Cyber security risks:
Comprehensive mitigation through technical, contractual and financial mitigation mechanisms

PROFESSOR GEORGE SPANOUDAKIS
CITY, UNIVERSITY OF LONDON

KEYNOTE PRESENTATION, FedCSIS 2019

Outline

- Cyber threats: the current picture
- Cyber risks: multiple level assessment & management
- Cyber risks: key challenges
- An integrated cyber security assurance approach
- Capabilities of integrated cyber security assurance
- The models
- Model based assessments
  - Intelligence sharing
  - Penetration testing
  - Monitoring
  - Hybrid assessments
  - Risk assessment
- Cyber range
- Cyber security SLAs
- Cyber insurance

Cyber risks: the current picture

- Mail and phishing attacks have become a primary threat (rapid increase of using HTTPs sites for phishing)
- Crypto miners have become an important monetization vector for cyber-criminals.
- State-sponsored threat agents
- Emergence of IoT environments vulnerability due to missing protection mechanisms in low-end IoT devices and services
- Fileless attacks (77% of attacks)
- Malware targeting critical infrastructures (e.g., Triton that targets safety instrumented industrial systems and processes)
- Growth of open source malware (e.g., Mimikatz, Powerspoilt) as it is harder to attribute malware and has reduced development cost

As reported by ENISA's 2018 Threat Landscape Report
(https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018)

Cyber risks: Multiple level assessment & management

HORIZON	*STRATEGIC*	+ strategic commitments + evolution	+ strategic commitments + evolution	+ strategic commitments + evolution
HORIZON	*TACTICAL (medium term)*	+ adaptation	+ adaptation	+ adaptation
HORIZON	*TACTICAL (short term)*	threat intelligence, risk assessments for security categorization; security control selection, implementation, and assessment; information system and common control authorization; and security control monitoring	assessment of risk in connection with mission/business processes, enterprise architecture, or the funding of information security programs.	assessment of systemic information security-related risks associated with organizational governance and management activities
		SYSTEM LEVEL	*BUSINESS PROCESS LEVEL/MISSION*	*ORGANISATIONAL*
		LEVEL / TIER		

Key challenges

- Effective and comprehensive threat information exchange
- Enhanced analytics & automation for establishing the S&P posture of an organization and/or supply supply chains
- "Out-of-the-box thinking" and support S&P risk management

Key challenges: Effective & Comprehensive Threat info exchange

- Fragmented taxonomies, no common vocabulary
  - Threat, vulnerabilities, weaknesses etc.
- Lack of contextual information
- Lack of threat triage (aka prioritization)
  - No prioritization, unclear basis of prioritization where it exists
- Unstructured information
  - Mostly free text
  - Very basic identification
- Trustworthiness
  - Trustworthiness of info, providers, threat platform operator
  - Lack of comprehensive threat info handling protocols & configurable access control mechanisms
- Diverse data formats and APIs
  - E.g., STIX 1.x, OpenIOC and MISP JSON

Key challenges:
Enhanced analytics and automation

- Automated assessments
  - For all levels of risk management (system, business processes & mission, organizational)
  - For all horizons of risk management (tactical short term, tactical medium term & strategic)
- Need for complementary assessments (e.g., vulnerability assessment, penetration testing, monitoring, consideration of existing certificates)
- Need for hybrid assessments, combining outcomes of individual assessments
  - Complementary outcomes
  - Conflicting outcomes
- Need for incremental assessments
- Automated adaptation and evolution of assessment schemes

CITY

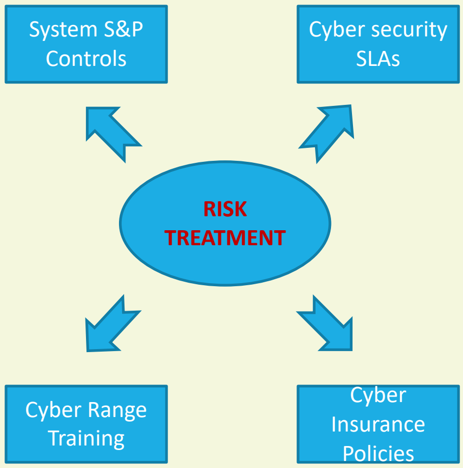
Key challenges:
Enhanced analytics and automation (cont'd)

- Difficult to generate executable assessments from higher level specifications
  - Difficult to propagate lower level system risk assessment to higher level organizational and business risk assessment
- Automated adaptation of
  - Security assurance models
  - Security assessments
- 0-day attacks

CITY

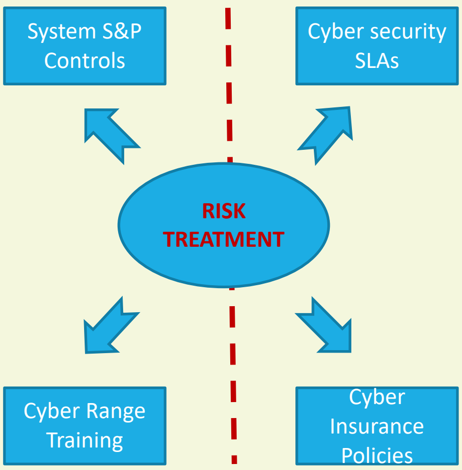
Key challenges:
"Out-of-the-box thinking" for risk treatment

- "Out-of-the-box thinking" for S&P risk controls
  - Traditional security controls
  - Risk treatment mechanisms for systems crossing organizational boundaries in service supply chains
    - Establishment, monitoring and management of Cyber Security Service Level Agreements (CSLAs)
    - Establishment, monitoring and management of Cyber Insurance Policies (CIPs)
  - (intra and inter organizational) cyber security training
- Effective decision support for risk treatment, through a mixture of
  - Development/deployment of own security mechanisms
  - Cyber range training
  - Coverage through CSLAs, CIPs?
- Comprehensive modelling for (cyber) security assurance is essential



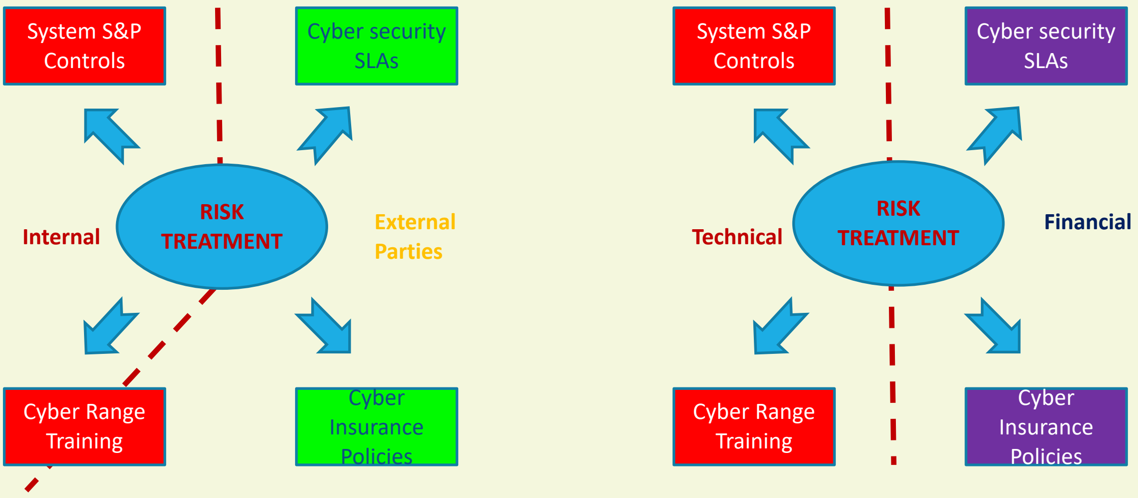
Key challenges:
"Out-of-the-box thinking" for treatment

Risk Avoidance
Risk Mitigation



Risk Transfer
(sharing)

