System Health Monitoring
and
Proactive Response Activation

Alireza Shameli Sendi
Michel Dagenais

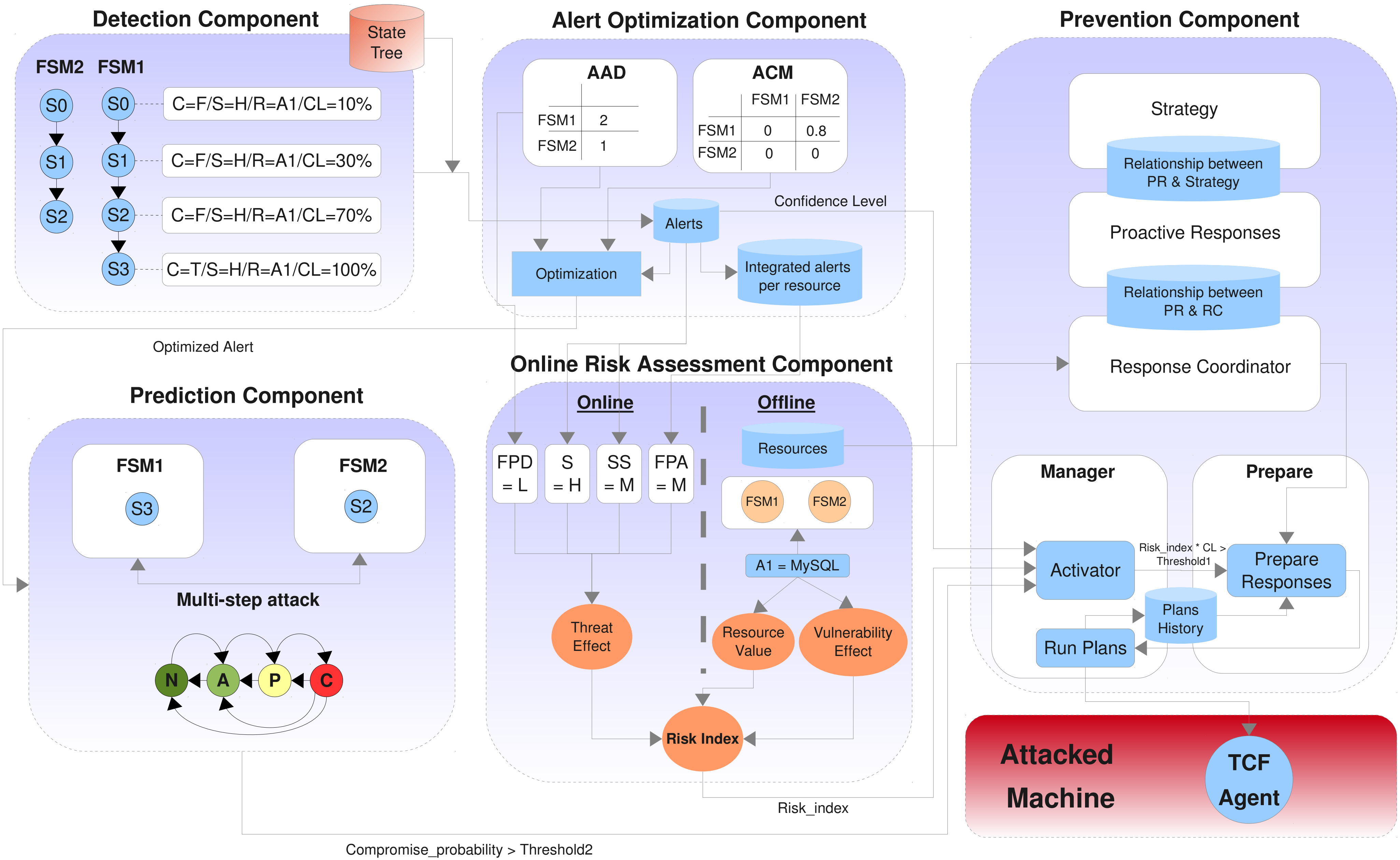
DORSAL

May 11, 2011
École Polytechnique, Montreal

Content

- Architecture
- Prevention
- Taxonomy of Intrusion Response Systems (IRS)
- An overview of development of IRS
- Prevention architecture
    - Proactive Response module
    - Strategy module
    - Response Coordinator module
    - Prepare module
    - Manager module
- Conclusion
- References

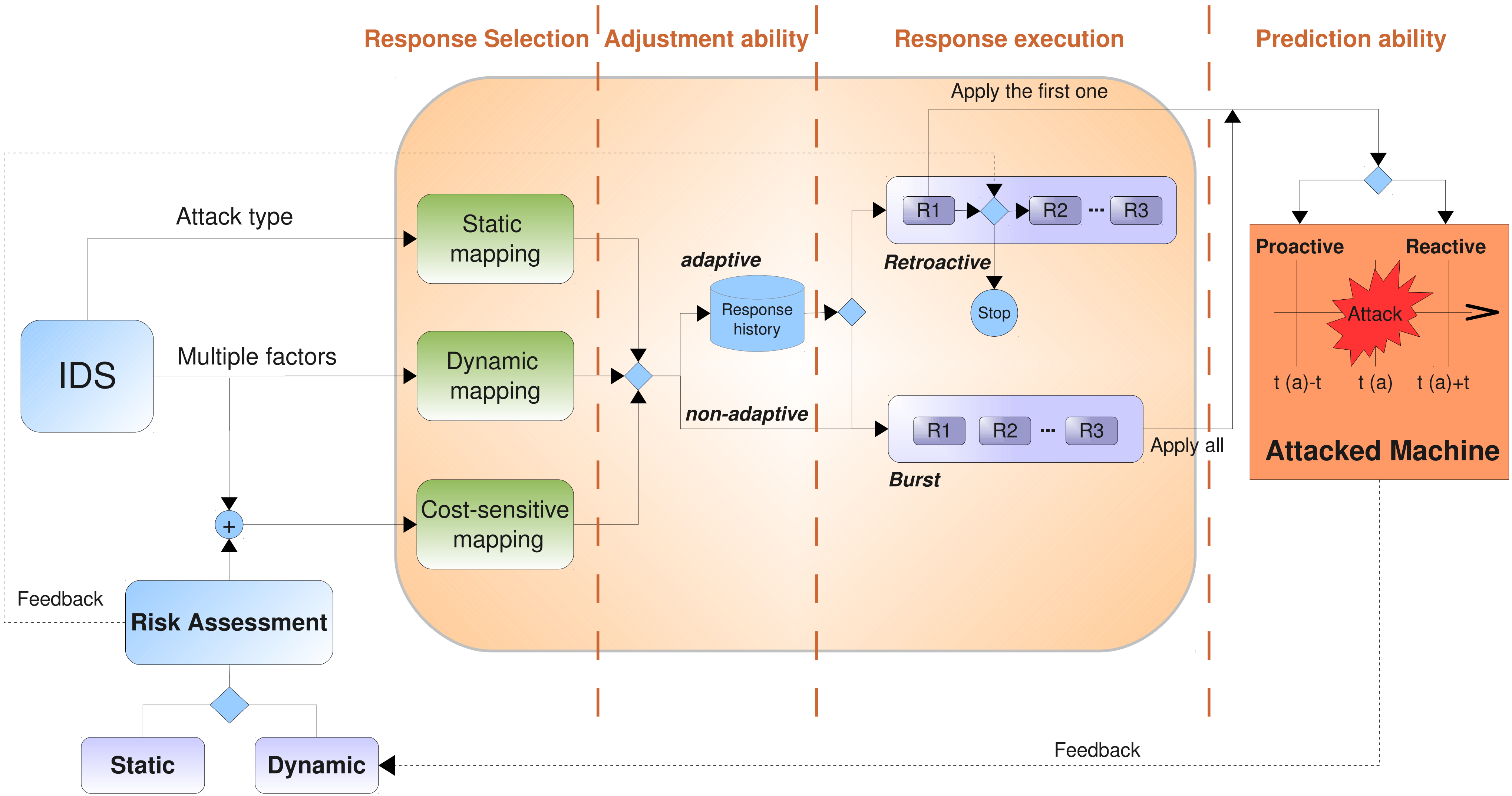
Architecture



Prevention

- Prevention component selects an appropriate level of responses and applies proactive responses with the objectives of:
  - Preventing the problem growth
  - Returning system to the healthy mode
- Selected responses have to be the best set of responses respect to:
  - Predefined strategy
  - Impact to network

