Network Incident Severity Assessment

Automatic Defense Mechanisms

Luis Francisco Servin Valencia

Till Dörges

Klaus-Peter Kossakowski

`ls,td,kpk@pre-secure.de`

Outline

- Introduction and motivation
- POSITIF
- Assessment Model
- Outlook & Future Work

Introduction

- Information Security

Introduction

- Information Security
  - attempts to preserve

Introduction

- Information Security
  - attempts to preserve
    - Confidentiality

Introduction

- Information Security
  - attempts to preserve
    - Confidentiality
    - Integrity

Introduction

- Information Security
  - attempts to preserve
    - Confidentiality
    - Integrity
    - Availability

Introduction

- Information Security
  - attempts to preserve
    - Confidentiality
    - Integrity
    - Availability
  - depends on

Introduction

- Information Security
  - attempts to preserve
    - Confidentiality
    - Integrity
    - Availability
  - depends on
    - Intrusion Prevention (isolation, data encryption, anti-virus software)

Introduction

- Information Security
  - attempts to preserve
    - Confidentiality
    - Integrity
    - Availability
  - depends on
    - Intrusion Prevention (isolation, data encryption, anti-virus software)
    - Intrusion Detection (IDS, IPS, Honeypots, Log analysis)

Introduction

- Information Security
  - attempts to preserve
    - Confidentiality
    - Integrity
    - Availability
  - depends on
    - Intrusion Prevention → reactive
    - Intrusion Detection → reactive

Introduction

- Intrusion Detection solutions work isolated and uncoordinated

Introduction

- Intrusion Detection solutions work isolated and uncoordinated
  - Different output formats

Introduction

- Intrusion Detection solutions work isolated and uncoordinated
  - Different output formats
  - Alert flood

Introduction

- Intrusion Detection solutions work isolated and uncoordinated
  - Different output formats
  - Alert flood
    - False Positives

Introduction

- Intrusion Detection solutions work isolated and uncoordinated
  - Different output formats
  - Alert flood
    - False Positives
    - Repeated alerts (same alert, different sensor)

Introduction

- Intrusion Detection solutions work isolated and uncoordinated
  - Different output formats
  - Alert flood
    - False Positives
    - Repeated alerts (same alert, different sensor)
    - Alert Correlation reduces information amount

Introduction

- Intrusion Detection solutions work isolated and uncoordinated
  - Different output formats
  - Alert flood
    - False Positives
    - Repeated alerts (same alert, different sensor)
    - Alert Correlation reduces information amount → doesn´t provide knowledge!

Motivation

- Incident Severity Assessment

Motivation

- Incident Severity Assessment
  - Incident’s effect on “health” of

Motivation

- Incident Severity Assessment
  - Incident's effect on "health" of
    - Affected system(s)

Motivation

- Incident Severity Assessment
  - Incident's effect on "health" of
    - Affected system(s)
    - Network as a whole

Motivation

- Incident Severity Assessment
  - Incident's effect on "health" of
    - Affected system(s)
    - Network as a whole
  - Manual Method

Motivation

- Incident Severity Assessment
  - Incident's effect on "health" of
    - Affected system(s)
    - Network as a whole
  - Manual Method
    - Time between alert and reaction

Motivation

- Incident Severity Assessment
  - Incident's effect on "health" of
    - Affected system(s)
    - Network as a whole
  - Manual Method
    - Time between alert and reaction
    - Evaluate impact on network

Motivation

- Incident Severity Assessment
  - Incident's effect on "health" of
    - Affected system(s)
    - Network as a whole
  - Manual Method
    - Time between alert and reaction
    - Evaluate impact on network $\Longrightarrow$ Topological knowledge helps, but challenging for big networks

Problem Statement

- Extract knowledge from information in alerts

Problem Statement

- Extract knowledge from information in alerts
- Determine influence of individual events on network

Problem Statement

- Extract knowledge from information in alerts
- Determine influence of individual events on network
- React to detected anomalies

Outline

- Introduction and motivation
- POSITIF
  - Goal
  - Workflow
  - Structure
  - Proactive Security Monitor
- Assessment Model
- Outlook & Future Work

POSITIF

- Policy-based Security Tools and Framework (POSITIF)

POSITIF

- Policy-based Security Tools and Framework (POSITIF)
- Goal: Provide a network administrator with tools for:

POSITIF

- Policy-based Security Tools and Framework (POSITIF)
- Goal: Provide a network administrator with tools for:
  - Centralized network management

POSITIF

- Policy-based Security Tools and Framework (POSITIF)
- Goal: Provide a network administrator with tools for:
  - Centralized network management
  - Definition of Security Policies

