Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Operations for Secure Use of Mobile Data Devices within a United States Criminal Justice Agency

CAPSTONE REPORT

Richard T. Habgood
IT Security Manager
Orange County Sheriff's Office

University of Oregon
Applied Information
Management
Program

February 2013

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

____

Dr. Linda F. Ettinger
Senior Academic Director, AIM Program

Operations for Secure Use of Mobile Data Devices in a United States Criminal Justice Agency

Richard T. Habgood

Orange County Sheriff's Office

Abstract

USB flash memory devices, mobile smartphones and mobile tablets are in wide use in organizations and personal life. United States criminal justice agencies are developing operations for mobile device adoption. Organizations responsible for the protection of citizens need to maintain confidentiality, integrity and availability of information whether it is stored, being processed or in transit. This annotated bibliography examines literature published between 2005 and 2012 to identify operations for secure mobile device implementation and use.

Keywords: availability, bring your own device (BYOD), confidentiality, criminal justice, data, drive, encryption, handheld, hard drive, integrity, law enforcement, mobile data, mobile device management, physical, remote wipe, smartphone, rest, security, transit, transport, usb devices

Table of Contents

List of Figures and Tables

Introduction to the Annotated Bibliography

Problem

The federal bureau of investigation (FBI) criminal justice information services (CJIS) security policy identifies two types of digital information within national and local criminal justice that must be secured using proper policies, procedures and controls: (a) criminal justice information (CJI), and (b) personally identifiable information (PII) (CJIS Security Policy Resource Center, 2012). Information security policies dictate acceptable behaviors (Whitman & Mattord, 2005, p. 89). Procedures exist to provide detailed instructions on how to carry out security policies (White et al., 2008). Controls act as a counter mechanism preventing security vulnerabilities or minimizing risks (Whitman & Mattord, 2005, p.30). While federal CJI and PII guidelines exist for traditional computers, mobile data security within criminal justice agencies has not fully developed and exist in the form of a draft document (Brown, 2012). The topic focus for this annotated bibliography examines how to secure mobile data devices in a United States criminal justice agency, with emphasis on operations.

Today, individuals are able to access a variety of information from devices that are small enough to fit in a person’s pocket (Wallach, 2011). Due to the portability and handheld size mobile devices are ubiquitous in the daily life activities of individuals (Distefano, Grillo, Lentini, & Italiano, 2010). Unfortunately, individual users of these technologies don’t always understand the security risks involved with mobile data device use (Allam & Flowerday, 2011). Companies and organizations have also launched a strong push for smartphone adoption, again with little concern for security risks (Ugus, Westhoff, & Rajasekaran, 2012). As a result, the number of smartphones in the marketplace grew greater than that of personal computers in late 2010 (Wang, Streff, & Raman, 2011); security risks are apparent through the rapid growth of malware since that time (Wang, Streff, & Raman, 2011). In 2011, 835 million mobile data smartphones were in use worldwide (Wang, Streff, & Raman, 2011).

Whitman and Mattord (2005) state that to be considered secure the information must be confidential, have integrity, and be readily available. Confidentiality, integrity, and availability are commonly referred to as the security triad or CIA (White et al., 2008). The fundamental security concept of the three information characteristics applies to all digital information regardless of the device environment or type (NSTISSI, 1994). Information security for mobile devices should rely on these three characteristics (Verma, 2011). Mobile data security challenges involve threats to data stored on the device, while the information is being utilized or when information is being transferred between a mobile device and another location within the electronic system (Wang, Streff, & Raman, 2011).

Purpose

The purpose of this annotated bibliography is to identify industry recognized operations that could best aid in developing a sound and uniform policy for securing mobile data within the context of a US criminal justice agency. Mobile data devices are small form factor devices with built-in data storage and a method to synchronize with another digital system (National Institute of Standards and Technology, 2012, p 2). Three distinct mobile data devices are addressed within this study: (a) USB flash memory devices (Lee, Yim, & Lee, 2010), (b) mobile smartphones (Wang, Streff, & Raman, 2011) and (c) mobile tablets (United States Government Accountability Office, 2012).

The bibliography divides discussion of securing these devices based on the following three information states: (a) while in storage (Lee, Yim, & Lee, 2010), (b) while being processed (Wang, Streff, & Raman, 2011) or (c) while in transmission (Milligan & Hutcheson, 2007). This approach follows a portion of an established model for determining information security, known as the McCumber Cube (McCumber, 2005). The McCumber Cube is a three dimensional model used to address the interactions of information state, categories of safeguards, and information characteristics (Hafiz & Johnson, 2006). Application of this model is addressed by Whitman and Mattord (2005) through examination of the intersection of the information states of storage, processing, and transmission states with information characteristics of confidentiality, integrity, and availability.

