Presentation on theme: "Complex Event Processing(CEP) for Intrusion Detection"— Presentation transcript:

[1](https://slideplayer.com/slide/12798227/77/images/1/Complex+Event+Processing%28CEP%29+for+Intrusion+Detection.jpg) **Complex Event Processing(CEP) for Intrusion Detection**  
Dimitris TsitsigkosAdviser : Efstathios Hadjieftymiades, Assistant Professor NKUAComplex Event Processing(CEP) for Intrusion Detection

[2](https://slideplayer.com/slide/12798227/77/images/2/Used+to+connect+digital+and+physical+world.jpg) **Used to connect digital and physical world**  
Internet of Things“Dense monitoring and analysis of complex phenomena over large regions of space for long periods”Many small, inexpensive devicesFrequent sampling over long durationsClose to physical phenomena of interestCompute, communicate and coordinateObserve complex interactionsDiversity?Intelligence?Used to connect digital and physical world

[3](https://slideplayer.com/slide/12798227/77/images/3/IoT+Networks.jpg) IoT NetworksKevin Ashton coined "Internet of Things" phrase to describe a system where the Internet is connected to the physical world via ubiquitous sensors

[4](https://slideplayer.com/slide/12798227/77/images/4/The+Challenges+%281%2F2%29.jpg) The Challenges (1/2)Every one of those sensor and control points is generating data. Systems are needed to help those devices talk to each other and manage all that data.

[5](https://slideplayer.com/slide/12798227/77/images/5/The+Challenges+%282%2F2%29+Wisdom+Knowledge+Information+Data.jpg) **The Challenges (2/2) Wisdom Knowledge Information Data**  
There is direct correlation between the input (data) and the output (wisdom). The more data that is created the more knowledge and wisdom people can obtain.WisdomKnowledgeInformationData

[6](https://slideplayer.com/slide/12798227/77/images/6/Motivation+Evolution+of+IoT+%EF%83%A0+A+whole+new+world+of+challenges.jpg)  **A whole new world of challenges◊Motivation Evolution of IoT**   
SecurityPrivacyData StorageEnergySecurity challenges :Heterogeneity of smart devices in IoT networkDetect quickly any abnormal activityComplex Event Processing(CEP) for Intrusion Detection

[7](https://slideplayer.com/slide/12798227/77/images/7/Problem+While+there+are+a+thousand+of+anomalies+events+in+a+normal+working+day%2C+such+activities+that+are+not+necessarily+defined+as+problems..jpg) ProblemWhile there are a thousand of anomalies events in a normal working day, such activities that are not necessarily defined as problems.Software aims to discover behaviors that could potentially provoke damage to your organization security. It is implemented to display you an accurate picture of the activity in your organization, concentrating more on events or likelihood of an event that could harm your company, rather than on minor activities that is ultimately harmless.

[8](https://slideplayer.com/slide/12798227/77/images/8/Problem+Example.jpg) Problem ExampleFor example, a single day spike of 300 outbound s from a single employee would not necessarily alarm you about the event, unless the account belonged to an employee that was fires the prior days. Or if an address that in a normal condition sends and receives 300 mails per day suddenly spikes 30,000 outbound s, then there is an obvious problem. Discovery anomalies is about cross-correlating multiple types of activities and weighting them by how rare they are or by how many other anomalies they generate. It is not just pointing out activities that are different.Complex Event Processing(CEP) for Intrusion Detection

[9](https://slideplayer.com/slide/12798227/77/images/9/Intrusion+Detection.jpg) Intrusion DetectionAn intrusion is defined as an unwanted or unauthorized interference to network normally with bad intentions. The intention of an attacker is, at first to discover information related to the organization network such as the structure of the internal networks or software systems like operating systems, tools/utilities, or software applications used by the organization and then initiate connections to the internal network and execute attacks.An Intrusion Detection System (IDS) is a combination of both hardware and software that discovers the attacks into a system or network. IDS control each and every packet’s content cross the network to discover any malicious behaviors.

[10](https://slideplayer.com/slide/12798227/77/images/10/Intrusion+Detection.jpg) Intrusion DetectionDenial of Service (DOS)/Distributed Denial of Service (DDoS) DoS (DDoS) attack is an explicit attack to block users from accessibility to the network and network services, such as flood the network, thereby preventing legitimate network traffic, target single device with too many requests thus bringing down the device, disrupt the connections between two legitimate devices thereby preventing access to a genuine service request, destruction or alteration of network configurations, consume the network bandwidth.HTTP Tunneling: This method may be used by the attackers in order to pass the firewall controls and send confidential information to the outside world without anyone inside being aware of the same.SSH Tunneling: These may be used to directly connect to a network stealthily and initiate attacks. This is an illegitimate use of a legitimate tool.

