Detection of Suspicious Patterns in Secure Physical Environments

Pengfan Yan, Robert P. Biuk-Aghai, Simon Fong and Yain-Whar Si

***Abstract*—Security in physical environments has become increasingly important in the wake of terror and criminal activity, particularly over the past decade. One of the challenges is to identify activities that may not be outright illegal or breaches of security, but that are suspicious, i.e. where there is a possibility that these activities may lead to breaches of security. Technology such as RFID is used to track the access and movement of people in highly security physical environments. This paper presents methods of detecting patterns of suspicious activity in logs collected by such physical access control systems. It also outlines methods of predicting future suspicious activities based on such logs.**

***Index Terms*—data mining, RFID, security.**

I. Introduction

In the wake of increased terrorist and criminal activity over the past decade, the security of physical environments has become an increasingly important topic. In many parts of the world the use of video surveillance technology has become widespread for detecting security breaches [1]. Moreover, electronic and information technology has been used to restrict access to physical environments. For example, smartcard-based access control systems have been used over the past decade to automate the identification and authentication of access to restricted physical environments such as buildings, rooms, etc. More recently, RFID (radio frequency identification) has emerged as a technology that has enjoyed quick and widespread adoption in the security domain. RFID allows a person or object to be tagged with a unique identifier that can be wirelessly sensed when the RFID tag enters the range of an RFID sensor. The low cost of RFID equipment coupled with the convenience of a wireless mode of operation and a fast detection rate makes this technology particularly suited for security applications. In 2005, the US Department of Homeland Security (DHS) announced that it would distribute 40,000 RFID-based access cards to its employees and contractors to control access to both physical environments and computer systems. Other US federal agencies also are making use of similar technology to strengthen the security of their physical environments, and this technology is being adopted by governments and private agencies around the world.

This research was sponsored by the University of Macau under grant number RG076/04-05S/06R27/BARP/FST.

All authors are with the Department of Computer and Information Science, Faculty of Science and Technology, University of Macau (email: {ma46602,robertb,ccfong,fstasp}@umac.mo).

Using RFID technology allows the physical access of people to secure areas to be controlled. Moreover, given enough sensors in a secure environment, it also allows the movement of people within the environment to be tracked. Current use of this technology, however, is mainly restricted to disallowing unauthorized access. Once a person has gained access to a secure physical environment, the actions of that person within that environment are usually not further monitored other than detecting outright breaches of security, e.g. through video surveillance. It is possible, however, that a given person within a secure environment behaves in a way that does not constitute an outright security breach, but that could be considered suspicious behaviour. Other security problems could arise if data from a valid RFID tag is surreptitiously obtained (RFID sniffing) and used to create a clone of the RFID tag which can then be used in RFID spoofing, replay attacks, or denial of service [2],[3]. If such suspicious behaviour could be detected, security personnel could be alerted to monitor the suspicious person closely to determine whether a security breach is about to be committed.

This paper presents a detection model to enable suspicious patterns of behaviour in secure physical environments to be detected using data mining techniques that are applied to data logged by RFID sensors. The remainder of this paper is organized as follows: Section II presents a case of a secure physical environment to which our methods are to be applied. Section III then defines four suspicious behavioural patterns. In Section IV our model of detection of these suspicious patterns is presented, and Section V outlines how future suspicious patterns can be predicted. Section VI compares our research with related work, and Section VII presents conclusions.

II. Secure Physical Environment

To make the following discussions more concrete, we present here a model of a secure physical environment in which our detection of suspicious behavioural patterns can be applied.

A. Basic Assumptions

We make following assumptions about this environment:

1. The environment consists of a building with *rooms* and *corridors* connected with *doors*. Doors separate parts of the building into different *areas*.
2. Every door is equipped with *RFID sensors* on its outside and inside that separately detect RFID tags on either side of the door. The directionality of the RFID sensors is such that they non-overlappingly detect only an area on one side of a door.
3. A door may be equipped with an electronic *locking*

mechanism that can be centrally controlled to unlock the door when authorized users request access, such as by presenting their access card (see below) and/or pressing a button to request unlocking of the door.

