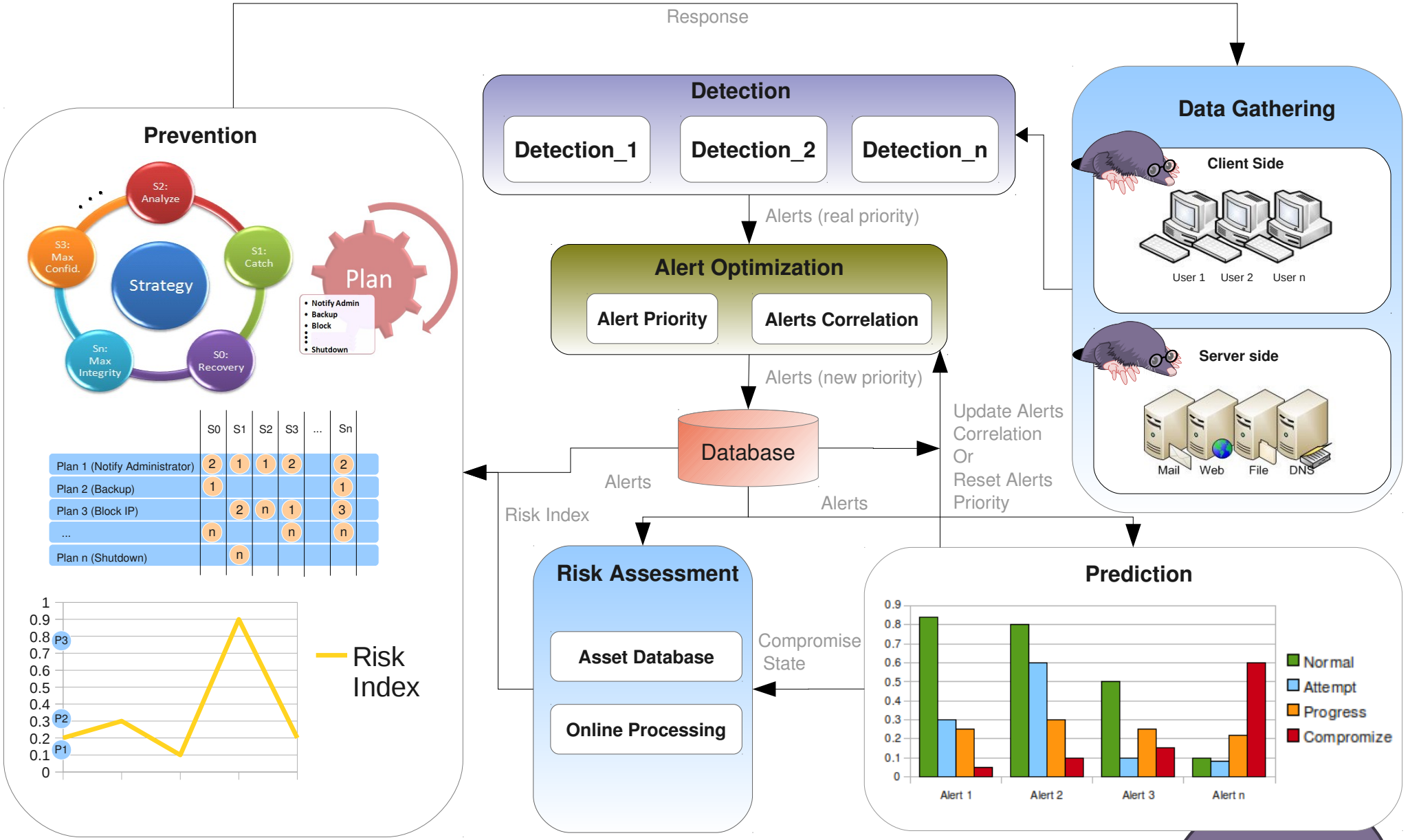
System Health Monitoring and Reactive Measures Activation

Alireza Shameli Sendi
Michel Dagenais
DORSAL
December 8, 2010
École Polytechnique, Montreal

Content

- **Definition, components and architecture**
- **Component Implementation Status**
- **Alert optimization**
- **Prediction**
- **Risk Assessment**
- **Prevention**
- **Future work**
- **Conclusion**
- **References**