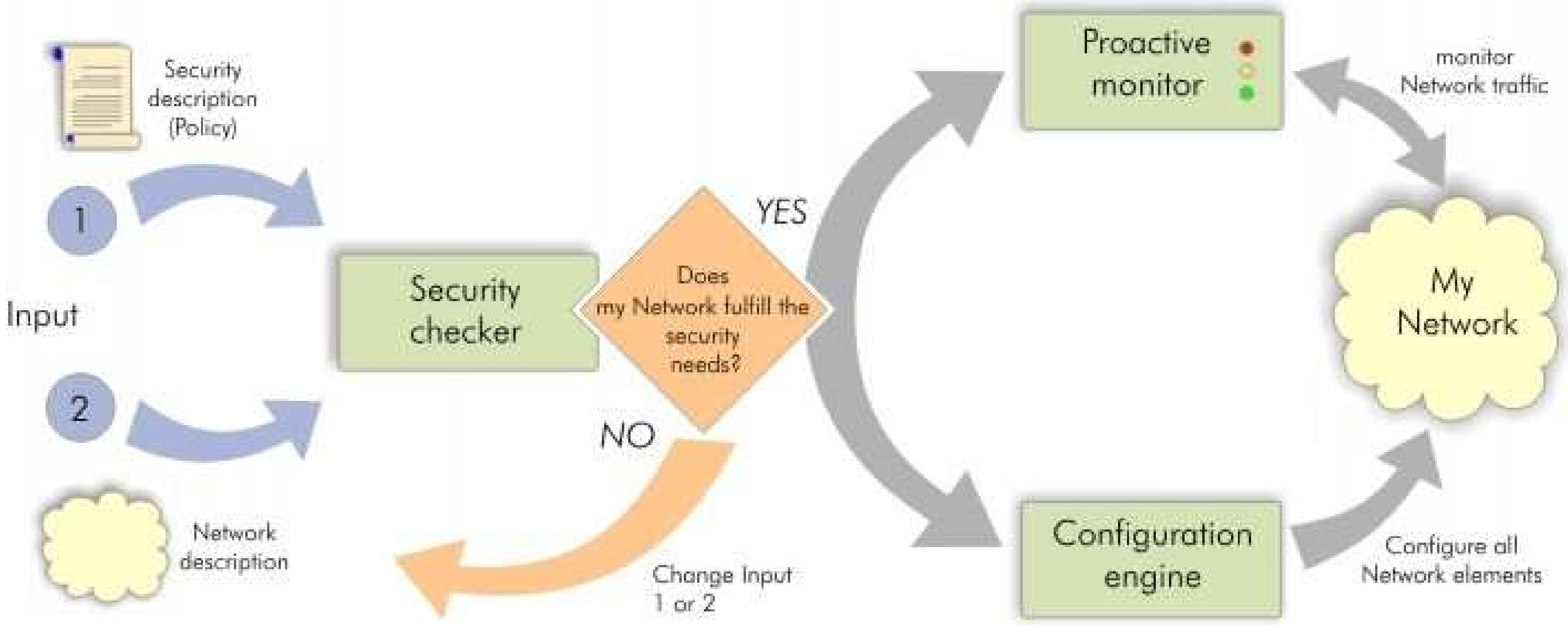
POSITIF

- Policy-based Security Tools and Framework (POSITIF)
- Goal: Provide a network administrator with tools for:
  - Centralized network management
  - Definition of Security Policies
  - Policy Monitoring