4. A corridor may be equipped with additional RFID sensors that detect RFID tags moving through the corridor.
5. Every person with permission to access the environment, such as regular employees, visitors and contractors, is supplied with an *access card* with an embedded RFID tag. This access card may store additional biometric identification data, such as fingerprint data, iris scan data, a facial photograph or others. For the purposes of this paper, however, the presence of additional security mechanisms based on biometric identification is considered optional.
6. A central system logs access events captured by the RFID sensors in the environment. An event log consists of a timestamp, an identification of the access point (i.e. the RFID sensor), and an identification of the access card (i.e. the RFID tag) used. Event logs are recorded in chronological sequence. The central system has information about the location of each access point, and about the person to whom a given access card is issued.

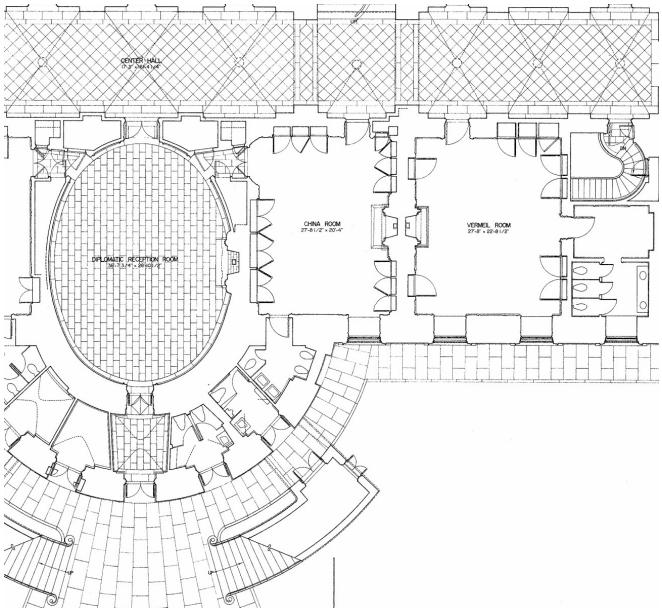

Fig. 1. Extract of a historic floor plan of the US White House*

As actual data from a real secure physical environment is not easily obtained (for obvious reasons), we have simulated such an environment as well as the movement of people within the environment. We have chosen the US White House as the case to apply our simulation to as it can be reasonably considered to be a highly secure physical environment (other candidates for modelling could have included parliament buildings, military installations, financial institutions, etc.). An extract of a historic floor plan of the White House is shown in Fig. 1. It consists of a number of external entrances, rooms, corridors, internal doors and staircases. According to our above assumptions, the entire building is equipped with numerous RFID sensors. A simplified view of a portion of the building, showing location and range of RFID sensors, is given in Fig. 2.

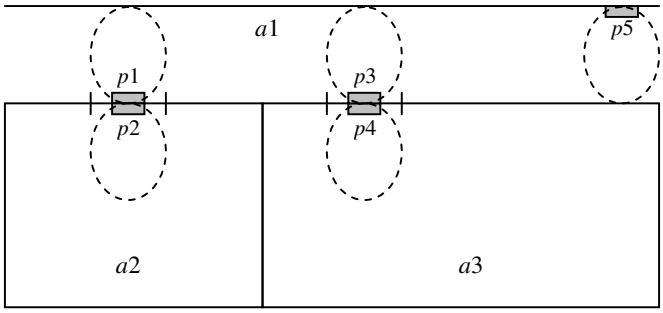

Fig. 2. Portion of a secure physical environment equipped with RFID sensors

This figure identifies three separate areas, $a1$ (a corridor) and $a2$ and $a3$ (rooms). At the door to each room there are two access points with RFID sensors, one each on its outside and inside. In long corridors additional access points may be placed for detecting people passing by, such as access point $p5$. The sensing range of each RFID sensor is indicated by the dashed ovals and extends some distance from the door forward, in the case of the sensors in the corridor all the way to the opposite wall. This allows a sensor to detect a person (holding an RFID tag) passing by at any point on the entire width of the corridor. For example, a person traversing the corridor from left to right would be detected, in sequence, by the RFID sensors at access points $p1$, $p3$ and $p5$. On the other hand, a person entering a room would be detected first by the sensor on the outside of the room, then by the sensor on its inside. For example, a person entering area $a1$ (the corridor) from the left and then entering area $a2$ (the room on the left) would be detected, in sequence, by access points $p1$ and $p2$.