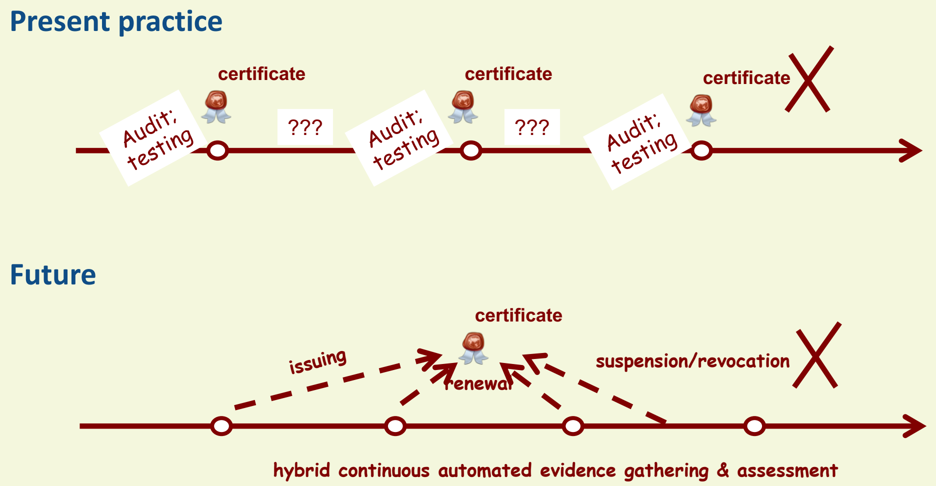
Key challenges:
"Out-of-the-box thinking" for treatment



An integrated cyber security assurance approach

- Security and privacy assurance centric
  - To enable continuous and comprehensive assessment in line with regulatory requirements
- Model driven
  - Based on comprehensive S&P assurance models
  - To provide a common (and uniform) basis for all sorts of reasoning required
  - To provide extensibility

An integrated cyber security assurance approach

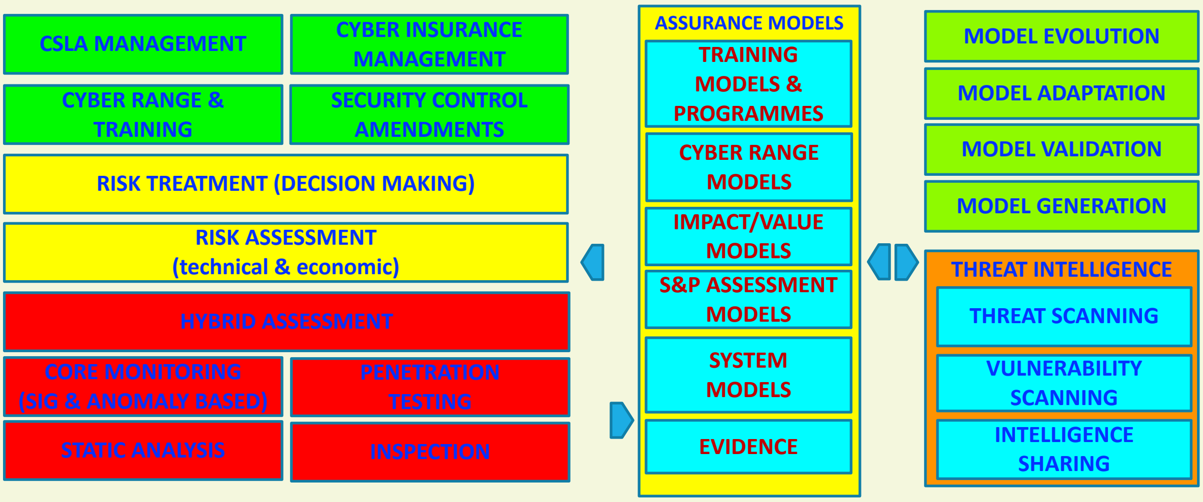


Capabilities for Integrated Cyber Security Assurance

- CSLA MANAGEMENT
- CYBER INSURANCE MANAGEMENT
- CYBER RANGE & TRAINING
- SECURITY CONTROL AMENDMENTS
- RISK TREATMENT (DECISION MAKING)
- RISK ASSESSMENT (technical & economic)
- HYBRID ASSESSMENT
- CORE MONITORING (SIG & ANOMALY BASED)
- PENETRATION TESTING
- STATIC ANALYSIS
- INSPECTION

THREAT INTELLIGENCE
- THREAT SCANNING
- VULNERABILITY SCANNING
- INTELLIGENCE SHARING

Capabilities for Integrated Cyber Security Assurance



CITY

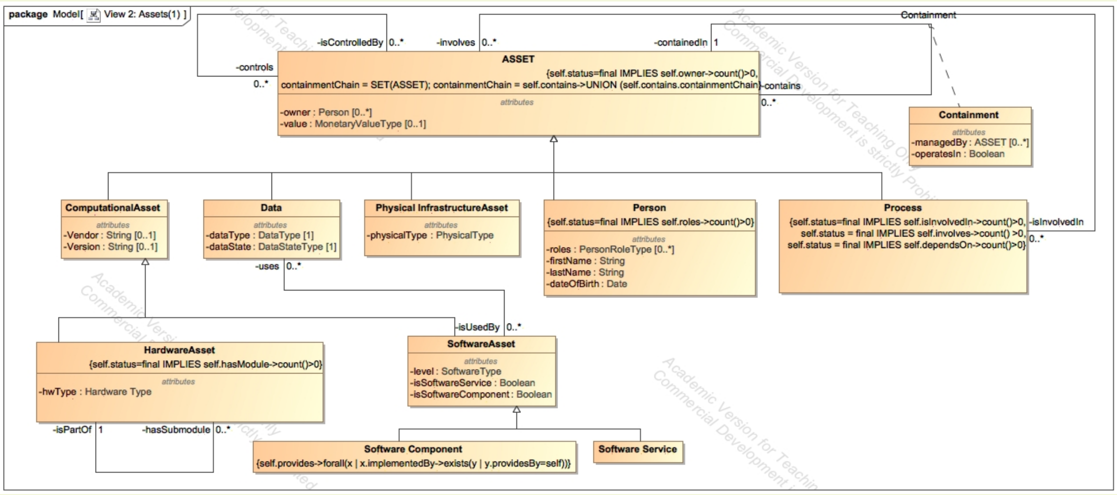
The Models

CITY

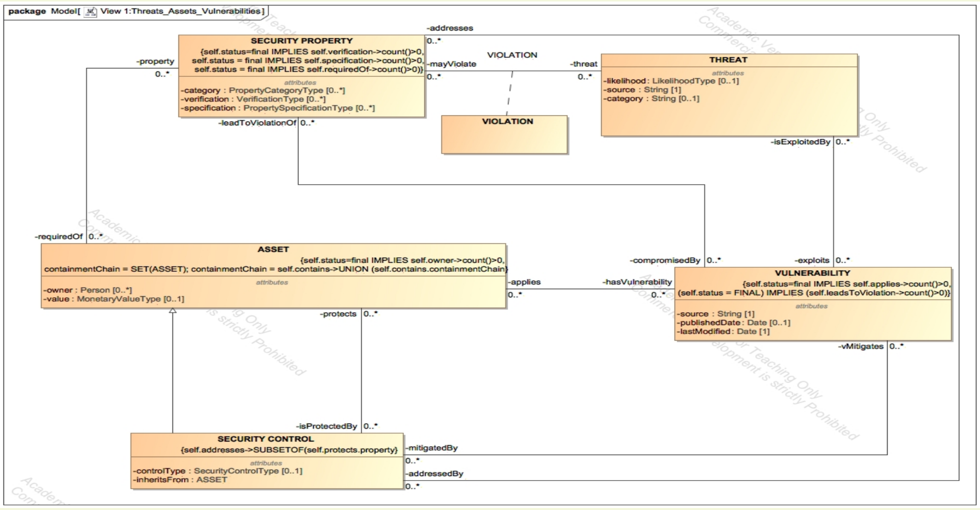
The Models: overview

- System models
- Assessment models
  - S&P Assessment models
  - Impact models
  - Risk models
  - Value models
- Cyber range & training models