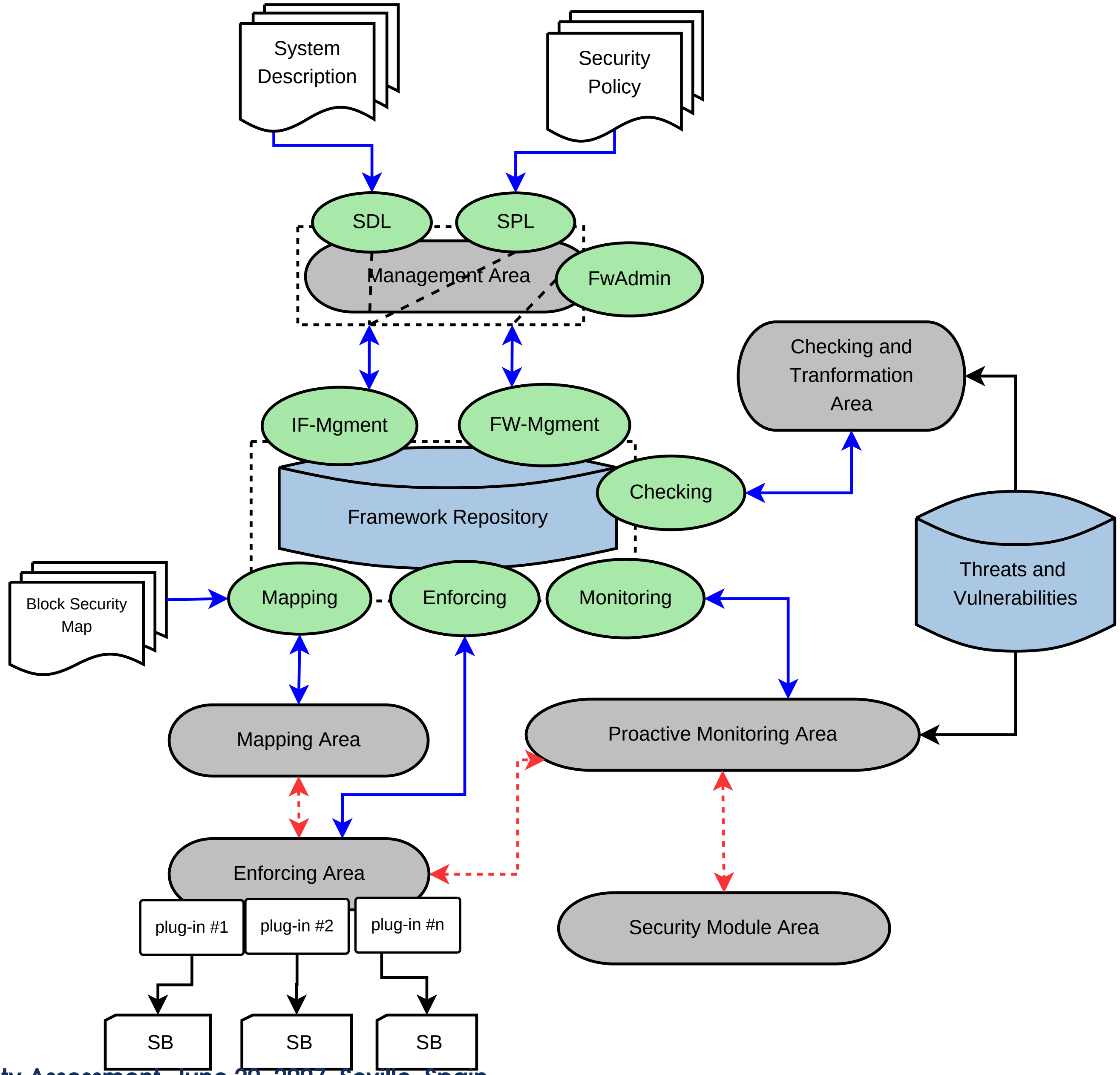
POSITIF

- Policy-based Security Tools and Framework (POSITIF)
- Goal: Provide a network administrator with tools for:
  - Centralized network management
  - Definition of Security Policies
  - Policy Monitoring
  - Reaction to intrusions

POSITIF Workflow



POSITIF Structure



POSITIF PSM

- Proactive Security Monitor

POSITIF PSM

- Proactive Security Monitor
- Functions:

POSITIF PSM

- Proactive Security Monitor
- Functions:
  - Monitor violations to policies

POSITIF PSM

- Proactive Security Monitor
- Functions:
  - Monitor violations to policies
  - Report detected problems

POSITIF PSM

- Proactive Security Monitor
- Functions:
  - Monitor violations to policies
  - Report detected problems
  - Situational assessment

POSITIF PSM

- Proactive Security Monitor
- Functions:
  - Monitor violations to policies
  - Report detected problems
  - Situational assessment
  - Corrective actions

POSITIF PSM

- Components:

POSITIF PSM

- Components:
  - Reactive Elements: IDS and Policy violation sensors (PVS)

POSITIF PSM

- Components:
  - Reactive Elements: IDS and Policy violation sensors (PVS)
  - Proactive Elements: Proactive Security Scanner (PSC) and Proactive Configuration Checker (PCC)

POSITIF PSM

- Components:
  - Reactive Elements: IDS and Policy violation sensors (PVS)
  - Proactive Elements: Proactive Security Scanner (PSC) and Proactive Configuration Checker (PCC)
  - Processing Elements: PSC & PCC Correlation,

    PSM-Assessment

POSITIF PSM

- Components:
  - Reactive Elements: IDS and Policy violation sensors (PVS)
  - Proactive Elements: Proactive Security Scanner (PSC) and Proactive Configuration Checker (PCC)
  - Processing Elements: PSC & PCC Correlation,

    PSM-Assessment
- Communication:

POSITIF PSM

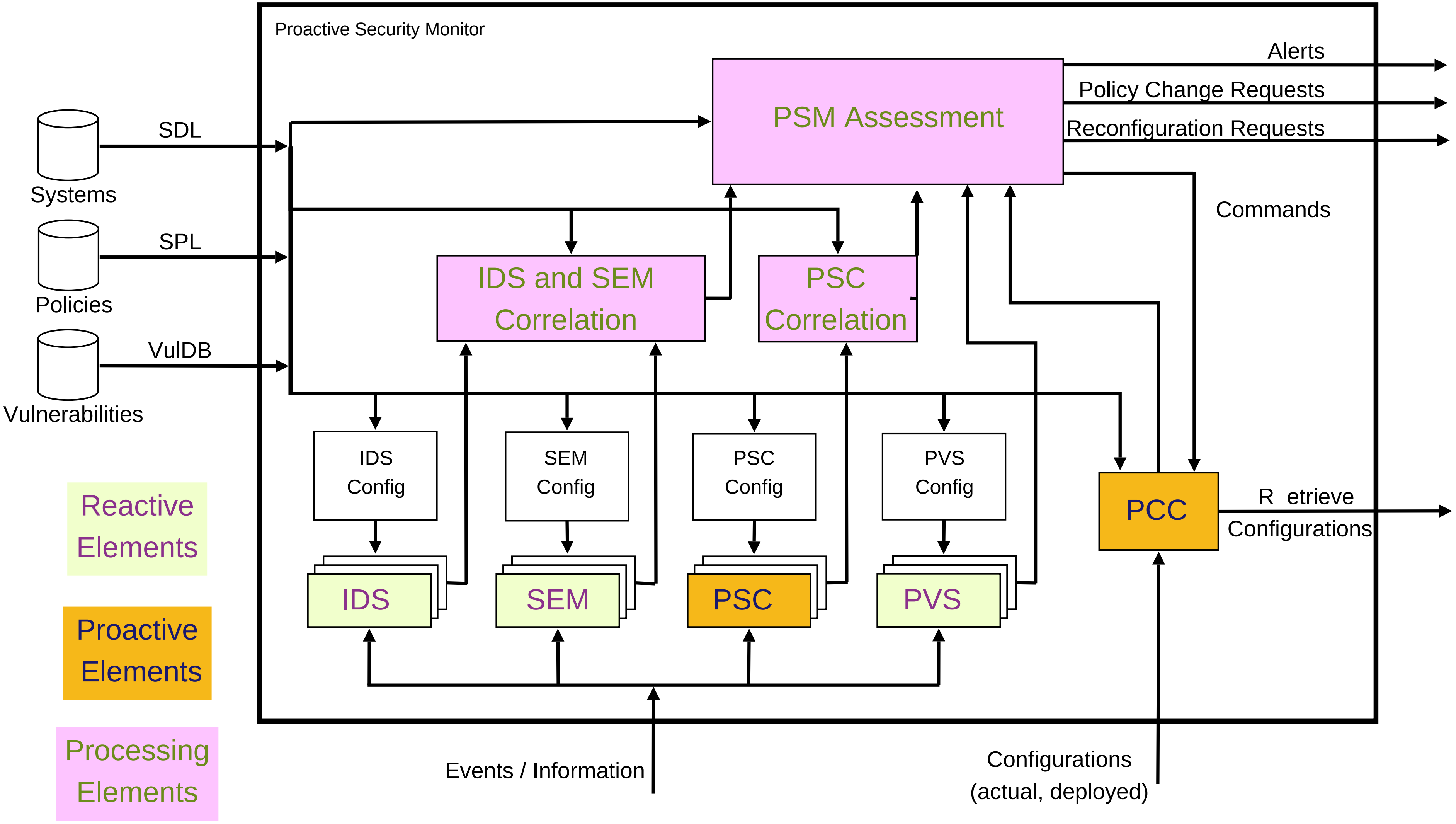
- Components:
  - Reactive Elements: IDS and Policy violation sensors (PVS)
  - Proactive Elements: Proactive Security Scanner (PSC) and Proactive Configuration Checker (PCC)
  - Processing Elements: PSC & PCC Correlation, PSM-Assessment
- Communication:
  - Format: IODEF messages

POSITIF PSM

- Components:
  - Reactive Elements: IDS and Policy violation sensors (PVS)
  - Proactive Elements: Proactive Security Scanner (PSC) and Proactive Configuration Checker (PCC)
  - Processing Elements: PSC & PCC Correlation,

    PSM-Assessment
- Communication:
  - Format: IODEF messages
  - Protocol: BEEP (Blocks Extensible Exchange P.)

PSM Structure



Outline

- Introduction and motivation
- POSITIF
- Assessment Model
  - Preparation
  - Model
  - Reaction State Machine
  - Process
- Outlook & Future Work

Assessment - Preparation

- Separate essential - non-essential services/hosts

Assessment - Preparation

- Separate essential - non-essential services/hosts
  - Sensitivity levels in SDL

Assessment - Preparation

- Separate essential - non-essential services/hosts
  - Sensitivity levels in SDL
- Defined security levels in network (SPL)

Assessment - Preparation

- Separate essential - non-essential services/hosts
  - Sensitivity levels in SDL
- Defined security levels in network (SPL)
- Current Security level

