International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(3): 18-26
The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)

# An Authentication Middleware for Prevention of Information Theft

S. Kami Makki, Md. Sadekur Rahman
Lamar University, Computer Science Department
{kami.makki, md.sadekur.rahman}@lamar.edu

## ABSTRACT

Information theft or data leakage is a growing concern for companies, as well as, individual users. Intruders can easily copy a huge amount of confidential data using hand-held devices such as USB flash drives, iPods, digital cameras or any other external storage devices. Data theft can simply occur through both insiders and outsiders of a corporation. It is becoming the biggest challenge for companies, since the storage devices are becoming smaller in size, easier to use, have higher capacity and data transmission speed. Furthermore, these devices can easily be misplaced or stolen and sensitive data can easily be exposed. In this paper we present a multilevel password verification system for prevention of information theft by removable devices to protect data leakage by various portable devices. Our proposed system consists of three main modules: 1) portable storage device monitoring, 2) activity logging and data encryption, and 3) device authorization. These modules cooperate with each other to provide required security, and prevent information theft from the individual users and companies.

## KEYWORDS

Data Privacy, Decryption, Encryption, Portable device, Security

## 1 INTRODUCTION

Data theft has become an immediate and important threat with the rapid advancement of portable storage technology. The inside information theft and data leakage have become as challenging as outside data thefts for corporate offices. Although attacks from outside the companies are real and significant, substantial data loss may result from internal activities which can threaten corporate reputation and customers' confidence [2, 3]. The act of stealing corporate and personal data by an insider is now a simple, non-technical and inconspicuous task due to the advancement of storage technology. For example, an office worker can plug-in a 128 GB flash memory into a workstation, and copies massive amount of data on the device swiftly with little efforts [13, 19].

To maintain a rigid protection against data theft and information leakage in a corporate or personal environment, employees or users' behaviors must be handled with a higher degree of care. Therefore, there is a need to identify the boundaries of data theft in different environments. Some research papers defined data theft as an unauthorized copying or destruction (removal) of data [4]. Other researchers defined it as stealing 'computerize information' from a person or organization [7]. In a deeper sense, copying any kind of data using external devices such as portable storage devices, iPods, or digital cameras by people other than the authentic user can be defined as data theft [5, 9]. From the viewpoint of confidentiality, data can be ranked as follows:

- Classified, restricted or personal information.
- Credit card and other financial information.
- Financial data, merger and acquisition plans.
- Scripts, storyboards, print material, photographic, video or animated film (software source code or database schema).
- Blueprints and Engineering plans.
- Customer records.
- Score sheets, lyrics, sound files and other forms of phonographic material.
- Proprietary product blueprints.

Loss of data undermines company's brand. It can cause enormous financial adversity and even jeopardizes the company's competitive edge. Also, for an individual, the loss of confidential data can cause hardships both physically and financially.

In this paper, we propose and develop a multilevel password verification system for prevention of information theft (AMPIT). Our proposed system also focuses on using less system resources, as well as, increasing adoptability with new requirements without affecting existing functionality (flexibility) of devices for data owners. The remainder of this paper is organized as follows: Section 2 reviews the research in data protection and security, and discusses the consequences of data theft or information leakage. Section 3 presents our proposed system and covers the overall system design, including discussion of different components, resource management, threat model and threat listing. Section 4 presents the implementation of our system which can enhance data storage security. Section 5 presents conclusion and remarks regarding corporate and personal data security.