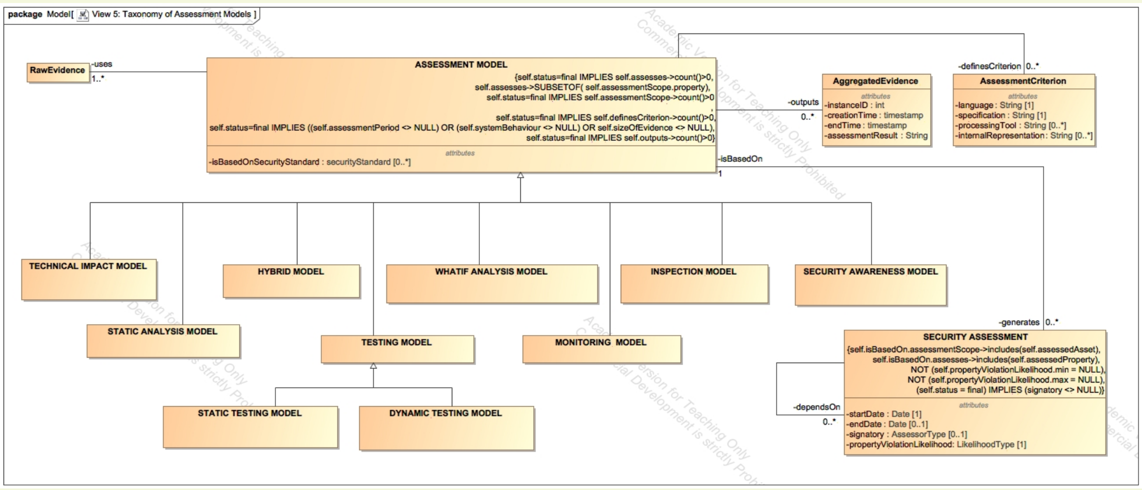
The Models: Assets



The Models: Threats & Vulnerabilities



The Models: Assessments



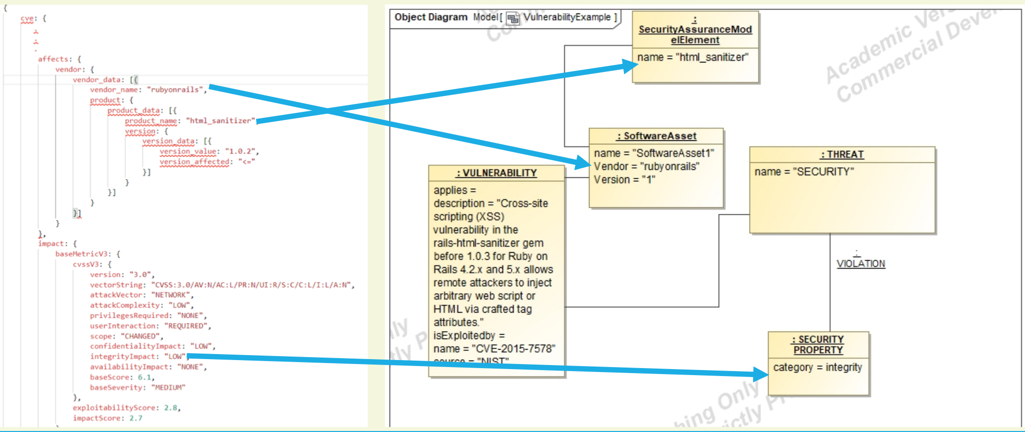
Intelligence Sharing

Intelligence Sharing: Vulnerability/Threat Scanning

- Get vulnerabilities from NISTdatabase
- Create common platform enumeration descriptors (CPEs) for Software and Hardware assets
- For each CPE find the vulnerabilities that can apply
- Store for each asset the common vulnerabilities and exposures (CVEs) that are applicable
- In-depth, more sophisticated search for vulnerabilities (based on asset relations such as control and containment relations

Intelligence Sharing: Vulnerability/Threat Scanning

Example



Intelligence Sharing: key challenges

- Open standard interfaces
- Privacy preserving sharing
- Intelligent sharing (what is important to send) – ML and Decision making
- Contextualization

Penetration Testing

Penetration Testing: overview

- Executing pre-encoded tests for known vulnerability and threats
- Automated generation of system model elements: assets, properties, threats, vulnerabilities and assessments
- Currently supported tools
  - OpenVAS:
    - vulnerabilities scanner (some are related to CVE/CVSS 2.0; some not)
    - covers platform and application layer software components, exposed to the net
  - Nessus:
    - vulnerabilities scanner (all alerts are related to some threat, only some are related to CVE/CVSS v3.0
    - covers platform and application layer software components, exposed to the net
  - Zap:
    - web apps scanner;
    - deeper checks (all active directories accessible), missing tags from HTTP requests, exposed cookies, unencrypted login pages
  - Nmap:
    - open gates, web apps listening to each port (SSH), software

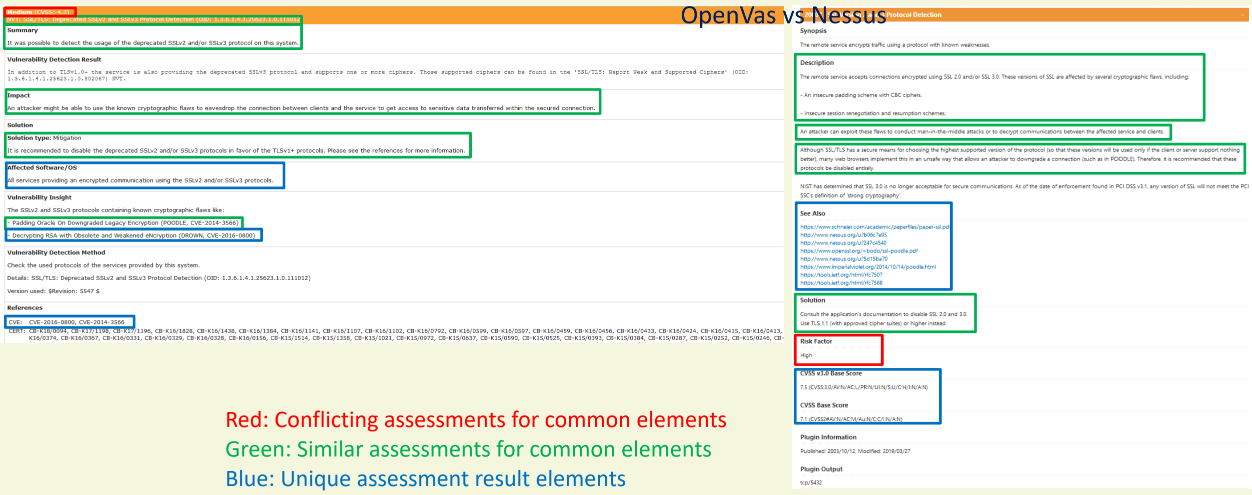
Penetration Testing: model driven

Assessment models:

- Map outputs to model elements
- Define patterns for content processing:
  - Keyword processing
  - Information extraction
  - Machine learning

OpenVas	Nessus	Nmap	Zap	Assurance Model
Summary	Synopsis	-	-	AssessmentResult.summary
-	Description	-	Description	AssessmentResult.description
Solution	Solution	-	Solution	Recommendation
Impact	Impact (in description)	-	Impact (in description)	AssessmentResult.Impact
Vuln. Detection Result	Plugin Output	Script output	Script output	Evidence
Port number & Protocol	Port number & Protocol	Port number & Protocol	Port number	Netport.port Netport.protocol
IP Address	IP Address	IP Address	IP Address	NetworkAdapter.Ipinfo
Product name	Product name	Product name	-	SoftwareAsset.Name
Product version	Product version	Product – extra info	-	SoftwareAsset.Version
Operating System	Operating System	Operating System	-	SoftwareAsset.Name, SoftwareAsset.Version
CVE	CVE	CVE	CVE	CVECore
Cvssv2	Cvssv2	-	-	CVSSV2
-	Cvssv3	-	-	CVSSV3
CPE	CPE	CPE	-	CPE
QoD	-	Confidence	-	QoD
Network Vulnerability Test	Plugin	Script	Script	NVT
Hostname	Hostname	Hostname	Hostname	SoftwareAsset.Name

Penetration Testing: Conflicting results



Red: Conflicting assessments for common elements
Green: Similar assessments for common elements
Blue: Unique assessment result elements

Penetration Testing: Open Issues

- Conflicting outcomes → hybrid assessment models
- More sophisticated processing
- Standards (especially for threats)
- Better context information

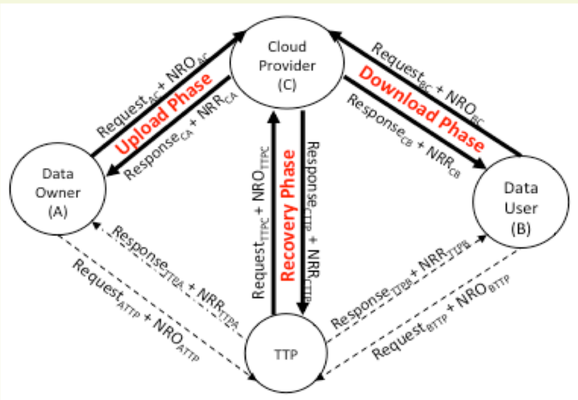
Monitoring

Monitoring: overview

- Depending on what needs to be assessed, monitoring should cover
  - The network
  - The computational infrastructure
  - The OS and any middleware layer
  - The application layer
  - Any devices connected to the system
- What may be monitored
  - Indicators of attacks (threats)
  - Indicators of system compromise (IOCs)
  - Indicators of correctness of operation of security controls
  - Performance of cyber range programmes as a whole and of trainees taking them

Monitoring: example

Non repudiation through Trusted Third Party (TTP)



Monitor whether the cloud provider implements correctly

- The upload phase
- The download phase
- The recovery phase

Implements correctly?