Assessment - Model

- Adaptation Dynamic Fusion Model

Assessment - Model

- Adaptation Dynamic Fusion Model
  - Use active & reactive elements

Assessment - Model

- Adaptation Dynamic Fusion Model
  - Use active & reactive elements
  - Incorporate event reactions

Assessment - Model

- Adaptation Dynamic Fusion Model
  - Use active & reactive elements
  - Incorporate event reactions
    - Check valid configuration

Assessment - Model

- Adaptation Dynamic Fusion Model
  - Use active & reactive elements
  - Incorporate event reactions
    - Check valid configuration
    - Check for vulnerabilities

Assessment - Model

- Adaptation Dynamic Fusion Model
  - Use active & reactive elements
  - Incorporate event reactions
    - Check valid configuration
    - Check for vulnerabilities
    - Initiate general network policy change (green level ↔ red level)

Assessment - Model

- Adaptation Dynamic Fusion Model
  - Use active & reactive elements
  - Incorporate event reactions
    - Check valid configuration
    - Check for vulnerabilities
    - Initiate general network policy change (green level ↔ red level)
    - Initiate service reconfiguration

Assessment - Model

- Adaptation Dynamic Fusion Model
  - Use active & reactive elements
  - Incorporate event reactions
    - Check valid configuration
    - Check for vulnerabilities
    - Initiate general network policy change (green level ↔ red level)
    - Initiate service reconfiguration
    - Emit alerts and warnings for human interaction

