Ontology-Based Inter-Domain Event Correlation

Hassan Rasheed
Deanship of Information Technology, Taif University, Taif Saudi Arabia
Email: hsrasheed@acm.org

ABSTRACT
The notion of event correlation has been around for some time. Most recently, event correlation has gotten a significant amount of attention in the intrusion detection community under the topic of alert correlation. The principles behind event correlation, however, can also be used to relate events in seemingly heterogeneous domains such as access control and intrusion detection. To address the need for event data sharing between different security mechanisms, we propose the use of ontologies for inter-domain event correlation. The relevant research on alert correlation is surveyed and two taxonomies are presented to classify the approaches used in that area. Then hybrid ontology is proposed that can serve as the integration point for event correlation between access control and intrusion detection systems. Examples are given from an implementation to show the capabilities of the correlation process.

Keywords: Event Correlation, Ontology-Based Event Analysis

1. INTRODUCTION
In many ways, security mechanisms are still largely viewed as isolated methods for security assurance in computer systems. This is largely to do with the beginnings of information security measures as ad-hoc stop gap measures in response to system vulnerabilities or changing application requirements.

Current paradigms in distributed computing, however, are causing a shift towards architectures capable of aggregating diverse groups of services (including security mechanisms) in order to better meet the needs of dynamic and rapidly changing application environments. In order to move security systems into this paradigm it is necessary to move away from the view that these mechanisms work in isolation, or, at the very least, devise strategies that allow them to be dealt with as members of a larger, integrated architecture.

One of the primary motivators for moving towards such an integrated architecture for security components is the ability to share information. This simultaneously preserves the modularity and specialization of components that allows for rapid evolution, but at the same time allows components to take advantage of the data and analysis produced by their peers in order to perform their own security assurance tasks more effectively.

Considering the large number of events that might be expected by a networked security component, it is necessary that this data sharing be on an as-needed basis as requested by the consumer and not initiated by the provider to avoid superfluous transmissions of data. This leads to the use of correlation to select relevant events from other sources based on the features of the current event being dealt with by that security mechanism.

The notion of event correlation has been around for some time. Most recently, event correlation has gotten a significant amount of attention in the intrusion detection community under the topic of alert correlation. The principles behind event correlation, however, can also be used to relate events in seemingly heterogeneous domains such as access control and intrusion detection.

The motivation for inter-domain event correlation is the notion that security mechanisms should make decisions and classify events based on all of the relevant information available. The data produced by a security mechanism such as an intrusion detection system can effectively inform other security systems about the current state of the system so that their behavior can adjust accordingly.

2. CHALLENGES AND SOLUTIONS
There are a number of obstacles which must be overcome in order to provide such data sharing – especially if the goal is to make current security mechanisms interoperable and integrated. Because of the fact that the goal is inter-domain information sharing, an additional level of complexity is introduced that is not necessarily present in correlation methods that only operate within one domain. In alert correlation, one of the primary challenges is managing syntactic heterogeneities such as different names being given to the same attack by different intrusion detection systems. When dealing with two different types of systems, however, semantic heterogeneities must be also be resolved. An example of such a semantic heterogeneity is the notion of target as expressed in the data models for two popular security standards the eXensible Access Control Modeling Language (XACML) for access control and the Intrusion Detection Message Exchange
Format (IDMEF) for intrusion detection. In XACML a target is the target for a policy: the set of subjects, actions and resources that the policy applies to. Under the IDMEF data model, a target is the entity to which an attempted intrusion is directed.

Different mechanisms are therefore needed to bridge these heterogeneities, before discovery of related events can take place. One such mechanism typically used to integrate software systems with semantic heterogeneities is ontology. In [13] three approaches for using ontologies in the explication of data are mentioned: a single, global ontology, individual ontologies and a hybrid approach. For a number of reasons, we opt for the hybrid approach and focus on producing a shared vocabulary that facilitates interoperability between different domain standards.