Produces an NRR to the relevant party (A, B or TTP) within the required time period

Establish sufficiency conditions for assessment

Check for anomalies. *see [4]*

Monitoring: example (cont'd)

Monitoring formulae for **upload phase** (in abstract syntax of Event Calculus)

Monitoring Rule:

Happens(e(_id1, _A, _C, REQ, RQS_{AC}, _C), $\_t_{req}$, [$\_t_{req}$,$\_t_{req}$]) ⇒
Happens(e(_id2, _C, _A, RES, RSP_{CA}, _C), $\_t_{g2}$,[$\_t_{req}$,$\_t_{req}$+f($\_t_{req}$)])

where:

RQS_{AC} = *rqs(_$f_{RequestAC}$, _L, _A, _C, TTP, _M, _H(M), _B_List, _H(B_List), _Seq_1, _T_{g1}, _T_1, _EG_B{K, L, S_A(H(M))}, _E_C{S_A(H(M)), H(B_List), EG_B{K,_L,S_A(H(M))}, H(_L,_Seq_1,T_{g1},T_1)}})*

RSP_{CA} = *rsp(_$f_{ResponseCA}$, _L, _A, _C, TTP, _H(M), _H(B_List), _Seq_2, _T_{g2}, _T_S, _E_A {S_C(H(M)), S_C(H(L, Seq_2, Tg2, T_S, _E_C{S_A(H(M)), H(B_List), EG_B{_K,_L, S_A(H(M)), H(_L,_Seq_1,_T_{g1},T_1)}))}})*

+ analogous monitoring rules for download and recovery phases

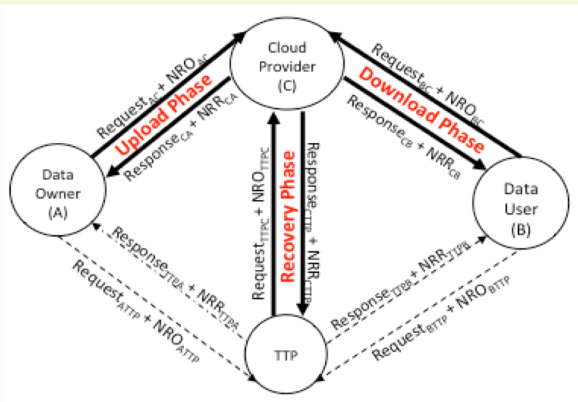
Hybrid assessment

Hybrid assessment: overview

- Combination of different types of assessments / evidence as, for example:
  - Monitoring
  - Testing
  - Penetration testing
  - Existing certificates
- Why?
  - Comprehensiveness
    - What if monitoring has not covered all possible computation paths?
    - Gaps in time
    - How can be sure of the completeness of scripts implementing penetration testing in existing tools (especially as threats and vulnerabilities evolve)
  - Identification and resolution of conflicts
    - Recall the conflicting assessments of OpenVas and Nessus

Hybrid assessment: example 1

Non repudiation through Trusted Third Party (TTP)



In the TTP non-repudiation protocol

- There might not have been even logs covering TTP
- Would you create a "sufficiently confident" assessment by simply relying on monitoring without testing?

Hybrid assessments:

- Test TTP; combine evidence
- Rely on a certificate for TTP or the oustome static analysis

Hybrid assessment: example 2

Security Property: cloud service availability

Probability of service producing a non faulty response within a given time period exceeds a given threshold

Why hybrid?

- To check if real service operation calls “around” the executed tests produced also an acceptable outcome (i.e., a non faulty response within the required time period) [local correlation 1]
- To check if for monitoring results that satisfy the conditions “marginally”, the available testing evidence (calls executed by testing) also satisfy the conditions [local correlation 2]
- To check if over the assessment period testing and monitoring evidence support consistently the same conclusion [global correlation]

Hybrid assessment: capabilities

- Correlate outputs of existing assessments
  - Through the definition of assessment criteria in hybrid assessment models
- Invoke testing tools through monitoring engine

Security Property: data integrity at rest

data modifications require authorisation

Monitoring Rule:

```
Happens(e(_e1,_sc,_TOC,REQ,_updOp(_cred,_data, _auth),_TOC),
t1,[t1,t1])  ^
Happens(e(_e2,_TOC,_AI,RES,_updOp(_cred,_data,_vCode1),_TOC),
t2,[t1,t2+d2]) ^ (_vCode1 ≠ Nil) ⇒
Happens(e(_e3,_CA,_AI,EXC,_authorO(_cred,_auth,_vCode2),_TOC),
t3,[t2,t2+d2])^(_vCode2≠Nil)
```

Monitoring log indicates a granted data update request

Test: execute the authorisation operation to check if appropriate authorisation rights were in place

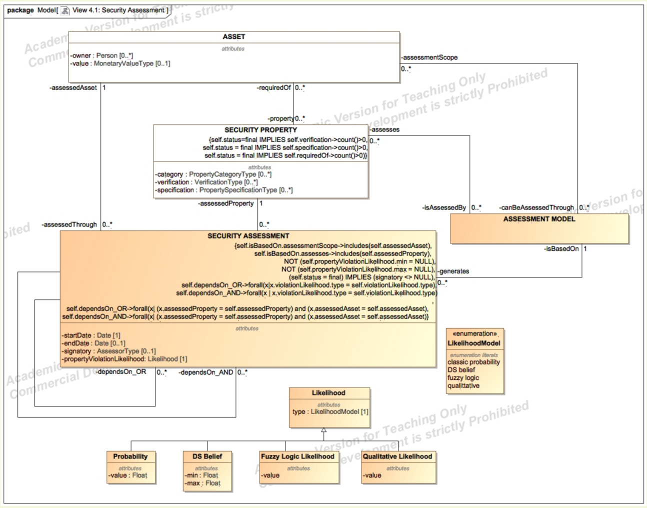
Risk assessment

Risk assessment: overview

- Likelihood of violation of required S&P properties
- Impact of violations
  - Direct and indirect
  - Technical vs. economic

Risk assessment: likelihood of property violations

- Different likelihood models
  - Classic probability
  - DS beliefs
  - Fuzzy likelihoods
  - Other qualitative likelihoods
- Explicit definition of likelihood model
- Assessments may depend on other assessments, e.g.,
  - CompSA dependsOn(or) $\{SA_1, \ldots, SA_n\} \rightarrow$ $CSA = SA_1$ or … or Sa_n
  - CompSA dependsOn(and) $\{SA_1, \ldots, SA_n\} \rightarrow$ $CSA = SA_1$ or … or Sa_n
- Dependencies may only exist between different assessments of the same asset and property