## 2 DATA THEFT

With the advancement of Smartphones technologies and ever increasing ubiquitous access and advances of storage technologies, the corporate and personal data are becoming more vulnerable. The usage of portable devices like iPods, USB sticks, PDAs is becoming commonplace in our society. Also, businesses are embracing new technologies and integrating with World Wide Web to increase productivity. Therefore, corporate data are becoming more mobilized and distributed leading to increasing security risk for enterprises. Therefore, it is important to evaluate the security risks related to all in use applications and resources (e.g. portable devices, network resources). The threats that data portability and network connectivity present often are not fully realized. Therefore, the outside and inside data thefts have been considered as the biggest threat for corporate offices. The attack from the outside of a company is real and can cause work disruption and loss of sensitive data. Also, considerable crucial data can get lost by insiders. This can immensely threaten the data security of the companies [4]. According to CSI, 44% of reported incidents were done by insiders, where 9% was due to loss of propriety information from mobile or other portable storage devices [15]. In 2008, Cisco system and InsightExpress have conducted a survey [3] from more than two thousands employees and information technology professionals from 10 different countries. According to this survey, around a third of the respondents were concerned about data being lost or stolen via portable devices, or were concerned about the threat from their co-workers. To address the security threats by insiders, system administrators must be vigilant and identify factors causing these threats. Also, to better understand the insiders' threats, the system administrators can categorize employees of an organization and put in place comprehensive security policies to eliminate insiders' threats. For example, the employees that present threat to the company can be categorized as "negligent" or "disgruntled" employees. These types of employees will compromise the company's data through unintentional or unwise behaviors [4]. Also, other types of employees' behaviors can put corporate data at serious risk. These behaviors are unauthorized application use (it may be spyware), misuse of corporate computers, unauthorized physical and network access and misuse of passwords and login or logout procedure.

To maintain a rigid protection against data theft in a corporate or personal environment, employee or user behavior must be handled with a highest degree of care. Data theft can be categorized as: Hacking, Rootkit or backdoor, Thumbsucking (copying confidential data using thumb devices), Posing (aggregation of users' information from cookies), Podslurping (data stealing using iPods), Bluesnarfing (stealing data using Bluetooth devices), and Spyware (gathers personal or system specific information without user notification and

sends to spyware creators) [1, 6, 12, 18]. In the last few years, data storage technology has advanced and increased device portability. There are mainly three important types of portable storage devices, such as flash drives, external hard drives, and travel drives. The latter is a compromise between the flash drives and external hard drives.

To provide a secure environment, implementation of both hardware and software solutions are necessary. Data leakage can be decreased by selection of a proper solution without compromising the overall system performance. An effective data leakage prevention mechanism should have at least the following properties [20]:

- Methodologies: Should clearly define data usage and data loss reporting policy. Adopt suitable policies to deal with data access and authentication process, and should maintain incident remediation workflow management.
- Detection: Should identify data sensitivity, and adopt an efficient mechanism for data cleanup. It also includes storing of sensitive data.
- Monitoring: Should scrutinize data confidentiality and monitor data in the moving state (when data is routing in communication media) to prevent any violation of policies. It should also monitor endpoints for guarding against copying of data.
- Protection: Should provide facility for encryption and quarantine of sensitive data. Also, should restrict moving and copying of data.

The following sections describe software and hardware solutions that can restrain data theft.

### 2.1 Software Solution

A number of companies have invested a lot of effort and money in developing a secure tool for protecting data theft through portable storage devices, such as M-File-Anti-Copy, Copy Protect, USB Secure, USB lock-RP, MyUSBOnly, ID-device lock, Gilisoft USB stick encryption, USB PC lock, USB Lock standard Endpoint, USB security, and Secure Lockware [8, 10, 14, 15, 16, 17, 18]. Each of these software solutions has its own advantages and disadvantages.

### 2.2 Hardware Solution

There are few devices to prevent physical access to USB ports, such as USB security Lock, USB port blocker, Matrix Dongle for USB-ports, Kensington USB port lock, NZXT bunker USB locking device [11, 15]. By using these devices computer owners can prevent users from connecting devices such as USB memories, MP3 players, or other portable devices to their computers. However, these types of devices are not widely accepted or used in corporations due to lack of flexibility and modularity. Furthermore, it is not feasible to buy many of these devices to lock all the USB ports of a corporate network. On the other hand, these devices can provide some reasonable solutions for the home users despite of their existing limitations.

## 3 SYSTEM DESIGN

This section presents the overall system architecture, different components and their interactions, functional design, system management and possible sources of threat and threat model.