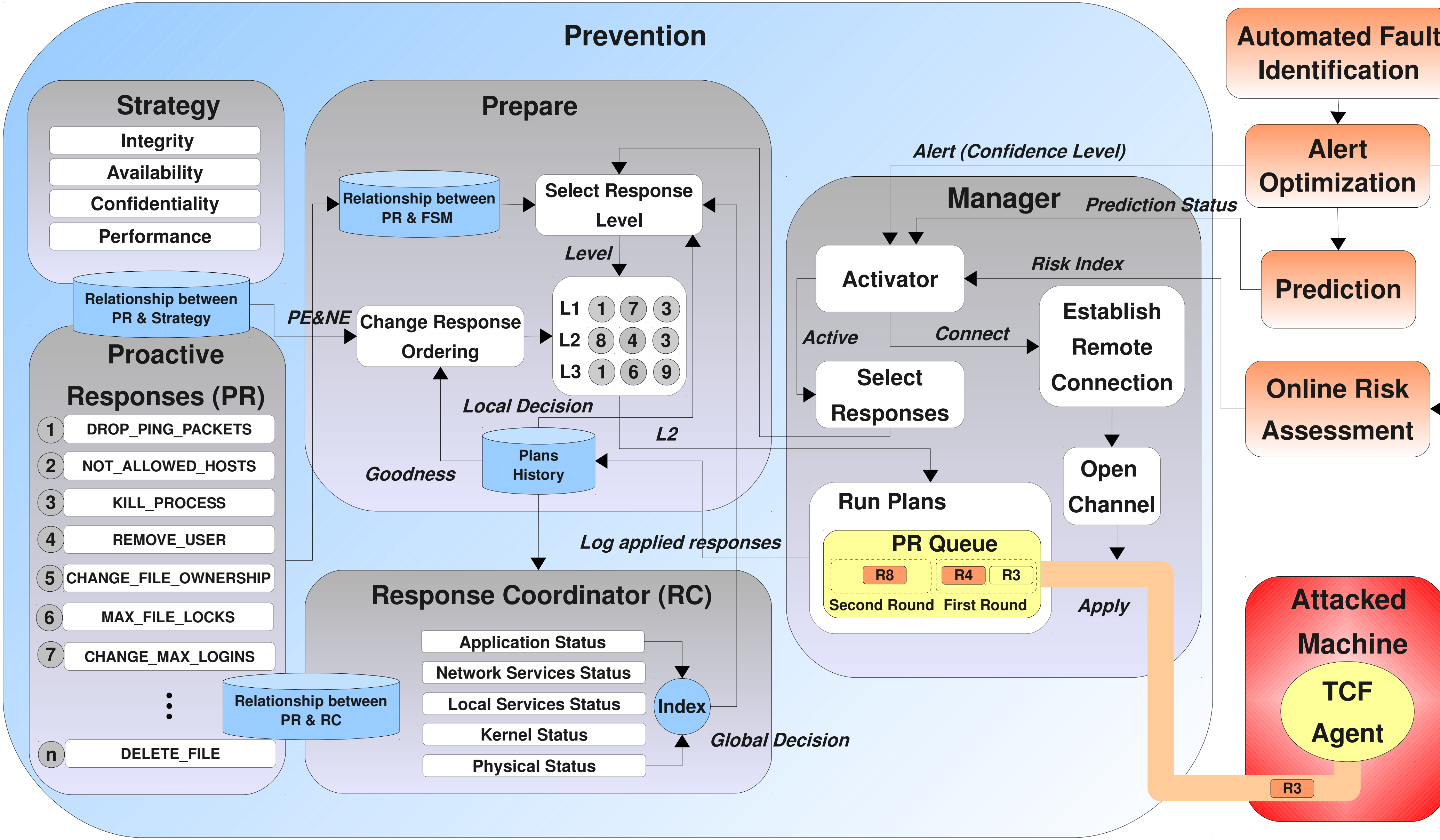
Taxonomy of Intrusion Response Systems



Development of IRS in the last two decade

Intrusion Response System (IRS)	Year Published	Response Selection	Type of Risk Assessment	Risk Assessment Criteria	Response Effectiveness	Adjustment Ability	Prediction ability	Predict Multi-step Attack	Response Execution	Response Feedback	Level of Responses per attack	Locality
DC&A (Fisch)	1996	Dynamic Mapping	-	-	-	non-adaptive	Reactive	No	Burst	-	One	Local
CSM (White et al.)	1996	Dynamic Mapping	-	-	-	non-adaptive	Reactive	No	Burst	-	One	Local
EMERALD (Porras and Neumann)	1997	Dynamic Mapping	-	-	-	non-adaptive	Reactive	No	Burst	-	One	Local
BMSL-based response (Bowen et al.)	2000	Static Mapping	-	-	-	non-adaptive	Reactive	No	Burst	-	One	Local
SoSMART (Musman and Flesher)	2000	Static Mapping	-	-	-	non-adaptive	Reactive	No	Burst	-	One	Local
PH (Somayaji and Forrest)	2000	Static Mapping	-	-	-	non-adaptive	Reactive	No	Burst	-	One	Local
Lee's IRS	2000	**Cost-sensitive**	Static	-	Static	non-adaptive	Reactive	No	Burst	-	One	Local
AAIRS (Curtis and Carver)	2001	Dynamic Mapping	-	-	-	**Adaptive**	Reactive	No	Burst	-	One	Local
SARA (Lewandowski et al.)	2001	Dynamic Mapping	-	-	-	non-adaptive	Reactive	No	Burst	-	One	Local
CITRA (Schnackenberg et al.)	2001	Dynamic Mapping	-	-	-	non-adaptive	Reactive	No	Burst	-	One	Local
TBAIR (Wang et al.)	2001	Dynamic Mapping	-	-	-	non-adaptive	Reactive	No	Burst	-	One	Local
Network IRS (Toth and Kruegel)	2002	**Cost-sensitive**	Static	-	Static	non-adaptive	Reactive	No	Burst	-	One	Local
Tanachaiwiwat 's IRS (Tanachaiwiwat et al.)	2002	**Cost-sensitive**	Static	-	Static	non-adaptive	Reactive	No	Burst	-	One	Local
Specification-based IRS (Balepin et al.)	2003	**Cost-sensitive**	Static	-	Static	non-adaptive	Reactive	No	Burst	-	One	Local
ADEPTS (Foo et al.)	2005	**Cost-sensitive**	Static	-	Static	**Adaptive**	**Proactive**	No	Burst	-	One	Local
Stakhanova's IRS (Stakhanova et al.)	2007	**Cost-sensitive**	Static	-	Static	**Adaptive**	**Proactive**	No	Burst	-	One	Local
DIPS (Haslum et al.)	2007	**Cost-sensitive**	**Dynamic**	Attack metrics	-	non-adaptive	**Proactive**	**Yes**	Burst	-	One	Local
IRDM-HTN (Mu and Li)	2010	**Cost-sensitive**	**Dynamic**	Attack metrics	Static	non-adaptive	Reactive	No	**Retroactive**	One by One	One	Local
Proposed Model	2012	**Cost-sensitive**	**Dynamic**	Attack metrics and **System State**	**Dynamic**	**Adaptive**	**Proactive**	**Yes**	Retroactive-Burst	**Round-based**	**Multi-level**	**Global**