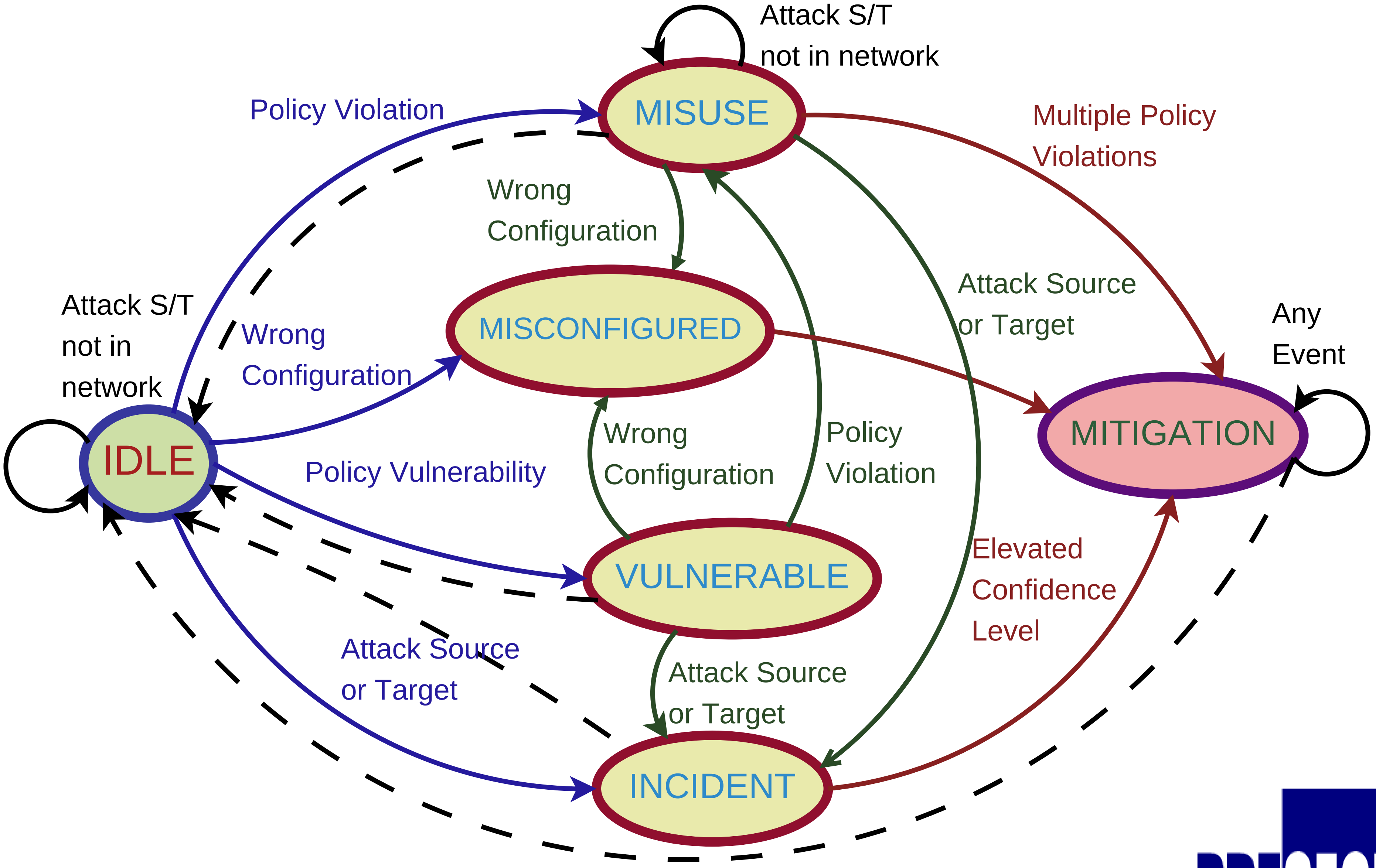
Assessment - Model

- Adaptation Dynamic Fusion Model
  - Use active & reactive elements
  - Incorporate event reactions
    - Check valid configuration
    - Check for vulnerabilities
    - Initiate general network policy change (green level ↔ red level)
    - Initiate service reconfiguration
    - Emit alerts and warnings for human interaction
  - Self-stabilization

Assessment - Model

- Adaptation Dynamic Fusion Model
  - Use active & reactive elements
  - Incorporate event reactions
    - Check valid configuration
    - Check for vulnerabilities
    - Initiate general network policy change (green level ↔ red level)
    - Initiate service reconfiguration
    - Emit alerts and warnings for human interaction
  - Self-stabilization
  - Extension to overall network health measure

PSM - State Machine



Assessment - Process

- Alert Prioritization

Assessment - Process

- Alert Prioritization
  - System’s Sensitivity

Assessment - Process

- Alert Prioritization
  - System´s Sensitivity
  - Impact Severity

Assessment - Process

- Alert Prioritization
  - System´s Sensitivity
  - Impact Severity
  - Corroborating / Contradicting successive events

Assessment - Process

- Alert Prioritization
  - System´s Sensitivity
  - Impact Severity
  - Corroborating / Contradicting successive events
- Alert Association

Assessment - Process

- Alert Prioritization
  - System's Sensitivity
  - Impact Severity
  - Corroborating / Contradicting successive events
- Alert Association
- System Situational Assessment

Assessment - Process

- Alert Prioritization
  - System's Sensitivity
  - Impact Severity
  - Corroborating / Contradicting successive events
- Alert Association
- System Situational Assessment
- Network Situational Assessment

Alert Association

- Clustering

Alert Association

- Clustering
  - Structural relations between alerts ($\approx$ Content, $\neq$ level)

Alert Association

- Clustering
  - Structural relations between alerts ($\approx$ Content, $\neq$ level)
  - Generalization hierarchies: IP Address, ports, time

Alert Association

- Clustering
  - Structural relations between alerts (≈ Content, ≠ level)
  - Generalization hierarchies: IP Address, ports, time
- Correlation

Alert Association

- Clustering
  - Structural relations between alerts ($\approx$ Content, $\neq$ level)
  - Generalization hierarchies: IP Address, ports, time
- Correlation
  - Cause-effect relations in abstract cognitive model

Alert Association

- Clustering
  - Structural relations between alerts ($\approx$ Content, $\neq$ level)
  - Generalization hierarchies: IP Address, ports, time
- Correlation
  - Cause-effect relations in abstract cognitive model
  - Correlates IDS Correlation with other sensor inputs

Alert Clustering

- “Attribute-Oriented Algorithm” to do clustering

Alert Clustering

- “Attribute-Oriented Algorithm” to do clustering
  - Cluster alerts together

Alert Clustering

- “Attribute-Oriented Algorithm” to do clustering
  - Cluster alerts together
    - Specific attributes first

Alert Clustering

- “Attribute-Oriented Algorithm” to do clustering
  - Cluster alerts together
    - Specific attributes first
    - Generalize attributes

Alert Clustering

- “Attribute-Oriented Algorithm” to do clustering
  - Cluster alerts together
    - Specific attributes first
    - Generalize attributes
  - Each belongs to only one (most specific attributes)

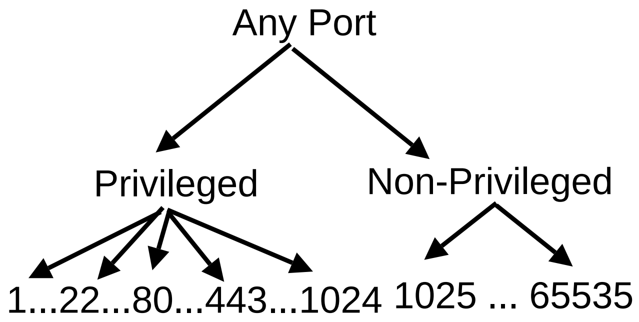
Alert Clustering

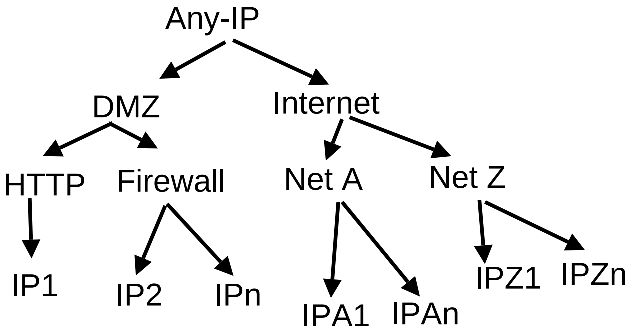
- “Attribute-Oriented Algorithm” to do clustering
  - Cluster alerts together
    - Specific attributes first
    - Generalize attributes
  - Each belongs to only one (most specific attributes)
  - Calculate ea. cluster’s elements “closeness”

