# Security Models for Contextual Based Global Processing an Architecture and Overview

Gregory Vert
Center for Secure Cyberspace
Computer Science
Louisiana State University
(206) 409-1434
gvert12@csc.lsu.edu

S.S Iyengar
Center for Secure Cyberspace
Computer Science
Louisiana State University
(225) 578-1252
iyengar@csc.lsu.edu

Vir Phoha
Center for Secure Cyberspace
Computer Science
Louisiana Tech. University
(318) 257-2298
phoha@coes.latech.edu

## ABSTRACT

In this paper, we introduce a new paradigm for global computation, one in which the context of collected information drives the type of processing and dissemination the information receives as it is dispersed around the world. The creation of this model has necessitated the development of new types of methods for securing contextual information because the internet itself inherently has not have security mechanisms. Security is typically localized at the nodes on the internet that process information. There are multiple models and methods that are under development to provide security for contexts. This paper presents the basics of a model that allows context consumers to determine the level of security contextual information should have. Security levels have a direct correlation with confidence in the integrity of contextual data and thus application of its processing.

## Keywords

global contextual processing, contextual processing security, security brane.

## 1. INTRODUCTION

The concept of context has existed in computer science for many years especially in the area of artificial intelligence. The goal of research in this area has been to link the environment a machine exist in to how the machine may process information. An example typically given is that a cell phone will sense that its owner is in a meeting and send calls to voicemail as a result. Application of this idea has been applied to robotics and to business process management [1].

Some preliminary work has been done in the mid 90's. Schilit was one of the first researchers to coin the term context-awareness [2,3]. Dey extended the notion of a context with that of the idea that information could be use to characterize a situation and thus could be responded to [4]. In the recent past more powerful models of contextual processing have in which users are involved [5] but most research has been focused on development of models for sensing devices [6].

Little work, if any has been done on the application of this idea to that of how information is processed. The model that we have developed is that meta data describing information events could model a context that then controls the processing and dissemination of such information in a hyper distributed global fashion. Section two will provide some overview of the newly developed model and what contexts are. Section three will look at the security issues for contextual information and section four will present a basic introduction to a model for determination of the level of security that a given context may require.

## 2. CONTEXTUAL PROCESSING

To understand the issues connected with security models for contexts we introduce some details about the newly developing model for contextual processing.

Contextual processing is based on the idea that information can be collected about natural or abstract events and that information surrounding that information, meta information, can then be used to control how the information is processed and disseminated. In its simplest form, a context is composed of a feature vector

$$F_n<a_1,..a_n>$$

where the attributed of the vector can be of any data type that can be collected about an event. This means that it can be composed of images, audio, alpha-numeric etc. Feature vectors can be aggregated via similarity analysis methods into super contexts $S_{c.}$ The methods that might be applied for similarity reasoning can be statistical, probabilistic (e.g. Baysian), possibilistic (e.g fuzzy sets) or machine learning and data mining based (e.g. decision trees). Aggregation into super sets is done to mitigate collection of missing or imperfect information and to minimize computational overhead when processing contexts.

*definition: A context is a collection of attributes aggregated into a feature vector describing a natural or abstract event.*

A complete context super context is described as a triple denoted by:

$$S_n = (C_n, R_n, S_n)$$

*Conference'04*, Month 1–2, 2004, City, State, Country.
Copyright 2004 ACM 1-58113-000-0/00/0004…$5.00.

where C is the context data, R are the processing rules derived from that data and S is the security processing vector. S is defined to be a feature vector in this model that hold information about security levels elements or $S_n$ overall security level.

*definition: A super context is a collection of contexts with a feature vector describing the processing of the super context and a security vector that contains security level and other types of security information.*

All of the above are feature vectors where the elements can contain any type of information including rule bases.