Prevention Architecture



Proactive Responses Module

- Set of 40 Proactive Responses based on interviews of industrial sites including Revolution Linux
- Different types of Proactive Responses:
  - Permanent vs. Transient
    - *PR_ALLOWED_HOSTS/PR_TRANSIENT_DROP_PING_PACKETS*
  - Parametric vs. Non-Parametric
    - *PR_REMOVE_USER/PR_RESET*
  - Pattern vs. Non-Pattern
    - *PR_IPTABLE/PR_LOCK_USER*
  - Strict vs. Non-Strict (limiting the resources consumed)
    - *PR_KILL_PROCESS/PR_MAX_FILE_LOCKS:*

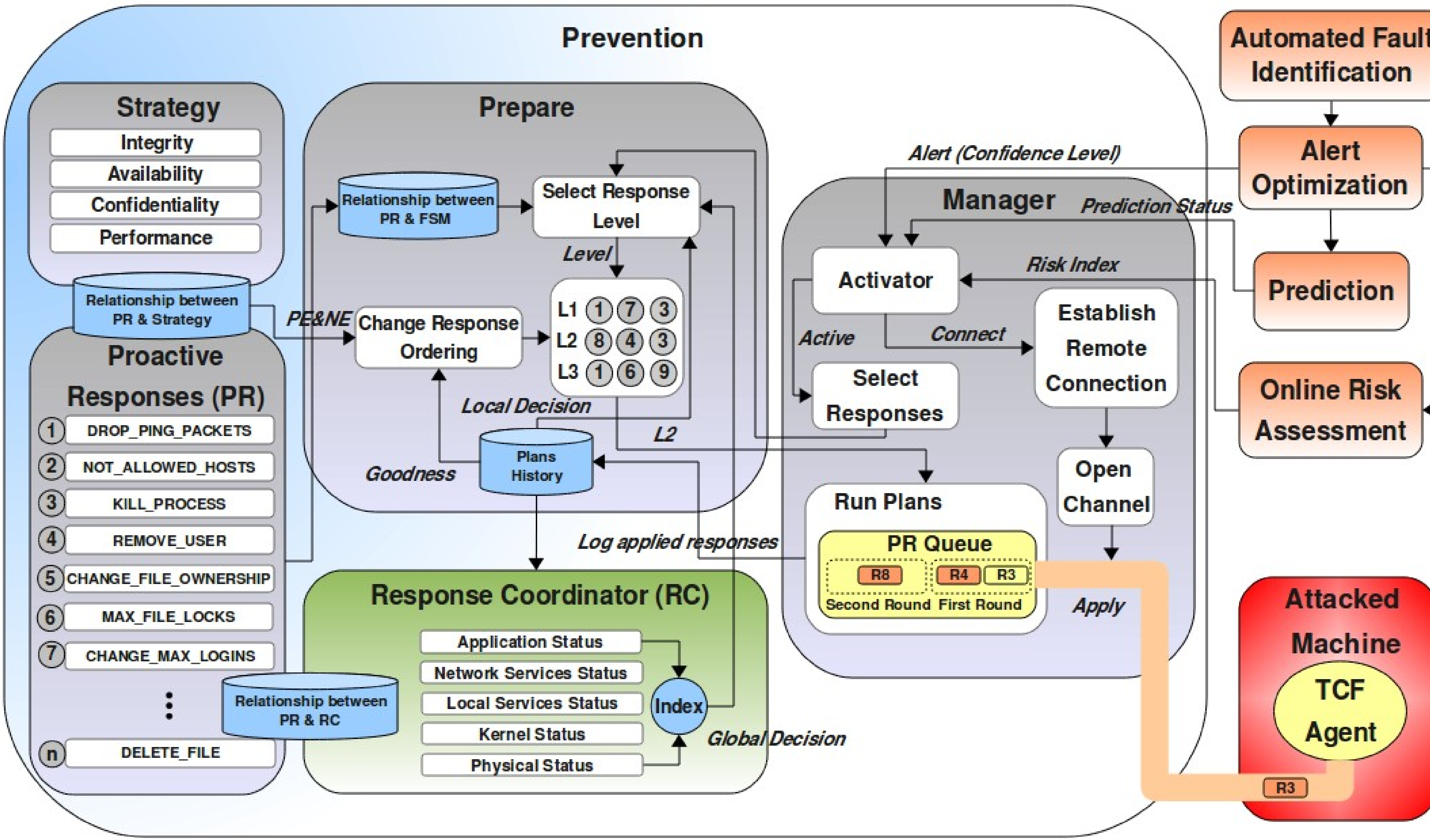
<domain>	<type>	<item>	<value>
smith	soft	nofile	500

Strategy Module

- To react against attacks, we have designed four strategies to evaluate all responses:
  - MAX-Confidentiality (C)
  - MAX-Integrity (I)
  - Availability (A)
  - Performance (P)

	Positive effect on the attacked resource				Negative effect on other resources	
	C	I	A	P	A	P
PR_ISOLATE_SUBNET_NETWORK	0.5	0.4	0	0.6	1	0
PR_REMOVE_USER	1	1	0	0.5	1	0
PR_CHANGE_FILE_OWNERSHIP	1	1	0	0	1	0.2
PR_ALLOWED_HOSTS	0.2	0.1	0	0.3	0.5	0
PR_START_ANTIVIRUS_ANALYSIS	0	0.2	0	0	0.1	0.7
...						

Prevention Architecture



Response Coordinator Module

- All of the proposed response mechanisms focus on the local view of threats and responses and do not have a general view of the network status
- We divide the system status into five general categories:
  - Application Status
  - Network Services Status
  - Local Services Status
  - Kernel Status
  - Physical Status
- The goal of Response Coordinator is:
  - Take a general overview of an attacker's goal in a distributed environment
  - Discover major health problems of the whole network
  - Decide a policy suited for the organization
  - Help the *select_response_level* process to select the more appropriate levels of responses