Alert Clustering

- “Attribute-Oriented Algorithm” to do clustering
  - Cluster alerts together
    - Specific attributes first
    - Generalize attributes
  - Each belongs to only one (most specific attributes)
  - Calculate ea. cluster’s elements “closeness”
  - Calculate effect of all clusters (Cluster Association Strength)

Alert Clustering Hierarchies





Levels of Generalization		IP Address	IP Port	Time
General	1	Any-IP		Within-Day
	2	Network	Any-Port	Within-Hours
	3	Subnet	(Non-)Privileged	Within-Minutes
Specific	4	Host	Actual port	Within-Seconds

Alert Correlation

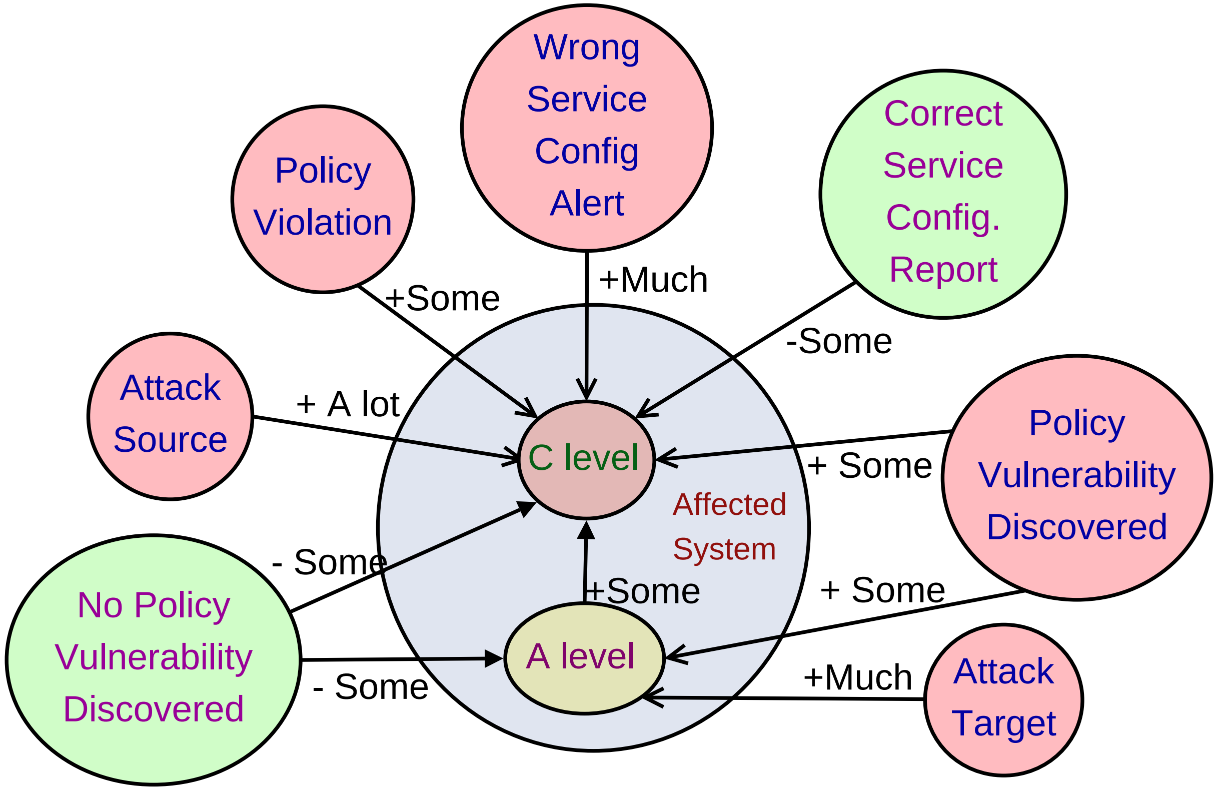
- Correlate IDS-Correlation w. other POSITIF Sensors.