### 3.1 System Overview

The goal of our proposed system is to provide a highly secure and flexible middleware to prevent data theft. To meet the goal, the following guiding principles have been considered:

- Flexibility: The ability of a system to adapt to new requirements without affecting its existing functionalities. To achieve this goal, the AMPIT system uses modular architecture to separate its functionalities from program complexity. Furthermore, a variety of user friendly interfaces have been designed to improve the AMPIT adaptability.

- Scalability: The system should have capacity to scale with varying number of clients or users. Our system is highly scalable because it has the ability to protect any number of portable storage devices under any circumstances.
- Security: The AMPIT system has implemented the following facilities to ensure higher level of security: 1) validation of user credibility; 2) data encryption for the authorized devices; 3) logging of suspicious activities.

Figure 1 shows the basic architecture of the AMPIT system. The main components of this system are: Device monitoring (DM); Credibility checking (CC); Silent activity logging (SAL); Advance alert system (AAS); Data encryption (DE). Each of these components is responsible for different unique set of tasks to prevent information theft effectively.

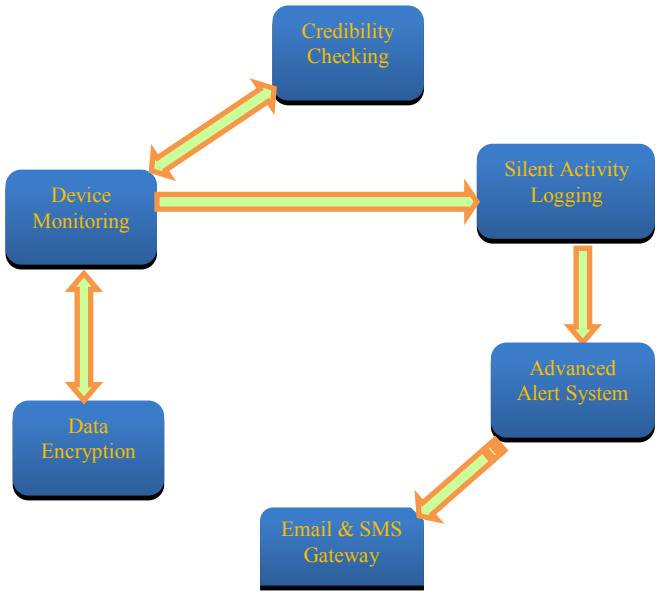


Figure 1: Basic Architecture of AMPIT System

### 3.1.1 Device Monitoring (DM)

The Device monitoring (DM) component monitors all kind of operations to all portable storage devices, which are plugged-in to the system. It communicates with the Credibility checking (CC) component after sensing any file system changes in the predefined locations. The DM component also interacts with the Silent activity logging (SAL) component after receiving a negative response from the CC component. However, the DM component can stop monitoring a connected device and considers it as trusted, once it receives a positive signal from the Credibility checking (CC) component.

### 3.1.2 Credibility Checking (CC)

The Credibility checking (CC) component is responsible for users' credibility verification. It provides a user interface to authorize a device, and it is the only legal entry point to the system. The CC component also maintains a bidirectional communication path with DM component to provide positive or negative signals.

### 3.1.3 Silent Activity Logging (SAL)

The Silent activity logging (SAL) component silently monitors all activities when it receives a signal from the Device monitoring (DM) component. To maintain a higher degree of protection it also interacts with the Advanced alert system (AAS) component. It has "snap-shot saving" facility to trace the possible intruders.

### 3.1.4 Advanced Alert System (AAS)

The Advanced alert system (AAS) component cooperates with the Silent activity logging (SAL) component to provide advance security and it has the following responsibilities:

- Emailing summary of suspicious activities to proper authority.
- Sending SMSs to proper authority.
- Locking the system completely, when an intruder performs too many suspicious activities.

### 3.1.5 Data Encryption (DE)

The Data encryption (DE) component maintains a bidirectional communication with the device

monitor (DM) component. It performs data encryption to an authorized device. In this way, DE component protects all sensitive data of a stolen or lost device. It uses Rijndeal algorithm to perform file encryption.