The aim is to express the features common to different security events that can allow one mechanism to discover events from other security services without explicit knowledge of the schema used to describe events in that domain. Subsequent analysis of said events will require a greater knowledge of the origin domain for the events, but the issue of data analysis is not addressed here.

To address these issues, we propose the use of an ontology for content explication between multiple security mechanisms, and then describe how current alert correlation methods can be extended and adapted to use an ontology to correlate events across different security domains.

This paper will be organized as follows: first there will be a discussion of current methods for correlating security events, specifically intrusion detection events, and we will offer a taxonomy of alert correlation aims and methods. This will provide an overview of what techniques are likely to be applicable to the problem of correlating security events – the greatest focus on this issue until now has been exclusively in the intrusion detection community. Next we will confront the major problem created by trying to achieve inter-domain event correlation: the semantic heterogeneities between the different mechanisms. The primary technique for bridging these gaps will be the use of ontologies. We will give an overview of the three primary approaches to using ontologies for content explication and then discuss why a hybrid ontology is most appropriate option for achieving the goals of event correlation. We will then detail the contents of the hybrid ontology, including a base vocabulary and basic ontologies for describing access control and intrusion detection events. Using these two concepts as a basis - the set of applicable correlation techniques from intrusion detection and the base vocabulary - we will detail an approach to inter-domain correlation that handles distribution and autonomy and mitigates enough of the heterogeneities to achieve the kind of semantic interoperability needed for event correlation. Following this, there will be a discussion of implementation including example scenarios of event correlation using the ontology. The paper will conclude with a discussion of related work and plans for future work.

3. A TAXONOMY OF ALERT CORRELATION APPROACHES

As a means of elucidating the most effective approaches for managing security event data we present two taxonomies for security event correlation. These two taxonomies encompass the same set of approaches, but each one organizes them in a different way. The first taxonomy looks at a set of approaches based on the goal of the approach or its output. The second taxonomy classifies the approaches based on the specific technique that is used to achieve the aim for which they were designed.

3.1 Classification Based on the Goal of the Approach

What is commonly referred to as simply alert correlation encompasses three very different tasks related to IDS alerts: alert reduction, alert association and alert analysis. The first to be discussed is alert reduction. Alert reduction strategies decrease the number of alerts presented to administrators by removing duplicate alerts, or merging alerts that pass a certain threshold of similarity.

Correlation methods that achieve alert reduction are typically referred to as fusion or merging. In reality, most of the merging techniques do not merge alerts in the sense of replacing two distinct alerts with a new one that somehow addresses them both. Instead, the approaches that perform merging (such as [1, 12, 5]) utilize the notion of a meta-alert which represents the information present in several distinct alerts through the use of lists for discrete values such as IP addresses and ports, or ranges for continuous values such as time. The effect of creating a meta-alert achieves alert reduction because it allows the administrator to quickly see similar alerts grouped together. In this way, the reduction of alerts is from the perspective of the administrator.

The next correlation task is alert association. This type of correlation method encompasses techniques that detect or assert an association between two or more alerts. This class encompasses the following approaches: aggregation [3, 12], clustering [1, 5, 10, 8, 15], multi-step attack detection [2, 12, 9], session reconstruction [12] and detection by chronicles [7]. All of these techniques have been grouped together because in the end they all express relationships between the alerts in a given set under analysis. In the case of clustering, the relationship is a similarity based on
perceived distance. For aggregation, the association is a set of one or more shared attributes (in that sense it is a stricter form of clustering). Multi-step attack detection associates alerts that are proper subsets of the same set. A high-level attack sequence is viewed as an ordered set of distinct actions that achieve a certain observable effect on the system. The individual alerts are therefore associated to each other through membership in a specific high level attack-sequence. The chronicles approach is similar to the multi-step detection approach with the addition of temporal constraints between various states.

The correlation techniques in the alert analysis class are impact analysis and prioritization [12]. Both of these approaches make a determination about an individual alert using only its features and data about the overall context of the system. In the case of impact analysis the context information is an asset database and whether or not the attack succeeded. For prioritization the context information is a weighting assigned to the class of the attack as well as the asset database also used for impact analysis.

