# Survey of Intrusion Detection and Prevention Systems

**Article** *in* Information Management & Computer Security · October 2010

DOI: 10.1108/09685221011079199

Ahmed Patel
Universal Universities, Earth
**233** PUBLICATIONS **1,800** CITATIONS

SEE PROFILE

Qais Saif Qassim
Universiti Tenaga Nasional (UNITEN)
**23** PUBLICATIONS **137** CITATIONS

SEE PROFILE

Christopher Wills
Kingston University London
**19** PUBLICATIONS **227** CITATIONS

SEE PROFILE

# A survey of intrusion detection and prevention systems

Ahmed Patel
*Department of Computer Science,
Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia (The National University of Malaysia),
Bangi, Malaysia and
Faculty of Computing Information Systems and Mathematics,
Kingston University, Kingston upon Thames, UK*

Qais Qassim
*Department of Computer Science,
Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia (The National University of Malaysia),
Bangi, Malaysia, and*

Christopher Wills
*Faculty of Computing Information Systems and Mathematics,
Kingston University, Kingston upon Thames, UK*

Received 2 February 2010
Revised 18 March 2010
Accepted 26 March 2010

## Abstract

**Purpose** – The problem of protecting information and data flows has existed from the very first day of information exchange. Various approaches have been devised to protect and transfer such information securely. However, as technology and communications advance and information management systems become more and more powerful and distributed, the problem has taken on new and more complex dimensions and has become a major challenge. The widespread use of wired and wireless communication networks, internet, web applications and computing has increased the gravity of the problem. Organizations are totally dependent on reliable, secure and fault-tolerant systems, communications, applications and information bases. Unfortunately, serious security and privacy breaches still occur every day, creating an absolute necessity to provide secure and safe information security systems through the use of firewalls, intrusion detection and prevention systems (ID/PSs), encryption, authentication and other hardware and software solutions. This paper aims to address these issues.

**Design/methodology/approach** – This survey presents an up-to-date comprehensive state of the art overview of ID/PSs based on risk analysis, a description of what ID/PSs are, the functions they serve, its two primary types and different methods of ID that may employ.

**Findings** – As security incidents are increasing and are more aggressive, ID/PSs have also become increasingly necessary, they compliment the arsenal of security measures, working in conjunction with other information security tools such as malware filters and firewalls. Because of a growing number of intrusion events and also because the internet and local networks together with user applications have become so ubiquitous, the need arises to use sophisticated advanced techniques from autonomic computing, machine learning, artificial intelligence and data mining to make intelligent/smart ID/PSs.

**Originality/value** – This paper perceives the requirements of developing a new detection mechanism to detect known and unknown threats, based on intelligent techniques such as machine learning and autonomic computing.

**Keywords** Information management, Data security, Risk management

**Paper type** Research paper

Information Management &
Computer Security
Vol. 18 No. 4, 2010
pp. 277-290
© Emerald Group Publishing Limited
0968-5227
DOI 10.1108/09685221011079199

## 1. Introduction

For several years now, society has been dependent on information technology (IT). With the rise of internet and e-commerce this is more applicable now than ever. People rely on computer networks to provide them with news, stock prices, e-mail and online shopping. People's credit card details, medical records and other personal information are stored on computer systems. Many companies have a web presence as an essential part of their business. The research community uses computer systems to undertake research and to disseminate findings. Computers control national infrastructure components such as the power grid. The integrity and availability of all these systems have to be protected against a number of threats. Amateur hackers, rival corporations, terrorists and even foreign governments have the motive and capability to carry out sophisticated attacks against computer systems. Therefore, the field of information and communication security has become vitally important to the safety and economic well being of society as a whole. Moreover, to expose privacy breaches, security needs powerful intrusion detection and prevention systems (ID/PSs).

This paper focuses on providing an up-to-date comprehensive state of the art of ID/PSs based on risk analysis. In Section 1.1, we present a background introduction to ID/PSs. In Section 2, we briefly outline the definition of risk management and its importance in developing well-managed security systems. In Section 3, we provide a brief overview of ID/PSs, including a description of what ID/PSs are, the functions they serve, the two primary types of detection and prevention systems and different methods of ID that may be employed. Finally, in Section 4, we present the main goal of this work when we discuss in detail, with examples of some threat incidents occurred during the years 2009 and 2010, the requirements driving the necessity of developing a new detection mechanism to detect known and unknown threats based on intelligent techniques such as machine learning and autonomic computing.

### *1.1 Background*

In order to understand the ID/PSs, first one must understand the nature of the event they attempt to detect. An intrusion is a type of attack on information assets in which the instigator attempts to gain entry into a system or disrupt the normal operations of a system. In Brown's *et al.* (2002) view, intrusions are actions that attempt to bypass security mechanisms of computer systems. They are any set of actions that threatens the integrity, availability or confidentiality of the information and the information system, where integrity means that data have not been altered or destroyed in an unauthorized manner and where confidentiality means that information is not made available or disclosed to unauthorized individuals, entities or processes. Availability means that a system that has the required data ensures that it is accessible and usable upon demand by an authorized system user. Occasionally, an intrusion is caused by an attacker accessing the system from the internet or the network, or from the operating system of the infected machine, or exploits any security flaw of third party (middleware) applications that manages the information system. Attacks that come from these external origins are called outsider attacks. Insider attacks, involve unauthorized internal users attempting to gain and misuse non-authorized access privileges.