# 3. SECURITY ISSUES ON CONTEXTS

## 3.1 Overview

A super context is composed of context data from many sensing event objects $Eo_i$ as shown in figure 1. As such contextual information collection works in a similar fashion to sensor networks and can borrow from theory in the field. Figure 1, shows the nature of collection of event object data over time. Once can visualize a region of interest, .e.g. the Indian ocean tsunami for which event object data is collected which is centered over a thematic event object, e.g. the origin of the tsunami.

*definition: A thematic event object is the topic of interest for which event objects are collecting data. An example of a Teo would be the center of a tsunami.*

As time passes in figure 1, event object data collection can be visualized as extruding the region of interest to the right and that event objects operate sporadically in collection of context information. This is the core nature of construction of super contexts.

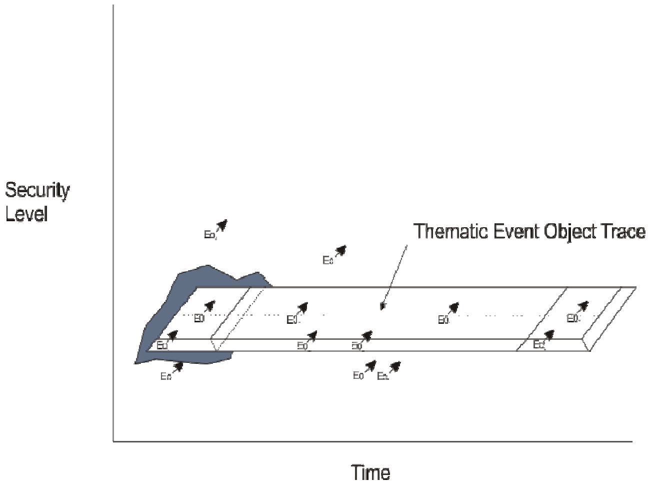

Figure 1 Visualization of the streaming collection of context data, irregularly over time for a region of interest

## 3.2 Information Assurance and Security

The key issue implied in the visualization of contexts data collection is that some $Eo_i$ are i) $S_n = (C_n, R_n, S_n)$ flow around the world on unsecured lines to information consumers, ii) that there must be standard security methods applied to super contexts (e.g. authentication, encryption) and that iii) computational resources are limited especially if continuously streaming and potentially ambiguous contextual information needs to be protected. Thus a model has been developed which states that i) not all contextual information has the same germanity to a theme ii) that some types of contextual information need higher levels of security than others based on proximity and limited resources. These key ideas have led to the concepts of using a brane to determine which contextual streams require the highest consideration for protection.

# 4. BRANES AND SECURITY LEVELS FOR CONTEXTS

## 4.1 General Operation and Concept

A brane is a term borrowed from Cosmology. I can have multiple mathematical dimensions and can be thought of a boundary for the purpose of organizing abstractions.

*definition: A brane can be is a three dimensional surface that is overlaid above a two dimensional object. Finding the intersection of the projection of event objects on the 2D surface with the brane can provide a value that can be utilized to calculate security level for the context of a given event object.*

It is often used to model parallel universes. In our case it was realized that a p-brane of order three could be utilized to determine levels of security required on context data. Because of the established mathematics of brane theory, they can be applied to n-dimensional abstractions and are not limited to physical events. To understand how a brane might classify $Eo_i$ objects, we had to define the key properties that influence classification.