3.2 Classification Based on the Technique Employed

The taxonomy for alert correlation methods based on means includes the following main categories of techniques: 1) those that merely look at the alerts themselves 2) those that attribute each alert to a specific attack and then correlate alerts based on how they fit in an attack progression. 

Correlation Using Alert Attributes

Correlation methods which rely on associating alert attributes will either do so based on their congruence or their similarity. In the first category of attribute congruence, there are two subcategories: syntactic and semantic. Aggregation is the only correlation approach that relies on complete syntactic attribute congruence to associate one or more alerts. This is as a result of establishing criteria for membership in an output set that certain attribute values \( a_1, a_2 \) and \( a_3 \) must be equal to values \( v_1, v_2 \) and \( v_3 \) respectively (in the case where all three values are used). The most thorough examination of aggregation is found in [3] but it is also discussed in [12], where it is divided into two distinct tasks: attack thread reconstruction and attack focus recognition. Attack thread reconstruction is aggregation of alerts with the same source and target, while attack focus recognition is aggregation of alerts with either the same source, or the same target.

The session reconstruction approach in [12] relies on what will be referred to as semantic attribute congruence. Session reconstruction links two alerts, issued at different deployment levels, that refer to different targets syntactically (a port number and service name), but are in reality describing the same system entity. Hence, although the attribute value mentioned in each of the alerts may be syntactically different, they are semantically congruent because they refer to the same entity.

Under the category of attribute similarity we place the clustering approaches [1, 5, 10, 8, 15]. Implicitly, merging is also placed in this category, because it is almost always preceded by clustering. A cluster of alerts is the product of using a set of expert-designed similarity measures to determine which alerts are most like one another.

![Figure 1: Taxonomy of Alert Correlation Methods Based on the Technique Employed](image-url)
Correlation Through Attack Attribution

The next general technique for alert correlation is through attack attribution. Alerts are first attributed to an attack which may consist of various steps and have several known alert manifestations. After a particular alert is associated with an ongoing attack, other prior or subsequent alerts will be connected to it based on the pre-determined attack progression.

Within the set of correlation methods that rely on attack-attribute there are two further divisions: methods that rely on shared membership and those that rely on a logical relationship between the attacks. Shared Membership techniques rely on the fact that the two alerts being correlated are both members of the same set: either having the same attack classification or both being members of a higher-level attack scenario. Both multi-step detection [2, 12, 9] and the chronicles approach [7], both of which link alerts based on the fact that they are associated with the same high-level attack description. The attack classification shared membership technique appears in [15], where a matching event type is one of the criteria used to identify events as being similar.

Under methods that associate attacks based on logical relationships, the first is the pre/post-condition approach. This approach is most thoroughly discussed in [1, 9] and relies on a specification of pre-conditions and post-conditions for each attack. When an alert arrives indicating an attack it is compared with other available alerts to find matches between its conditions and the conditions of other alerts. The second approach is the cause and effect or triggering approach used in [15]. Although the pre/post condition approach is also a part of the method used in [15], it is somewhat distinct because the complete functionality relies on a specification of events and the alerts that they trigger. These triggering relationships are used also to cluster events.

The full taxonomy is presented in Figure 1. The main elements of the taxonomy are as follows:

- Techniques relying on attack attributions: these approaches rely on expert systems that describe the relationships between distinct attacks
- Logical Relationship: those relationships that identify a specific logical relationships between two attacks
- Pre/Post Condition: one attack requires certain conditions as a precondition and another attack is known to produce those conditions
- Cause/Effect: one attack is identified as the trigger or cause for another
- Shared Membership: two alerts are correlated because they are both members of the same set
- Attack Classification: both attacks are in the same general class. A class may be identified by specific values in certain fields
- High Level Attack Scenario: both attacks are members of a single high-level attack scenario made up of multiple steps
- Alert Attributes: two alerts are correlated because of the attributes which they contain
- Congruence: the two alerts contain the same values
- Semantic: the two attributes are related through a third element that indicates that they refer to the same entity
- Syntactic: the value for the specified attribute is the same in both alerts
- Similarity: the two alerts contain values which are similar based on a specific measurement
- Positive (Proximity): based on a pre-designed distance measure, the attributes for the two alerts exceed a threshold for the maximum separation
- Negative (Separation): based on a pre-designed distance measure, the attributes for the two alerts exceed a threshold for minimum separation
- Covariance: specific sets of attributes vary in the same way from one alert to the other