ID is the process of monitoring computers or networks for unauthorized entry, activity or file modification. An intrusion detection system (IDS) is a software or hardware device that automates the ID process. IDSs can respond to suspicious events in one of several ways, which includes displaying an alert, logging the event or even paging an administrator. Intrusion prevention is the act of intercepting detected system threats in real time by preventing them from continuing to their intended destinations. It is useful against denial of services, floods and brute force attacks (Martin, 2009). An intrusion prevention system (IPS) is a software or hardware device that has all the capabilities of an IDS and can also attempt to stop possible incidents. An IPS can respond to a detected threat in several ways:

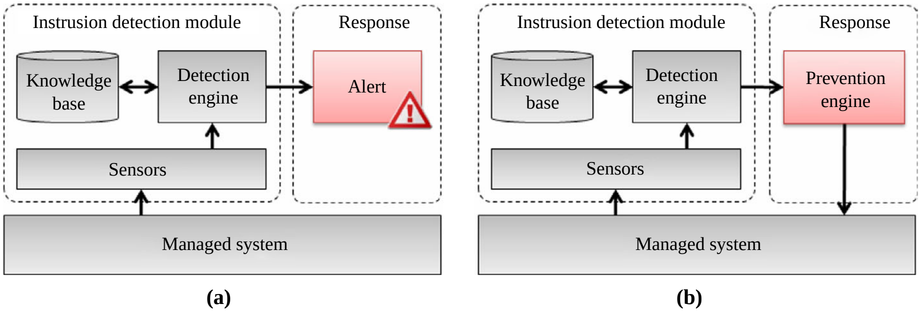
- it can reconfigure other security controls in systems such as a firewall or router to block future attacks;
- it can remove malicious content of an attack in network traffic to filter out the threatening packets; or
- it can (re-)configure other security and privacy controls in browser settings to prevent future attacks.

Usually, disable prevention features in IPS products cause them to function as IDSs. IPSs are considered to be an extension of IDSs, although IPS and IDS both examine network traffic searching for attacks, there are critical differences. IPS and IDS both detect malicious or unwanted traffic. They both do so as completely and accurately as possible, but they differ in the type of response provided by each. As shown in Figure 1, the main function of an IDS product is to warn of suspicious activity taking place while IPS is designed and developed for more active protection to improve upon the IDS and other traditional security solutions, which can react in real time to block or prevent those activities.

An effective risk management process is an important component of a successful IT security system. Organizations should use risk management techniques to identify the security controls necessary to mitigate risk to an acceptable level. To design an effective ID/PS, proper requirements capture based on risk management is essential.

## 2. Importance of risk management

It is expected that all computer and communication systems, including all the applications, system softwares and infrastructure and networking services, are protected from accidents and abuse by a set of safety measures composed from security, privacy, trust, audit, digital forensics and fault-tolerance functions, in order that they are to be available, reliable, trusted, safe, identifiable and auditable. Equally, these functions



**Notes:** (a) IDS; (b) IPS

**Figure 1.** Typical intrusion detection and intrusion prevention systems

must provide the necessary facilities to end-users, make them feel safe and trusted in the complex world of information communication technology driven by the web, the internet, mobile and *ad hoc* wireless networks where today everything from business to leisure has become e-everything. These safety measures are vital in economic terms (Patel, 2010).

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. It is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions (Chichakli, 2009). A strong security program reduces levels of threat to reputation, operational effectiveness, legal and strategic risk by limiting an organization's vulnerability to attempted intrusion, thereby maintaining confidence and trust in the institution. Security concerns can quickly erode customer confidence and potentially decrease the adoption rate and rate of return on investment for strategically important products or services. An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to achieve its mission, rather than simply its IT assets. Therefore, the risk management process should not be treated as merely a technical function carried out by the IT experts who operate and manage the IT system, but as an essential mission-critical management function of the organization.

Risk-based protection strategies are characterized by identifying, understanding, mitigating as appropriate and explicitly accepting the residual risks associated with the operation and use of information systems. To help protect organizations from the adverse effects of ongoing, serious and increasingly sophisticated threats to information systems, organizations should employ a risk-based protection strategy along with ID/PSs, as a complete system of protection to ensure the integrity, availability and confidentiality of the information and the information systems.

## 3. Intrusion detection and prevention systems

Whitman and Mattord (2005) defined ID as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies or standard security practices. An IDS is a device or software application that monitors network and/or information system for malicious activities or policy violations and responds to that suspicious activity by warning the system administrator by one of several ways, including displaying an alert, logging the event or even paging the administrator.