System Health Monitoring Architecture



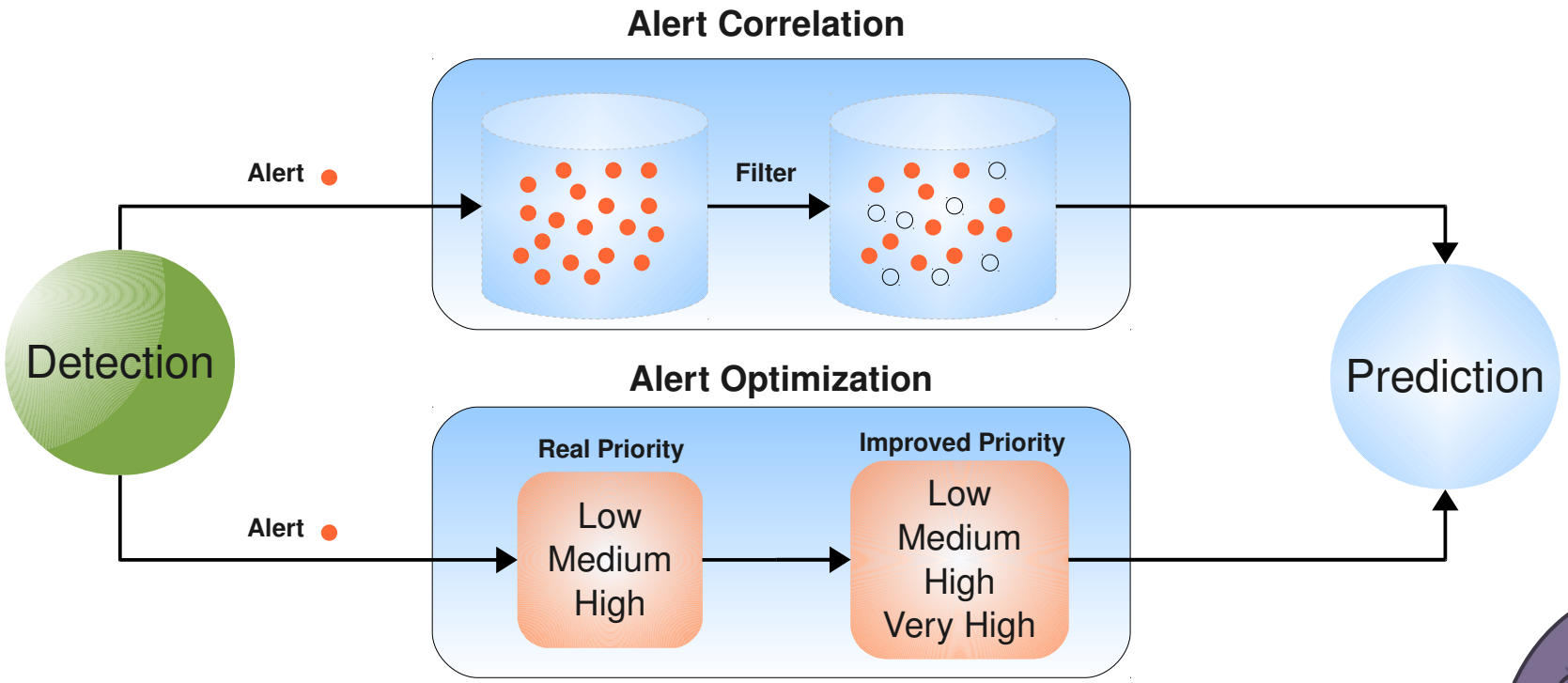
Component Implementation Status

Component	Design & Implementation Status	Integration status
Alert Optimization	- Implementing a framework to improve alert priority based on: - Effect of Alert - Frequency of each Alert - Acceptable number of alert per day	- Prediction - Risk Assessment
Prediction	- Testing prediction algorithm(HMM) with MIT Dataset (Network packets)	- Alert Optimization
Online Risk Assessment	- Designing Asset Database for risk assessment - Testing risk assessment algorithm(HMM) with MIT Dataset (Network packets)	- Alert Optimization
Prevention	- Using Target Communication Framework (TCF) to apply Reactive Measures - Identified 35 Reactive Measures - Implemented 20 Reactive Measures	

Alert Optimization

Alert Optimization

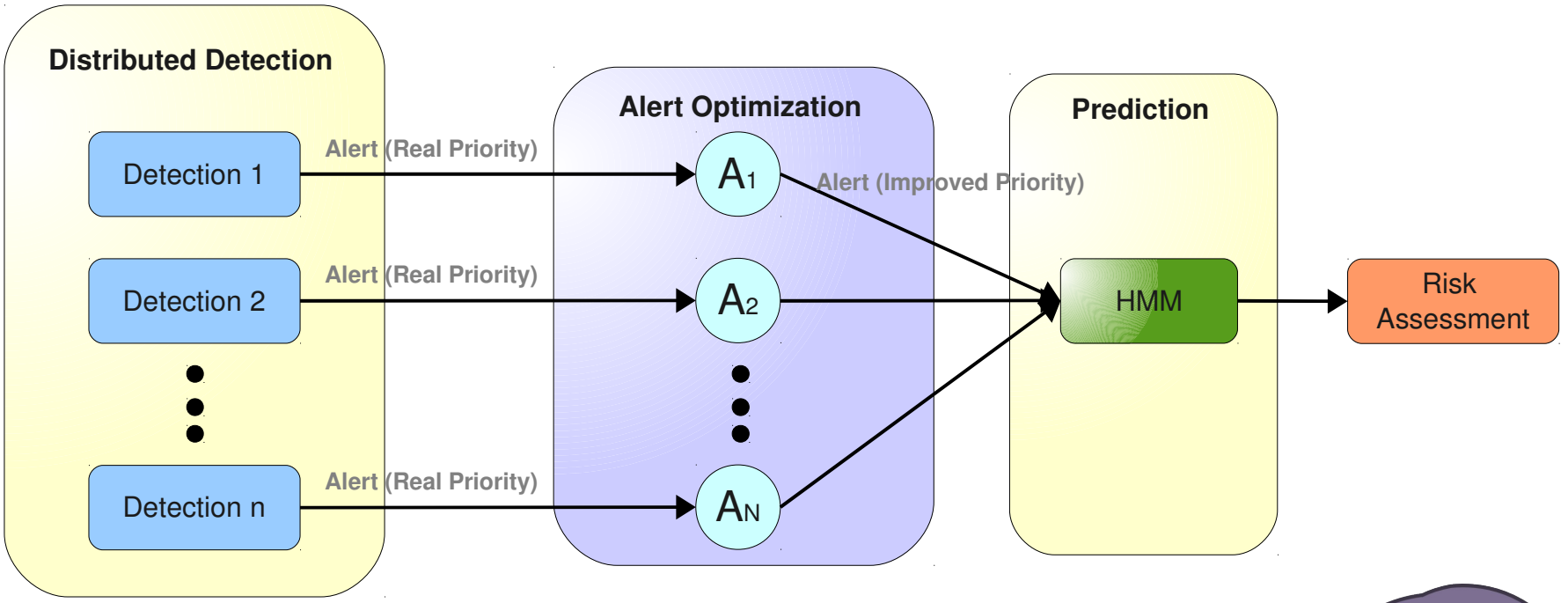
- Alert optimization component keeps all alerts but **increases some alert priority with correlation concepts**
- Alert correlation means to extract true alerts from alerts generated by detection component (filter view)
- Multi steps attack's actions are unknown but may be partially detected by detection component and reported as alerts