Relationship between PR & RC

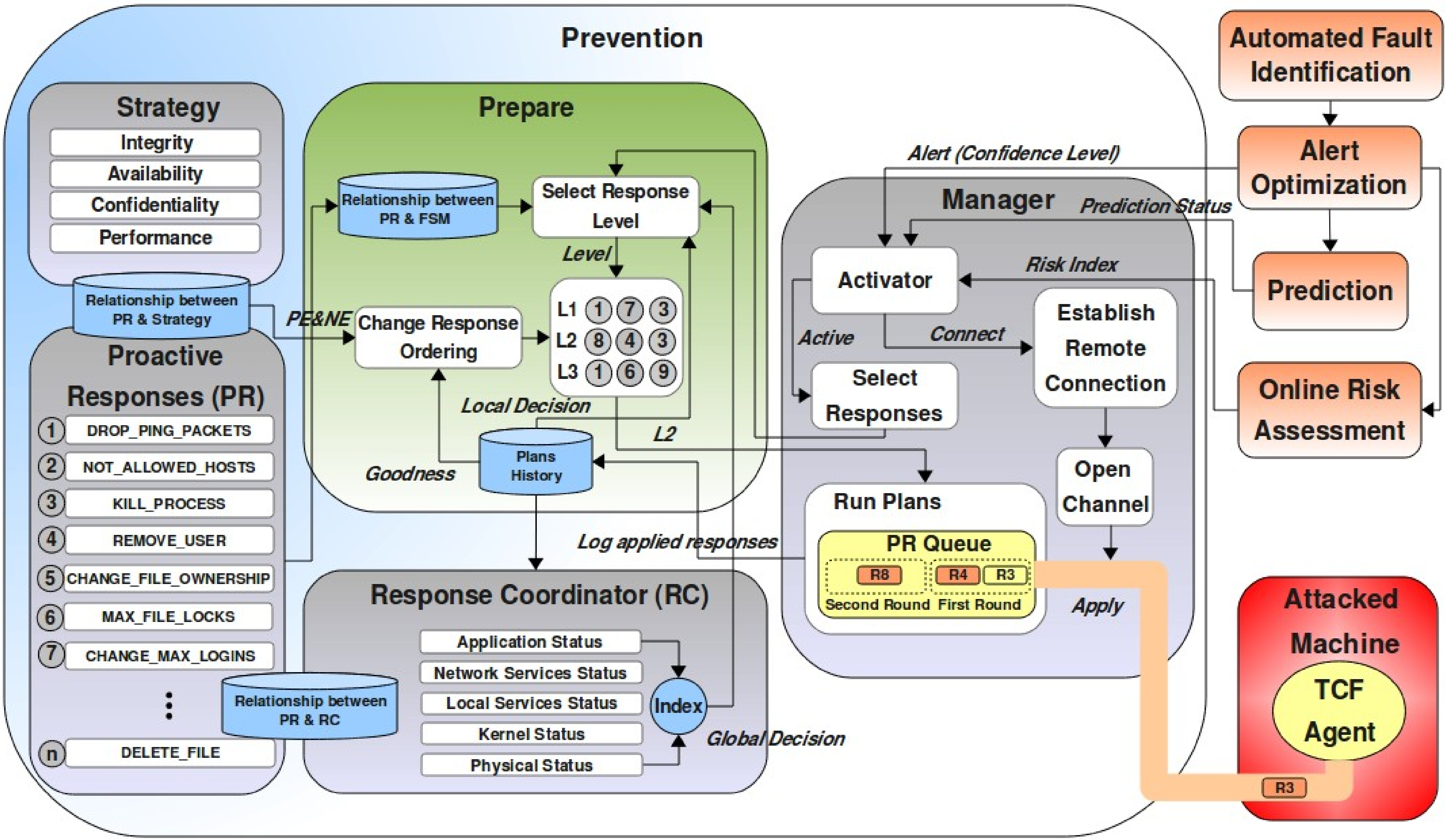
- Each response is associated with one or more Response Coordinator (RC) category
- Each RC category has a weight which represents the importance of the category for the organization (W_A, W_{NS}, W_{LS}, W_K, W_P)
- We activate the categories associated with a response when the sum of the values of the hosts (which applied this response) is greater than a threshold

$\sum_{i=1}^{n} V_{Hi} > THRESHOLD$, **n** is a subset of hosts that a specific response has been applied on them

$$RC_{Index} = \sum_{i=1}^{5} w_i * status_i$$

	Response Coordinator					HOSTS					
	Application	Network Services	Local Services	Kernel	Physical	H1	H2	H3	H4	...	Hn
	w_A	w_{NS}	w_{LS}	w_K	w_P	V_{H1}	V_{H2}	V_{H3}	V_{H4}	...	V_{Hn}
R1	○		○	○				A			
R2	●	●				A	A	A			
R3	●	●		●	●	A		A			A
R4	○		○	○	○		A		A		
...											
Status	M	H	0	L	M						
Index	L										

Prevention Architecture

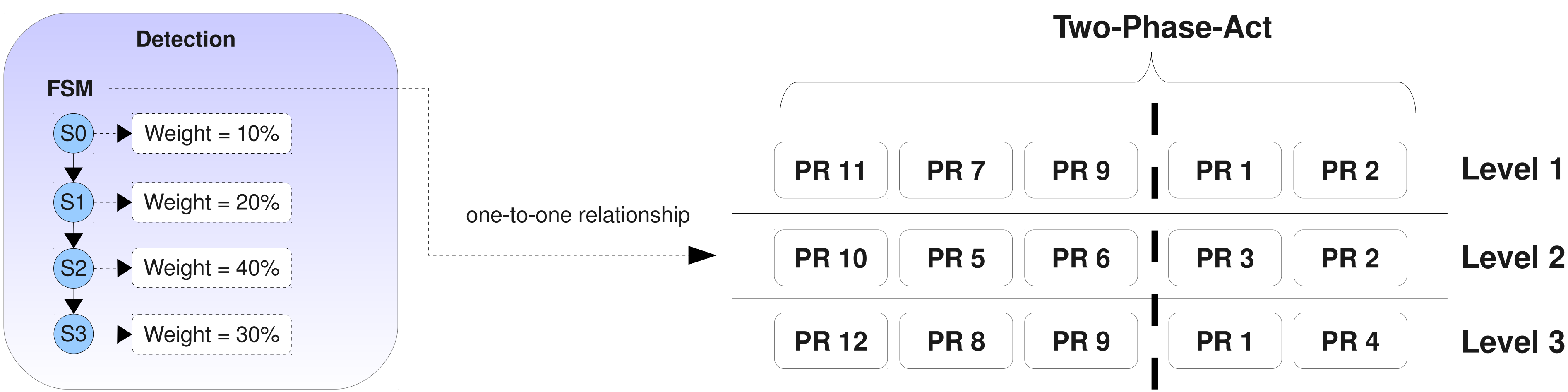


Prepare Module (1)

- Is responsible to select a set of responses
- This module is composed of two processes and two databases:
  - Relationship between PR&FSM DB
  - Plans_history DB
  - Change_response_ordering process
  - Select_response_level process

Prepare Module (2)

- ***Relationship between PR&FSM DB:***
  - Each attack pattern is associated with a FSM
  - For each defined FSM, <u>multiple response</u> actions can be defined in advance
  - Each level is separated into two phases called <u>*two-phase-act*</u>
    - The first phase is composed of the <u>non-disruptive</u> responses
    - The second one can trigger responses that may <u>disrupt</u> the availability of the embedded remote TCF agent



Prepare Module (3)

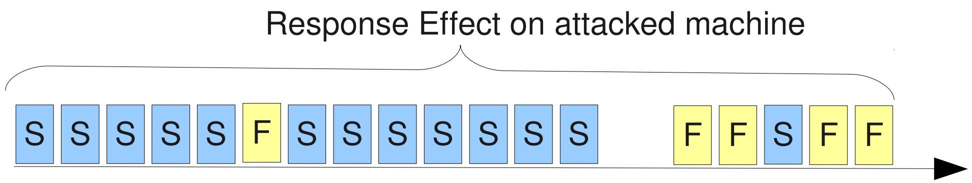
- ***Plans_history DB:***
  - A log file to store: *Target IP, User_Name, Date, Time, Resource, Alert_Name, Level_Id, Round_Responses* and *Round_Success*

- ***Change_response_ordering process:***
  - Is responsible to order the responses of the selected level
  - There are two phases in each level. Ordering algorithm has to be done in each phase separately

$$\text{Response Effectiveness} = [(\text{Positive\_effect}) - (\text{Negative\_effect})] * \text{Goodness}$$

Prepare Module (4)