4. IMPLICATIONS OF THE TAXONOMY FOR INTER-DOMAIN EVENT CORRELATION

The taxonomy is an important tool to characterize the available methods for analyzing and relating events based on data from Intrusion Detection Systems. However, intrusion detection data is just one of the types of events that would be correlated in a system that draws on multiple data sources. This is the first point of departure that the current study makes from the methods previously explored: our aim is to be able to relate events occurring in different domains with significant semantic heterogeneities. We examine alert correlation, because the intrusion detection field has done more analysis and exploration of the topic of event correlation. The drive behind exploring event correlation for intrusion detection data has been because it provides a practic-
al solution to managing what can be an overwhelming amount of data coming from intrusion detection sensors. And thus alert correlation, in many cases, has been looked at as a technique for primarily managing event data – manipulating it so that it is in a form that is more easily digested by a system administrator. This is the second point of departure of the current study from the previous research in this area: we propose to use event correlation as a technique for discovering relevant information. The distinction is subtle but important. Under the task of managing data many of the design requirements and aims are different than when the task is relating events so that security mechanisms can acquire information about the state of the system. Thus, the taxonomy is in many ways a library of techniques: some of which are not suited to the problem of correlating heterogeneous events, and others that are. One of the factors in determining which correlation methods will be used, however, is the exact nature of the methods used to bridge semantic heterogeneities. For that reason, we explore the topic of ontology development next.

5. TOWARDS AN ONTOLOGY FOR MANAGING SECURITY EVENT DATA

In [13] three methods are discussed for developing ontologies whose purpose is content explanation in an integrated system: a global shared ontology, multiple isolated ontologies and a hybrid approach. In the first approach, one global ontology is devised to provide a shared semantic vocabulary across all of the information sources. This approach is most suited to situations where all of the information sources share a similar view of the domain – if even one information source has a slightly different view it can become difficult to produce an effective global ontology. The second approach of constructing a separate ontology for each information source has the advantage that it supports evolution of the information source, and the addition and removal of information sources. Under this approach, however, in order to compare ontologies, it is necessary to define an inter-ontology mapping. Inter-ontology mappings, however can be difficult to define in practice, not to mention the fact that as the number of information sources expands the number of mappings that are necessary grows exponentially. The hybrid approach allows for the semantics of each information source to be described by its own database, but with the requirement that the individual ontologies are built from a global shared vocabulary. The shared vocabulary contains the basic terms that are combined in local ontologies to produce more complex semantics. The hybrid approach supports addition and evolution of ontologies, but has the drawback that existing ontologies must be rebuilt from scratch.

The global ontology option is not suited to providing inter-domain event correlation, because different views of the domain do exist, even if only considering access control and intrusion detection. While the task of producing a global ontology for access control and intrusion detection might not be that infeasible, there are a few additional goals present in this case which make this option inappropriate. One such goal is to provide a semantically explicit description of the elements in current data models to facilitate adoption and interoperability. Another is to preserve a degree of modularity between the systems. The approach of producing multiple, isolated ontologies also does not meet the design requirements in this case, because the primary goal is to compare events based on these ontologies. And the need to provide pair wise mappings between every set of ontologies would makes such a system difficult to produce. The hybrid approach best meets the requirements in this situation. It can allow a particular security mechanism to discover events from a variety of potential data sources, only using the information contained in the base vocabulary. It can also allow the ontologies for the individual domains to evolve individually.
6. A HYBRID EVENT ONTOLOGY

6.1 The basis for a common ontology

In order to produce a base vocabulary we will use the Intrusion Detection Message Exchange Format (IDMEF) [4] and eXtensible Access Control Modeling Language (XACML) [6] schemas, both of which provide representations for events, although in different domains. The goal of this process is to extract enough common elements from these two data models to form the basis of a shared vocabulary for cross-domain event correlation.