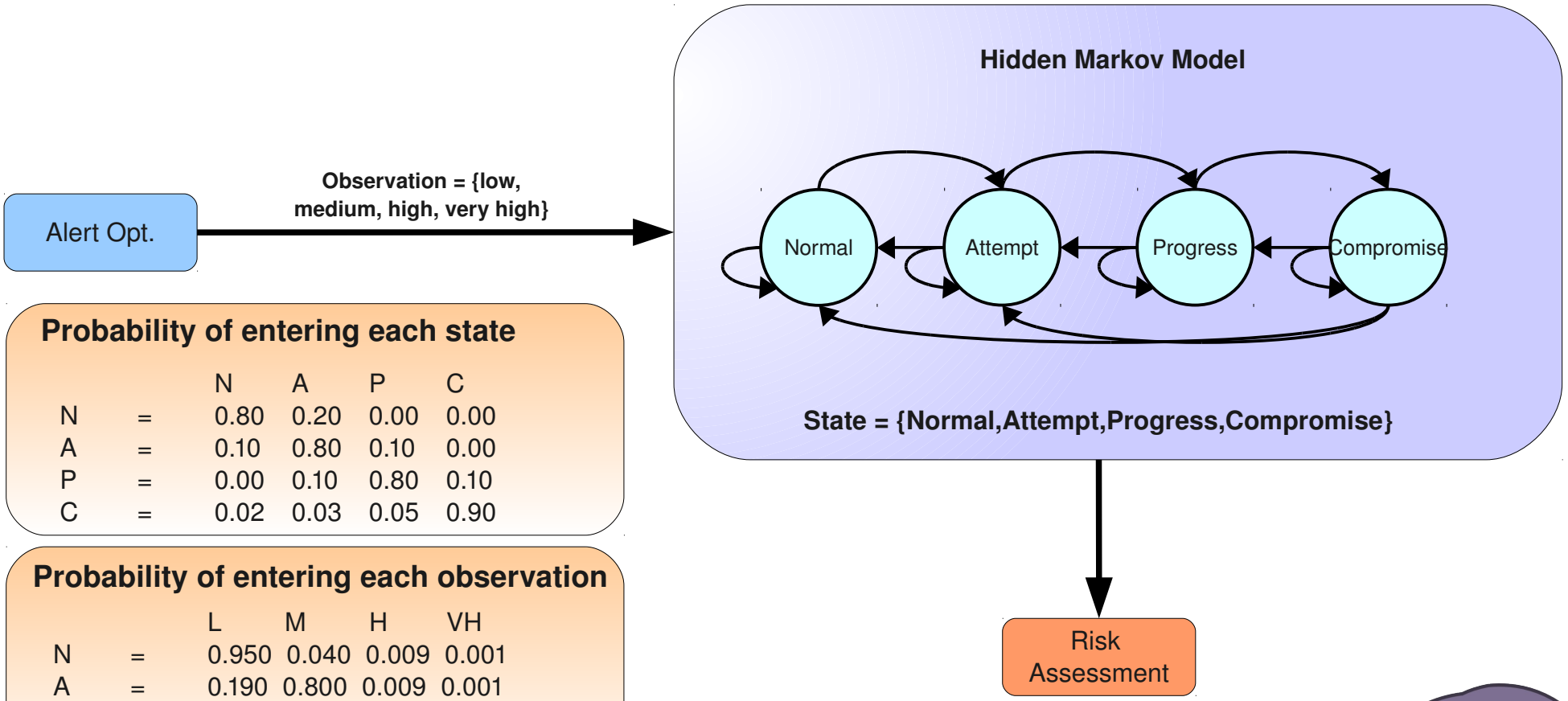
Prediction

Prediction Structure

- The prediction component will attempt to make a prediction of a possible future problem
- A model is needed to capture the interaction between the attacker and the distributed network