1

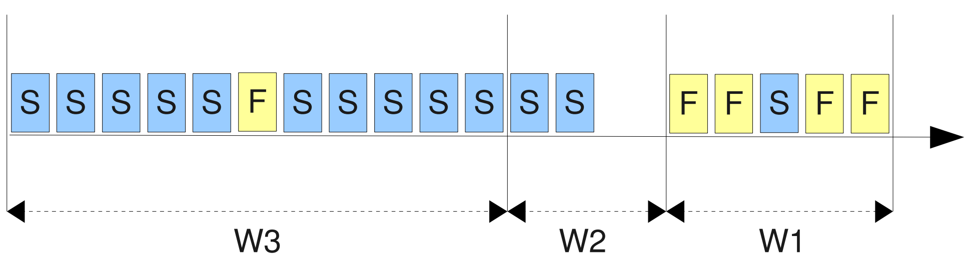


$$Goodness = \frac{\sum_{i=1}^{n} S_i - \sum_{j=1}^{m} F_i}{\sum_{i=1}^{n} S_i + \sum_{j=1}^{m} F_j} = (13-5)/(13+5) = 0.44$$

-1 < Goodness < +1

2

- <u>Sliding window:</u> 1 month
- <u>Calculation technique:</u> Aging algorithm



-2 < Goodness < +2

$$Goodness_{w(k)} = \frac{\dfrac{\sum_{i=1}^{n} S_i - \sum_{j=1}^{m} F_i}{\sum_{i=1}^{n} S_i + \sum_{j=1}^{m} F_j}}{2^{(k-1)}}$$

$$Goodness = \sum_{k=1}^{n} Goodness_{w(k)}$$

$$Goodness_{w(1)} = [(1-4)/(1+4)]/1 = -0.6$$

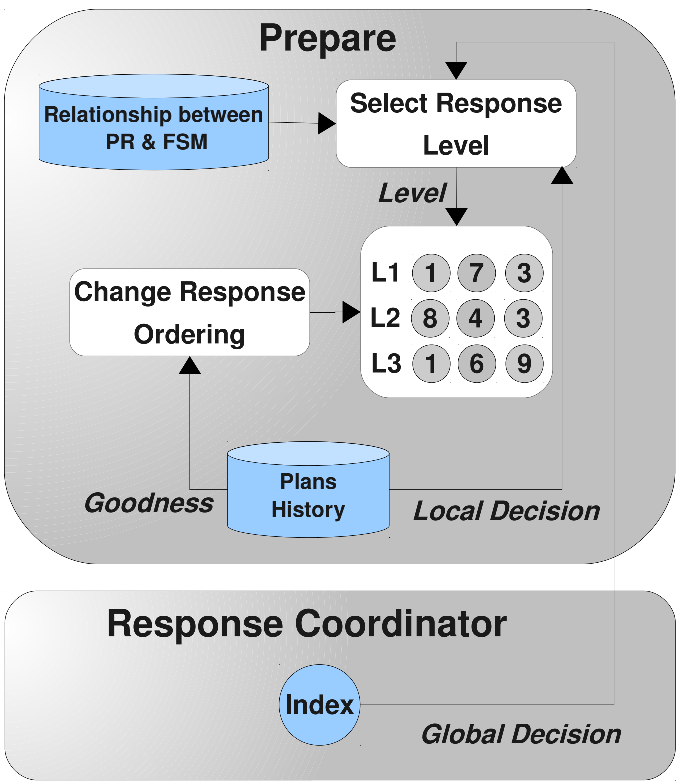
$$Goodness_{w(2)} = [(2-0)/(2+0)]/2 = +0.5$$

$$Goodness_{w(3)} = [(10-1)/(10+1)]/4 = +0.2$$

$$Goodness = 0.1$$

Prepare Module (5)

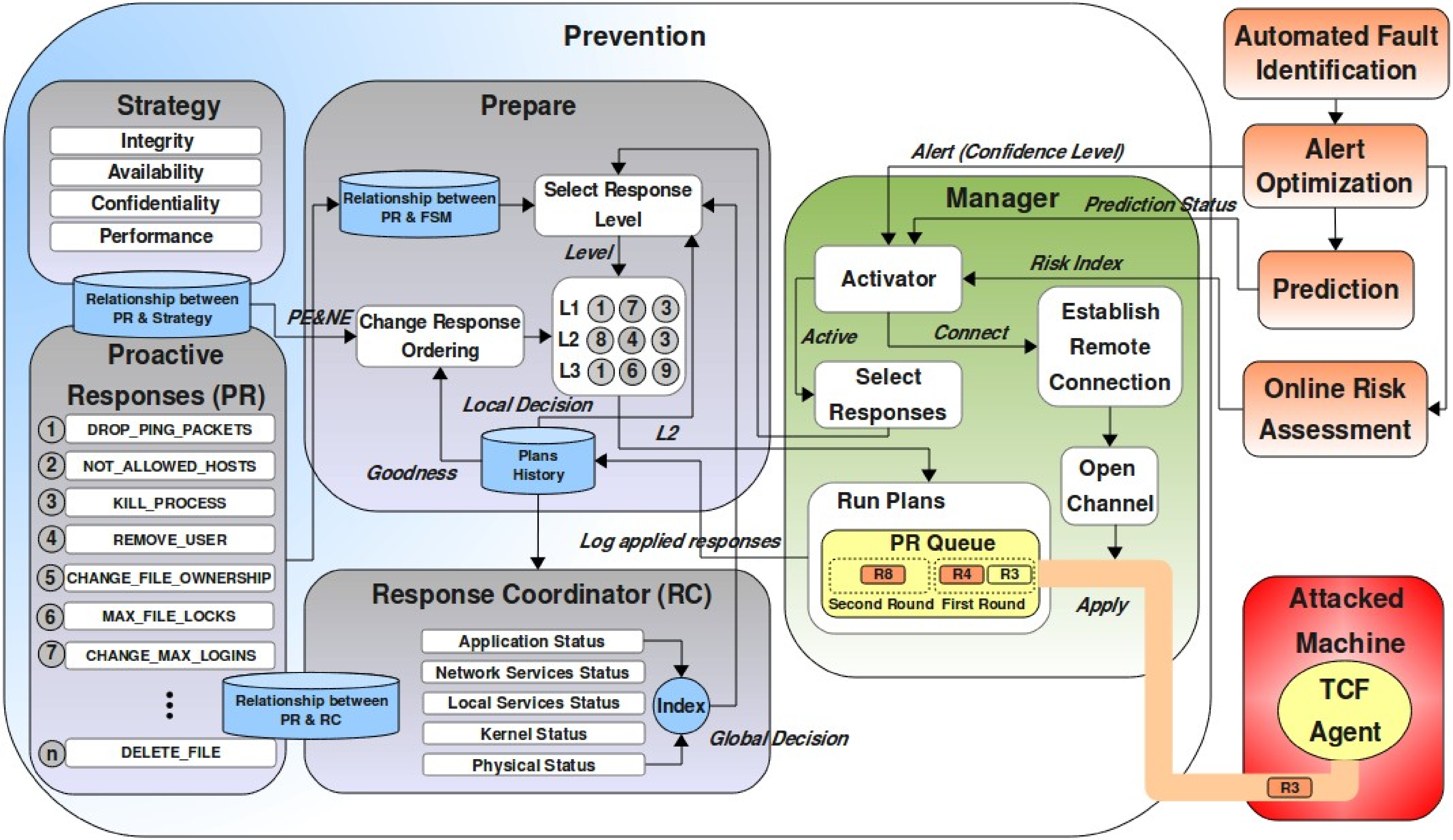
- ***Select_response_level process:***
  - *Local Decision:* comes from *Plans_History DB* that has all history about the target host
  - *Global Decision:* comes from Response Coordinator module which has a general overview of an attacker's goal in a distributed environment
  - If the compromised state of prediction component indicates that a multi-step attack will compromise the system in a close future, the select_response_level process selects the last level of response without any processing