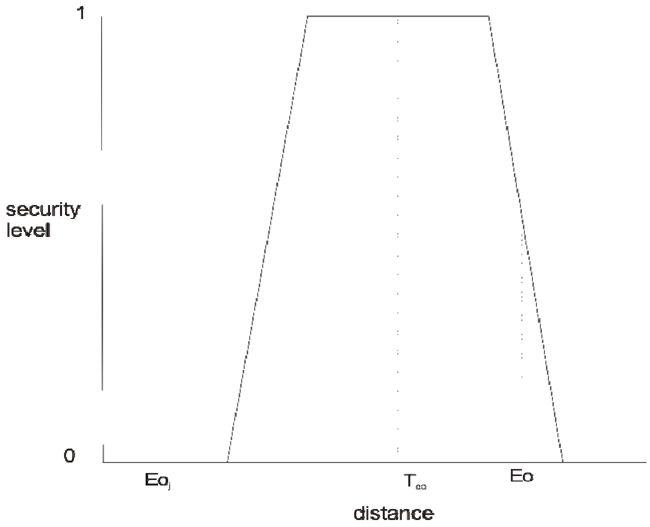

Figure 2 Security level calculation utilizing a p-brane of order two

In figure 2, the event $Eo_i$ projects onto the brane producing a security level of about .5. The $T_{eo}$ projects onto the brane with security level 1, where objects outside of the brane receive a security level of 0. A security level of 1 could mean that context data originating from the $T_{eo}$ need full encryption, whereas event objects with level 0 could be ignored or sent in clear text.

## *4.1.1 Brane Classification Properties*

Our model of the application of branes has determined several critical properties that need to be considered when applying brane theory to information assurance.

### *4.1.1.1 Inclusivity*

Before presenting some example Branes that might be utilized for security level determination, it is important to understand the properties that describe a brane. These properties directly affect how a brane classifies event objects and derives their security levels. The first of these properties is that of inclusiveness. Inclusiveness is the property that describes how a brane classifies points and has three categories.

An *exclusive* brane can only classify one point of the region it is centered over as having a value of 1 for security level. This property means that all other points that can be classified will have values between 0 to <= 1. Because of this fact, this type of brane should be considered to have the least security, and in fact imposes the least amount of security on classifications of event objects. As a result this type of brane has the least computational overhead because a point depending on the referencing of the brane may classify at most one event object. A conic volume is an example of this.

The next type of brane property is that of being *partially inclusive*. In this type of structure, some points are classified as having a security level of 1 and others have a value between described by a closed interval Mathematically this can be described as:

$$\text{security level} = [0,1], \text{ where } 0 <= \text{security level} <= 1$$

These types of branes typically have a frustum but not always. They are characterized by having a flattened top to the structure. An interesting fact about these types of branes is that the shape of the brane can be modified to control the ratio of classification between partial security values where 0 <= security level <= 1 and full values where security level = 1. The equation describing this classification ratio is given by:

$$C_r = \text{Area(frustum)} / \sum(\text{Area(Sides)})$$

given equal numbers of event objects in both regions.

Because of this property the partially inclusive branes are probably the most powerful and flexible type of brane to apply for security classification.

The final type of property for inclusiveness is that of *complete inclusivity*. This type of brane is characterized by have a flat structure on top that classifies all event objects with security level as 1. Therefore this type of structure is the most secure. However because all events are classified as 1, they all must have maximum security procedures applied to them, therefore this is the most computationally expensive model.

### *4.1.1.2 Continuity*

Branes have another property to their geometry and classification that for lack of better terms may be referred to as their continuity. This means that certain types of branes are super types of simpler structures with fewer sides. Consider figure 3.

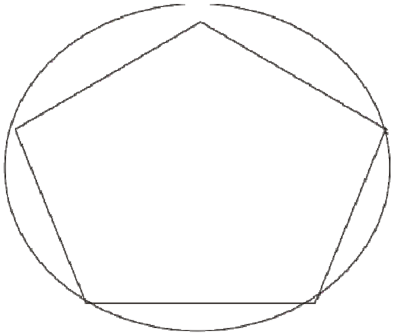

Figure 3, Continuity property, a cone is a super type of a N sided pyramid

In this model only one version of a brane can have continuity, which is defined to be that the second derivative f''() of any point on the surface of the brane cannot equal the f''() of any other event objects point on the brane surface. The brane with this property is a super type and there can only exist one for given form. This property is found in conics surface with α number of side in the sweep construction of the surface.