Prediction Algorithms-HMM



Probability of entering each state

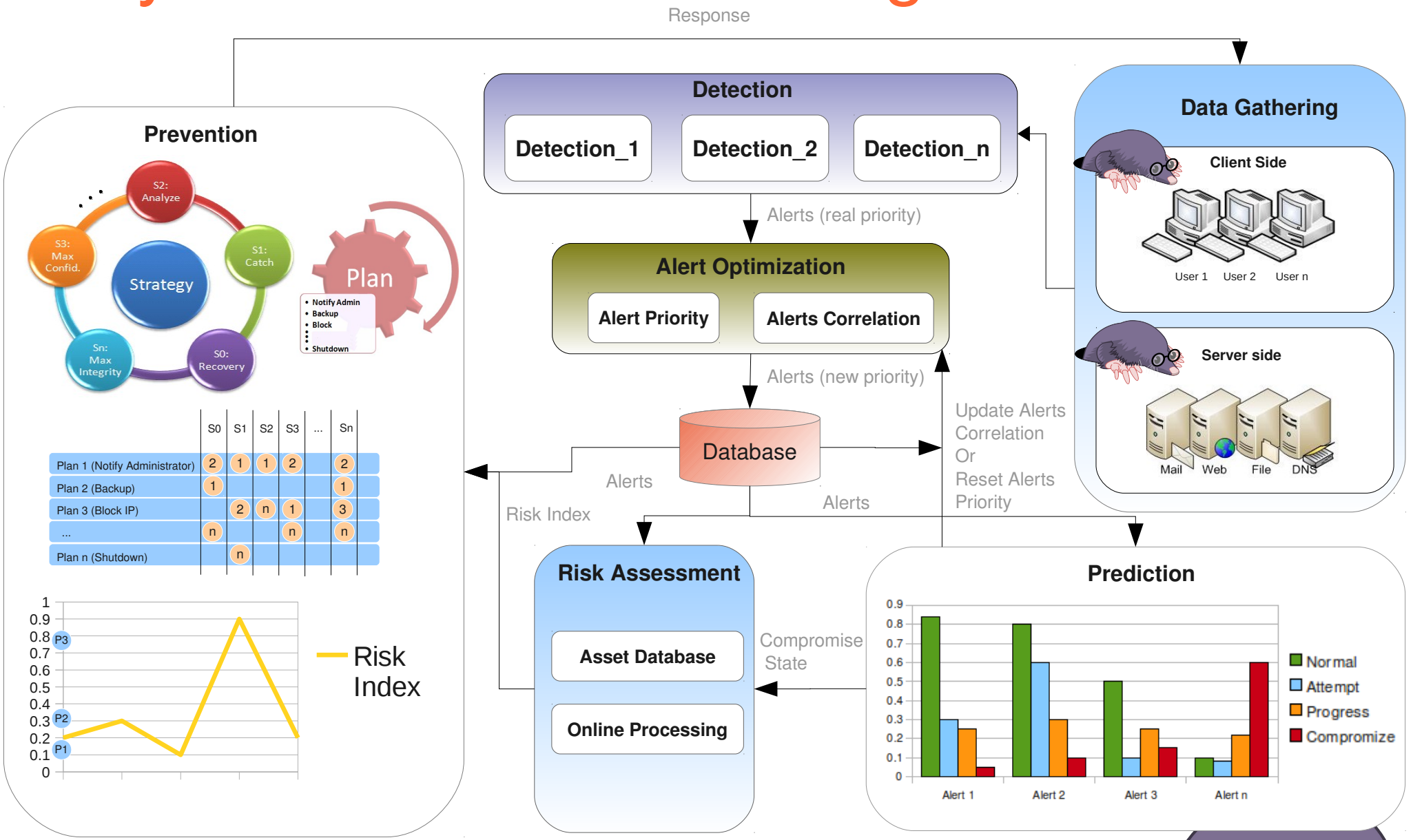
		N	A	P	C
N	=	0.80	0.20	0.00	0.00
A	=	0.10	0.80	0.10	0.00
P	=	0.00	0.10	0.80	0.10
C	=	0.02	0.03	0.05	0.90