Policies for Dynamic Response Selection

Policy	Prediction condition	Local Condition	Global Condition	Level
P1	FALSE	There is not any information in plans_history	RC.index = low	level = 1
			RC.index = Medium	level = 1
			RC.index = high	level = 2
P2	FALSE	(There is related information in plans_history) **and** (Previous status was successful) **and** (Time of previous run is far to current time)	RC.index = low	level = current_level
			RC.index = Medium	level = current_level
			RC.index = high	level = current_level + 1
P3	FALSE	(There is related information in plans_history) **and** (Previous status was successful) **and** (Time of previous run is near to current time)	RC.index = low	level = current_level
			RC.index = Medium	level = current_level + 1
			RC.index = high	level = current_level + 2
P4	FALSE	(There is related information in plans_history) **and** (Previous status was not successful) **and** (Time of previous run is far to current time)	RC.index = low	level = current_level + 1
			RC.index = Medium	level = current_level + 2
			RC.index = high	level = current_level + 3
P5	FALSE	(There is related information in plans_history) **and** (Previous status was not successful) **and** (Time of previous run is near to current time)	RC.index = low	level = current_level + 2
			RC.index = Medium	level = last_level
			RC.index = high	level = last_level
P6	TRUE	-	-	level = last_level

Prevention Architecture

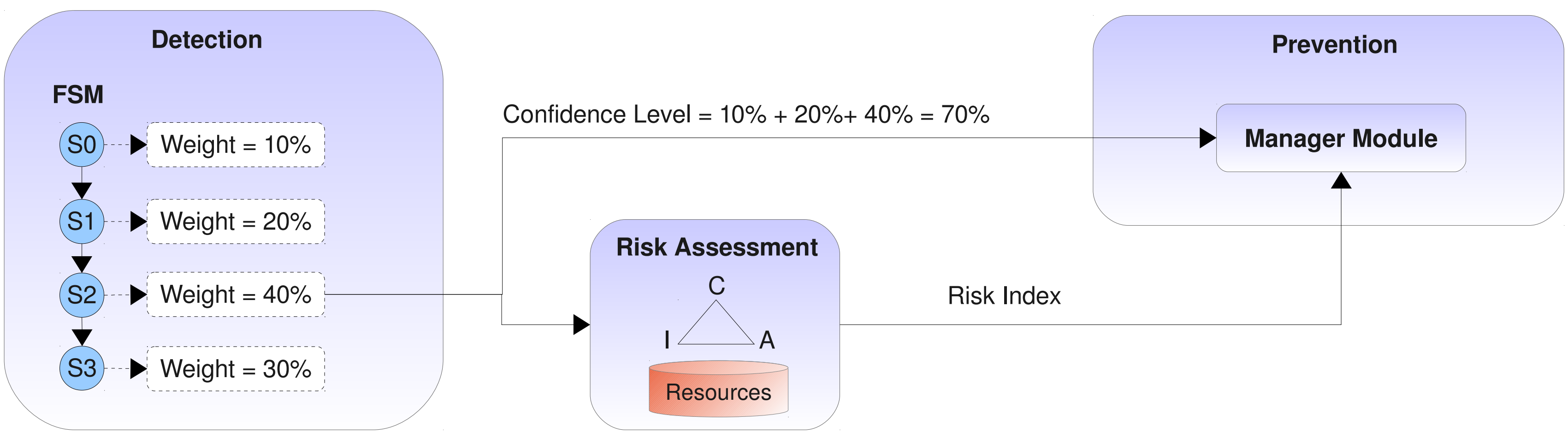


Manager Module (1)

- Receive alerts from the detection, online risk assessment and prediction components and activate the prevention mechanism if the below condition is true:

Risk_index * Confidence_level > Threshold

- Create a channel to the target computer using the Target Communication Framework (TCF) facility
- Apply the first round of Proactive Responses on target computer
- Send the next round of Proactive Responses based on Risk Index of network

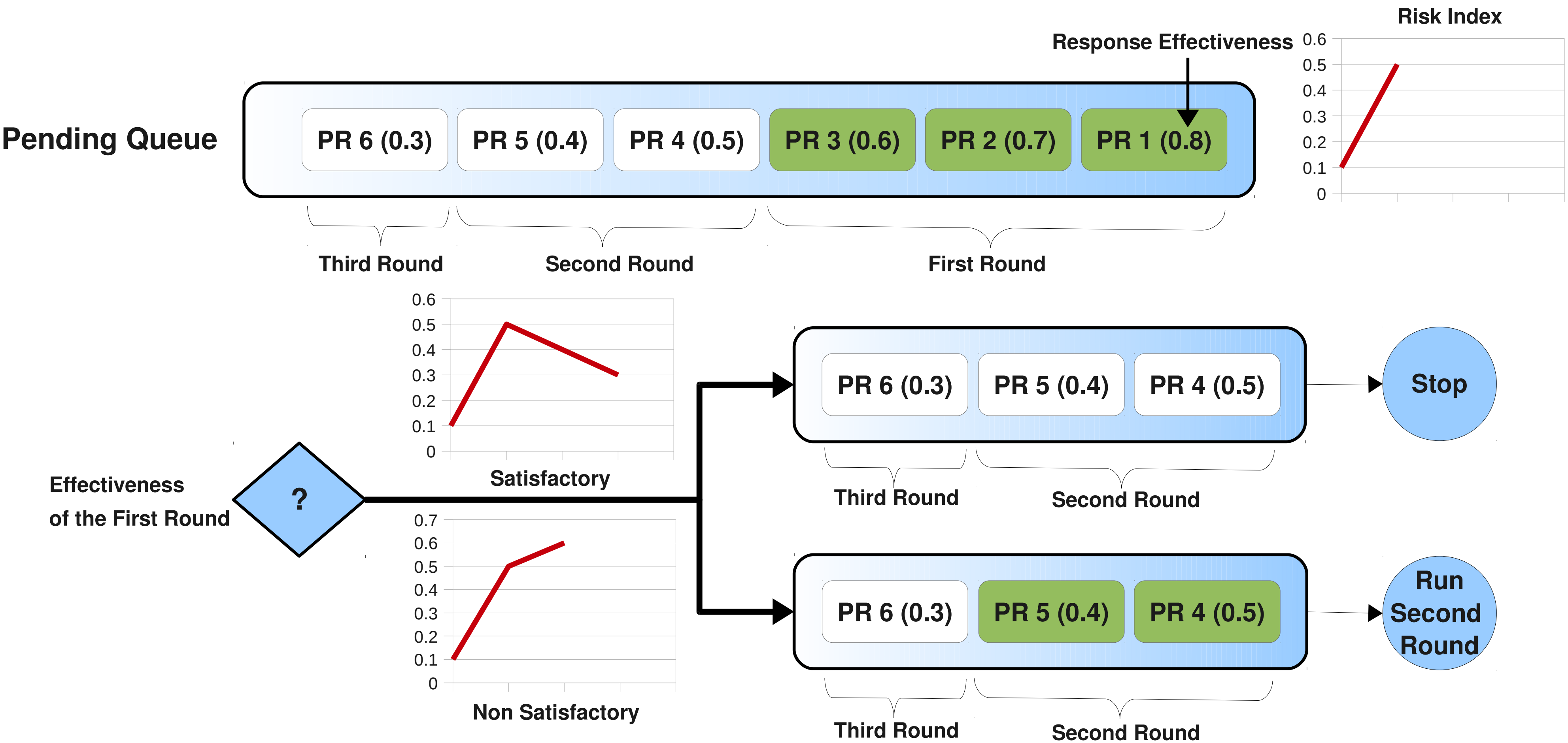


Manager Module (2)

- Why Retroactive-burst approach?
- **Burst approach**
  - Disadvantage:
    - ✓ Cost in performance caused by applying all responses
  - Advantage:
    - ✓ Does not have any delay to mitigate the attack
- **Retroactive approach**
  - Disadvantage:
    - ✓ Attacker has quite some time between responses
    - ✓ Measurement is not accurate enough after applying each response
  - Advantage:
    - ✓ It tries to control the cost in performance by measuring the risk index

Manager Module (3)

- The Run_Plans process is the core of prevention framework and has the *retroactive-burst* execution ability
- A *round-based response mechanism* is proposed



Conclusion

- System health monitoring with the following characteristics:
  - Response actions are triggered **automatically**
  - Response selection model is **cost-sensitive**
  - Application of responses is **adaptive**
  - Response actions are triggered **proactively**
  - Response effectiveness is **dynamic** and is based on previous success or failure of response
  - **Multi-level** responses are available for each attack pattern
  - A **global index** of system health is available
  - Deeper knowledge of operating system such as resource graph (provided by LTTng) lead us to have an accurate online risk assessment

References (1)

[1] F. Xiao, S. Jin and X. Li, "A Novel Data Mining-Based Method for Alert Reduction and Analysis," Journal of Network, vol. 5, no. 1, 2010, pp. 88-97.