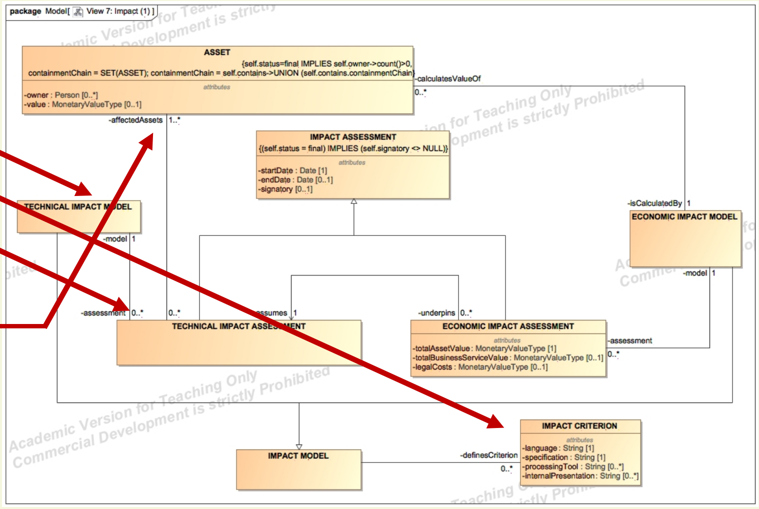
Risk assessment: technical impact assessment

- Technical impact
  - Is generated by a technical impact model, defined as a set of impact identification criteria
  - generates a technical impact assessment that is evaluated according to the model and includes a set of affected assets

© G. SPANOUDAKIS, FedCSIS 2019

Risk assessment: technical impact assessment

- Technical impact
  - Is generated by a technical impact model, defined as a set of impact identification criteria
  - generates a technical impact assessment that is evaluated according to the model and includes a set of affected assets

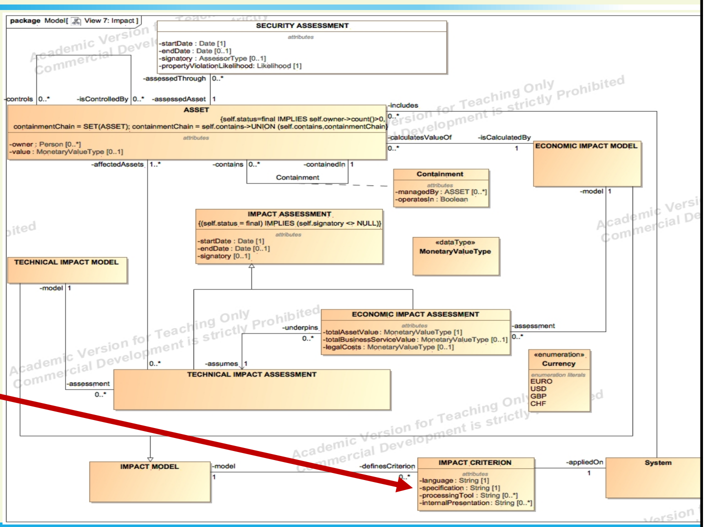


Risk assessment: technical impact assessment (examples)

- **Example 1:** Identify the assets of a system, whose confidentiality has been directly compromised by a confidentiality breach, as assessed by a security assessment model X or are contained in the containment closure of assets compromised in this way.
- **Impact criterion:**
  Language: OCL
  Specification:

```
Def DC = self.appliedOn.includes->
select(A | A.assessedThrough->
exists(SA | (SA.isBasedOn.name ="X")
and (SA.assessedProperty.category =
PropertyCategoryType::Confidentiality))

self.model.assessment =
DC->closure(X: Asset | X.contains))
```



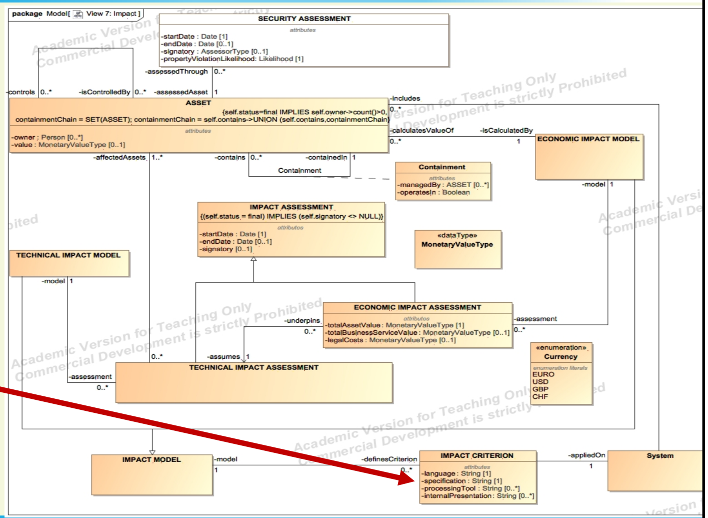
Risk assessment: technical impact assessment (examples)

- **Example 2:** Identify all data assets of a system, which are controlled by an asset that has an authentication vulnerability.

- **Impact criterion:**
  Language: OCL
  Specification:

```
Def A_AUTHV = self.appliedOn.includes->
select(A| a.hasVulnerability->
exists(V| (V.leadToViolation->
exists(P|(P.category =
PropertyCategoryType::authentication))

Def ALL_A_AUTHV =
self.model.assessment =
A_AUTHV.controls->closure(X: Data |
X.contains))
```

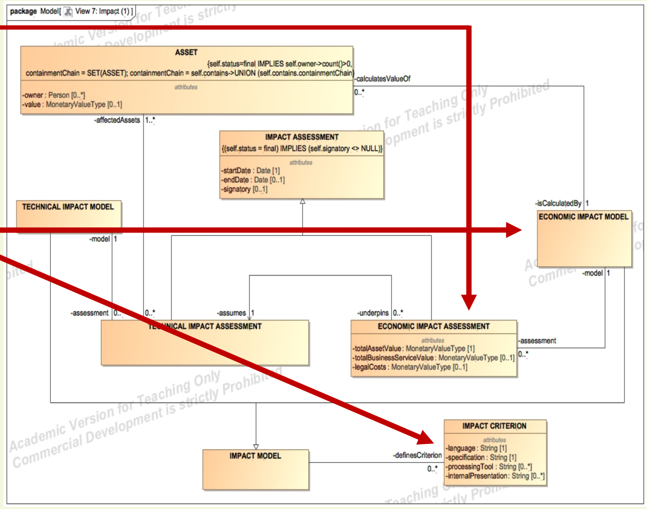


Risk assessment: economic impact assessment

- An economic impact assessment
  - is always based on an technical impact assessment (i.e., a set of affected assets as defined by a technical impact assessment model)
  - Is generated by an economic impact model, defined as a set of economic impact calculation criteria
  - Includes
    - an evaluation of the cost of affected assets, and possibly
    - the total value of the business processes which involve the affected assets
    - the costs of any legal procedures that may be needed due to the compromised assets

Risk assessment: economic impact assessment

- An economic impact assessment
  - is always based on an technical impact assessment (i.e., a set of affected assets as defined by a technical impact assessment model)
  - Is generated by an economic impact model, defined as a set of economic impact calculation criteria
  - Includes
    - an evaluation of the cost of affected assets, and possibly
    - the total value of the business processes which involve the affected assets
    - the costs of any legal procedures that may be needed due to the compromised assets



Risk assessment: economic impact assessment (examples)

Example 1:

- Identify all data assets of a system, which are controlled by an asset that has an authentication vulnerability (as in 2nd example of technical assessment).
  `See ALL_A_AUTHV`
- Find the business processes that may be affected due to using these data.
  `Def BP = self.isInvolvedIn`
- Evaluate the total value of these processes
  `DP.value.value->sum()`

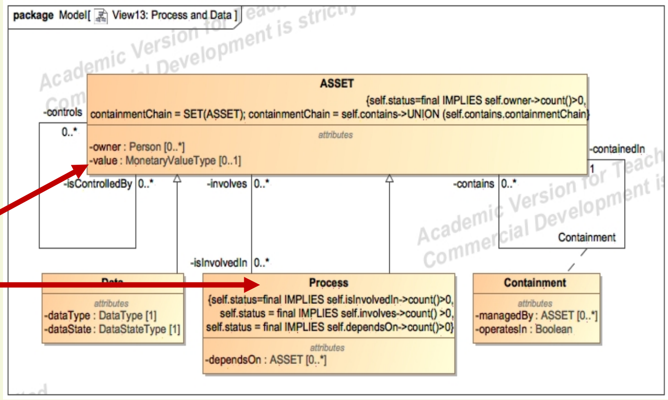
Risk assessment: economic impact assessment (examples)

Example 1:

- Identify all data assets of a system, which are controlled by an asset that has an authentication vulnerability (as in 2nd example of technical assessment).
  `See ALL_A_AUTHV`

- Find the business processes that may be affected due to using these data.
  `Def BP = self.isInvolvedIn`

- Evaluate the total value of these processes
  `DP.value.value->sum()`



Risk assessment: Open Issues

- Definition of appropriate assessment criteria
  - For example
    - Identified threats → monitoring rules for assessment
    - Detected vulnerabilities → penetration tests
- Validation of criteria
  - Correctness of monitoring rules
- Intra, intra and extra system coverage is needed
  - For example
    - ensure than no screenshot is taken when a system containing privacy sensitive data is in use
    - no access is allowed to a directory holding sensitive system data by a process other than the processes of the system itself
- Meaningful baseline economic models are difficult to define

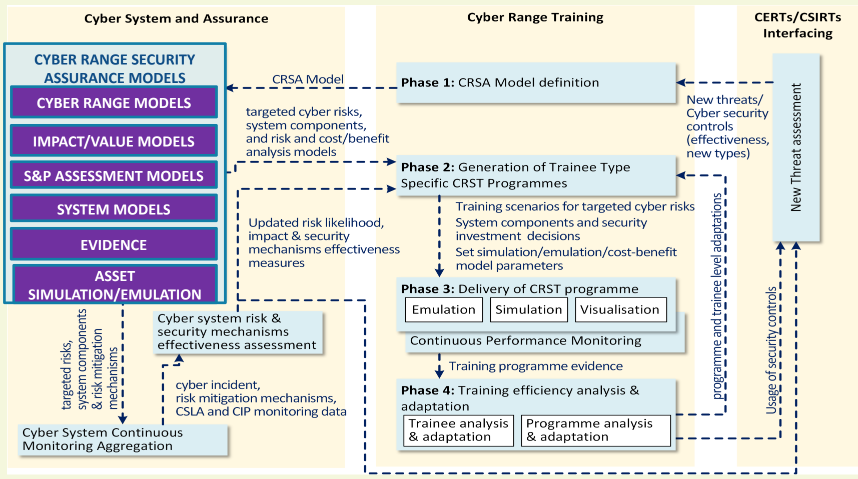
Cyber Range

- Overview
- Overall process
- Cyber range model – basics

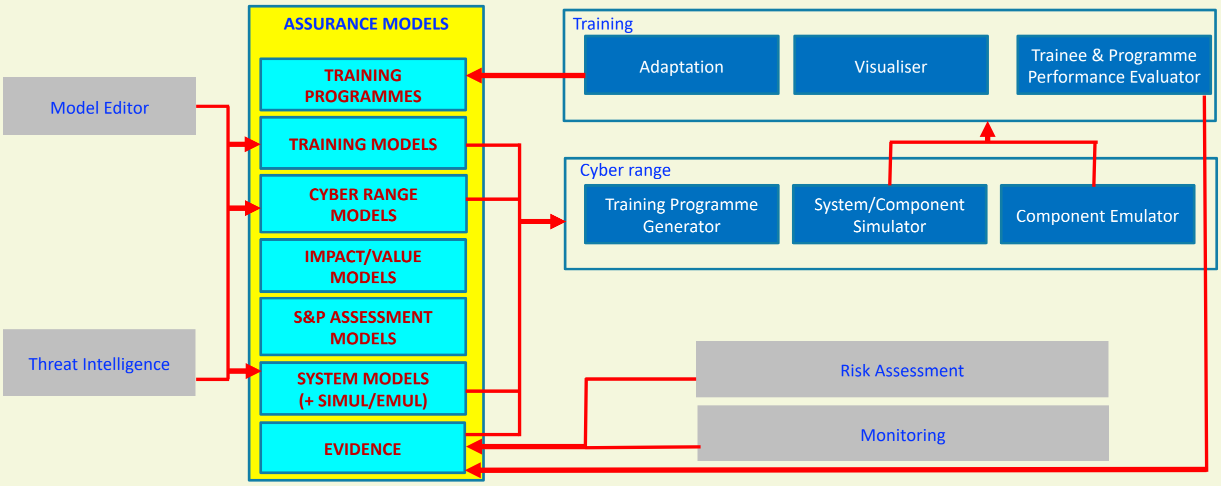
Cyber Range: overview

- Integrated with a security assurance and risk treatment programme
- Model driven
- Seen as as alternative/complementary risk treatment mechanism which should be selected based on
  - Effectiveness
  - Cost

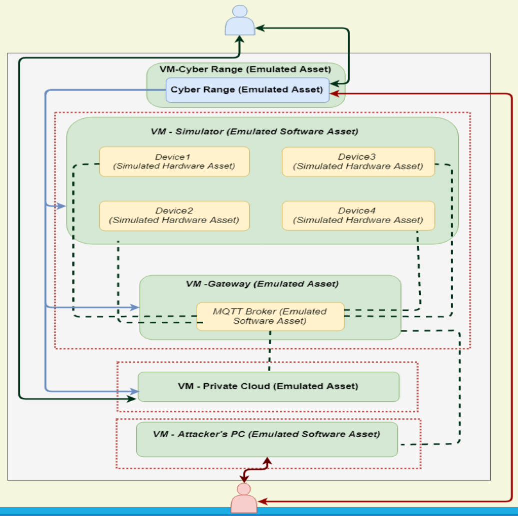
Cyber Range: overall process



Cyber Range: Capabilities



Cyber Range:
Mixture of simulated/emulated assets



Cyber Range:
programme selection and customisation

- Selection
  - Threat (particular scenarios under which an attack may manifest itself)
  - Asset
  - Security controls
  - Stakeholders (e.g., end user, administrator, CISO etc)
- Configuration
  - Simulated and emulated components
  - Simulation and emulation model parameters
  - Stakeholders
  - Level of difficulty
- Based on
  - Estimated risk (penetration testing, monitoring etc)
  - Existing coverage and past performance

Cyber Range:
evidenced based programme adaptation

- Evidence
  - trainee performance monitoring
    - Individual trainee
    - groups of trainees (use of ML techniques such as clustering)
  - continuous security status assessments (including effect of training programme on security posture)
- Adaptation types
  - Increase threat/attack rates
  - Decrease allowed response time
  - Eliminate/add/modify security controls
  - Add/remove simultaneous attacks
  - Change mixture of simulated and emulated components
- Level
  - Trainee
  - Programme

CITY

Cyber security SLAs

- Precise Cyber security SLA (CSLA) specification
- Monitoring
- Validation/risk assessment

CITY

© G. SPANOUDAKIS, FedCSIS 2019

CSLAs specification: Service Level Objectives

- Precise SLOs are specified as tuples of

```
<Computational Asset, Property Category,
Monitoring Rule(s)/Template, GuardedActions>
```

- Computational assets
  - Services/Operations (interface level) or internal
  - Data (interface level or stored)
- Property categories
  - Standardised property lists (e.g., CSA catalogue) + monitoring templates (if applicable)
- Monitoring Rule(s) / Template
  - Expressed in EC Assertion [4], an Event Calculus[18] based monitoring language

CSLA Specification: SLO Example

```
<
CAELC(HouseData),
Availability,
EC-Availability(CAELC(HouseData),
3, 0.01)
[TotalMonthlyViolations >10],
Penalty1>
```

```
EC-Availability(CAELC(HouseData), 3, 0.01):
1R.Availability.<CaseId>:
Happens(e(_id1, _Snd, _Rcv, Call(CAELC(HouseData)), _Rcv), t1, [t1,t1]) ∧
Happens(e(_id2, _Rcv, _Snd, Response(CAELC(HouseData)), _Rcv), t2,
[t1,t1+3]) ∧∃ _PN, _ST, _P []: HoldsAt(Unavailable(_PN, _Rcv,
_ST), t1)) ∧
HoldsAt(UnavailablePeriods(_Rcv, _PN, _P[]), t2) ∧
HoldsAt(LastServiceMonitoringPeriod(_Rcv, _lmsTime), t2)) ⇒
sum(_P[]) / (t2 – _lmsTime) < 0.01
2R.Availability.<CaseId>:
Happens(e(_id1, _Snd, _Rcv, Call(CAELC(HouseData)), _Rcv), t1, [t1,t1]) ∧
Happens(e(_id2, _Rcv, _Snd, Response(CAELC(HouseData)), _Rcv), t2,
[t1,t1+3]) ∧∃ _PN, _ST, _P []: HoldsAt(Unavailable(_PN, _Rcv,
_ST), t1)) ∧
HoldsAt(UnavailablePeriods(_Rcv, _PN, _P[]), t2) ∧
HoldsAt(LastServiceMonitoringPeriod(_Rcv, _lmsTime), t2)) ⇒
sum(_P[]) / (t2 – _lmsTime) < 0.01
```

CSLA Specification: Actions

Two predefined action types:

- **renegotiate** *Pred*, which causes the SLA to be renegotiated when the guard *Pred* is satisfied
- **penalty** *Pred Int*, which causes a penalty (or reward if negative) to be incurred.