Probability of entering each observation

		L	M	H	VH
N	=	0.950	0.040	0.009	0.001
A	=	0.190	0.800	0.009	0.001
P	=	0.010	0.190	0.700	0.100
C	=	0.010	0.040	0.200	0.750

Risk Assessment

System Health Monitoring Architecture

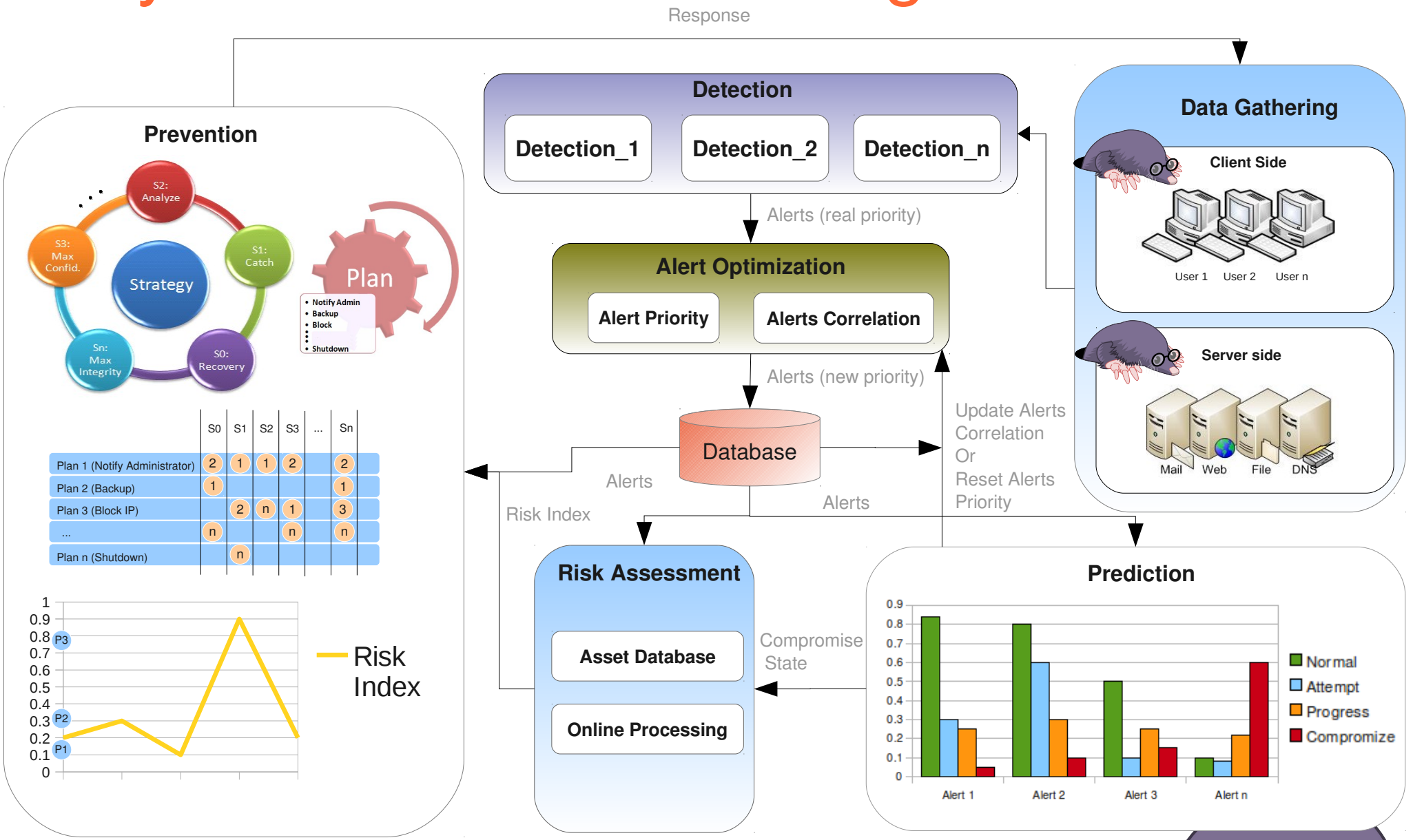


Risk Assessment

- Risk assessment is the process of identifying, characterizing, and understanding risk.
- The result of risk assessment, risk index, provides decision support for the prevention component.
- Risk index has three aspects:
  - The probability that an abnormal activity detected is a true problem
  - The probability that a problem can successfully compromise its target
  - The severity of the consequences