XACML specifies a language for access control policies as well as access requests and responses, all in XML. The XACML schema provides two event representations: access control requests from a source, and the response from the policy enforcement mechanism. The XACML request context schema contains the following elements: 1) Subject - information about the subject of the request 2) Resource -- the resource or resources for which access is being requested 3) Action -- attributes about the action being requested and 4) Environment -- attributes of the environment in which the request is occurring. The XACML response context schema includes the following elements: 1) Decision 2) Status 3) Obligations.

The IDMEF standard describes a messaging format for intrusion detection systems to exchange information about ongoing attacks. A message in the Alert Class contains the following relevant properties: 1) Classification - The name of the alert 2) Source - The source of the event described in the alert 3) Target - The target of the event described in the alert 4) Assessment - Information about the impact of the event, actions taken by the analyzer in response to it, and the analyzer's confidence in its evaluation 5) Additional Data - Information included by the analyzer that does not fit into the data model.

6.2 The proposed ontology

The ontology being proposed (see Figure 2) consists of three main parts: a base vocabulary, an access control domain ontology and an intrusion de-
tection assessment ontology.

The base security event vocabulary

The common elements to these two event schemas are the access source, target and the action being performed. Combining all of the preceding discussion regarding existing data models and the taxonomy of system actions, we therefore offer a base vocabulary for inter-domain event correlation of assessment data in access control systems based on the following primary elements:

- SystemEntity – the class containing all valid system entities. The Subclasses of SystemEntity are Node, Process, User, Service and File. The first four subclasses are valid domains for the EventSource property, and the latter four subclasses are valid domains for the EventTarget property.
- SecurityEvent – a generic type of event possessing the properties of an event source, event target and event action. The subclasses of SecurityEvent needed for detailed data description are Access Request, Access Response and Assessment.
- Action – the class containing all of the distinct system actions. Subclasses needed for detailed data description are ClientAction and ServerAction.

Access control domain ontology

In order to provide a more detailed description of information at the access control level utilizing the base vocabulary, we develop two subclasses of the Security Event Class (AccessRequest and AccessResponse) and two subclasses of the SystemAction class (ClientAction and ServerAction). The class AccessRequest has the properties hasSource, hasTarget and requestAction. The first two properties range over SystemEntity and are inherited from the parent SecurityEvent classes. requestAction ranges over the class of ClientAction. The Access Response has the property hasResponse which references an Access Request, a responseString dataType property that contains the actual request response (permit or deny) and a hasResponseAction has a range of the set of ServerAction actions. In the case of the AccessResponse, the hasSource and hasTarget properties are still present, but the relationship between client and server has been flipped: the source of the AccessResponse is the server that was initially contacted with the access request.

There are two subclasses of the Action class generated for access control: ClientAction and ServerAction. ClientActions are the desired manipulations of system resources that are specified in Access Requests. They are subdivided into Malicious and Non-Malicious. Non-Malicious actions include CommandExecution, DataAccess and DataAlteration. Subclasses of ServerAction actions are RequestDecision and EvaluationObligation. RequestDecisions are the basic permit/deny decision issued for each request: EvaluationObligation refers to the obligations mentioned in the XACML schema [6], which constitute actions performed by the policy decision point as a result of evaluating an access request.

Intrusion assessment domain ontology

Assessment is the class of analyses regarding events or entities. Each assessment has an assessmentSource property whose range is an AssessmentSensor. Each Assessment Sensor has a confidenceRating that affects the way its analyses are viewed; in this case the confidence rating is given by the access control system utilizing events from that sensor. The primary subclass included in the event ontology is the IntrusionAssessment class. Other assessment types will be discussed under the topic of context analysis.