### 3.2 Functional Design

Functional design is a process which describes whether a system performs correctly under any circumstances, and it ensures user requirements. It precisely shows how to handle different errors and make sure the system works properly on their presence. In the following sections we will cover: how different components can co-ordinate with each other under the presence of erroneous information, and how to tackle information flow from different sources.

#### 3.2.1 Information Flow

To accomplish a task efficiently, the components of a system has to communicate with each other. All the components that we have described in Section 3.1 coordinate with each other through a message or information passing mechanism. Also, different components may generate different messages under various circumstances. These messages can be classified in the AMPIT system as: Events, User inputs, Emails, SMSs and Log messages.

#### 3.2.2 System Management

This section explains how different resources and components are managed in our proposed system; and how these components can co-operate with each other to make proper usage of the resources.

##### 3.2.2.1 Component Management

Component management is a process which defines the life cycle of each component for a system. Based on a component's life time we can categorize the components of AMPIT system as follows: Transient, Long-lived, and Eternal.

The Transient components will exist for a very short period of time. They can be activated by any event generated from other components, and die after performing a specific job. For example, when the Device monitoring (DM) component detects an operation in portable storage device, it instantaneously sends a signal to the credibility check (CC) component. The Credibility checking (CC) component activates itself to perform a specific task after receiving a signal from the Device monitoring (DM) component and terminates itself after finishing the job.

On the other hand, the Long-lived components are needed to be shutdown explicitly once they are started. Long-lived components should terminate properly otherwise they will lead to deadlock situation, and in the worst case they may create orphan processes. Those orphan processes will consume resources; increase system burden and lead to increase system hang state. In the AMPIT system, the Device monitoring (DM) component activates the Silent activity logging (SAL) component after it receives a negative signal from the Credibility checking (CC) component and the Silent activity logging (SAL) component stays alive throughout the whole process.

However, the Eternal components are the components that exist throughout the whole life cycle of the system, and sometimes they are treated as mandatory components. To minimize system initialization time, the number of eternal components must be kept as low as possible. We should allocate minimum number of resources to these types of components because of their longevity. In AMPIT system, Device monitoring (DM) component starts immediately after the system is powered-on, and continues to monitor predefined devices through-out the system's life time.

##### 3.2.2.2 Resource Management

Every system has a finite number of resources, which have to be managed in a way that it can maximize system's efficiency and resource availability. Although the AMPIT system hardly

suffers from resource scarcity, it needs a suitable mechanism for resource management to control unexpected system behaviors. The AMPIT system has the following two types of resources: 1) The physical resources are CPU, webcam and portable storage devices. 2) The logical resources are network bandwidth (used for SMS or email messages), and different system APIs. We have to follow a number of rules so that the system can work efficiently with a variety of resources. Therefore, the following rules should be considered carefully for proper resource management processes:

- No component should suffer from resource starvation.
- No component should block a resource for a long period of time.
- Race condition should mitigate competently.

For example, the Device monitoring (DM) and Data encryption (DE) components work with similar resources and therefore, they have to deal with race condition problem. Also components that work with several resources are more vulnerable and prone to faulty behavior. On the other hand, the Silent activity logging (SAL) and Advanced alert system (AAS) components work entirely with their own resources and they are less prone to a faulty behavior.

### 3.3 Threat Model

We need to find out all the security risks for any system, since vulnerability in one part of an application can open the system to calamity. To focus on all the real risks or attacks, a system should have a realistic threat model, and it is an important part in the design phase of any application development process. The threat model examines or views a system through a potential attackers or hackers' viewpoint. It also identifies the root causes of attacks.

A threat model uses the following three steps:

- Identify security objective: In this step, we have to ensure the protection of users' identity abuse. Also, we have to measure the security levels of users' data.
- Application overview: After defining the security objectives, we will have to identify components, data flows and trust boundaries. Also data movement between trust boundaries should be analyzed carefully.
- Decompose application: Once the system architecture is completed, we need to decompose the application to find out the modules that need to be evaluated further.