Prevention

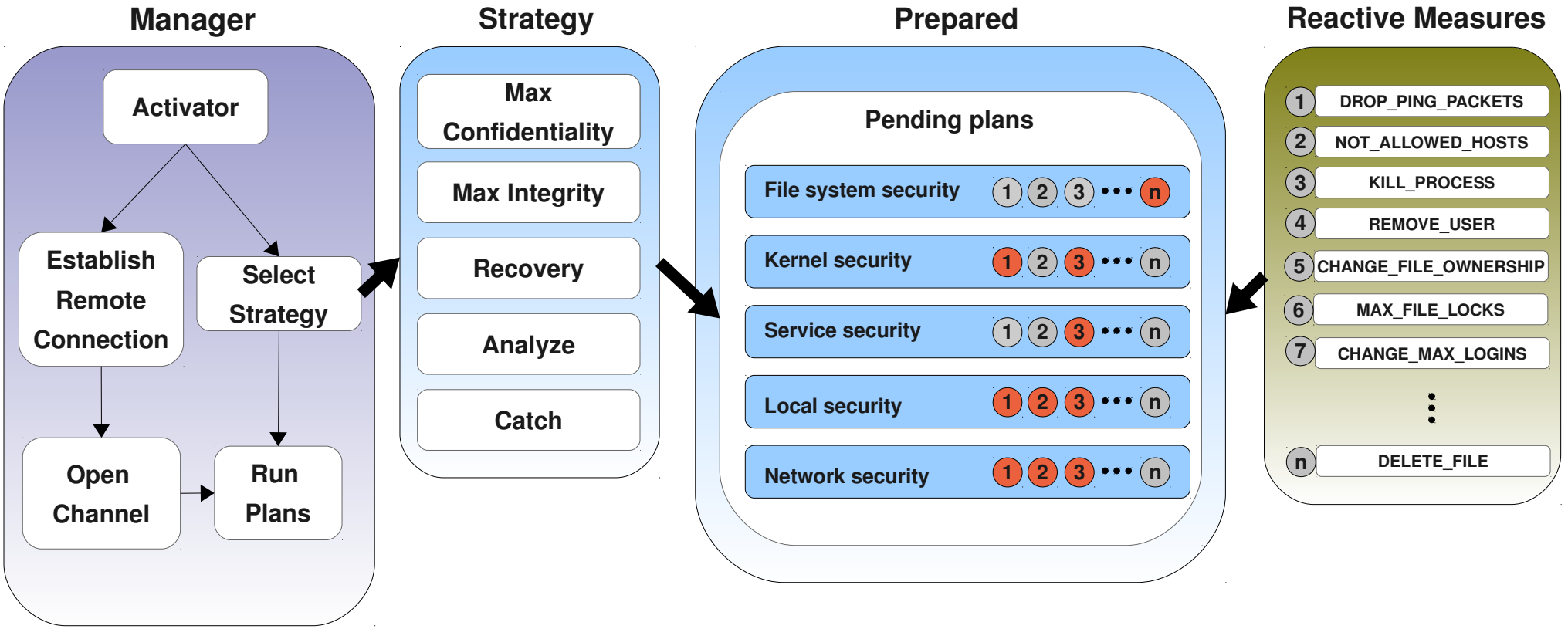
System Health Monitoring Architecture



Prevention

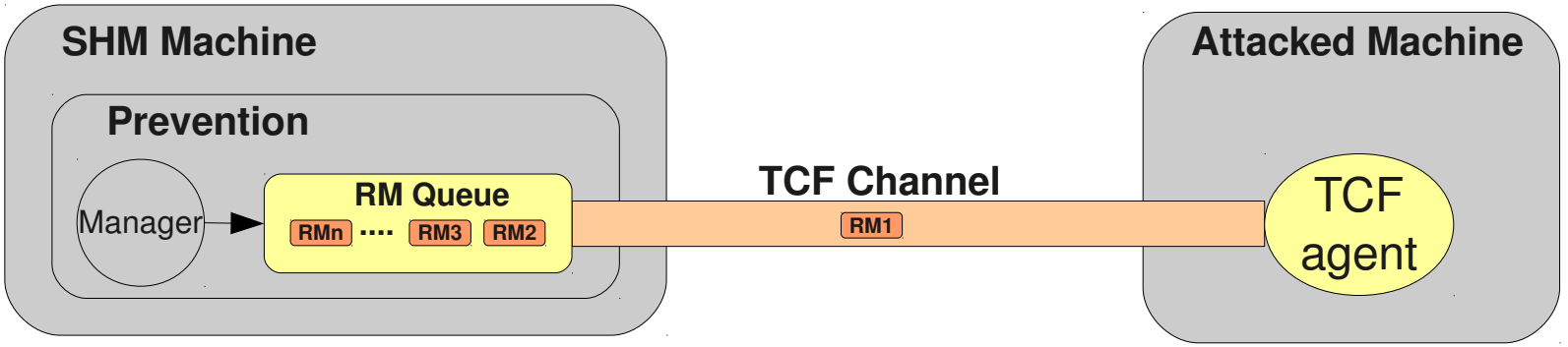
- Prevention component will try to run good strategies to trigger reactive measures with the objective of:
  - Preventing the problem growth
  - Returning system to the healthy mode

Prevention Architecture



Manager Section

- Manager activates
  - Create a channel to the target computer by TCF facility
  - Select appropriate strategy (it can be static and depends on organization policy)
  - Send the next round of Reactive Measures based on Risk Index of network
  - Apply Reactive Measure on target computer by TCF agent