Intrusion prevention is the process of performing ID and attempting to stop detected possible incidents. The IPS is a device or software application that has all the capabilities of an IDS and can also attempt to stop possible incidents. IPS is designed and developed for more active protection to improve upon the IDS and other traditional security solutions. An IPS is definitely the next level of security technology with its capability to provide security at all system levels from the operating system kernel to network data packets (Martin, 2009). IPSs are designed to protect information systems from unauthorized access, damage or disruption, IDS informs of a potential attack, whereas, IPS makes attempts to stop it. IPS has another benefit or advantage over IDS in that it has the ability to prevent known intrusion detected signatures, besides the unknown attacks originating from the database of generic attack behaviors (Beal, 2005).

Modern ID/PSs are comprised two basically different approaches, network-based and host-based. A relatively recent addition of special IDS called application-based is a refinement of the host-based ID (Brown *et al.*, 2002). Both servers and workstations are protected by host-based intrusion detection/prevention systems (HID/PSs) through secure and controlled software communication channels between system's applications and operating system kernel. The software is preconfigured to determine the protection rules based on intrusion and attack signatures. The HID/PS will catch suspicious activity on the system and then, depending on the predefined rules, it will either block or allow the event to happen. HID/PS monitors activities such as application or data requests, network connection attempts and read or write attempts to name a few. One potential disadvantage with this approach is that, given the necessarily tight integration with the host operating system, future operating system upgrades could cause problems. Network-based intrusion detection/prevention system (NID/PS) is a software or dedicated hardware system that connects directly to a network segment and protects all of the systems attached to the same or downstream network segments. Network ID/PS devices are deployed in-line with the network segment being protected (Martin, 2009). All data that flows between the protected segment and the rest of the network must pass through the network ID/PS device. As the traffic passes through the device, it is inspected for the presence of an attack. When an attack is identified, the network ID/PS discards or blocks the offending data from passing through the system to the intended victim thus blocking the attack. NID/PS will intercept all network traffic and monitor it for suspicious activity and events, either blocking the requests or passing it along should it be deemed legitimate traffic. One interesting aspect of network intrusion prevention system is that if the system finds an offending packet of information, it can rewrite the packet so the hack attempt will fail, but it means the organization can mark this event to gather evidence against the would be intruder, without the intruder's knowledge. Regardless of whether they operate at the network, host or application level, all ID/PSs use one of two detection methods; signature-based or anomaly-based (Whitman and Mattord, 2005).

Anomaly detection is designed to uncover abnormal patterns that deviate from what is considered to be normal behavior, whereas ID/PS establishes a baseline of normal usage patterns and anything that widely deviates from it gets flagged as a possible intrusion. Anomaly detection can also vary but one should be aware that if any incident occurs more or less than two standard deviations from the statistical norm would raise an alarm. An example of this would be if a user logs on and off of a machine eight times a day instead of the normal one or two. Also, if a computer is used at 2:00 AM when normally no one outside of business hours should have access, this should raise some suspicions. At another level, anomaly detection can investigate user patterns, such as profiling the programs executed daily. Once again, if a user in an IT department suddenly starts to access accounting programs or recompiles them, then the system must immediately raise an alarm or alert its administrators (Innella and McMillan, 2001). The major benefit of anomaly based detection methods is that they can be very effective at detecting previously unknown threats (Scarfone and Mell, 2007). Usually, in the first stage of a deployment of an anomaly-based ID/PS, the system learns what a normal behavior is. The controlled system is running as usual under the assumption that there is no abnormal behavior. During the learning stage, no attack must occur in the controlled system so that the ID/PS does not learn to ignore the attacks. The learning process can be addressed by variety of means such as machine learning or building statistical behavioral profiles. In the second stage of the deployment, in which the system possibly faces attacks, the ID/PS monitors the activities in the controlled system and compares them to the learned normal behavioral patterns. If a mismatch occurs, a level of "suspicion" is raised and when the suspicion, in turn, trespasses a given threshold, the system triggers an alarm. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may not be able to describe what an attack is and may have high false positive rate.

Unauthorized behavior is normally detected by their misuse and is also commonly referred as signature detection. However, this method uses known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures. For host-based intrusion detection/prevention, one example of a signature is "three failed logins." For network intrusion detection/prevention, a signature can be as simple as a specific pattern that matches a portion of a network packet (Whitman and Mattord, 2005). For instance, packet content signatures and/or header content signatures can indicate unauthorized actions. The occurrence of a signature might not signify an actual attempted unauthorized access (for example, it can be an honest mistake), but it is a good idea to take each alert seriously. Depending on the robustness and seriousness of a signature that is triggered, some alarm, response or notification should be sent to the proper authorities. The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. This means that these systems are not unlike virus detection systems, they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior. Misuse detection systems try to recognize known "bad" behavior. The main issues in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity (Newman *et al.*, 2004). The main advantage of misuse detection paradigm is that it can accurately and efficiently detect instances of known attacks. The main disadvantage of misuse detection method is that it lacks the ability to detect the newly invented attacks. Signature databases must be constantly updated, and IDSs must be able to compare and match activities against large collections of attack signatures.