Figure 2 shows the threat model of the AMPIT system.


Figure 2: Threat model

#### 3.3.1 Threat Listing

Threat is an activity which negatively affects an asset. If we are able to figure out the threats, then we will have to determine which asset is being threatened. For a threat model we have to find out all attack vectors. An attack vector is a mechanism for gaining access to a system in order to do some malfunctioning or to steal data. In the AMPIT system there are two types of attack vectors, 1) mitigated; 2) Unmitigated.

A mitigated attack vector has low impact on system efficiency, and a system can work properly with its existence. However, an unmitigated attack vector has the highest vulnerability and can collapse the functionality of the whole system.
In our system we consider both mitigated and unmitigated attack vectors to identify all the potential attacks. The following major problems can occur in the AMPIT system:

- Unauthorized portable storage devices plugged-in to the system.
- Authorized device has been lost, which had contained sensitive data.

## 4 IMPLEMENTATION

The AMPIT system has been designed and implemented to ensure data security for the system. It is designed to work with Windows operating system (Vista or higher), and was implemented using C# language. Figure 3 shows partial class diagram of the AMPIT system which shows operations and interrelationship between different classes.

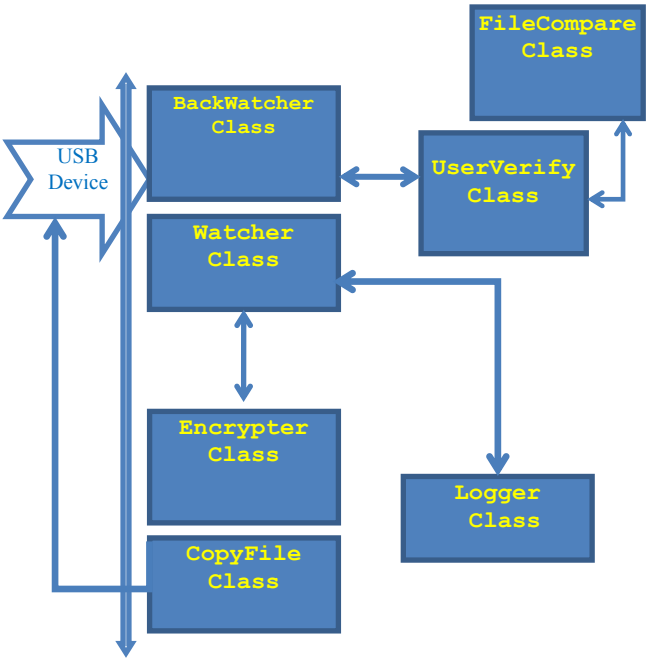


Figure 3: The Class diagram for AMIPT system

Figure 4 shows the required number of treads for 2 USB devices for AMPIT and other similar systems such as MyUSBOnly, USB-LockRP and USB Secure. As the figure demonstrates, our proposed system imposes lower load on the CPU by requiring less number of threads than other similar systems.
Also, the AMPIT system efficiently prevents information loss in comparison with the other similar systems (e.g. MyUSBOnly, USB-LockRP and USB Secure). It prevents data theft through a variety of portable media including USB flash drives, thumb drives, memory sticks, external drives, CD-RWs, USB card readers, iPods, Bluetooth transceivers, DVDs, SDs (Secure Digital), MMCs (Multi Media), and HDMI (High-Definition Multimedia Interface). Furthermore, AMPIT system protects users' data by blocking off the unauthorized users from any ports of the computer.