B. Control System

Central to the security of the physical environment is an access control system that maintains a database of all access cards and access points. A system diagram depicting the main components is shown in Fig. 3.

The access control system performs following main functions:

Logging: when an access card held by a person is detected by an RFID sensor at an access point (shown on the left), the logging server records this as an access event in the system database.

Authentication: when an access event is received, the authentication server decides, based on definitions of access permissions stored in the system database, whether or not to grant access to the person holding the access card, such as by releasing a door's security lock.

* Picture is in the public domain, source: US Library of Congress, online at: http://commons.wikimedia.org/wiki/Image:White-house-floorG-plan.jpg

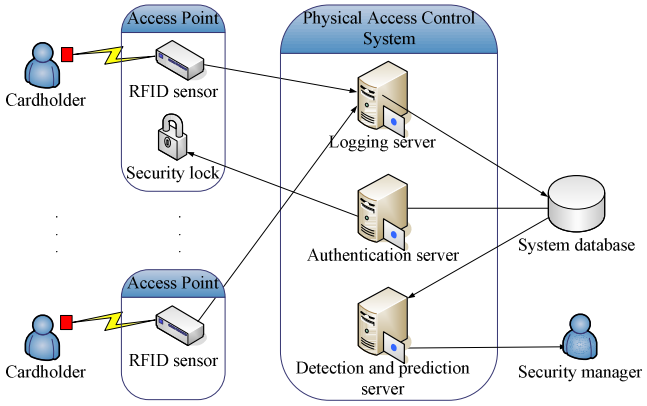

Fig. 3. Main components of physical access control system

Detection & prediction: when an access event is received, the detection and prediction server analyzes it, in relation to previously observed access events, to detect a suspicious pattern of activity, and to predict possible future suspicious patterns.

The system database not only records access events on an ongoing basis, but also contains definitions of the environment and the persons in it. The main information recorded in the system database is as follows:

1. *Access points*: identifier and location of each access point, including the area which it belongs to (e.g. access point $p1$ in Fig. 2 belongs to area $a1$).
2. *Access card*: identifier of each access card, and which person is the current holder of the card.
3. *Access event*: identifier of the access card and access point involved in the event, and a timestamp.
4. *Person*: name and other personal information of each person allowed access to the environment.
5. *Neighbour*: identifiers of pairs of neighbouring access points, their distance, and the average and minimum time needed to traverse the distance between them (e.g. access points $p1$ and $p3$ in Fig. 2 are neighbours).
6. *Area*: area name, type, and maximum normal continuous stay time in the area (e.g. the maximum normal stay time of a washroom may be one hour, whereas for an office it may be eight hours).
7. *Access permission*: identifier of the access points which a certain access card has the permission to access. In the case of a centrally controlled door, the permission includes the unlocking of the door and thus access to the connected area on the other side of the door.

Given the definitions in the system database, particularly information such as access permissions, neighbouring access points and maximum stay time of areas, allows the detection and prediction server to carry out sophisticated analyses of logged access events in order to detect and predict suspicious behavioural patterns.

III. Suspicious Patterns

In this paper, we propose techniques that detect a person's suspicious behaviour by analyzing movement patterns and identifying potential security threats in the secure physical environment. The suspicious behaviour in our system is represented by a collection of *suspicious patterns*. Each of these patterns is a sequence of actions performed by a person that may be completely legitimate when the level of analysis is a single event. However, when these events are combined over time and viewed together as a sequence they give rise to certain kinds of suspicion.

