higher level models (summarising, hide details, use abstract type)
- explore only interesting parts of the state space
- assume monotonic attacker behaviour

- use property preserving abstractions
- compositional method
  → to-do item: apply in CIIP context

Related Work

Attack graphs

- Steven Noel, Sushil Jajodia, Paul Ammann et al, Center for Secure Information Systems, George Mason University
- Oleg Sheyner, Jeanette Wing et al, CMU
- Laura Swiler, Cynthia Phillips et al, Sandia National Laboratories, Albuquerque
- Igor Kotenko, Mikhail Stepashkin, SPIIRAS, St. Petersburg

Or-BAC

- Frédéric Cuppens et al.

ICT network modelling

- Benjamin Morin, Hervé Debar et al.

Asynchronous product automata

- Formal methods team, Fraunhofer-SIT

Related Work

Vulnerability assessments

MITRE Corporation: Common Vulnerabilities and Exposures (CVE/CAN) descriptions.
`http://www.cve.mitre.org/`

National Institute of Standards and Technology (NIST): Vulnerability *range* and *impact type* assessments.
`http://nvd.nist.gov/`

Common Vulnerability Scoring System (CVSS): CVSS provides universal severity ratings for security vulnerabilities.
`http://www.first.org/cvss/cvss-guide.html`

US-CERT: Another vulnerability metric.
`http://www.kb.cert.org/vuls/html/fieldhelp#metric`

Related Work

Standards

BS 7799-3: Guidelines for information security risk management (2006)

ISO 27005: Emerging standard covering information security risk management (based on BS7799-3)

ISO 27004: Emerging standard covering information security management measurement and metrics (not expected to be published in the immediate term)

EU FP6 projects

IRRIIS: Integrated Risk Reduction of Information-based Infrastructure Systems

CRUTIAL: Critical Utility InfrastructurAL Resilience

CI2RCO: Critical Information Infrastructure Research Co-ordination Project

Looking further . . .

Towards robustness and attack resiliency in the context of dynamic environments

Self-adaptation to changing context - plasticity

monitor system behaviour, intrusions, anomalies

complex event processing ⇒ situated risk evaluation

policy-based automated threat response ⇒ impact minimisation ▸ threat-response

multi-scale models organisational & ICT networks ⇒ integrated approach (complexity theory) ▸ musca

Reasoning about incomplete or uncertain knowledge

- combine abstraction & plausibility/probability
- reasoning about unknown vulnerabilities

Develop metric for security/robustness

CIIP vs. Complex Threats
Roland Rieke
CIIP Process
Example Scenario
Modelling ICT Infrastructures
Network Security Policies
Modelling Threats
Attack Graph Computation
Assess Risks
Countermeasures
Problems
Related work
Outlook

Apply Approach to Networked Infrastructures

Support critical networked infrastructure protection

model networked infrastructures, the threats, and the mutual dependencies

analyse interplay of component vulnerabilities & threats

reveal complex threat combinations, and cascading effects of | malfunctions | accidents | attacks |

raise risk awareness

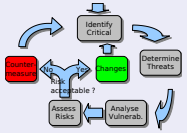
support systematic evaluation of possible solutions

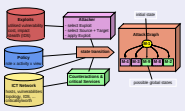
aim at optimising security & protection with given resources

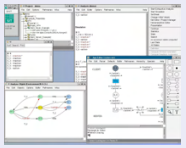
CIIP vs. Complex Threats
Roland Rieke
CIIP Process
Example Scenario
Modelling ICT Infrastructures
Network Security Policies
Modelling Threats
Attack Graph Computation
Assess Risks
Countermeasures
Problems
Related work
Outlook

Conclusions

Objective: Support analytical CIIP process







model based approach
to specify critical infrastructures and threats

analysis methods and tools
reveal complex threat combinations and
support systematic evaluation of alternatives

complexity inherits state space explosion
solutions: clever modelling, abstraction, composition

generalisation and extensions
adaptation to other contexts,
self-adaptation, security/robustness metric

CIIP vs. Complex Threats
Roland Rieke
CIIP Process
Example Scenario
Modelling ICT Infrastructures
Network Security Policies
Modelling Threats
Attack Graph Computation
Assess Risks
Countermeasures
Problems
Related work
Outlook