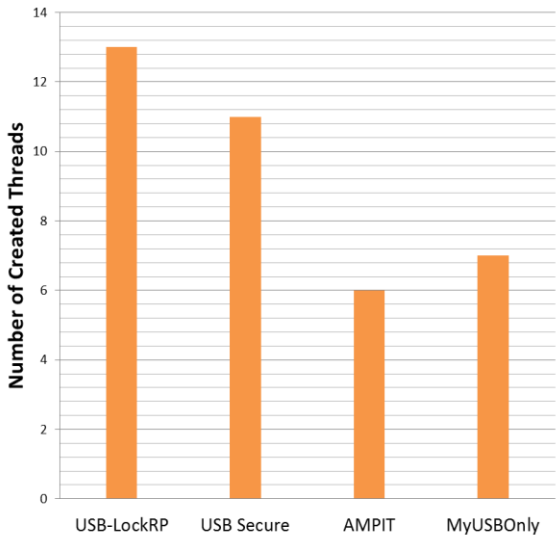


Figure 4: Performance comparison of AMPIT system

### 4.1 User Interfaces

A fully functional user interface involves a systematic approach to the design process of the AMPIT development phases. Therefore, one of the key tasks of the AMPIT system is to provide convenient user interfaces. Furthermore, an easily understandable user interface leads to higher user

acceptance. The Form designer (visual C#) of Windows has been used to design all user interfaces.


Figure 5: Device authorization

Figure 5 shows the user interface for Credibility checking component. This interface enables the users to get authorization for their portable devices so that they can connect their portable device to the computer that has the AMPIT system. As shown in this figure, a drop down list allows the selection of the portable storage devices, and the text fields allow the user to enter his/her user name and password. Then, the Authorize button (shown in blue color) interacts with the Windows system API to verify user authenticity based on the provided data. This interface ensures that AMPIT protects the system from any suspicious device.

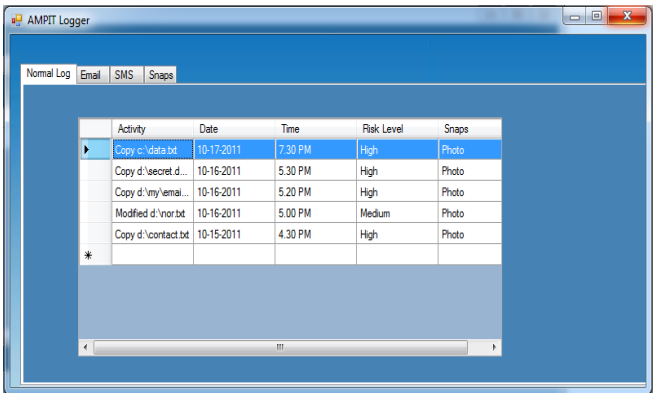


Figure 6: Email logger

Figure 6 shows the email logger interface of the AMPIT system. From this interface an authorized person can see all the email alerts which are sorted according to date and time.
Figure 7 shows the list of events performed by the intruders. The Activity column gives the details of the actions performed. These actions are listed according to their time of occurrences.

## 5 CONCLUSIONS

Corporate environments cannot be fully protected with any software or hardware solution because of their variations around the world. This research designs and implements the AMPIT middleware system which provides strong safeguard for protecting personal and corporate data from susceptible persons. This middleware consists of two major sub-modules: monitoring all USB or portable storage devices, and authorization of devices. The AMPIT system is highly sensible for logging user activities; it has local activity logging ability, and it also provides SMS, snapshot and email alert facilities. Therefore, it carefully monitors and handles all types of suspicious activities performed in a machine. Furthermore, the AMPIT system imposes lower burden on CPU, and consumes less physical memory than other similar systems such as MyUSBOnly, USB-LockRP and USB Secure. In addition, using AMPIT system allows the corporations to address the insider threats with the same devotion as the outsider threats. This will result in significant security improvement as the companies must adopt proper security policies for their employees and fully communicate with their employees the danger of disregarding these policies.