[2] M. Desnoyers and M. Dagenais, "LTTng: Tracing across execution layers, from the hypervisor to user-space," Linux Symposium, 2008, Ottawa, Canada.

[3] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems," 2007, http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf .

[4] N. Stakhanova, S. Basu and J. Wong, "Taxonomy of Intrusion Response Systems," Journal of Information and Computer Security, vol. 1, no. 2, 2007, pp. 169-184.

[5] D. B. Payne and H. G. Gunhold, "Policy-based security configuration management application to intrusion detection and prevention," IEEE International Conference on Communications, 2009, Dresden, Germany.

[6] A. Curtis. And J. Carver, "Adaptive agent-based intrusion response," Ph.D thesis, Texas A&M University, USA, 2001.

[7] W. Lee, W. Fan and M. Miller, "Toward Cost-Sensitive Modeling for Intrusion Detection and response," Journal of Computer Security, vol. 10, no. 1, 2002, pp. 5-22.

[8] T. Toth and C. Kregel, "Evaluating the impact of automated intrusion response mechanisms," In proceeding of the 18^{th} Annual Computer Security Applications Conference, Los Alamitos, USA, 2002.

[9] C. P. Mu and Y. Li, "An intrusion response decision-making model based on hierarchical task network planning," Expert systems with applications, vol. 37, no. 3, 2010, pp. 2465-2472.

[10] C.P. Mu, X. J. Li, H.K. Huang and S.F. Tian, "Online risk assessment of intrusion scenarios using D-S evidence theory," 13th European Symposium on Research in Computer Security, pp. 35-48, Malaga, Spain, 2008.

[11] K. Haslum, A. Abraham and S. Knapskog, "DIPS: A framework for distributed intrusion prediction and prevention using hidden markov models and online fuzzy risk assessment," In 3rd International Symposium on Information Assurance and Security, pp. 183-188, Manchester, United Kingdom, 2007.

References (2)

[12] K. Haslum, M. E. G. Moe and S. J. Knapskog, “Real-time intrusion prevention and security analysis of networks using HMMs,” 33rd IEEE Conference on Local Computer Networks, 2008, Montreal, Canada.

[13] B. Zhu and A. A. Ghorbani, “Alert correlation for extracting attack strategies,” International Journal of Network Security, vol. 3, no. 3,2006, pp. 244-258.

[14] C. Kruegel, F. Valeur and G. Vigna, “Alert Correlation,” In Intrusion Detection and Correlation, 1st ed., vol. 14., New York: Springer, 2005, pp. 29-35.

[15] G. Stein, C. Bing, A. S. Wu and K. A. Hua, “Decision Tree Classifier For Network Intrusion Detection With GA-based Feature Selection,” In Proceedings of the 43rd annual Southeast regional conference, Georgia, ISBN:1-59593-059-0, pp. 136-141, 2005.

[16] D. Yu and D. Frincke, “Improving the quality of alerts and predicting intruder's next goal with Hidden Colored Petri-Net,” Computer Networks, pp. 632–654, 2007.

[17] N. B. Anuar, H. Sallehudin, A. Gani and O. Zakaria, “Identifying False Alarm for Network Intrusion Detection System Using Hybrid Data Mining and Decision Tree,” Malaysian Journal of Computer Science, ISSN 0127-9084, 2008, pp. 110-115.

[18] T. Ozyer, R. Alhajj and K. Barker, “Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule pre-screening,” Journal of Network and Computer Applications, SSN:1084-8045, 2007, pp. 99-113.

[19] H. Jin, J. Sun, H. Chen and Z. Han, “A Fuzzy Data Mining Based Intrusion Detection Model,” 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, pp. 191-197, 2004.

[20] Q. Xu, W. Pei, L. Yang and Q. Zhao, “An Intrusion Detection Approach Based On Understandable Neural Network Trees,” Journal of Electronics, 2007, pp. 574-579.

[21] Y. Bouzida and F. Cuppens, “Neural networks vs. decision trees for intrusion detection,” IEEE/IST Workshop on Monitoring, Germany, September, 2006.

References (3)

[22] R. C. Chen, K. F. Cheng, Y. H. Chen, C. F. Hsieh, “Using Rough Set and Support Vector Machine for Network Intrusion Detection System,” First Asian Conference on Intelligent Information and Database Systems, pp. 465-470, 2009.

[23] L. Khan, M. Awad and B. Thuraisingham, “A new intrusion detection system using support vector machines and hierarchical clustering,” ISSN:1066-8888, pp. 507-521, 2007.

[24] J. C. Liu, C. H. Lin, J. L. Yu, W. S. Lai and C. H. Ho, “Anomaly Detection Using LibSVM Training Tools,” International Journal of Security and Its Applications, Vol.2 , No.4, ISBN: 978-0-7695-3126-7, 2008, pp. 166-177.

[25] R. Zhang, S. Zhang , S. Muthuraman and J. Jiang, “One class support vector machine for anomaly detection in the communication network performance data,” Proceedings of the 5th conference on Applied electromagnetics, wireless and optical communications, Spain, ISBN:1790-5117, pp. 31-37, 2007.

[26] A. Abraham, R. Jain, J. Thomas and S. Y. Han, “D-SCIDS: Distributed soft computing intrusion detection system,” Journal of Network and Computer Applications, pp. 81–98, 2007.

[27] Abdelhamid, “Réseaux Bayésiens Naïfs Augmentés TAN pour les Systèmes de Détection d’Intrusions,” PhD thesis, Université de Nice Sophia Antipolis, 2007.

[28] N. Abouzakhar, A. Gani, G. Manson, M. Abuitbel and D. King, “Bayesian Learning Networks Approach to Cybercrime Detection,” Proceedings of the 2003 PostGraduate Networking Conference, Liverpool, United Kingdom, 2003.

[29] Difference between Signature Based and Anomaly Based Detection in IDS, URL http://www.secguru.com/forum/difference_between_signature_based_and_anomaly_based_detection_in_ids.

[30] http://www.prelude-technologies.com/en/welcome/index.html.

[31] L. Feng, W. Wang, L. Zhu and Y. Zhang, “Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation,” Journal of Networks and Computer Applications, vol. 32 n. 3, 2009, pp. 721-732.

[32] A. O. Adetunmbi, S. O. Falaki, O. S. Adewale and B. K. Alese, “Network Intrusion Detection based on Rough Set and k-Nearest Neighbour,” International Journal of Computing and ICT Research, Vol. 2, No. 1, 2008, pp. 60–66.

References (4)

[33] A. Lazarevic, L. Ertöz, V. Kumar, A. Ozgur, J. Srivastava, “A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection,” Proceedings of the Third SIAM International Conference on Data Mining, 2003.