The McCumber Cube assists in determining how to apply measures that will ensure security of information through a dimension described as security measure safeguards (McCumber, 2005). Security safeguards address (a) technology, (b) human factors, and (c) operations (McCumber, 2005). Technologies are defined by McCumber (2005) as "any physical device or technique implemented in physical form that is specifically used to ensure that critical information characteristics are maintained through any of the information states." Human factor safeguards are achieved through information security training and awareness (White et al., 2008). Security operations consist of a combination of security policies and practices. Policies provide a guide for acceptable behaviors, while a practice is a procedure used to ensure a policy is followed (McCumber, 2005). The scope of this annotated bibliography addresses only the interaction of mobile data security operations on information state and information characteristics.

Research Questions

The annotated bibliography is focused on determining sound security operations that have already been developed for use with mobile devices. The bibliography takes into consideration the following research questions:

Central question. How can a criminal justice agency establish confidentiality, integrity and availability (i.e., security) of information that is stored, processed, or transmitted on a mobile device (USB flash memory device, mobile smartphone, and mobile tablet)?

Sub-questions.

- How is information securely stored on a mobile data device?
- How is information securely processed while it is in use on a mobile device?
- How is information securely transmitted from a mobile device to and from another location?

Audience

The audience for the study is information technology personnel and key decision makers within a criminal justice agency who need to understand mobile data security operations in order to avoid vulnerabilities and the risks associated with those vulnerabilities.

The FBI designates a criminal justice agency as:

> A governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. (CJIS Security Policy Resource Center, 2012, p A-3)

Stakeholders include top management of a criminal justice agency, chief information officers (CIO), IT managers and information security officers (ISO). An ISO is defined as “a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs” (CJIS Security Policy Resource Center, 2012, p. A-2).

Significance

Criminal justice communications benefit from the ability to share mobile data including CJI, reports, text messages and pictures (Tabourin, 2010). Criminal justice personnel, according to Straus (2010), “require real-time information access and rapid communication to diagnose potential threats, analyze problems and coordinate actions”. As an example, the Los Angeles County Sheriff’s Office uses Blackberrys^{TM} to retrieve driver’s license photos (Weier, 2009). Federal agencies are working to develop security standards which address new computer security procedures (Corbin, 2012).

In a 2009 survey and report from the Computer Security Institute, 42% of the respondents indicated that a laptop or mobile device had been either lost or stolen (Ben-Asher et al., 2011). In the case of USB memory devices, personal information is frequently exposed once a device is lost (Lee, Yim, & Lee, 2010). In a study conducted by Panda Security, nearly half of the companies in the United States have reported systems infected via the use of USB devices (Lemos, 2010). During the year 2012, there has been a 185% increase in the variety of malware that targets mobile data devices (United States Government Accountability Office, 2012). Organizations equipping their employees with mobile data devices must take these security risks into consideration (Distefano, Grillo, Lentini, & Italiano, 2010).

Research Delimitations

Time frame. The materials that are contained in the annotated bibliography are selected primarily from sources published between 2005 and 2012. The focus is intended to find materials that discuss relevant security operations concerning current selected mobile technologies. Definitions for traditional security concepts are located in text with copyright dates as old as 2005 (Whitman & Mattord, 2005). Vulnerabilities and threats to mobile devices are seen back to

2004 (Wang, Streff, & Raman, 2011). The majority of the documentation located has been produced since 2009.

Types of sources. Contained within the annotated bibliography are sources located through online searches through the University of Oregon Libraries, including access to computer science databases (IEEE Xplore, CiteSeerX), the Criminal Justice Collection, and EBSCOHost. Additional search engines are utilized including Google Scholar and Microsoft Academic Search. Information regarding federal and state standards is located through organization websites and portals. These organizations include the FBI, US Department of Commerce, the National Institute of Standards and Technology as well as the US Government Accountability Office.

Reference selection criteria. The search strategy for reference material attempts to first locate a broad set of material regarding security of mobile devices. The references located discuss topics in the expanded use of the worldwide market. This includes areas outside of the criminal justice scope. The focus is narrowed towards criminal justice as sufficient information is gathered and understood regarding technologies and methods of use. Primary interest is in publications from the FBI, NIST, and state governments that specifically describe methods, procedures and examples of use in a criminal justice agency. A Principles of Information Security text by Whitman and Mattord (2003) is selected for common security concepts, methods and definitions due to its use within academic education materials (University of Oregon, 2012).