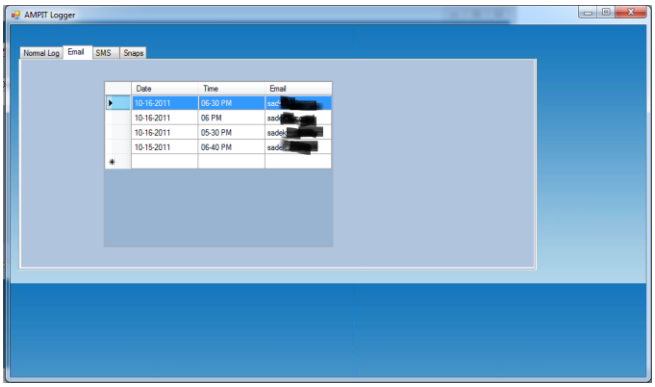


Figure 7: Events logger

## Acknowledgement

This material is based upon work supported partially by the National Science Foundation under Grant No. 0851912. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

## 6 REFERENCES

1. Buffalo Advantage - Secure LockWare, http://www.buffalotech.com/technology/buffalo-advantage/secure-lockware (accessed Oct 10, 2012).
2. Data leakage worldwide: Common risks and mistakes employees make, White Paper, CISCO Systems, 2008.
3. Data leakage worldwide: The high cost of Insider threats, White Paper, CISCO system, 2008.
4. Data Theft and State Law: When Data Breaches Occur, http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_032261.hcsp?dDocName=bok1_032261 (accessed Dec 3, 2012).
5. Jon Meling, Bjornstein Lilleby, Paul Levlin, Tor Erik Sonvisen, Stig Johansen, Dag Johansen, Age Kvalnes. "Gohcci: Protecting sensitive data on stolen or misplaced mobile devices". 10th international conference on mobile data management: systems, services and middleware, IEEE Computer Society, pp. 348-354, 2009.
6. Device Lock, http://www.devicelock.com/dl/devicelock.pdf (accessed November 20, 2012).
7. Former Reddit Employee Indicted, Charged With Data Theft, http://mashable.com/2011/07/19/reddit-co-founder-indicted-data-theft/ (accessed Oct 17, 2012).
8. GiliSoft USB Stick Encryption, http://www.gilisoft.com/product-usb-stick-encryption.htm (accessed Oct 15, 2012).
9. Data theft: Top 5 most expensive data breaches. http://www.csmonitor.com/Business/2011/0504/Data-theft-Top-5-most-expensive-data-breaches/5.-US-Veterans-Affairs-25-30-million (accessed Dec 20, 2012).
10. MyUSBOnly: USB Control Software, USB Security, Device Control, Endpoint Security, Block USB Port: Index, http://www.myusbonly.com/usb-security-device-control/index.php (accessed Oct 10, 2012).
11. NZXT Bunker USB Locking Device. http://www.sweetwater.com/store/detail/Bunker/?gclid=CJzggLmpy6sCFRFR7AodHGvC1w (accessed Sept 17, 2012).
12. Pod Slurping-an easy technique for stealing data, GFI software, white Paper, 2007.
13. Sandhu, Ravi, "The challenge of data and application security and privacy (DASPY): are we up to it?" Institute for Cyber Security, University of Texas at San Antonio, CODASPY'11, February 21–23, 2011, San Antonio, Texas, 2011.
14. USB Lock RP Operation Manual. http://www.slideshare.net/JavierArrospide/usb-lock-rp-operation-manual-presentation (accessed Oct 22, 2012).
15. USB Port Lock & Usb Port Security Systems, http://accoblobstorageus.blob.core.windows.net/literature/1378.pdf (accessed Nov 16, 2012).
16. USB Secure Features. http://www.newsoftwares.net/usb-secure/features (accessed Oct 23, 2012).
17. USB Security Lock – A little hardware security for your PC. http://www.slashgear.com/usb-security-lock-a-little-hardware-security-for-your-pc-047772/ (accessed Oct 10, 2012).
18. Wagner, Joe, The Thumb-sucking Threat. http://www.csoonline.com/article/356964/the-thumb-sucking-threat (accessed Oct 20, 2012).
19. Where is Your Data? http://whereismydata.wordpress.com/2009/01/07/data-loss-examples-in-2008/ (accessed Oct 10, 2012).
20. Simon Liu, Rick Kuhn, Data Loss Prevention, US National Institute of Standards and Technology, 2010.