The exact definition of the suspicious movement of people usually varies from one environment to another, and subjectively depends on the security requirements of each different situation. Nevertheless, the following shows four types of suspicious patterns that are generic and that can be detected and predicted by our methods:

1. Temporal pattern

A temporal pattern is an unusually long period of stay by a person in a given area, i.e. when the stay period exceeds the maximum normal stay time defined for that area. For example, if a person enters a room and stays there continuously for more than 12 hours before leaving the room, this may be considered suspicious.

2. Repetitive access pattern

A repetitive access pattern exists when unusual repetitive accesses occur within a given period of time. For example, if a person enters and leaves a room ten times within one minute, this may be considered as suspicious.

3. Displacement pattern

Another type of pattern is based on the displacement of people. A displacement pattern exists when a person consecutively accesses distinct neighbouring locations within an unusually short period of time. For example, if a person exits one room and three seconds later enters another room located 100 m away, this may be considered as suspicious.

4. Out-of-sequence pattern

The final type of pattern is the out-of-sequence pattern. Certain accesses must occur in a specific sequence to be classified as normal, as defined by pairs of neighbouring access points. Whenever consecutive accesses occur in an undefined sequence, this constitutes an out-of-sequence pattern. For example, if a person passes one access point, and subsequently passes a third access point without having passed a second access point located between the two, this may be considered as suspicious.

These generic types of suspicious patterns are applied in our detection and prediction model. Whenever a sequence of access events are recorded that match the definition of one of these types of patterns, that pattern is *detected* in the data; whereas when a sequence of access events matches only the beginning of one of these types of patterns, the occurrence of that type of pattern can be *predicted*.

IV. Pattern Detection

In this section we describe the functions for detecting suspicious access patterns. These functions can be used in an existing physical environment that has surveillance sensors

installed, as described in Section II. These functions are designed to detect suspicious patterns from a sequence of access events over time in addition to usual rules for detecting outright security breaches. For our research we have generated simulated data based on the environment described in Section II.

In a typical access control system, access events and related access right policies are stored in a system database. Our detection functions access this data in real time, group access events based on each card holder, and evaluate against the administrator-defined thresholds for detection of suspicious patterns. We define following parameters for designing detection functions (see Table I).

Table I parameters for detection model

Parameter	Description
$event_i$	i^{th} *access event*
cid	$cid = cardID(event_i)$ Access card ID of i^{th} access event
AP_i	$AP_i = accessPoint(event_i)$ Access point of i^{th} access event
repThreshold	The maximum allowable number of repeated accesses in normal situation
repAccMinDuration	The minimum allowable duration for a sequence of normal repeated accesses

A. Detection of Temporal Pattern

A pattern is considered to be temporal when the system detects that a person has spent an unusually long duration in one location. Let $timeStamp(AP_i, cid)$ be the function which returns the timestamp of the i^{th} detected access point of the person holding card *cid* from the historical log. Let $location(AP_i)$ be the function which returns the location of the i^{th} access point, and let $maxStay(loc, cid)$ be the function which retrieves the predefined maximum duration the person holding card *cid* is allowed to stay at the location *loc*. We define the algorithm for detecting temporal patterns as follows:

```
for each new detected event_i
{
t_pre  = timeStamp(AP_i-1, cid);
t_cur  = timeStamp(AP_i, cid);
t      = t_cur – t_pre;
t_max  = maxStay(location(AP_i-1), cid);
if (t_max < t )
      pattern = "Temporal";
else
      pattern = "Normal";
}
```

B. Detection of Repetitive Pattern

A pattern is considered to be repetitive when the system detects that a person performs unusually repetitive accesses within a given period of time. When the system detects the repetitive pattern, it focuses on access events detected from a pair of access points (sensors) installed at two opposite sides of a door. In addition, two conditions must hold for a repetitive pattern: (1) the total number of repeated accesses should be greater than the predefined threshold, and (2) the total time spent during the repeated accesses must be shorter than the minimum allowable duration for a sequence of normal repeated accesses.