Industry-recognized method. Within this annotated bibliography, an industry recognized method refers to a process that has been created, endorsed or prescribed by a standards organization or information technology institute. The National Institute of Standards and Technology is a government entity that develops methods for use of information technology

(National Institute of Standards and Technology (2012). The SANS Institute is a non-government research and education organization that deals with information security certifications, education and documentation (The SANS Institute, 2012).

Mobile technology selections. USB flash memory devices, mobile smartphones and mobile tablets are capable of being categorized under the definition of a small and compact handheld electronic device that is capable of storing and transferring information (Wang, Streff, & Raman, 2011). In a 2010 survey 32% of small and medium size businesses indicated employee USB devices were the cause of computer virus infections (Lemos, 2010). Near the beginning of this year nearly 46% of US adults own a mobile smartphone (United States Government Accountability Office, 2012). While considerably fewer individuals own tablets, there are still over 19% of US adults who own these devices (United States Government Accountability Office, 2012). The selection of the trio of devices is based on the popularity and widespread use.

Reading and Organizational Plan Preview

Reading plan. The literature referenced within the annotated bibliography is read and analyzed through a conceptual analysis process determining relevance to the three research sub questions (Busch et al., 2003). Eight steps of the coding and analysis process are detailed within the Research Parameters section. The readings are stored in a digital format for reference and review. Searches through the materials for relevance are conducted with the aid of electronic keyword searches. Results from the searches are stored and used for organizing references.

Organizational plan. The results of the reading plan are organized thematically and presented in the Annotated Bibliography section of this paper (Labaree, 2012). Results are divided among three main themes: (a) operations that secure stored data on a mobile device, (b) operations that secure mobile device data being processed and (c) operations that secure mobile device data while it is transferred to and from the device. Within each theme three devices are examined: (a) USB flash memory devices, (b) mobile smartphones and (c) mobile tablets. Results determined within each theme serve to answer the research sub questions and highlight whether operations provide data with (a) confidentiality, (b) integrity and/or (c) availability.

Definitions

Terms within this annotated bibliography may be unique to individuals working within United States criminal justice agencies. Definitions contained within this section serve to provide understanding for this audience and other readers who may be less familiar with specific language. Each definition is cited to a reference selected for use in this study and examined within this discussion of secure mobile data device policies.

Confidentiality – “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information” (McCumber, 2005).

Criminal justice agency – “a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice” (CJIS Security Policy Resource Center, 2012).

Criminal justice information – “the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions” (CJIS Security Policy Resource Center, 2012).

Data leakage – Non-authorized transmission or distribution of data within an organization to an external recipient (Sun, Choi, Lee, & Noh, 2008).

Distributed hash table network – A distributed data structure used to store and manage data in a peer to peer type network (Yue, Wang, & Liu, 2010).

Information security – “the protection of information and its critical elements, including the systems and hardware that use, store and that transmit information” (Whitman & Mattord, 2005, p.8).

Integrity – “guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity” (McCumber, 2005).

Mobile device – a small and compact handheld electronic device that is capable of storing and transferring information (Wang, Streff, & Raman, 2011).

On-scene triage – The process of extracting information from a computing device without having to physically move the device from the location of a crime or event (Mislan, Casey, & Kessler, 2010).

Personally Identifiable Information (PII) — “PII is information which can be used to distinguish or trace an individual’s identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name” (CJIS Security Policy Resource Center, 2012).

Risk – “The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.” (US Department of Commerce, N., 2011).

Self-destructing scheme for electronic data (SSDD) – An acronym used to describe a process where data stored on a device will permanently delete itself without interaction from a user or application (Yue, Wang, & Liu, 2010).

Safeguard – “the management, operational and technical controls prescribed for an information system that, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information” (McCumber, 2005).

Smartphone – an advanced telephone that utilizes a mobile operating system, communicates across both voice and data networks, accesses the internet, is able to run applications and potentially contains both a camera and microphone (Wang, Streff, & Raman, 2011).

Threat – “Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.” (US Department of Commerce, N., 2011).

USB data device – a small Universal Serial Bus (USB) electronic memory device weighing approximately 30g that is capable of fitting within a person’s hand. (Lee, Yim, & Lee, 2010)

Virtual Private Network (VPN) - a method of creating secure communications through a public telecommunications structure by utilizing a digital tunneling protocol and procedures (Jaha et al., 2008).