Each IntrusionAssessment has the following dataType properties: impactSeverity, impactType and attackCompletion (indicating whether the attack completed successfully or not). Assessments also have the following object properties: describedBy, triggeredBy, hasIntrusiveAction, hasSource and hasTarget. The describedBy property has the range of a VulnerabilityDescription and denotes that the vulnerability whose exploitation was detected is described in the referenced description. Each VulnerabilityDescription has a referenceID, an originDB and a referenceURL. The triggeredBy property has a range of the set of AccessRequests and denotes the access request to which the assessment applies. The properties hasSource and hasTarget both refer to SystemEntities that are the source and target of the intrusive event, respectively and are inherited from the parent SecurityEvent class. The hasIntrusiveAction property has a range of the class of Malicious client actions, which gives a general description of the kind of attack being perpetrated. The following subclasses of malicious client action are included in the ontology and are based on the taxonomy from [14]:

- Probing -- all activities related to gathering data about a system. Subdivided into probing of users, services and nodes.
- Denial of Service -- hindering legitimate access to the system. Subdivided into Temporary, Administrative and Permanent. A temporary denial of service is one that will be automatically recovered from. An administrative denial of service is one that will re-
require administrator intervention for recovery. Permanent denial of service attacks are those whose effects are indefinite.

- Interception/Reading Data -- subdivided into interception of files or of network traffic.
- Alteration/Creation of Data -- subdivided into modifying system data or modifying intrusion traces such as log files

7. INTER-DOMAIN EVENT CORRELATION THROUGH ONTOLOGY-BASED EVENT AGGREGATION

Based on the requirements of correlating events across domains, and the relative strengths of the three ontology approaches outlined, we advocate the use of aggregation through a hybrid ontology as the primary means for inter-domain event correlation. Because the extent of the heterogeneity between different domains could potentially be very large, it is important to select a correlative approach that can function using the elements explicated in the base vocabulary. These are the primitives that will be present in each domain, and will consequently be the essential features that make it possible to relate events in very different application areas. The focus, therefore, must be on the correlation techniques that rely on explicit event attributes, rather than on properties of the events that are only known implicitly, possibly through a knowledge base or other secondary source. Within the category of attribute-based correlative methods, aggregation (both semantic and syntactic) is the most consistent with the capabilities for correlation that are provided by an ontology. By using the aggregation technique of relating events through shared attributes, the correlation can function solely on the basis of the base vocabulary. The function of the base vocabulary is now to serve as a query model, in addition to unifying the view of critical primitives that are present in all of the involved domains. The correlation process will rely on the base vocabulary to specify the axes that events can be aggregate on. In essence this implies that the correlation of security events will be based on congruence in one or more of the attributes of event source, event target, or event action. As discussed in [3] using these three axes for event aggregation leads to seven basic event groupings:

1. All of the events from the same source - grouping all of the intrusion detection alerts citing a specific source, as well as all of the access control requests originating from that source. This could be used to characterize the predominate nature of the interactions that the source has with the system in question.
2. All of the events with the same target - grouping alerts from attacks on a specific resource as well as access requests for that resource. This could be used to characterize the predominate nature of most interactions with the system resource.
3. All of the events with the same action -- this type of aggregation could provide a set of events that have the same action or are all subclasses of the same action if a parent is asserted as the parameter for aggregation.
4. All of the events with the same source and target -- joining these two parameters will group events that share the endpoints specified and consequently could be used to summarize the interaction between the two entities, based on the actions being performed.
5. All of the events with the same source and action -- this aggregate set will gather events referring to the same source executing the same action, potentially with different system entities. This will summarize the prevailing type of system use that the source is engaged in.
6. All of the events with the same target and action -- this aggregate set will gather events referring to a specific action being performed on a certain target. This can indicate the different sources that are engaged in the specified behavior with that resource.
7. All of the events with the same source, target and action -- as the most specific aggregation type, this will gather all alerts and access requests of a specific type between a known source and target.