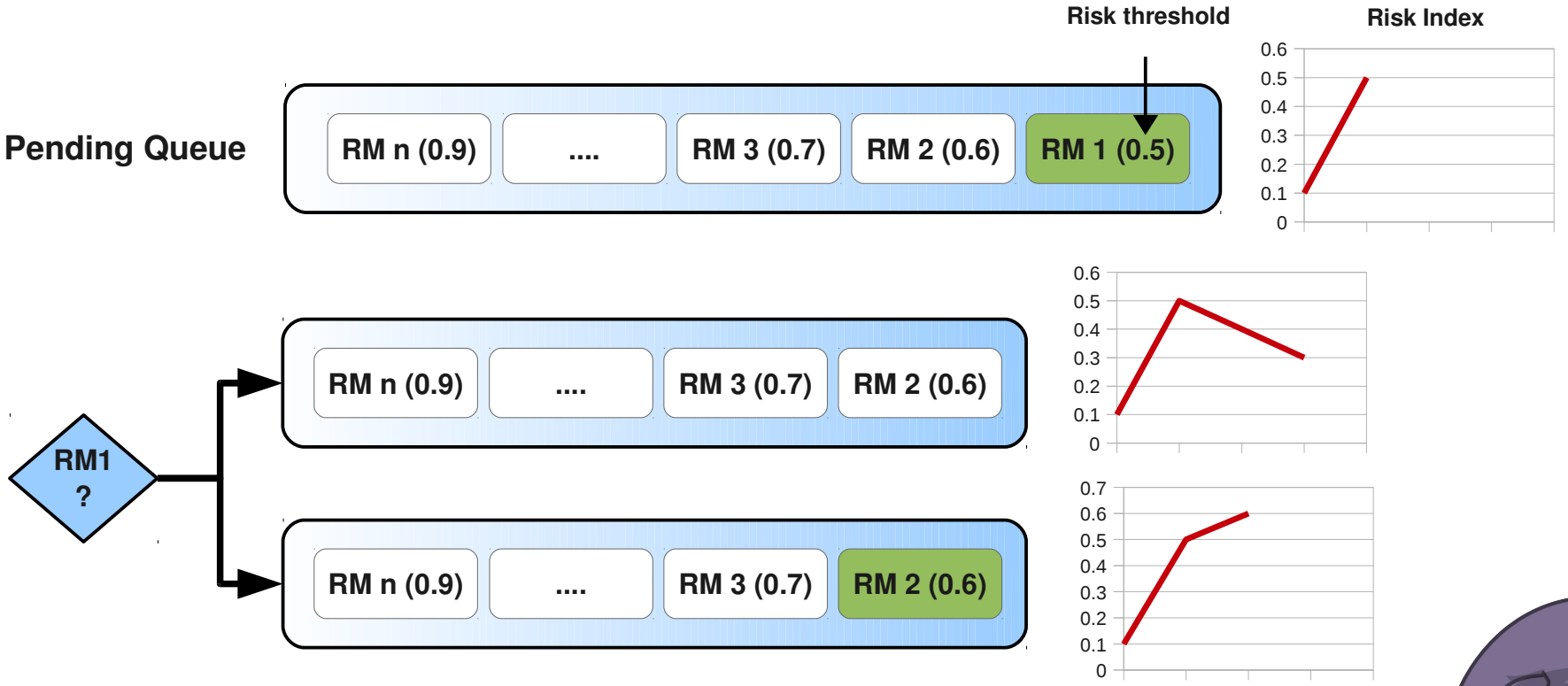


Strategy Section

- An intrusion can be defined as any set of actions that threaten the Integrity, Confidentiality and Availability of host/network resources such as:
  - User account
  - File
  - Kernel
  - ...
- So, our strategies to tackle this problems are:
  - MAX-Confidentiality (e.g. Military organization)
  - MAX-Integrity (e.g. Bank service)
  - Recovery (e.g. Scientific organization - University)
  - Analysis (e.g. Security laboratory)
  - Catch (e.g. Security laboratory - Police)

Reactive Measures running policy

- Each strategy has its own ordering of reactive measures
- Each reactive measure has a static **risk threshold** to apply in target
- Upon running a reactive measure, new risk index of network has to be measured from Online Risk Assessment Component



Reactive Measures

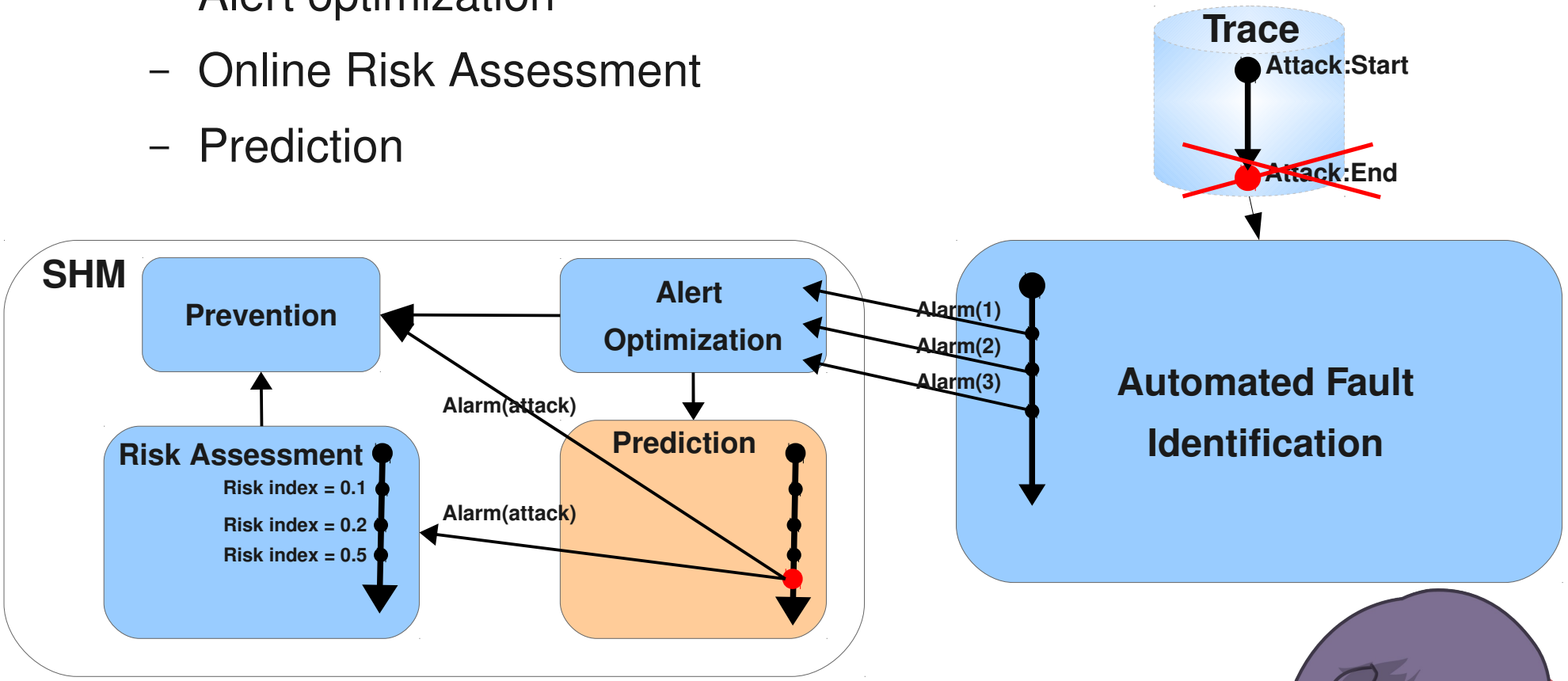
- Set of 35 reactive measures based on interviews of industrial sites including Revolution Linux
- Different types of Reactive Measures:
  - Permanent vs. Transient
    - *RM_ALLOWED_HOSTS/RM_TRANSIENT_DROP_PING_PACKETS*
  - Parametric vs. Non-Parametric
    - *RM_REMOVE_USER/RM_RESET*
  - Pattern vs. Non-Pattern
    - *RM_IPTABLE/RM_LOCK_USER*
  - Strict vs. Non-Strict (limiting the resources consumed)
    - *RM_KILL_PROCESS/RM_MAX_FILE_LOCKS:*