Vulnerability – “Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source” (US Department of Commerce, N., 2011).

Research Parameters

This section provides a description of the methods and processes used to develop and execute the annotated bibliography. Included within the contents are (a) the search strategy for literature, (b) the development and list of keywords for searches, (c) the documentation approach used to retain a bibliography and list of references, (d) the evaluation criteria used in selecting literature, and (e) the reading and organization plan used in formulating a conceptual analysis and applying literature into themes.

Search Strategy

The annotated bibliography incorporates references that are located in peer-reviewed academic journals, industry publications, published security textbooks, certification materials, government guidelines and directives. Topic searches are focused on returning information that pertains to the security of mobile devices within a law enforcement context. Materials are not necessarily precluded to law enforcement scenarios; many references identify security measures used in both the corporate and public domain. The use of these materials is relevant due to the limited development of defined security procedures within the law enforcement community (National Institute of Standards and Technology, 2012).

The strategy involves searches based on three device types: (a) USB flash memory devices, (b) mobile smartphones and (c) mobile tablets. Within each device type, a subset of searches is divided into the concept of data in three distinct states: (a) while stored/at-rest, (b) being processed, or (c) being transmitted.

Key Words

A list of keywords is useful in the location of reference material with a few additional terms more widely used within articles and research (Creswell, 2009). As an example, a term used for mobile phones possessing the ability to access and retain digital data is *smartphone* (Wang, Streff, & Raman, 2011). Along with this term, a set of 20 keywords assists in narrowing search. These additional terms are added to create the following list of keywords:

- Availability
- Bring Your Own Device (BYOD)
- Confidentiality
- Criminal justice
- Data
- Drive
- Encryption
- Handheld
- Hard drive
- Integrity
- Law enforcement
- Mobile data
- Mobile device management
- Physical
- Remote wipe
- Smartphone
- Rest
- Security
- Transit
- Transport

- USB devices

Documentation Approach

As useful and pertinent documents are located, bibliographic information is bookmarked and saved into the Zotero bibliography management software. The entry is cataloged into a specific folder structure based on the content addressed within the reference according to the following scheme:

- Two parent folders indicating whether material pertains directly to criminal justice or not.
- A subfolder structure that organizes references based on the three research sub-questions. Four subfolders separate materials by designation mobile data device storage, processing, transmission or multiple information state.
- A lowest set of folders indicating whether materials are either relevant or beyond the scope of the bibliography.

Evaluation Criteria

The references selected for use in this annotated bibliography should be considered current, relevant and hold a level of authority (LSU Libraries, 2012). The materials referenced must have been published within the past ten years, i.e., since 2002. This assists in ensuring that the information pertains to mobile devices that are still or potentially in use. The exception to this pertains to established information security procedures developed prior to this time limitation, and which remain in current use. Relevance pertains to each material's ability to address the research question and sub questions in some useful manner. A level of authority is established through industry expert recognition or peer-review. Journal articles contain this level of authority if they are peer-reviewed. Industry publications, security textbooks and certification materials hold a level authority if they have been produced by industry recognized experts or organizations. Government guidelines and directives are designated as authoritative at the federal and state institution level.

Reading and Organization Plan

Reading plan. The approach to the reading plan for this annotated bibliography involves examining collections of text for the existence of concepts, identified by keyword terms, and recording the occurrence of keyword combinations present within each document. Busch et al. (2013) describe this process as conceptual analysis. The concepts are used to analyze selected references in relation to content categories pertaining to the research questions presented (Busch et al., 2013). This reading plan using conceptual analysis is conducted through the following eight steps of analysis:

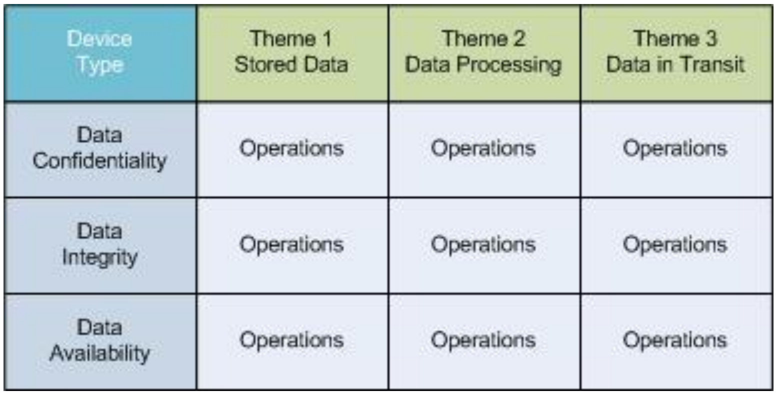
- **Level of analysis.** Single word terms are considered insufficient for proper identification of the content required. Multiple word terms are used within the analysis to more closely identify devices with a state of data. As an example of term pairing, an *usb* device term is combined with *transmit* for a state of data.
- **Number of concepts coded.** Three devices types are combined with three states of data. To account for the possibility of multiple terms describing a unique device or state of data, three separate terms are initially searched in each coding attempt. As necessary the quantity of terms used for a category are expanded or contracted based on the presence of useful content.
- **Coding for existence or frequency of concept.** Only the existence of terms is searched due to the large quantity of terms and concepts that are examined. The presence of the combination of terms leads to an analysis of whether content is

capable of addressing any of the three security goals: (a) confidentiality, (b) integrity or (c) availability.

- **Distinguishing among concepts.** Results for concepts are generated in a number of different forms. The reading plan allows for terms to appear in a variety of forms beyond a root searched. For example, the terms *encryption* and *encrypted* potentially discuss the same concept. Varying order of terms returned is also acknowledged and accepted.
- **Rules for coding of text.** Search terms are organized and placed within a device or data state heading. This method of coding text provides a level of consistency and is utilized to provide accurate results. Combinations of terms are not utilized in multiple categories.
- **Irrelevant information.** Results that provide information not pertaining to the categories determined or addressing the research question and sub questions are disregarded.
- **Coding text.** The specific context of concept presence in the various documents is noted and used to determine extended relevance or meanings. Location of the search terms within the document is electronically recorded for simplicity of referral. Documents are moved into the respective folder structures according to the design noted within the documentation approach section. The same method is used within all readings to provide the most stable and reproducible results.
- **Analyze the results.** The information provided through the reading plan and conceptual analysis is utilized to determine if sufficient material is present to

address the research questions; further iterations are conducted if additional text is required. The results are examined through an organizational plan.

Organizational plan. The results of the reading and coding efforts are organized thematically, focused on security operations pertaining to (a) stored data, (b) data while it is being processed and (c) data while it is involved in transit. Within Figure 1, a preliminary schema structures the data analysis and presentation approach. The research sub questions, addressed within the three themes, are answered by further segregating the results into the two dimensional intersection of concepts presented within the McCumber Cube (McCumber, 2005). Security operations are identified within these cross sections.



Device Type	Theme 1 Stored Data	Theme 2 Data Processing	Theme 3 Data in Transit
Data Confidentiality	Operations	Operations	Operations
Data Integrity	Operations	Operations	Operations
Data Availability	Operations	Operations	Operations

Figure 1. Security operations preliminary display model.

The first theme addresses three selected mobile devices: (a) USB flash memory devices, (b) mobile smartphones, and (c) mobile tablet devices. The section provides a discussion of how these devices can secure data at rest stored on the devices. Operations supported by the bibliography are subdivided and address protection of data (a) confidentiality (Witman & Mattord, 2005), (b) integrity (White et al., 2008), or (c) availability (McCumber, 2005).

The second theme focuses on how these same three selected mobile devices are able to secure data while it is being processed within the device. Again, operations are segregated based on whether (a) confidentiality (Witman & Mattord, 2005), (b) integrity (White et al., 2008) or (c) availability (McCumber, 2005).

The third theme addresses how these same three selected mobile devices can secure data while in transit to and from other devices or networks (McCumber, 2005). Operations identified are handled and subdivided in the same manner as the two other themes.

Annotated Bibliography

The annotated bibliography contains 32 references selected to address the defined research question and sub questions. Annotations include: (a) an APA formatted bibliographic citation, (b) an abstract of the content contained within the text, (c) a description of credibility, and (d) a summary. A section of credibility is included to demonstrate the authority of the author and the qualification of the reference for inclusion. A summary is provided to demonstrate a level of connection between the content and a theme in this study. The references are categorized into three themes, described in the reading and organization plan. The themes include: (a) operations that secure stored data on a mobile device, (b) operations that secure mobile device data being processed, and (c) operations that secure mobile device data while it is transferred to and from the device.

Theme 1 – Operations to Secure Stored Data

Kleidermacher, D. (2012). Enhance system security with better data-at-rest encryption. *Embedded Systems Design*, *25*(3), 19-23.