## 4. Why be serious about intrusion?

Every organization using information systems must take information security seriously. The fact that information security is a discipline that relies on experts in addition to technical controls to improve the protection of an organization's information assets cannot be overemphasized. Most organizations solely implement perimeter-based security solutions, even though the greatest threats are from internal sources. Additionally, companies implement network-based security solutions that are designed to protect network resources, despite the fact that the information is more often the target of the attack. ID/PSs can supplement protection of network and information systems by rejecting the future access of detected attacks and by providing useful hints on how to strengthen the defense. Cryptographic methods have their own problems. Passwords can be cracked, users can lose their passwords and entire crypto-systems can be broken. Even a truly secure system is vulnerable to abuse by insiders who abuse their privileges. In order to understand the needs for new advanced ID/PSs, a deeper look into the reported data breaches should be examined. According to Kouns *et al.* (2009), the total number of incidents occurred during the last year were about 436, which affected about 218,756,349 records from different organizations and companies. In this paper, we list in Table I some of these incidents that occurred during the year 2009.

A summary of these incidents during 2009 are as follows:

- From Table I (1), in January, an employee in the human resource department of the Library of Congress was charged with conspiring to commit wire fraud in which he stole information on at least ten employees from library databases. He passed the information to a relative, who used it to open the accounts. Together, the two are alleged to have bought $38,000 worth of goods through these accounts (Jackson, 2009). In the same month, also CheckFree Corp (Adams, 2009) and some of the banks that use its electronic bill payment service reported of security breach when criminals took control of several of the company's internet domains and redirected customer traffic to a malicious web site hosted in Ukraine. The breach affected about 160,000 of the bank consumers who were exposed to the Ukrainian attack site.
- Table I (2), in February, law enforcement agency seized a computer file with Kaiser Permanente data from a person who was subsequently arrested. The suspect was not a Kaiser employee. Kaiser Permanente notified nearly 30,000 Northern California employees about the security breach that may have led to the release of their personal information. The stolen information included names, addresses, dates of birth and social security numbers for Kaiser employees (Cluley, 2009). In February also, an unidentified hacker gained access to databases used by the usa.kaspersky.com web site, allowing access to users' accounts, activation codes and possibly personal data about Kaspersky customers (MacRonin, 2009). In February also, four-hundred databases were tapped by hackers from University of Alabama. Personal information may have been stolen. One of those computers contained lab results for people tested at the campus medical center. The servers had a database containing 37,000 records of lab data. They contained the names, addresses, birthdates and social security numbers of each person who had lab tests, such as a blood or urine test, done on the University of Alabama campus since 1994 (Harper, 2009).
- Table I (3), in March, Symantec had issued warnings to a small number of customers that their credit card numbers may have been stolen from an Indian call center used by the security vendor. Symantec sent out warning letters to just over 200 customers. Most of those notified were in the USA, but the company also notified a handful of customers in the UK and Canada (McMillan, 2009). Also in March, Sprint warned several thousand customers that a former employee sold or otherwise provided their account data without permission. The information that may have been compromised included names, addresses, phone numbers,

**Table I.**
Some of the data breaches that occurred during the year 2009

| No. | Date (2009) | Attack target (location) | Breach method | Cost | No. of victims |
|---|---|---|---|---|---|
| 1 | January | Library of Congress (Washington, District of Columbia) | Employee theft | $38,000 | 10 |
| | | CheckFree Corp. (Atlanta, Georgia) | Hacked web server | Unknown | 5,000,000 |
| 2 | February | Kaiser Permanente (Oakland, California) | Stolen records | Unknown | 30,000 |
| | | Kaspersky.com (web site) | Hacked database | Unknown | Unknown |
| | | University of Alabama (Tuscaloosa, Alabama) | Hacked database | Unknown | 37,000 |
| 3 | March | Google.com | Hacked web server | Unknown | < 0.05% of docs |
| | | Symantec.com | Hacked web server | Unknown | 200 |
| | | Sprint (Overland Park, Kansas) | Stolen records | Unknown | Thousand |
| 4 | April | New York State Tax Department | Employee theft | $200,000 | Thousands |
| | | Federal Reserve Bank of New York | Employee theft | $73,000 | Thousands |
| 5 | July | AT&T (Chicago, Illinois) | Employee theft | $70,000 | 2,100 |
| | | Network Solutions (Herndon, Virginia) | Hacked web server | Unknown | 573,000 |
| 6 | August | University of Massachusetts | Hacked server | Unknown | Thousands |
| 7 | September | Downeast Energy & Building Supply | Hacked server | $200,000 | 850 |
| | | UNC Chapel Hill (Chapel Hill, North Carolina) | Hacked server | Unknown | 236,000 |
| 8 | October | US Army Special Forces | Hacked server | Unknown | 463 |
| | | PayChoice.com | Hacked web server | Unknown | Unknown |
| | | New York Mellon Corp. | Employee theft | $1.1 million | 150 |
| 9 | November | Hancock Fabrics (Baldwyn, Missouri) | Stolen records | Unknown | More than 70 |
| 10 | December | University of Nebraska (Omaha, Nebraska) | Hacked database | Unknown | 1,400 |
| | | Pennsylvania State University (University Park, Pennsylvania) | Malware attack | Unknown | 30,000 |

sprint account numbers and the name of the authorized point of contact on their accounts (Messmer, 2009).