[11](https://slideplayer.com/slide/12798227/77/images/11/Signature-Based+Detection.jpg) **Signature-Based Detection**  
Pros and consComplex Event Processing(CEP) for Intrusion Detection

[12](https://slideplayer.com/slide/12798227/77/images/12/Anomaly-Based+Detection.jpg) **Anomaly-Based Detection**

[13](https://slideplayer.com/slide/12798227/77/images/13/Proposed+Method.jpg) Proposed MethodOur goal was to implement a framework for event detection in real time input streams. In more details, we track information from smart devices and feed them to our framework, in order to detect critical events and inform the smart devices for the possibility of an intrusion. Our framework consists of three parts:SNMPEsper EngineRules: feature extraction

[14](https://slideplayer.com/slide/12798227/77/images/14/SNMP.jpg) SNMP

[15](https://slideplayer.com/slide/12798227/77/images/15/Proposed+Method+Our+framework+consists+of+three+parts%3A+SNMP.jpg) **Proposed Method Our framework consists of three parts: SNMP**  
Esper EngineRules: feature extraction

[16](https://slideplayer.com/slide/12798227/77/images/16/Esper+-+CEP.jpg) Esper - CEP

[17](https://slideplayer.com/slide/12798227/77/images/17/Proposed+Method.jpg) Proposed MethodOur goal was to implement a framework for event detection in real time input streams. In more details, we track information from smart devices and feed them to our framework, in order to detect critical events and inform the smart devices for the possibility of an intrusion. Our framework consists of three parts:SNMPEsper EngineRules: feature extraction

[18](https://slideplayer.com/slide/12798227/77/images/18/Rules-+Feature+Extraction.jpg) **Rules- Feature Extraction**  
For the master thesis purposes three algorithms are being presented:Algo1ShewhartAdaptive Reasonance Theory(ART) .

[19](https://slideplayer.com/slide/12798227/77/images/19/CEP+Architecture+Manager+Listeners+Smart+Devices.jpg) CEP ArchitectureManagerListenersSmart Devices

[20](https://slideplayer.com/slide/12798227/77/images/20/Event+Listeners+%28+Esper+First+Layer%29.jpg) **Event Listeners ( Esper First Layer)**  
Dynamic Listeners:TCP: The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLODED stateUDP: The total number of received UDP datagrams for which there was no application at the destination port.Memory: total RAM used.Static listeners:Bandwidth: Bandwidth of the networkCPU: percentage of idle CPU time

[21](https://slideplayer.com/slide/12798227/77/images/21/Manager%28+Esper+Second+Layer%29.jpg) **Manager( Esper Second Layer)**

[22](https://slideplayer.com/slide/12798227/77/images/22/Machine+Learning+Algorithms%28+%29.jpg) **Machine Learning Algorithms(?????)**  
Algo1: Using static thresholds.Queries and Changes in dynamic variables:TCP :Query : TCP > avg(TCP) + 8Change : avg(TCP) + 8UDP :Query :  UDP > avg(UDP) + 3Change: avg(UDP) + 3Memory :Query : avg(Memory)+1000Change : Memory > avg(Memory)Queries of non dynamic variables:CPU : CPU < 49Bandwidth : Bandwith > 20

[23](https://slideplayer.com/slide/12798227/77/images/23/Machine+Learning+Algorithms.jpg) **Machine Learning Algorithms**  
Shewart :The control limits are defined as the distance from the current mean value of the process which is:for UCL, andfor LCLThat is, is detected to fire an alarm if or The and values are defined as follows (through incremental methods):andThe controller returns if , if and normality, i.e., 0 if The parameter is usually defined to be

[24](https://slideplayer.com/slide/12798227/77/images/24/Machine+Learning+Algorithms.jpg) **Machine Learning Algorithms**  
Adaptive Reasonance Theory:Equations in the Euclidean Distance at each update:Euclidean Distance:Where:

[25](https://slideplayer.com/slide/12798227/77/images/25/Machine+Learning+Algorithms.jpg) **Machine Learning Algorithms**  
Adaptive Reasonance Theory(example)

[26](https://slideplayer.com/slide/12798227/77/images/26/Input+Datasets+We+used+UNB+ISCX+Intrusion+Detection+Evaluation+DataSet+%2C+which+contains+real+traces..jpg) Input DatasetsWe used “UNB ISCX Intrusion Detection Evaluation DataSet”, which contains real traces.We use five days of measurements :12/6/ Normal Activity. No malicious Activity.14/6/2010 HTTP Denial of Service + Normal Activity.15/6/2010 Distributed Denial of Service and IRC Botnet16/6/2010 Normal Activity. No malicious Activity17/06/2010 Brute Force SSH + Normal Activity