Abstract. The article discusses data-at-rest protection to ensure that unauthorized persons do not gain access to sensitive information contained in lost or stolen media like medical records, bank details or government top security information. Encryption is mentioned as the most common solution. Approaches are presented, including the choice among (a) multiple layers in the data storage stack, (b) symmetric encryption algorithms or cipher modes, and (c) the management of the long term storage encryption keys.

Credibility. Dave Kleidermacher is the Chief Technology Officer of Green Hills Software. He has worked for over 21 years in the field of systems software and security. He writes articles and teaches for the Embedded Systems Conference. Embedded is a resource and brand provided by UBM Electronics. UBM brands serve 2.25 million executives and engineers through UBM Tech's world-class content, events, and specialized communities for the electronics industry.

Summary. The author provides a detailed description of multiple device layers where encryption can be utilized. He discusses encryption handled at the hardware layer, block manager layer, file system layer, and the application layer. The focus of the article is centered on protecting data at rest. This directly addresses the topic sub question and theme of operations to secure stored data. The author highlights the primary purpose of securing data at rest as prevention of unauthorized parties from extracting or using data on lost or stolen devices. This primary purpose, when tied to listed operations, provides data confidentiality.

Lee, S.-H., Yim, K.-B., & Lee, I.-Y. (2010). A secure solution for USB flash drives using FAT file system structure. *Network-Based Information Systems, International Conference on* (Vol. 0, pp. 487–492). Los Alamitos, CA, USA: IEEE Computer Society. doi:http://doi.ieeecomputersociety.org/10.1109/NBiS.2010.30

Abstract. The portable storage market environment is rapidly changing due to the emergence of USB memory. USB memory is used as a portable storage device by many users. However, due to the high portability of USB memory, USB sticks are frequently lost and stolen. In this paper we suggest a secure user authentication method in which it is hard to guess the password and bypass authentication. In addition, security and efficiency are provided through a user authentication password backup and recovery mechanism to access the secure area.

Credibility. Sun-Ho Lee is a research assistant at Soon Chun Hyang University in South Korea. Kang-Bim Yim has served as a Visiting Professor at Purdue University, a research fellow at the University of Arizona, and is currently a professor in the department of information security engineering at Soon Chun Hyang University in South Korea. The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest professional association dedicated to advancing technological innovation and is comprised of more than 400,000 members.

Summary. The paper specifically addresses a method of securing data at rest on a USB device. Considerations are made regarding confidentiality, authentication, access control, attacks and efficiency of the proposed method. Each of these areas is compared through analysis against a set of four other security techniques. Based on their conclusions the proposed method is capable of providing both confidentiality and integrity of data. The paper is solely focused on USB storage with no mention of smartphone or tablet devices.

Mislan, R. P., Casey, E., & Kessler, G. C. (2010). The growing need for on-scene triage of mobile devices. *Digital Investigation, 6*(3–4), 112–124. doi:10.1016/j.diin.2010.03.001

Abstract. Criminal justice agencies and military agencies encounter situations where information needs to be quickly extracted from mobile data devices. The devices often need to be taken or delivered to Digital Forensic Laboratories (DFLs) to retrieve the necessary data at rest. The delay in this process creates a less efficient and responsive criminal justice system. The author discusses an on-scene triage process for extracting data without having to transport the device.

The paper formalizes the on-scene triage process, placing it firmly in the overall forensic handling process and providing guidelines for standardization of on-scene triage. In addition, the paper outlines basic requirements for automated triage tools.

Credibility Richard P. Mislan served as a professor in Purdue University's College of Technology. He currently is a professor at the Rochester Institute of Technology. Mislan has acted as an editor for the Small Scale Digital Device Forensics Journal and as a reviewing editor for the National Institute of Standards and Technology (NIST). Eogan Casey is a professor at Johns Hopkins University Information Security Institute and is the creator of mobile device forensics courses taught through the SANS Institute. Gary C. Kessler is an Associate Professor at Embry-Riddle Aeronautical University and an adjunct professor at Edith Cowan University in Perth, Australia. Digital Investigation is a peer-reviewed journal covering current developments in digital forensics and incident response around the world.

Summary. The authors of the article provide an understanding of methods, tools and recommended procedures for extracting information from mobile devices that are at rest through a process termed *on-scene triage*. Focus is on the mobile phone, which is segregated into three categories:

- Type 1: Basic phone
- Type 2: Camera phone
- Type 3: Smartphone

The article addresses the topic sub-question of how to secure data at rest on a mobile device by providing an understanding of how information can be extracted from a device. A device known as Athena has the capability to be directly connected to a mobile device and is referenced within the article. Also provided is an understanding of operations that provide data integrity and availability for criminal justice agencies during investigations. Legal considerations during the data acquisition process include (a) consent, (b) a search incident to arrest, (c) exigent circumstances and (d) a search warrant.