First, the system derives the total number of repeated accesses from the last detected access event. For instance, two repeated accesses are detected from the sequence $AP_{i-4} \rightarrow AP_{i-3} \rightarrow AP_{i-2} \rightarrow AP_{i-1} \rightarrow AP_i$, where AP_i is the i^{th} detected access point. Note that $AP_i = AP_{i-2} = AP_{i-4}$, and $AP_{i-1} = AP_{i-3}$. Let $repAccessCount(AP_n)$ be the function which counts the total number of repetitive accesses for access point AP_n. For the above sequence, $repAccessCount(AP_i)$ is equal to 2.

Next, the system derives the total time spent during the repeated accesses. Let $timeSpent(AP_x, AP_y)$ be the function which returns the time spent by the person when accessing point *y* after accessing *x*. Therefore, the total time spent by the person for the previous access sequence can be denoted as $timeSpent(AP_{i-4}, AP_i)$. Based on these functions, we define the algorithm for detecting repetitive access patterns as follows:

```
for each new detected event_i
{
if ((repAccessCount(AP_i) > repThreshold)
   and
   (timeSpent(AP_i - 2(repAccessCount(APi)), AP_i) <
   repAccMinDuration))
      pattern = "Repetitive";
else
      pattern = "Normal";
}
```

The problem of detecting repetitive patterns can be solved by using classical computing techniques, such as detecting cycles in Directed Graph Theory, and Hidden Markov Model; the implementation details can be found in [3] and [4] respectively.

C. Detection of Displacement Pattern

A pattern is considered to be a displacement when the system detects that a person makes consecutive accesses to two distinct locations within an unusually short period of time. Let $minMove(AP_{i-1}, AP_i)$ be the function which returns the minimum time required to travel from $(i-1)^{th}$ access point to i^{th} access point. We define the algorithm for detecting displacement patterns as follows:

```
for each new detected event_i
{
   t_pre  = timeStamp(AP_i-1, cid);
   t_cur  = timeStamp(AP_i, cid);
   t      = t_cur – t_pre;
   t_min  = minMove(AP_i-1, AP_i);
   if (t < t_min)
      pattern = "Displacement";
   else
      pattern = "Normal";
}
```

D. Detection of Out-of-Sequence Pattern

Depending on the architectural layout of the building, certain access events must occur in a specific sequence. For instance, an access point B cannot be reached from an access point A if both access points are located in two different rooms and there is no direct path between them. A pattern is considered to be out-of-sequence when the system detects that a person attempts consecutive accesses to two distinct locations whereby the second location is unreachable from the first one. Let *isNeighbor*(AP_{i-1}, AP_i) be the function which returns true if AP_i can be reached from AP_{i-1}. We define the algorithm for detecting out-of-sequence patterns as follows:

```
for each new detected event_i
{
   if (isNeighbor(AP_{i-1}, AP_i))
      pattern = "Normal";
   else
      pattern = "Out-of-sequence";
}
```

Using the above four detection algorithms, the system may decide to raise an alarm when a suspicious access pattern is detected. However, in some situations a sequence of access events may not be considered as suspicious since its degree of suspicion does not exceed pre-defined threshold values. For instance, the total number of repeated accesses by a person may not exceed the limit and hence the system may not raise the alarm. In such cases, the system may not be able to detect mild cases of access right violations. To alleviate this problem, we define a model which is capable of predicting future suspicious access patterns from historical records.

V. Pattern Prediction

Our main work to date has focused on detecting suspicious behavioural patterns in a body of access event data. Taking this further, we are currently extending our work on detection of actual suspicious behavioural patterns to *prediction* of potential future suspicious patterns. The aim of prediction is to be able to give early warnings of suspicious activity as it unfolds, and thereby to enable security personnel to take timely action.

Unlike the technology for detection which depends on finding a complete match of a sequence of access events with a type of suspicious pattern, the technology for prediction is more complicated as it focuses not only on the immediate past sequence of access events, but also on an analysis of the history of all previous access events, the history of suspicious patterns of an individual person, and other factors. As this is work in progress, we only briefly discuss the approach for prediction here.