- Table I (4), in April, a former New York state tax department worker was accused of stealing the identities of thousands of taxpayers and running up more than $200,000 in fraudulent charges. The former employee gathered credit cards, brokerage accounts and social security numbers that he used to open more than 90 credit card accounts and lines of credit (Virtanen, 2009). Also in April, a former employee at the Federal Reserve Bank of New York and his brother were arrested on suspicion of obtaining loans using stolen identities. The former employee previously worked as an IT analyst at the bank and had access to sensitive employee information, including names, birthdates, social security numbers and photographs. A thumb drive attached to his computer had applications for $73,000 in student loans using two stolen identities. They also found a fake driver's license with the photo of a bank employee who was not the person identified in the license (Annese, 2009).
- Table I (5), in July, a temporary employee for AT&T was arrested on charges. She stole the personal information of 2,100 co-workers and then pocketed more than $70,000 by taking out short-term payday loans in the names of 130 of them (Coen, 2009). Also in July, hackers broke into the web servers owned by domain registrar and hosting provider Network Solutions LLC, by planting malicious code that resulted in the compromise of more than 573,000 debit and credit card accounts (Krebs, 2009a, b, c).
- Table I (6), in August, hackers broke into a computer server of University of Massachusetts and obtained the social security numbers and credit card information pertaining to graduates who attended the university between 1982 and 2002 (Dayal, 2009) and defrauded them.
- Table I (7), in September, attackers planted keystroke logging malware on Downeast Energy & Building Supply's computer systems and stole the credentials, which the company uses to manage its bank accounts online. Subsequently the hackers broke into the system and stolen by transferring more than $200,000 from the company's online bank account (Krebs, 2009a, b, c). Also in September, a hacker infiltrated a computer server housing the personal data of 236,000 women enrolled in a UNC Chapel Hill research study. Among the information exposed was the social security numbers of 163,000 participants. The data is part of the Carolina Mammography Registry, a 14-year-old project that compiles and analyzes mammography data submitted by radiologists across North Carolina (Ferreri, 2009).
- Table I (8), in October, a security breach involved a US Army Special Forces document containing the names, social security numbers, home phone numbers and home addresses of 463 soldiers. The document also contained names and ages of soldiers' spouses and children (Moscaritolo, 2009). Also in October, hackers broke into the company's servers and stole customer user names and passwords. The attackers then included that information in e-mails to PayChoice's customers warning them that they needed to download a web browser plug-in in order to maintain uninterrupted access to onlineemployer.com. The plug-in was instead a malicious software designed to steal the victim's user names and passwords

(Krebs, 2009a, b, c). A computer technician in New York Mellon Corp. was charged with allegedly stealing the identities of more than 150 Bank of New York Mellon Corp. employees and using their identities to steal more than $1.1 million from charities, non-profit groups and others (Bray, 2009).

- Table I (9), in November, Hancock Fabrics Bank customers in California, Wisconsin and Missouri reported fraudulent ATM withdrawals that were tied to transactions conducted with the Hancock Fabrics retail chain. A total of 70 victims informed the bank of suspicious ATM withdrawals from their accounts (McGlasson, 2009).
- Table I (10), in December, a computer in the College of Education and Human Sciences at the Lincoln campus was breached and the names, addresses and social security numbers of 1,400 Hinsdale High School District 86 graduates stolen. The university's investigation revealed the computer had not been adequately secured, allowing unauthorized external access to the computer and its information (Bosch, 2009). Also in December, Pennsylvania State University sent out letters notifying those graduates potentially affected by malware infections that were believed to be responsible for fraudulent and misuse of their information. The colleges and extent of the records involved in the malicious software attacks included Eberly College of Science, 7,758 records; the College of Health and Human Development, 6,827 records; and one of the Pennsylvania State's colleges outside of the University Park campus, approximately 15,000 records (Schackne, 2009).

For the year 2010 (to-date), in January 2010, users of the do-it-yourself trading site collective2.com received an urgent e-mail notifying them that the company's computer database had been breached by a hacker and that all users should log into change their passwords immediately. That e-mail stated that the information accessed by the hacker included names, e-mail addresses, passwords and credit card information (Janowski, 2010). Also in January, Suffolk County National Bank in New York stated that hackers have stolen the login credentials for more than 8,300 customers of small New York banks after breaching its security and accessing a server that hosted its online banking system (Goodin, 2010). In February 2010, a hacker attack at payroll processing firm Ceridian Corp. of Bloomington had potentially revealed the names, social security numbers, and, in some cases, the birth dates and bank accounts of 27,000 employees working at 1,900 companies nationwide (Alexander, 2010).