Myers Jr, J. P., & Riela, S. (2008). Taming the diversity of information assurance & security. *Journal of Computing Sciences in Colleges*, *23*(4), 173–179.

Abstract. Contemporary presentations of Information Assurance & Security (IAS) are far broader than older notions of "computer security," "network security," "OS security," and the like. The field has become so broad that it is only a slight exaggeration to state that it is difficult to find a sub-discipline of CS to which IAS is not relevant. This broadening of scope leads to many challenges as to how to structure such a course so that it does not appear intimidating in scope or merely a potpourri of marginally related topics. A means of structuring a course to avoid these pitfalls is presented here.

Credibility. J. Paul Meyers, Jr. holds a PhD from the University of Denver. He is a Professor of Computer Science at Trinity University in San Antonio, TX. Sandra Riela is a graduate of Trinity University and is currently an IAS Consultant. The Journal of Computing Sciences in Colleges is distributed to over 200 colleges and is archived in the ACM Digital Library. The journal contains conference proceedings for the regional conferences sponsored by the Consortium for Computing Sciences in Colleges. The consortium is concerned with the advancement of college programs in Computer Science and Computer Information Systems. The CCSC is partnered with the National Science Foundation.

Summary. The article discusses the instruction and implementation of the McCumber Cube model in information security. The information states during (a) transmission, (b) storage and (c) processing interact at a high level with the information characteristics of (a) confidentiality, (b) integrity and (c) availability in creating security policy. The discussion also highlights the interaction of information states and information characteristics as they pertain to selecting technology and human factors, although focus on these aspects of the McCumber Cube is outside the scope of this bibliography. Within the context of the article the use of information stored in a database is used to demonstrate the intersection of confidentiality and storage. A password policy is recommended for a security control policy to protect unauthorized access to data or information.

Seifert, J., De Luca, A., Conradi, B., & Hussmann, H. (2010). TreasurePhone: Context-sensitive user data protection on mobile phones. In P. Floréen, A. Krüger, & M. Spasojevic (Eds.), *Pervasive Computing* (Vol. 6030, pp. 130–137). Springer Berlin / Heidelberg. Retrieved from http://www.springerlink.com/content/n12l6hqj22j30435/abstract/

Abstract. Due to increased input and output capabilities, mobile phones hold many different kinds of data. There are no appropriate concepts and implementations yet to handle and limit access to data on mobile phones.

TreasurePhone has been designed to address this specific problem. It protects the users' mobile phone data based on their current context. Privacy protection is realized by *spheres*, which represent the users' context-specific need for privacy. That is, users can define which data and services are accessible in which sphere. TreasurePhone exploits context information to support authentication and automatic activation of spheres by *locations* and *actions*. A user study was conducted with 20 participants to gain insights on how well users accept such a concept. One of the main goals was to find out whether such privacy features are appreciated by the users even though they make interaction slower and might hinder fast access to specific data. Additionally, it was shown that integration of context information significantly increases ease-of-use of the system.

Credibility. Julian Seifert is a research associate in the Human Computer-Interaction group at the University of Ulm in Germany. Dr. Alexander De Luca is a Professor in the Department for Informatics at the University of Munich. His research at the University of Munich is funded in part by the 2010 Google Research Award. Bettina Conradi is a graduate student in the Department of Media Informatics at the University of Munich. Heinrich Hussmann received a PhD from the University of Passau. He is a Professor of Computer Science at the University of Munich. He has participated in over 10 national and international projects in the area of software engineering and telecommunications. He has also authored over 50 scientific publications and three internationally published books. The Pervasive and Mobile Computing journal is a professional, peer-reviewed journal that publishes high-quality scientific articles regarding ubiquitous computing and communications.

Summary. The authors provide and conduct a survey using a mobile device that has the capability to segregate data and functions based on the type or intended use. The phone provides confidentiality in a scenario where work information needs to be separated for home or personal use. Without the proper authentication, the features from one sphere or the other are incapable of being accessed. This assists in whether the user is a known entity or an unknown attacker. The authors only examine a smartphone within the scope of their research.