Given the nature of the prediction task, which must perform partial matching of access data with pattern types, we cannot achieve the same accuracy as in pattern detection. Therefore, we define a *suspicious rate*, which indicates the probability of the corresponding suspicious pattern occurrence. The suspicious rate is calculated by using a *suspicious threshold*, which is defined for each suspicious pattern type. Below the threshold behaviour is considered normal, above the threshold it is considered increasingly suspicious. For instance, for a given area five consecutive entrance and exit events may be defined as the threshold of suspicion for a repetitive pattern. If fewer than five entrance and exit events occur, the activity is considered normal, with five such events it will start to be considered suspicious, and with more than five such events it will be considered even more suspicious. Prediction can begin when the sequence of patterns is still normal but approaching the suspicious threshold. For instance, when already four consecutive entrance and exit events have occurred, the sequence can be predicted to continue and to become suspicious. A well-defined threshold for each pattern type is thus essential for achieving more accurate prediction.

Based on the detection algorithms and pattern definitions in the previous sections, it is possible to define empirical algorithms for predicting applicable suspicious behavioural pattern. Suitable techniques that can be applied here include some statistical techniques, such as Hidden Markov Models (HMM) [6][7] and other data mining techniques.

A. Empirical Techniques

The main idea is based on the knowledge of a given pattern's characteristics. For instance, for a repetitive pattern to occur, a number of preceding access events would have involved a transition back and forth between the same two areas, and these access events would have occurred within a certain short time period. Because of this characteristic we can monitor subsequent access events to observe whether they involve the same two areas and whether they continue to occur within a short time period, and thus determine a corresponding suspicious rate.

B. Statistical Techniques

In a real physical environment, people usually perform actions in the same specific areas, because of their work requirements, given access privileges, routines, habits, and many other reasons. For suspicious behaviours the same can be assumed, as differences in physical environments afford different opportunities for would-be violators and therefore certain locations can be assumed to be used in different types of suspicious patterns. For instance, an out-of-sequence pattern may frequently occur at a location where it is possible to circumvent access control, such as by climbing out of a window and re-entering somewhere else. The next access event would then reveal that some access points were omitted. Moreover, a given person may have a history of past suspicious patterns that could make a future suspicious pattern more probably for that person. Prediction of an out-of-sequence pattern would thus use location and the identity of the person, as well as other factors such as day of week or time of day, as contextual information to determine the probability of such a pattern to occur. Determining such probabilities in a certain context can be performed well using statistical methods.

We are considering the use of HMM which can output the

most probable sequential hidden states based on the given sequential observable states. We assume the detected access event to be the observable state, and the type of pattern of the corresponding access event as hidden states. The access events in the historical log of a specific person are ordered chronologically as HMM is well-suited for dealing with sequential analysis. So, when analyzing a fixed length sequence of consecutive access events, HMM can be applied to predict which pattern will have the highest probability to be the next one.

VI. Related Work

Over the past few decades techniques and systems for intrusion detection have been studied and developed extensively [8]. Intrusion detection systems (IDS) can be divided into two main categorizes: misuse detection and anomaly detection [9]. In misuse detection, intrusion is detected by comparing a person's activities with the known intrusive patterns. In anomaly detection, IDS identifies intrusion by monitoring deviation from the normal behaviours. Traditional intrusion detection systems perform tasks related to computer network and operating systems security whereas in our approach, we focus on identifying suspicious access patterns in physical environment.

Access control systems [10][11][12][13][14] are widely used in securing government departments, offices, and university campuses. In general, these systems provide access card administration, access right management, and alarm monitoring functions. To the best of our knowledge, there is no commercial tool supporting detection of suspicious patterns based on access events in physical environment.

Detection of suspicious access patterns in smart card-based environment is analyzed in [15]. Our approach extends the framework described in [15] by taking into account the situation where contact less proximity cards such as RFID are used for authentication and access control.