Over the last ten years, statistical investigations show that as technology and communications advance and become more complicated, security incidents become more numerous as summarized in Table II and showed in Figure 2 (Kouns *et al.*, 2009). It also shows that the impact of incidents increased and became more affective and aggressive than before as shown in Figure 3, which encourages many organizations to take a more holistic view of security and focus on the overall health of their information security programs.

In the last five years, the networking revolution has finally come of age as mentioned previously. More than ever before, we see that web access, mobile working and the use of the internet for communications is changing computing as we know it today. The possibilities and opportunities are limitless for the creation and delivery of new services through the use of these technologies. Unfortunately, so too are the risks and

| Year | No. of incidents | No. of records affected |
|---|---|---|
| 2000 | 8 | 374,075 |
| 2001 | 17 | 199,674 |
| 2002 | 5 | 64,998 |
| 2003 | 14 | 7,055,450 |
| 2004 | 24 | 32,317,590 |
| 2005 | 140 | 55,988,256 |
| 2006 | 533 | 51,144,506 |
| 2007 | 489 | 165,192,571 |
| 2008 | 717 | 86,311,058 |
| 2009 | 436 | 218,756,349 |

**Table II.** Total number of incidents and affected records during the last ten years

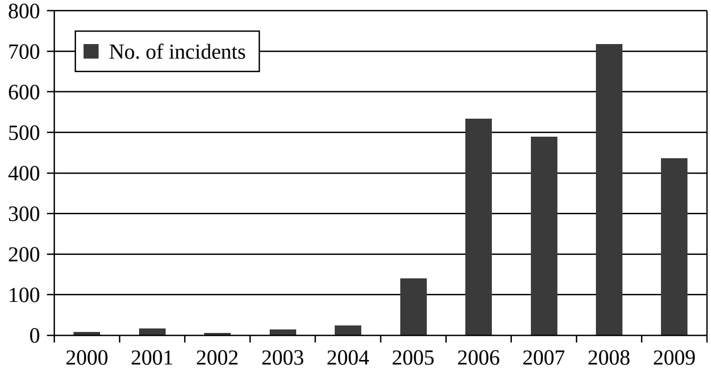


**Figure 2.** Number of incidents during the last ten years

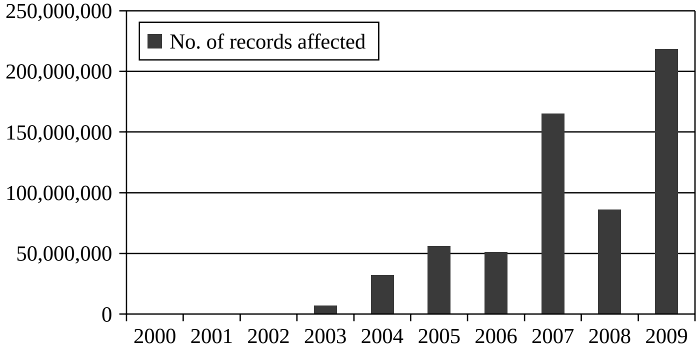


**Figure 3.** Number of affected records during the last ten years

dangers of malicious intrusions, security breaches and privacy violations. IDSs have previously been simple, basic and traditional, with hardly any prevention mechanisms.

Together with the usage, growth of the information and communication systems and the enormous increase in the number of the threats have become more effective, affective, and more aggressive than ever before as shown in Table II. Their growth cannot be simply handled by just observing huge quantities of similar or dissimilar alarms running into reams of paper or flying across the screens of the observer. The traditional information security systems with old computing environments and programming methods have difficulty in successfully identifying new intruders, breaches and violations, and require a significant amount of storage space and computational power to create robust real-time ID/PSs. From all of the above-mentioned incidents and threats that occurred in the last few years, it is clear that organizations need advanced intelligent information security systems like ID/PS that can detect newly created unknown attacks to prevent data loss and maintain data privacy with immediate response. These systems will evolve through the use of intelligent programming techniques together with knowledge-based systems and technologies that can reduce the human effort required to build these smart systems and can improve their performance.

## 5. Conclusion and future recommendations

Today's interrelated computer network is a dangerous realm, filled with people that have millions of man-hours available to employ against the strongest of security strategies. The only way to beat them is to know when they are attempting an attack and counter their attempts. Strategy is the key and selecting the right ID or prevention system will be instrumental in ensuring that an enterprise's networks and systems remain secure. As security incidents become more numerous, ID/PS and supporting tools are becoming increasingly necessary. These intelligent ID/PSs and tools should use a combination of several intelligent techniques from the subject areas of autonomic computing, machine learning, artificial intelligence and data mining to assist them to determine what qualifies as an intrusion, versus normal activity, by building a knowledge base which grows as and when new facts or knowledge come to light.

ID/PSs are still a fledgling field of research. However, it is beginning to assume enormous importance in today's computing environment. The combination of facts such as the unbridled growth of the internet, the vast financial possibilities opening up in electronic trade and the lack of truly secure systems make it an important and pertinent field of research and development.