CSLA Specification: Actions Example

Assets		Security Properties / GTs		
		Confidentiality	Integrity	Availability
Data Assets	A1	-	[v<3] NOTIFY [v>=3] RENEG $\lambda = 0.6$	-
	A2	[v>1] PENALTY(10) & NOTIFY $\lambda = 0.15$	-	-

Number of violations

Actions

Violation Rate

Two actions

Penalty amount

CSLA Specification: Actions Example (cont'd)

Assets		Security Properties / GTs		
		Confidentiality	Integrity	Availability
Data Assets	A1	-	[v<3] NOTIFY [v>=3] RENEG $\lambda = 0.6$	-
	A2	[v>1] PENALTY(10) & NOTIFY $\lambda = 0.15$	-	-
Operation Assets	A3	-	-	$\lambda = 0.2$ [v<k] MOD $\rightarrow \lambda = 0.1$ [v>3k] RENEG [true] NOTIFY
	A4	-	[v<3] NOTIFY [v>=3] RENEG $\lambda = 0.6$	-

Change of violation rate

CSLA Validation: Translation to Prism for model checking

- PRISM – formal modelling and analysis of systems that exhibit random or probabilistic behaviour [14, 16]
- PRISM supports the specification and analysis of different types of probabilistic models, i.e.:
  - discrete-time Markov chains (DTMCs)
  - continuous-time Markov chains (CTMCs)
  - Markov decision processes (MDPs)
  - probabilistic automata (PAs)
  - probabilistic timed automata (PTAs)
- PRISM models are expressed in a simple state based language

```
[Name] Guard -> Rate/Prob: Assignments;
```

- The properties to be validated for a system are expressed in a temporal logic language supporting expressions in different temporal logics (PCTL, CSL, LTL and PCTL*)

CSLA Validation: Translation to Prism for model checking

- PRISM – formal modelling and analysis of systems that exhibit random or probabilistic behaviour [14, 16]
- PRISM supports the specification and analysis of different types of probabilistic models, i.e.:
  - discrete-time Markov chains (DTMCs)
  - continuous-time Markov chains (CTMCs) — Allows the expression of rates of SLA guarantee terms violations
  - Markov decision processes (MDPs)
  - probabilistic automata (PAs)
  - probabilistic timed automata (PTAs)
- PRISM models are expressed in a simple state based language

```
[Name] Guard -> Rate: Assignments;
```

- The properties to be validated for a system are expressed in a temporal logic language supporting expressions in different temporal logics (PCTL, CSL, LTL and PCTL*)

CSLA validation: Translation to Prism

- Basic PRISM model
  - CSLA Manager environment
  - CSLA Manager

CSLA MANAGER ENVIRONMENT

- a Prism module for each SLA GT firing a violation at a given rate

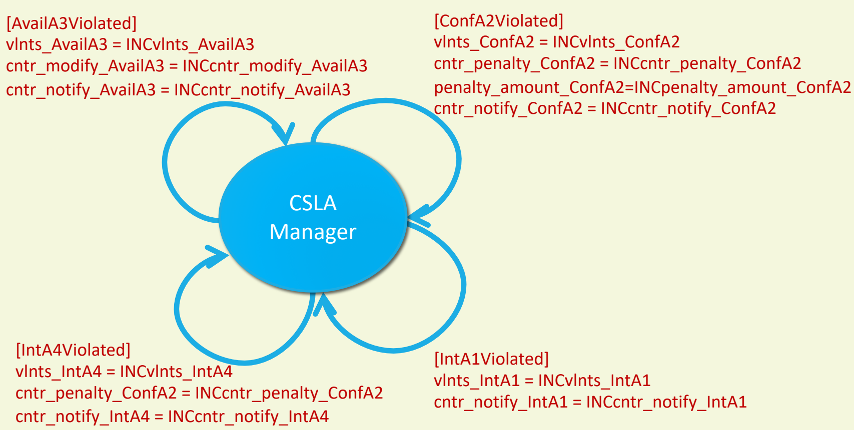
violations →

← active / inactive CSLA

CSLA MANAGER

- one transition per GT, enabled when the SLA is active and disabled when renegotiation occurs
- the rate of GT transitions is always 1 (→ only the env. transition rate affects time)
- each GT transition has one or more guarded SLA management actions & actions updating counters
- guard formulas for the actions

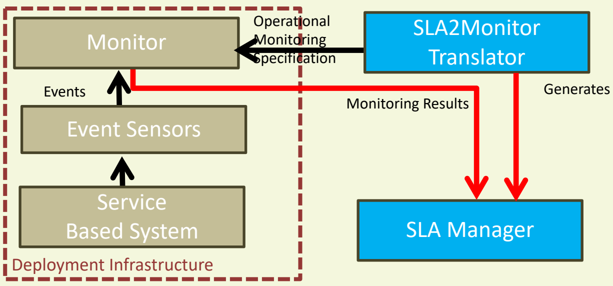
CSLA Validation: CSLA Manager module



- The SLA Manager module has one transition per GT, which is enabled when the SLA is active and becomes disabled when renegotiation occurs.
- All transitions are responsible for incrementing the value of the different counters to capture the fact that a particular GT_i has been violated. This allows us to produce GT-specific versions of the different guards and variable updates in the model.

Execution of CSLA management actions: Runtime CSLA Manager

- Receives Monitoring Results from the Monitoring component
- Based on the results it process the actions of each Guarantee Term, stated in the CSLA, i.e. :
  - Executes the Notifications to the relevant parties;
  - Calculates the Penalty amounts to be paid;
  - Executes the Renegotiation action; etc.



CSLA Experimental Evaluation:
Validation Results

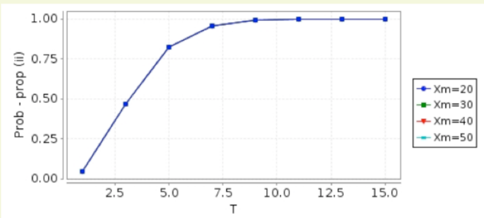
Based on case studies of CSLAs:

Assets		Security Properties / GTs		
		Confidentiality	Integrity	Availability
Data Assets	A1	-	[v<3] NOTIFY [v>=3] RENEG $\lambda = 0.6$	-
Data Assets	A2	[v>1] PENALTY(10) & NOTIFY $\lambda = 0.15$	-	-
Operation Assets	A3	-	-	$\lambda = 0.2$ [v<k] MOD ➔ λ=0.1 [v>3k] RENEG [true] NOTIFY
Operation Assets	A4	-	[v<3] NOTIFY [v>=3] RENEG $\lambda = 0.6$	-

CSLA Experimental Evaluation:
Validation Results

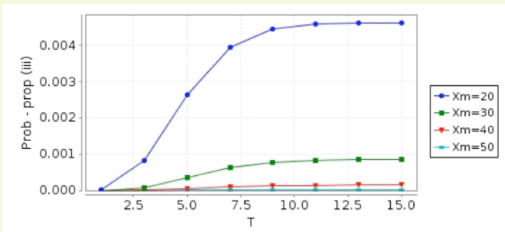
What is the probability that a renegotiation will occur within the first 4 days?

- P=? [F<=(4*day) !SLAactive]



What is the probability to pay more than Xm currency units in the first month?