Alert Correlation

- Correlate IDS-Correlation w. other POSITIF Sensors.
- Determine effect on system "Compromise" and "Attack" levels

Alert Correlation

- Correlate IDS-Correlation w. other POSITIF Sensors.
- Determine effect on system “Compromise” and “Attack” levels



Situational Assessment

- Fuse “Compromise” level w. Cluster Association Strength

Situational Assessment

- Fuse “Compromise” level w. Cluster Association Strength
  - Fuzzify values

Situational Assessment

- Fuse “Compromise” level w. Cluster Association Strength
  - Fuzzify values
  - Calculate Consensus ($h = sup(min(C_f, CAS_f))$)

Situational Assessment

- Fuse “Compromise” level w. Cluster Association Strength
  - Fuzzify values
  - Calculate Consensus ($h = sup(min(C_f, CAS_f))$)
  - Aggregate them

Situational Assessment

- Fuse “Compromise” level w. Cluster Association Strength
  - Fuzzify values
  - Calculate Consensus ($h = sup(min(C_f, CAS_f))$)
  - Aggregate them
    - Partial Agreement: additive

Situational Assessment

- Fuse “Compromise” level w. Cluster Association Strength
  - Fuzzify values
  - Calculate Consensus ($h = sup(min(C_f, CAS_f))$)
  - Aggregate them
    - Partial Agreement: additive
    - Partial Disagreement: compromising

Situational Assessment

- Fuse “Compromise” level w. Cluster Association Strength
  - Fuzzify values
  - Calculate Consensus ($h = sup(min(C_f, CAS_f))$)
  - Aggregate them
    - Partial Agreement: additive
    - Partial Disagreement: compromising
    - Total Agreement: h

Situational Assessment

- Fuse "Compromise" level w. Cluster Association Strength
  - Fuzzify values
  - Calculate Consensus ($h = sup(min(C_f, CAS_f))$)
  - Aggregate them
    - Partial Agreement: additive
    - Partial Disagreement: compromising
    - Total Agreement: h
  - Centroid Defuzzification → Overall Degree Concern (System)

Situational Assessment

- Network Degree of Concern (NDOC) → Weighted average of “healthy” and ODC of affected systems

Situational Assessment

- Network Degree of Concern (NDOC) → Weighted average of “healthy” and ODC of affected systems
    - weights are represented by their SDL Sensitivity

Situational Assessment

- Network Degree of Concern (NDOC) → Weighted average of “healthy” and ODC of affected systems
  - weights are represented by their SDL Sensitivity
- Information clutter reduced to single value: low, caution, elevated, high, severe

Situational Assessment

- Network Degree of Concern (NDOC) → Weighted average of "healthy" and ODC of affected systems
  - weights are represented by their SDL Sensitivity
- Information clutter reduced to single value: low, caution, elevated, high, severe
- Level changes can trigger (de-)increase in Network Security Level

Outline

- Introduction and motivation
- POSITIF
- Assessment Model
- Outlook & Future Work

Outlook

- Network Situational Assessment is the process of winning knowledge from a set of heterogeneous sensors′ output.

Outlook

- Network Situational Assessment is the process of winning knowledge from a set of heterogeneous sensors' output.
- Proposed method pairs-up alerts with actions through a Finite State Machine

Outlook

- Network Situational Assessment is the process of winning knowledge from a set of heterogeneous sensors' output.
- Proposed method pairs-up alerts with actions through a Finite State Machine
  - Aims to:

Outlook

- Network Situational Assessment is the process of winning knowledge from a set of heterogeneous sensors' output.
- Proposed method pairs-up alerts with actions through a Finite State Machine
  - Aims to:
    - Obtain confirming/denying evidence

Outlook

- Network Situational Assessment is the process of winning knowledge from a set of heterogeneous sensors' output.
- Proposed method pairs-up alerts with actions through a Finite State Machine
  - Aims to:
    - Obtain confirming/denying evidence
    - Survivability

Outlook

- Network Situational Assessment is the process of winning knowledge from a set of heterogeneous sensors' output.
- Proposed method pairs-up alerts with actions through a Finite State Machine
    - Aims to:
        - Obtain confirming/denying evidence
        - Survivability
        - Self-Stabilize

Outlook

- Alerts aggregated into clusters and correlated to measure the impact they have on the affected resource

Outlook

- Alerts aggregated into clusters and correlated to measure the impact they have on the affected resource
- Confidence values for all affected resources are merged to determine overall health of the network.

Outlook

- Alerts aggregated into clusters and correlated to measure the impact they have on the affected resource
- Confidence values for all affected resources are merged to determine overall health of the network.
  - Deteriorating / improving conditions are reflected by changes in the overall Policy Security Level

Future Work

- Project’s Current Status: Component Integration for Review

Future Work

- Project’s Current Status: Component Integration for Review
- Issues:

Future Work

- Project's Current Status: Component Integration for Review
- Issues:
  - Quality of Information from sensors

Future Work

- Project's Current Status: Component Integration for Review
- Issues:
  - Quality of Information from sensors
  - Interoperability w/ framework

Future Work

- Project's Current Status: Component Integration for Review
- Issues:
  - Quality of Information from sensors
  - Interoperability w/ framework
  - Tests

Questions?