Future research and development trends seem to be converging towards a model that is based on multi-agent ID/PSs based on and managed by autonomic computing paradigm together with advanced techniques from natural language processing, artificial intelligence and data mining to help improve anomaly ID, based on its self-managed properties such as self-configuration, self-optimization, self-healing and self-protection. These autonomic computing properties have to be extended to include self-detection and self-prevention. The results from these techniques will aid an analyst to clearly distinguish malicious attack activities from normal everyday non-attack activities. They will make ID/PSs smart and a formidable part of security management system with a rich but simplified alarm handling and presentation of security violation activities for easy human consumption.

## References

Adams, J. (2009), "CheckFree's hack attack has a long tail", available at: www.americanbanker.com/btn_issues/22_1/-370036-1.html (accessed 7 November 2009).

Alexander, S. (2010), "Hacker attacks Ceridian; data from 27,000 at risk", *Star Tribune*, available at: www.startribune.com/business/83505102.html (accessed 28 February 2010).

Annese, J. (2009), "Former Federal Reserve Bank employee from Elm Park admits fraud", available at: www.silive.com/news/advance/index.ssf?/base/news/1254915027102700.xml&coll=1 (accessed 12 November 2009).

Beal, V. (2005), "Intrusion detection (IDS) and prevention (IPS) systems", available at: www.webopedia.com/DidYouKnow/Computer_Science/2005/intrusion_detection_prevention.asp (accessed 16 October 2009).

Bosch, S.I. (2009), "Security breach compromises information on 1,400 district 86 grads", available at: http://securityheadhunter.wordpress.com/2009/12/07/security-breach-compromises-information/ (accessed 23 December 2009).

Bray, C. (2009), "Computer technician charged in identity theft (Bank of New York Mellon)", available at: www.advfn.com/news_UPDATE-Computer-Technician-Charged-In-Identity-Theft_40104352.html (accessed 12 November 2009).

Brown, D.J., Suckow, B. and Wang, T. (2002), *A Survey of Intrusion Detection Systems*, University of California, California, CA, available at: cseweb.ucsd.edu/classes/fa01/cse221/projects/group10.pdf

Chichakli, R. (2009), "Information systems risk management", available at: www.iscpa.com/Risk_Management.htm (accessed 16 October 2009).

Cluley, G. (2009), "30,000 Kaiser Permanente workers warned of identity theft risk", available at: www.sophos.com/blogs/gc/g/2009/02/11/30000-kaiser-permanente-workers-warned-identity-theft-risk/ (accessed 7 November 2009).

Coen, J. (2009), "AT&T temp charged with stealing worker info", available at: www.chicagobreakingnews.com/2009/07/att-temp-charged-with-stealing-co-worker-info.html (accessed 12 November 2009).

Dayal, P. (2009), "Hackers gained access to UMass info", available at: www.telegram.com/article/20090821/NEWS/908210393/1116 (accessed 12 November 2009).

Ferreri, E. (2009), "Hacker breaks into research study data", available at: www.charlotteobserver.com/2009/09/25/967722/hacker-breaks-into-research-study.html (accessed 12 November 2009).

Goodin, D. (2010), "Hackers pluck 8,300 customer logins from bank server", available at: www.theregister.co.uk/2010/01/12/bank_server_breached/ (accessed 22 February 2010).

Harper, I. (2009), "Hacker taps into University of Alabama computer system; lab records exposed", available at: www.abc3340.com/news/stories/0209/594921.html (accessed 7 November 2009).

Innella, P. and McMillan, O. (2001), "An introduction to intrusion detection systems", available at: www.symantec.com/connect/articles/introduction-ids (accessed 16 October 2009).

Jackson, W. (2009), "Continued exposure of data through inside threats shows need for improved security", available at: fcw.com/sitecore/content/Home/GIG/gcn/Articles/2009/01/05/Lock-down-that-data.aspx (accessed 7 November 2009).

Janowski, D.D. (2010), "Security breach reported by internet trading site collective2.com", available at: www.investmentnews.com/article/20091230/FREE/912309990 (accessed 22 February 2010).

Kouns, J., Martin, B., Shettler, D. and Todd, K. (2009), "Data loss database", available at: datalossdb.org/ (accessed 27 December 2009).

Krebs, B. (2009a), "Data breach highlights role of money mules", available at: voices.washingtonpost.com/securityfix/2009/09/money_mules_carry_loot_for_org.html?wprss=securityfix (accessed 12 November 2009).

Krebs, B. (2009b), "Network solutions hack compromises 573,000 credit, debit accounts", available at: voices.washingtonpost.com/securityfix/2009/07/network_solutions_hack_comprom.html?hpid=topnews (accessed 12 November 2009).

Krebs, B. (2009c), "PayChoice suffers another data breach", available at: voices.washingtonpost.com/securityfix/2009/10/paychoice_suffers_another_data.html (accessed 12 November 2009).

McGlasson, L. (2009), "Hancock Fabrics linked to fraud in 3 states", available at: www.bankinfosecurity.com/articles.php?art_id=1961 (accessed 23 December 2009).