### *4.1.1.3 Discreetness*

A final property we have defined is that of discreetness. This can be described by the fact that the number of sides of a brane must be ≥ 3, the figure is closed. A *continuous brane* has the property that i) the horizontal tangent vectors (f'') must all be different, and ii) the vertical vectors must all be the same. In contrast a *discrete* brane has the properties that i) classes of similar horizontal tangent vectors may exists and that ii) vertical tangent vectors can also fall into classes.

### *4.1.1.4 Hexahedron Brane*

To understand how a brane and its properties can be applied two of the simplest branes are presented. There are many more with very different properties being studied.

A hexahedron is often referred to as a cube. Because of its properties it classifies all event objects $Eo_i$ that are within the base cube as security level = 1. It is therefore completely inclusive in how it classifies. It also has the property of being discrete which means that it will

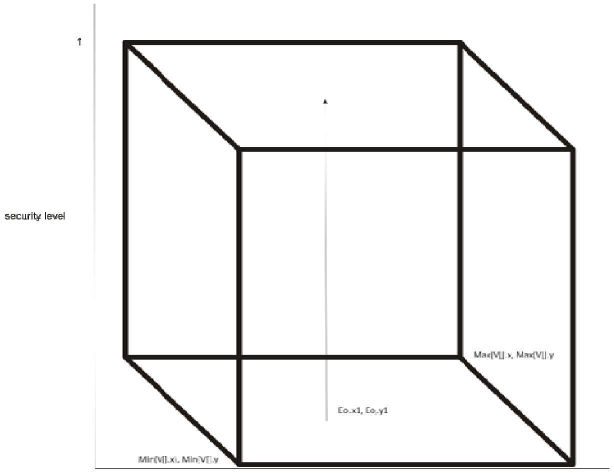

Figure 4, A hexahedron brane will classify all $Eo_i$ objects on the 2D flat base surface that are within the base cube as security level = 1

*definition: computational overhead and security level classification is related the the properties of a brane. Medium variable security level means classification on event objects will be a set of mixed values ranging from 0 to 1. A value of 1 means full security measures thus the highest computational overhead.*

The hexahedron has the following properties in how it classifies as shown in table 1:

**Table 1. Brane properties of the hexahedron**

| **Inclusivity** | **Continuity** | **Overhead Computational** | **Security Level Classification** |
|---|---|---|---|
| Complete | Discrete | Medium / Variable | Medium / Variable |

Determination of the security level using this brane does a range check to determine if an event object is located within the cube on the base of the brane (security level= 1) and can be calculated by the following algorithm:

```
HexahedronSecLevel($Eo_i$, V[])
{ $Eo_i$ event object
  V[] vertices base rectangle
  if ( $Eo_i$.x1, $\geq$ Min(V[].x) ^ $Eo_i$.x1, $\leq$ Max(V[].x))
        if  ($Eo_i$.y1, $\geq$ Min(V[].y) ^ $Eo_i$.x1, $\leq$ Max(V[].y)) return 1
  else
        return 0
}
```

### 4.1.1.5 Cylinder Brane

The cylindrical brane is the most computationally intensive and is also the most secure brane to utilize in setting security levels for contexts. This fact is based on it being continuous and because it is completely inclusive in the way it classifies. An example of the brane can be found in figure n

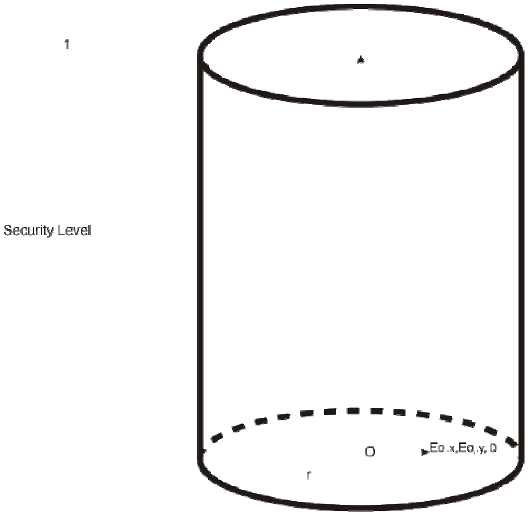

Figure 5, The cylindrical brane. will classify like a hexahedron but because it is continuity is continuous it can contain more event objects context data its security can be higher and thus its overhead.