[27](https://slideplayer.com/slide/12798227/77/images/27/Simulation+Environment.jpg) **Simulation Environment**  
ObjectMachineCPUMemoryDiskSNMP Managers/AgentsVMsDual Core 2.6Ghz4GB60GBEsperPhysicalInter(R) Core(TM) i5-4300U 2.50Ghz8GB80GB

[28](https://slideplayer.com/slide/12798227/77/images/28/Evaluation+We+run+our+three+algorithms+for+the+five+datasets..jpg) **Evaluation We run our three algorithms for the five datasets.**  
Algo1 and Shewart run for one time for each dataset.Vector algorithm ART, has two arguments: r(radius) and η(defines the velocity of centroid updates) and the executions for each dataset are :r = 50, η= 0.5r = 50 , η = 1r = 100, η = 0.5r = 100, η = 1

[29](https://slideplayer.com/slide/12798227/77/images/29/Evaluation+All+the+metrics+of+the+dynamic+variables+for+each+dataset.jpg) EvaluationAll the metrics of the dynamic variables for each dataset

[30](https://slideplayer.com/slide/12798227/77/images/30/Evaluation+Comparison+ART+algorithms+for+day+17..jpg) EvaluationComparison ART algorithms for day 17.

[31](https://slideplayer.com/slide/12798227/77/images/31/Evaluation+Event+counters+for+dynamic+variables+of+all+ART+Algorithms+for+each+day..jpg) EvaluationEvent counters for dynamic variables of all ART Algorithms for each day.

[32](https://slideplayer.com/slide/12798227/77/images/32/Evaluation+Comparison+fo+Algo1%2C+Shewart+and+Art+algorithms+on+day+17.+Day+17+has+Brute+Force+SSH+%2B+Normal+Activity..jpg) EvaluationComparison fo Algo1, Shewart and Art algorithms on day 17. Day 17 has Brute Force SSH + Normal Activity.Complex Event Processing(CEP) for Intrusion Detection

[33](https://slideplayer.com/slide/12798227/77/images/33/Related+Work+-+Machine+Learning+for+IDS.jpg) **Related Work - Machine Learning for IDS**  
Decision tree classifiersB.Pfahringer, Winning the KDD99 Classification Cup: Bagged Boosting, in SIGKDD Explorations, 2000.I. Levin, KDD-99 Classifier Learning Contest: LLSoft’s Results Overview SIGKDD Explorations, 2000.V. Miheev, Vopilov.A and Shabalin.I., The MP13 Approach to the KDD’99 Classifier Learning Contest’ SIGKDD Explorations, 2000.Use of fuzzy logic is proposed inJonatan Gomez and Dipankar Dasgupta. Evolving fuzzy classifiers for intrusion detection. In Proceedings of the 2002 IEEE Workshop on Information Assurance, West Point, NY, USA, 2002.Markov Model classifiersJiankun Hu and Xinghuo Yu, ”A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection”, IEEE Network Journal, Volume 23 Issue 1, February 2009Jiong Zhang and Mohammad Zulkernine, Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection IEEE International Conference on Communications, 2006.Bayesian classification algorithmZhenghong Xiao, Chuling Liu, Chaotian Chen, ”An Anomaly Detection Scheme Based on Machine Learning for WSN” IEEE International Conference on Information Science and Engineering, 2009Complex Event Processing(CEP) for Intrusion Detection

[34](https://slideplayer.com/slide/12798227/77/images/34/Related+Work+-+CEP+Frameworks.jpg) **Related Work - CEP Frameworks**  
Tiny DBDroolsQuery LanguageEPLSQL LikeDRLInputStreamsDatabaseProcess TimeFastSlowCEP and Tiny DB uses SQL Like query language, which is by far more easier than DRL of DroolsCEP and Drools take streams as input, so are capable for real time analytics.In Drools rules declare the conditions specifying when the actions should be performed. The rule engine takes the data, examines the rules and evaluates them in a most efficient way and finally executes those conditions whose rules have been evaluated to true.ESPER can be used to rate limit traffic on a flow and for doing QoS checks on endpoints. It is also extremely useful in developing and maintaining integration applications.

[35](https://slideplayer.com/slide/12798227/77/images/35/Possible+features+directions.jpg) **Possible features directions**  
Implement a Multivariate Autoregressive (MAR) modelCompare MAR with the existing Algorithms calculate latency and the communication overhead of the transactions◊Connect big number of smart devices Complex Event Processing(CEP) for Intrusion Detection