McMillan, R. (2009), "Symantec warns customers of call center theft", available at: www.csoonline.com/article/487372/Symantec_Warns_Customers_of_Call_Center_Theft (accessed 9 November 2009).

MacRonin, P. (2009), "Kaspersky database exposed", available at: www.privacydigest.com/2009/02/09/kaspersky%20database%20exposed (accessed 7 November 2009).

Martin, C. (2009), "What is IPS and how intrusion prevention system works", available at: www.aboutonlinetips.com/what-is-ips-and-how-intrusion-prevention-system-works/ (accessed 10 October 2009).

Messmer, E. (2009), "Data breach costs top $200 per customer record", available at: www.networkworld.com/news//012510-data-breach-costs.html (accessed 9 November 2009).

Moscaritolo, A. (2009), "Army special forces document leaked on P2P network", available at: www.scmagazineus.com/Army-Special-Forces-document-leaked-on-P2P-network/article/151309/ (accessed 15 November 2009).

Newman, D., Manalo, K.M. and Tittel, E. (2004), "Intrusion detection overview", available at: www.informit.com/articles/article.aspx?p=174342 (9 October 2009).

Patel, A. (2010), "Concept of mobile agent-based electronic marketplace – safety measure", in I. Lee (IGI Global Publications) (Ed.), *Encyclopedia of E-Business Development and Management in the Digital Economy*, Vol. 1, Business Science Reference, pp. 252-64 (release date: February 2010).

Scarfone, K. and Mell, P. (2007), "Guide to intrusion detection and prevention systems (IDPS)", *Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology, Maryland.

Schackne, B. (2009), "Records of 30,000 at Penn State hacked", available at: www.post-gazette.com/pg/09363/1024361-100.stm (accessed 16 February 2010).

Virtanen, M. (2009), "NY tax worker accused of stealing taxpayers'", *IDs. ABC News*, available at: abcnews.go.com/US/wireStory?id=7402108 (accessed 12 November 2009).

Whitman, M.E. and Mattord, H.J. (2005), *Principles of Information Security*, Thomson Course Technology, Boston, MA.

**Corresponding author**
Ahmed Patel can be contacted at: whinchat2010@gmail.com

**This article has been cited by:**

1. Sunil Kumar, Kamlesh Dutta. 2016. Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges. *Security and Communication Networks* . [CrossRef]
2. Rup Kumar Deka, Kausthav Pratim Kalita, D.K. Bhattacharya, Jugal K. Kalita. 2015. Network defense: Approaches, methods and techniques. *Journal of Network and Computer Applications* **57**, 71-84. [CrossRef]
3. Mohammed Ennahbaoui, Hind Idrissi, Said El HajjiSecure and flexible grid computing based intrusion detection system using mobile agents and cryptographic traces 314-319. [CrossRef]
4. Alfredo Cuzzocrea, Gianluigi Folino, Pietro SabatinoA distributed framework for supporting adaptive ensemble-based intrusion detection 1910-1916. [CrossRef]
5. Rodrigo Sanches Miani, Bruno Bogaz Zarpelao, Bertrand Sobesto, Michel CukierA Practical Experience on Evaluating Intrusion Prevention System Event Data as Indicators of Security Issues 296-305. [CrossRef]
6. Kai S. KoongDepartment of Computer Information Systems and Quantitative Methods, University of Texas Pan American, Edinburg, Texas, USA Mohammad I. MerhiDepartment of Computer Information Systems and Quantitative Methods, University of Texas Pan American, Edinburg, Texas, USA Jun SunDepartment of Computer Information Systems and Quantitative Methods, University of Texas Pan American, Edinburg, Texas, USA. 2013. Push and pull effects of homeland information security incentives. *Information Management & Computer Security* **21**:3, 155-176. [Abstract] [Full Text] [PDF]
7. S. Laniepce, M. Lacoste, M. Kassi-Lahlou, F. Bignon, K. Lazri, A. WaillyEngineering Intrusion Prevention Services for IaaS Clouds: The Way of the Hypervisor 25-36. [CrossRef]
8. Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, Joaquim Celestino Júnior. 2013. An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications* **36**:1, 25-41. [CrossRef]
9. Wei Wang, Huiran Wang, Beizhan Wang, Yaping Wang, Jiajun Wang. 2013. Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks. *Information Sciences* **220**, 580-602. [CrossRef]
10. Karen A. Garcia, Raúl Monroy, Luis A. Trejo, Carlos Mex-Perera, Eduardo Aguirre. 2012. Analyzing Log Files for Postmortem Intrusion Detection. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* **42**:6, 1690-1704. [CrossRef]
11. F M Sibai, D A MenasceDefeating the insider threat via autonomic network capabilities 1-10. [CrossRef]
12. Usman Asghar Sandhu, Sajjad Haider, Salman Naseer, Obaid Ullah Ateeb. 2011. A Study of the Novel Approaches Used in Intrusion Detection and Prevention Systems. *International Journal of Information and Education Technology* 426-431. [CrossRef]