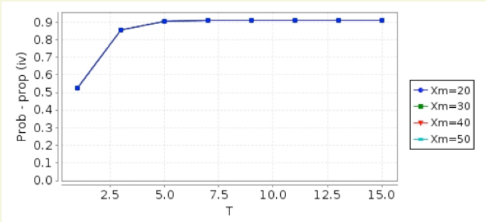
- P=? [F<=month (penalty_amount_ConfA2>Xm)]



CSLA Experimental Evaluation:
Validation Results (cont'd)

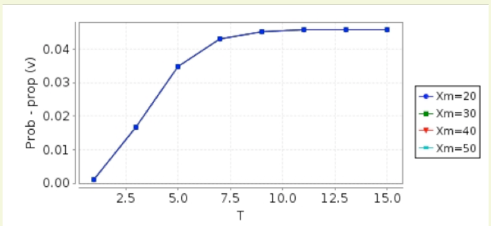
What is the probability to have a violation on confidentiality or integrity of any data asset within a month?

- P=? [F<=month (vltns_IntA1+vltns_ConfA2>=1)]



What is the probability to reach double the infrastructure resources (i.e., to have 2*k* number of modifications for the operation assets) within the first month?

- P=? [F<=month (cntr_notify_AvailA3 >(2*k))]
  (For k = 1)



Cyber insurance

- Key activities
- Existing techniques
- Key activities coverage
- Models
- Management process
- Capabilities
- Challenges

Cyber Insurance: key activities

Risk Identification
- Asset Identification.
- Threat Identification.
- Security/Vulnerability Identification.

Risk Analysis
- Likelihood Determination.
- Impact Determination.
- Risk Estimation.

Policy Management
- Coverage Specification.
- Premium Estimation.
- Write and Sign Contract.
- Claim Handling.

Cyber Insurance: existing techniques

Phases	Steps	Techniques
Risk identification	Asset identification	Business documentation Meetings/interviews Questionnaires/checklists/worksheets Knowledge base
	Threat identification	Business documentation Meetings/interviews Questionnaires/checklists/worksheets Knowledge base Threat trees/FTA/attack trees
	Security/Vulnerability identification	ETA Attack graphs Vulnerability scanning Penetration testing Meetings/interviews Questionnaires/checklists/worksheets Knowledge base Delphi method
Risk analysis	Likelihood determination	History/log analysis Meetings/interviews Questionnaires/checklists/worksheets Knowledge base Delphi method
	Impact determination	Meetings/interviews Questionnaires/checklists/worksheets Knowledge base Delphi method
	Risk estimation	Risk table ALE

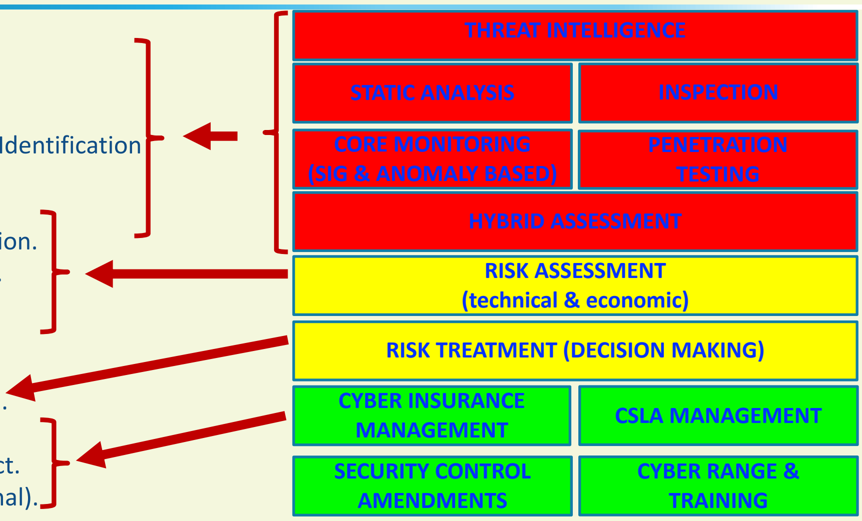
© G. SPANOUDAKIS, FedCSIS 2019

Cyber Insurance: key activities coverage

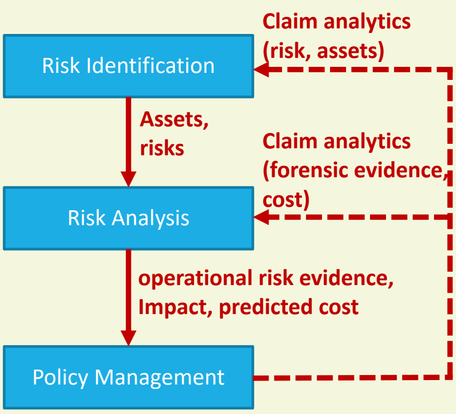
Risk Identification
- Asset Identification.
- Threat Identification.
- Security/Vulnerability Identification

Risk Analysis
- Likelihood Determination.
- Impact Determination.
- Risk Estimation.

Policy Management
- Coverage Specification.
- Premium Estimation.
- Write and Sign Contract.
- Claim Handling (optional).



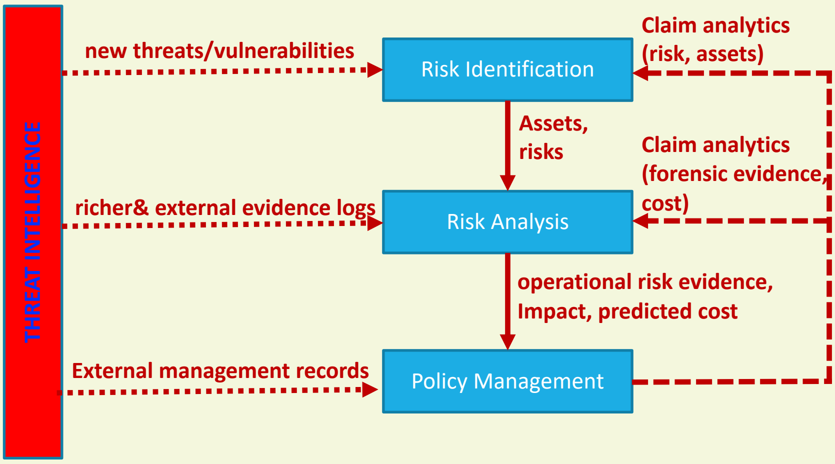
Cyber insurance: adaptive management



Risk analysis (→ risk exposure, impact)
- comprehensive assessment of risk for formulating and pricing cyber insurance policies
- dynamic, continuous certificates based risk exposure
- impact of risk on cyber system providers (e.g., impact on business reputation, theft of intellectual property) and the cost of eliminating it

Policy management (→insurable assets, costs, premiums)
- vulnerable assets → candidate subjects of insurance
- risk estimates, value assets → policy pricing
- certificates → prerequisite to policy validation
- claim analytics (in reference to assurance evidence & prior risk estimates) → insurable assets, insurance cost & premiums

Cyber insurance: adaptive management



Cyber insurance: challenges

- Lack of experience and standards
- System evolution
- Technology evolution
- Information asymmetry
- Hard to measure rate of
  - Threat occurrence
  - Correct operation of security controls
- Interdependence of security
  - Internal
  - External (chains of systems)
- Lack of statistical data
  - Hidden data
  - Scarcity of similar systems
- Hard to estimate impact
  - Intangible
  - Unpredictable impact
- Correlated risks
  - Geographic similarity
  - Monoculture
  - Simultaneous replication of attacks
- Additional liability
- Time to claim
  - Unnoticed attacks

Cyber insurance: challenges

- Lack of experience and standards
- System evolution
- Technology evolution
- Information asymmetry
- Hard to measure rate of
  - Threat occurrence
  - Correct operation of security controls
- Interdependence of security
  - Internal
  - External (chains of systems)
- Lack of statistical data
  - Hidden data
  - Scarcity of similar systems
- Hard to estimate impact
  - Intangible
  - Unpredictable impact
- Correlated risks
  - Geographic similarity
  - Monoculture
  - Simultaneous replication of attacks
- Additional liability
- Time to claim
  - Unnoticed attacks

CITY

On going work

- Automated assessments
  - For all levels of risk management (system, business processes & mission, organizational)
  - For all horizons of risk management (tactical short term, tactical medium term & strategic)
- Need for hybrid assessments, combining outcomes of individual assessments
  - Complementary outcomes
  - Conflicting outcomes
- Incremental assessments
- Automated adaptation and evolution of assessment schemes
- Adaptive cyber range

CITY

Thank You !