Various kinds of perimeter intruder detection systems (PIDS) [16] are also widely used to deter unauthorized access to restricted areas such as embassies, warehouses, and others. AMETHYST [17] is an automatic event authentication system based on video assessment for perimeter intrusion detection. AMETHYST assesses the CCTV pictures and generates an alarm when an intrusion or a suspicious event is detected. PIDS are also essential for Airport security applications. Barry et al. [18] have analyzed the deployment of Airport Surface Detection Equipment (ASDE-3) radar for Airport security surveillance and perimeter monitoring. The radar-based PIDS are capable of tracking and identifying human-sized targets within radar's detection range.

The difference between PIDS and our approach is that in PIDS, tracking persons or target objects do not take into account the access right assignments whereas in our approach, people under surveillance are uniquely identified and their access patterns are evaluated against their privileges. In addition, PIDS generate alarms based on in-progress intrusion behaviours whereas in our approach, alarms can be generated based on history of past access events.

VII. Conclusions

In this paper, we have described a novel approach for the detection of suspicious access patterns in physical environments. In this framework, a detection mechanism is designed to utilize the history of past access events to identify four major types of suspicious access patterns. Our framework also takes into account the circumstances unique to the RFID-based access control environment such as tracking the movement of target objects (persons) in communal areas. Future work will be focused on developing a system based on Hidden Markov Models (HMM) to predict future suspicious access patterns from event records. We are also developing information visualization tools to display access events in real time augmented by the alarms generated from the detection and prediction systems.

References

[1] US Department of Justice, CCTV: Constant Cameras Track Violators, *National Institute of Justice Journal*, issue 249, July 2003, pp. 16-23.

[2] Frank Thornton, Brad Haines, Anand Das and Anita Campbell, *RFID Security*, Syngress, 2006.

[3] D.J. Cook and L.B. Holder, Graph-Based Data Mining, IEEE Intelligent Systems, 15(2), pp. 32-41, 2000.

[4] James F. Bowring, James M. Rehg, Mary Jean Harrold, Active learning for automatic classification of software behavior, Proceedings of the 2004 ACM SIGSOFT international symposium on Software testing and analysis ISSTA '04, Volume 29 Issue 4, pp. 195 – 205, July 2004.

[5] Melanie R. Rieback, Bruno Crispo and Andrew S. Tanenbaum, The Evolution of RFID Security, *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 62-69, Jan.-Mar. 2006.

[6] L. R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proceedings of the IEEE*, vol. 77, pp. 257-286, February 1989.

[7] B. H. Juang, "Maximum likelihood estimation for mixture multivariate stochastic observations of Markov chains," *AT&T Technical Journal*, vol. 64, no. 6, pp. 1235-1249, 1985.

[8] Y. Bai and H. Kobayashi. Intrusion Detection Systems: Technology and Development. In Proceedings of the IEEE International Conference on Advanced Information Networking and Applications, pp. 710-715, 2003.

[9] T.F. Lunt, "A Survey of Intrusion Detection Techniques", Computer Security, Vol. 12, No. 4, pp. 405-418, October 1997.

[10] Warwick Wireless Ltd, http://www.radiotelemetry.co.uk/rfidsystems.htm

[11] AMAG Technology, http://www.amag.com

[12] Lenel Systems International Inc. http://www.lenel.com

[13] MAXxess Systems, http://www.maxxess-systems.com

[14] MDI Security Systems, http://www.mdisecure.com

[15] A. Leong, S. Fong, and S. Siu. "Smart Card-Based Irregular Access Patterns Detection System," in Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04), pp. 546- 553, 2004.

[16] J.O. Peralta and M.T.C. de Peralta, "Security PIDS with physical sensors, real-time pattern recognition, and continuous patrol," IEEE Transactions on Systems, Man and Cybernetics, Part C, vol.32, no.4, pp. 340- 346, Nov 2002.

[17] M. Horner, G. Leach. and T. O'Dwyer, "AMETHYST: automatic alarm assessment: operational experience," in Proceedings of IEEE 34th Annual 2000 International Carnahan Conference on Security Technology, pp.107-112, 2000.

[18] A.S. Barry and J. Czechanski, "Ground surveillance radar for perimeter intrusion detection," in Proceedings of the 19th Digital Avionics Systems Conferences, (DASC 2000) , vol.2, pp.7B5/1-7B5/7, 2000.