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

Future work

Future work

- **Connect the loop from detection to reaction**
  - Improve Prevention mechanism by importing:
    - Alert optimization
    - Online Risk Assessment
    - Prediction



Conclusion

- Integration of SHM, Automation Fault Identification and Trace Abstraction
- Improving prevention mechanism to minimize impact to network
- Implementing a large set of Reactive Measures to counter cyber-attacks:
  - limiting the resources consumed
  - protecting the quality of service for critical functions
  - Adapting the firewall configuration

References (1)

[1] http://en.wikipedia.org/wiki/Anomaly

[2] http://en.wikipedia.org/wiki/Anomaly_detection

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

[4] http://en.wikipedia.org/wiki/Fuzzy_logic

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

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

[7] Ozyer T., Alhajj R. and Barker K., **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, pp. 99-113, 2007

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

[9] http://en.wikipedia.org/wiki/Neural_network

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

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

References (2)

[12] http://en.wikipedia.org/wiki/Support_vector_machine

[13] Rung-Ching Chen, Kai-Fan Cheng, Ying-Hao Chen, Chia-Fen 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

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

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

[16] Zhang R., Zhang S., Muthuraman S. and Jiang J., **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

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

[18] http://en.wikipedia.org/wiki/Bayesian_network

[19] Abdelhamid, **Réseaux Bayésiens Naïfs Augmentés TAN pour les Systèmes de Détection d'Intrusions**, PhD thesis, Université de Nice Sophia Antipolis, 2007

[20] Abouzakhar N., Gani A., Manson G., Abuitbel M. and King D., **Bayesian Learning Networks Approach to Cybercrime Detection**, In proceedings of the 2003 PostGraduate Networking Conference, Liverpool, United Kingdom, 2003

References (3)

[21] http://en.wikipedia.org/wiki/Hidden_Markov_model

[22] Forrest S., Hofmeyr S.A. and Somayaji A., **The Evolution of System-call Monitoring**, Proceedings of the Annual Computer Security Applications Conference, USA, ISBN1063-9527, pp. 418-430, 2008

[23] Forrest S., Hofmeyr S.A., Somayaji A. and Longstaff T.A., **A sense of self for Unix processes**, Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 120–128, 1996

[24] Feng Li, Wang W., Zhu L. and Zhang Y., **Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation**, Journal of Network and Computer Applications, pp. 721-732, 2009

[25] http://en.wikipedia.org/wiki/K-nearest_neighbor_algorithm

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

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

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

[29] Cherednichenko S., **Outlier Detection in Clustering**, 2005

[30] Wang Q. and Megalooikonomou V., **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

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

References (4)

[32] Haslum K., Abraham A. and Knapskog S., **DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment**, Third International Symposium on Information Assurance and Security, IEEE Computer Society press, USA, ISBN 0-7695-2876-7, pp. 183-188, 2007

[33] Salfner F. and Malek M., **Using Hidden Semi-Markov Models for Effective Online Failure Prediction**, 26th IEEE International Symposium on Reliable Distributed Systems, pp.161-174, 2007

[34] Feng Li, Wang W., Zhu L. and Zhang Y., **Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation**, Journal of Network and Computer Applications, pp. 721-732, 2009

[35] Mu C. P., Huang H. K. and Tian S. F., **Online risk assessment of intrusion scenarios using D–S evidence theory**, In Proceedings of 13th European symposium on research in computer security a LNCS, Málaga, Spain, ISBN 978-3-540-88312-8 , pp. 35-48, 2008

[36] Mu C. P, and Li Y., **An intrusion response decision-making model based on hierarchical task network planning**, Journal of expert systems with applications, 2009

[37] N. Stakhanova, S. Basu and J. Wong, **Taxonomy of Intrusion Response Systems**, International Journal of Information and Computer Security. Vol. 1. No. 1/2, pp.169-184, Inderscience, 2007

[38] Foo B., Wu Y., Mao Y., Saurabh Bagchi, Spafford E, **ADEPTS: Adaptive Intrusion Response Using Attack Graphs in an E-Commerce Environment**, International Conference on Dependable Systems and Networks, pp. 508-517, 2005

[39] Wu Y. S., Foo B., Mao Y. C., Bagchi S. and Spafford E. H., **Automated adaptive intrusion containment in systems of interacting services**, The International Journal of Computer and Telecommunications Networking, ISSN:1389-1286, Pages 1334-1360, 2007

References (5)

[40] Xiao F., Jin S. and Li X., **A Novel Data Mining-Based Method for Alert Reduction and Analysis**, Journal of Network, vol. 5, pp. 88-97, Jan. 2010

[41] Stakhanova N. and Mell P., **Guide to Intrusion Detection and Prevention Systems,** http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

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

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

[44] Zhu B. and Ghorbani A. A., **Alert correlation for extracting attack strategies**, International Journal of Network Security, vol. 3, pp. 244-258, 2006.

[45] Kruegel C. , Valeur F. andVigna G., **Alert Correlation**, in Intrusion Detection and Correlation, first edition, vol. 14., Ed. New York: Springer, 2005, pp.29-35.

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