8. IMPLEMENTATION

Next, some examples of event correlation will be given based on a preliminary implementation of the ontology. The Inter-Domain Event Correlation ontology has been implemented as an OWL ontology using the Jena ontology API. Querying for events is currently supported using any of the three properties of events expressed in the base vocabulary: EventSource, EventTarget or EventAction. We provide the following as examples of using the base vocabulary to discover events of variant types. The query could merely specify the source of the event, such as in the following query that returns all security events (Access requests and Attacks) that have as their source, a node with IP address 75.185.221.159

```
SELECT ?event_name
WHERE {
  ?a rdfs:subPropertyOf correlation:EventSource.
  ?b corr:IPAddress ?c
  FILTER regex(?c, "75.185.221.159", "i")
}
```
The query could also similarly seek events with a given specified target, such as the following query that looks for all events targeted at a file “wguest.exe”

```
SELECT ?event_name
WHERE {
  ?a rdfs:subPropertyOf correlation:EventTarget.
  FILTER regex(?file_path, "wguest.exe", "i")
}
```

In a similar fashion as the first two, the query could also look for all events with a specific action – in this case “ServiceProbe” or “MachineProbe”

```
SELECT ?event_name
WHERE {
  {?event_name ?b correlation:ServiceProbe}
  UNION
  {?event_name ?b correlation:MachineProbe}
}
```

Any combination of the above options is also possible, such as simultaneously searching for all events with a target of 75.185.221.159 and with an action of AttackStaging.

```
SELECT ?event_name
WHERE {
  ?event_name ?x correlation:AttackStaging.
  ?a rdfs:subPropertyOf correlation:EventTarget.
  ?b correlation:IPAddress ?c.
  FILTER regex(?c, "75.185.221.159", "i")
}
```

9. RELATED WORK

Undercoffer et al. [11] has examined the use of ontologies in performing intrusion detection. Using empirical evidence of different attacks and seeking to remedy some of the gaps left unaddressed by the IDMEF standard they propose a set of attributes for a class Intrusion and then demonstrate some use case scenarios in which the ontology can detect intrusions of varying types. Security Event Correlation The principle of event correlation has been used most in the security field in the area of intrusion detection alert correlation. All of the techniques for alert corre-

lation are aimed at either reducing the number of alerts that must be viewed by administrators, associating one or more alerts, or analyzing characteristics of an alert such as impact. All of the techniques seen by the authors to date assume that the consumer of the information produced by the correlation process is a system administrator. This is due to factors such as lack of explicit semantics for IDS alerts and heterogeneous alert representations.

10. CONCLUSION AND FUTURE WORK

We have proposed a base vocabulary for correlating events between access control and intrusion detection, primarily using attribute congruence and aggregating events into sets based on search criteria. This base vocabulary uses the abstraction of a security event and poses three main properties: EventSource, EventAction and EventTarget that can be sub-classed in domain-specific ontologies to increase the amount of information available about events, while still allowing the ontologies to be interoperable due to the hybrid nature of the ontology construction. We also proposed a taxonomy of alert correlation aims and methods as a summary of the existing research that has been performed in the alert correlation area. The base vocabulary was the product of synthesizing the most relevant aspects of the IDMEF schema with the XACML specifications for access requests and access decisions and using a taxonomy of system actions discussed in [14]. Once events are instantiated into one of the domain-specific ontologies, they can be correlated through checking for congruence in one or more attributes. The impact of this effort is that it serves as a first step towards building a more complete system capable of collecting event information from various security mechanisms and then facilitating the dissemination of that information to requesting parties. In this paper we have not explored the process of event analysis and that will be the subject of future research.

REFERENCES


[3]. Hervé Debar and Andreas Wespi. Aggregation and correlation of intrusion-detection alerts. RAID ’00: Proceedings of the 4th International Sym-