[34] V. Chandola, A. Banerjee and V. Kumar, “Anomaly Detection: A Survey, ACM Computing Surveys,” Vol. 41(3), 2009.

[35] S. Cherednichenko, “Outlier Detection in Clustering,” 2005.

[36] Q. Wang and V. Megalooikonomou, “A Clustering Algorithm for Intrusion Detection,” The SPIE Conference on Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, Florida, vol. 5812, pp. 31–38, 2005.

[37] J. Hanand M. Kamber, “Mining: Concepts and Techniques,” 2nd ed., San Francisco: Elsevier, 2006.

[38] P. Domingos and G. Hulten, “Mining high-speed data streams,” In Proc. 2000 ACM SIGKDD Int. Conf. Knowledge Discovery in Databases (KDD’00), pp. 71–80, Boston, MA, Aug. 2000.

[39] P. Domingos and G. Hulten, “Mining High-Speed Data Streams,” Proceedings of the Association for Computing Machinery Sixth International Conference on Knowledge Discovery and Data Mining, pp. 71–80, 2000.

[40] G. Hulten, L. Spencer, and P. Domingos, “Mining time-changing data streams,” In Proc. 2001 ACM SIGKDD Int. Conf. Knowledge Discovery in Databases (KDD’01), San Francisco, CA, Aug. 2001.

[41] M. Gaber, A. Zaslavsky and S. Krishnaswamy, “Mining Data Streams: A Review,” ACM SIGMOD Record, Vol. 34, 2005.

[42] C. Aggarwal, J. Han, J. Wang, and P. Yu, “A Framework for Projected Clustering of High Dimensional Data Streams,” Proceedings of the 30th VLDB Conference, Toronto, Canada, 2004.

[43] MIT Lincoln Laboratory, 2000 darpa intrusion detection scenario specific data sets, 2000.

References (5)

[44] J. Han, H. Cheng, D. Xin, and X. Yan. "Frequent pattern mining: Current status and future directions," Data Mining and Knowledge Discovery, 2007.

[45] G. Manku and R. Motwani, "Approximate frequency counts over data streams," In Proc. 2002 Int. Conf. Very Large Data Bases (VLDB'02), pp. 346–357, Hong Kong, China, 2002.

[46] T. Zhang, R. Ramakhrisnan, M. Livny, "BIRCH: An Efficient Data Clustering Method for Very Large Databases," Proc. ACM SIGMOD Int. Conf. Management of Data, 1996.

[47] North Carolina State University Cyber Defense Laboratory, "Tiaa: A toolkit for intrusion alert analysis," http://discovery.csc.ncsu.edu/software/correlator/ver0.4/index.html.

[48] L. R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," Proc. IEEE, 77, pp. 257-286, 1989.

[49] RealSecure Signatures Reference Guide. Internet Security Systems, http://documents.iss.net/literature/RealSecure/RS_Signatures_6.0.pdf.

[50] The Snort Project, Snort users manual 2.8.5, 2009.

[51] G. Antoniol. Keynote paper "Search based software testing for software security: Breaking code to make it safer," In ICSTW '09: Proceedings of the IEEE International Conference on SoftwareTesting, Verification, and Validation Workshops, IEEE Computer Society, 2009.

[52] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[53] H. Debar, D. Curry and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)," http://www.ietf.org/rfc/rfc4765.txt.

[54] http://wiki.eclipse.org/DSDP/TCF.

References (6)

[55] G. Matni and M. Dagenais, "Automata-based approach for kernel trace analysis," Canadian Conference on Electrical and Computer Engineering, pp. 970-973, 2009.

[56] NCSA Security Research, "Mithril: An Experiment in Adaptive Security," 2006, http://security.ncsa.illinois.edu/research/mithril/Mithril.html.

[57] Y.-M. Chen and Y. Yang, "Policy management for network-based intrusion detection and prevention," In IEEE Network Operations and Management Symposium, 2004.

[58] G. White, E. Fisch and U. Pooch "Cooperating security managers: a peer-based intrusion detection system," IEEE Network, Vol. 10, 1996, pp. 20–23.

[59] P. Porras and P. Neumann, "EMERALD: event monitoring enabling responses to anomalous live disturbances," National Information Systems Security Conference, 1997.

[60] B. Foo, Y.-S. Wu, Y.-C. Mao, S. Bagchi and E. Spafford, "ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment," International Conference on Dependable Systems and Networks, pp. 508–517, 2005.

[61] I. Balepin, S. Maltsev, J. Rowe and K. Levitt "Using specification-based intrusion detection for automated response," In 6th International Symposium on Recent Advances in Intrusion Detection, pp. 136–154, 2003.

[62] T. Toth, and C. Kruegel, "Evaluating the impact of automated intrusion response mechanisms," In 18th Annual Computer Security Applications Conference, 2002.

[63] S. Tanachaiwiwat, K. Hwang, and Y. Chen, "Adaptive Intrusion Response to Minimize Risk over Multiple Network Attacks," ACM Trans on Information and System Security, 2002.

[64] N. B. Anuar, M. Papadaki, S. Furnell and N. Clarke, "An investigation and survey of response options for intrusion response systems," Information Security for South Africa, pp. 1-8, 2010.

[65] K. Nielsen, "Gentoo Security Handbook," 2010.

References (7)

[66] K. Fenzi and D. Wreski, “Linux Security HOWTO,” http://tldp.org/HOWTO/Security-HOWTO .

[67] J. Turnbull, “Hardening Linux,” USA: Apress, 2005.

[68] M. F. Yusof, “Automated Signature Generation of Network Attacks,” B.S thesis, University Teknologi Malasia, 2009.

[69] A. S. Sendi, M. Jabbarifar, M. Shajari, and M. Dagenais, “FEMRA: Fuzzy Expert Model for Risk Assessment,” Fifth International Conference on Internet Monitoring and Protection, pp. 48-53, Barcelona, Spain, 2010.

[70] A. S. Sendi and M. Dagenais, “Real Time Intrusion Prediction based on improving the priority of alerts with Hidden Markov Model,” has been submitted to the *Journal of network*.

[71] P. Arnes, F. Valeur and R. Kemmerer, “Using hidden markov models to evaluate the risk of intrusions,” Int. Symp. Recent Advances in Intrusion Detection, Hamburg, Germany, 2006.

[72] W. Li, Z. Guo, "Hidden Markov Model Based Real Time Network Security Quantification Method," nswctc, International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 94-100, 2009.

[73] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems,” http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[74] International Standard Organization, ISO/IEC 27005, Information Security Risk Management, 2008.

[75] Z. Li, Z. Lei, L. Wang and D. Li, “Assessing attack threat by the probability of following attacks,” in Proceedings of the International Conference on Networking, Architecture, and Storage, IEEE, pp. 91–100, 2007.

[76] N. Stakhanova, S. Basu and J. Wong, “A cost-sensitive model for preemptive intrusion response systems,” Proceedings of the 21st International Conference on Advanced Networking and Applications, IEEE Computer Society, Washington, DC, USA, pp. 428–435, 2007.

References (8)

[77] C. Strasburg, N. Stakhanova, S. Basu and J. S. Wong, “A Framework for Cost Sensitive Assessment of Intrusion Response Selection,” Proceedings of IEEE Computer Software and Applications Conference, 2009.

[78] https://help.ubuntu.com/community/AppArmor.

[79] A. S. Sendi, M. Dagenais, J. Desfossez and M. Couture, “A Health Framework for Automated Intrusion Response System,” has been submitted to the *Ninth Annual Conference on Privacy, Security and Trust.*

[80] http://www.nsa.gov/research/selinux/.