The cylinder has the following properties in how it classifies as shown in table 2:

**Table 2. Classification properties of the Cylindrical brane**

| **Inclusivity** | **Continuity** | **Overhead Computational** | **Security Level Classification** |
|---|---|---|---|
| Complete | Continuous | Highest | Highest |

Determination of the security level can be calculated by determination of whether an event object is within the circle at the base of the cylinder, if so its security level is 1. This is described in the following algorithm:

```
CylinderSecLevel($Eo_i$,r, o])
{ $Eo_i$ event object in form (x,y, 0)
  r  radius of cylinder
  o orgin of cylinder in form (x, y, 0)
 $Eo_{radious}$ = sqrt(($Eo_i$.x-o.x)$^2$ + ($Eo_i$.y-o.y)$^2$ +( 0))
        if  ($Eo_{radious} \leq$ r) return 1
  else
        return 0
}
```

These are two of the simplest branes studied for application determination of the levels of security that need to be applied to contexts information. The security level has a relationship to application of the R rules in the tuple $S_n = (C_n, R_n, S_n)$. While this model is under development, it is thought the there is a relationship between security level and how confidently the processing rules are applied in other words, how believable the information derived from the context processing is.

# 5. CONCLUSIONS

## 5.1 Future Work

The modeling notion of contextual processing and how it flows in a flat, peer based security environment is the subject of ongoing analysis, research and the subject of a new book currently being developed for at LSU in conjunction with the Center for Secure Cyberspace. This paper provides a simple introduction to the subject; much more elaborate branes are being evaluated. Additionally, research is being given to i) how security levels from branes correlate with application of R in $S_n = (C_n, R_n, S_n)$, ii) development of “spot security” based on security level to limit computational overhead and iii) the integration of contextual similarity into the brane models, what the semantics might mean and how they can be related to streaming contexts with high computational overhead for security processing

.

# 6. REFERENCES

1. Rosemann, M., & Recker, J. (2006). "Context-aware process design: Exploring the extrinsic drivers for process flexibility". T. Latour & M. Petit *18th international conference on advanced information systems* engineering. proceedings of workshops and doctoral consortium*: 149-158, Luxembourg: Namur University Press.*
2. Schilit, B.N. Adams, and R. Want. (1994). "Context-aware computing applications" (PDF). *IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'94), Santa Cruz, CA, US*: 89-101.
3. Schilit, B.N. and Theimer, M.M. (1994). "Disseminating Active Map Information to Mobile Hosts". *IEEE Network* **8** (5): 22–32. doi:10.1109/65.313011.
4. Dey,Anind K. (2001). "Understanding and Using Context".*Personal Ubiquitous Computing* **5** (1): 4–7. doi:10.1007/s007790170019.
5. Cristiana Bolchini and Carlo A. Curino and Elisa Quintarelli and Fabio A. Schreiber and Letizia Tanca (2007). "A data-oriented survey of context models" (PDF). *SIGMOD Rec.* (ACM) **36** (4): 19--26. doi:10.1145/1361348.1361353. ISSN 0163-5808. http://carlo.curino.us/documents/curino-context2007-survey.pdf.
6. Schmidt, A.; Aidoo, K.A.; Takaluoma, A.; Tuomela, U.; Van Laerhoven, K; Van de Velde W. (1999). "Advanced Interaction in Context" (PDF). *1th International Symposium on Handheld and Ubiquitous Computing (HUC99), Springer LNCS, Vol. 1707*: 89-101.