Sun, K., Choi, J., Lee, D., & Noh, S. H. (2008**).** Models and design of an adaptive hybrid scheme for secure deletion of data in consumer electronics. *IEEE Transactions on Consumer Electronics*, *54*(1), 100 –104. doi:10.1109/TCE.2008.4470030

Abstract. Mobile storage devices are gaining popularity and use in consumer electronics. These devices are prone to loss of data referred to as *data leakage*. Data from USB devices can often be retrieved even after it has been deleted from a device. Two techniques are presented to eliminate this occurrence of data leakage. Experiments were conducted with block cleaning and zero overwriting to determine efficiency and security of their use.

Credibility. Kyoungmoon Sun attended Dankook University in South Korea as a master's candidate in information and computer science with a research focus on operating systems, file systems and flash memory. Jongmoo Choi previously held a position as a visiting faculty member of the University of California, Santa Cruz. He is an Assistant Professor of information and computer science at

Dankook University. Donghee Lee holds a PhD from the Seoul National University and is an Associate Professor at the University of Seoul. Sam H. Noah holds a PhD from the University of Maryland at College Park. The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest professional association dedicated to advancing technological innovation and is comprised of more than 400,000 members. IEEE Transactions on Consumer Electronics is published four times a year; article submissions are reviewed by selected members of a volunteer review committee. The review process establishes a level of approval by industry experts and peers.

Summary. The paper focuses on flash memory that may be present in one of three devices: (a) USB flash memory devices, (b) mobile smartphones or (c) mobile tablets. The authors are concerned about the proper deletion of information off of devices, as a way to ensure that information is not unknowingly made available to others when lost, disposed or stolen. Using a combination of two deletion methods the authors are able to provide an efficient solution that is capable of effectively deleting data. Methods include (a) block cleaning and (b) zero overwriting. The selection of which method is determined by size of information being deleted and how focused the deletion needs to be performed. Proper deletion assists in securing the confidentiality of information.

Tetmeyer, A., & Saiedian, H. (2010). Security threats and mitigating risk for USB devices. *IEEE Technology & Society Magazine*, *29*(4).

Abstract. Computer users have consistently sought out improvements to devices for removable storage to provide the quickest and most efficient means of transferring data from one computer to another. Portable storage media have always been fraught with risk. Security considerations are a concern and organizations have tried to mitigate threats through the use of controls. The article highlights security threats and potential security controls.

Credibility. At the time of publication, Annette Tetmeyer was a PhD student in Computer Science at Kansas University. Hossein Saiedian is a Professor and Associate Chair of the department of Electrical Engineering & Computer Science at Kansas University. He has served as a guest editor and associate editor for numerous peer-reviewed journals. The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest professional association dedicated to advancing technological innovation and is comprised of more than 400,000 members. The Society on Social Implications of Technology (SSIT) of the IEEE produces a quarterly journal focused on the implications of technology, titled *IEEE Technology & Society Magazine*. Feature articles are refereed.

Summary. This article addresses a wide variety of security aspects of USB and mobile data device types, although it does not distinguish mobile smartphones and mobile tablets specifically. The authors refer to these types of devices as transient storage devices (TSD). Risk mitigation and system protection techniques are addressed ranging from physical access to encryption techniques. IEEE standards regarding an authentication protocol are discussed in some detail. The article provides information pertaining to all three concepts: (a) confidentiality, (b) integrity, and (c) availability of data.

Yue, F., Wang, G., & Liu, Q. (2010). A secure self-destructing scheme for electronic data. In

2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC) (pp. 651 –658). Presented at the 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC). doi:10.1109/EUC.2010.104

Abstract. The focus of this paper is the development of a scheme to more securely store content extracted from the Internet. The paper notes that traditional methods of encryption may not be viable enough to secure changing technologies and counter the ability to more quickly discover security keys. The authors propose a secure self-destructing scheme for electronic data (SSDD for short). They demonstrate that their scheme can resist not only the traditional cryptanalysis and brute-force attacks, but also the attacks in a distributed hash table network.

Credibility. The work was supported by the National Natural Science Foundation of China, Hunan Provincial Science and Technology Program and the Changsha Science and Technology Program. The paper was presented at the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. The article is peer-reviewed and published in the IEEE publication the Journal of Computer & System Sciences. The Institute of Electrical and Electronics Engineers (IEEE) is the world’s largest professional association dedicated to advancing technological innovation and is comprised of more than 400,000 members.

Summary. This paper provides an intriguing concept of encryption, storage and time of data at rest. By limiting the time that data is available on a device there is also a possible reduction in time that the data can be compromised. If an item is lost or stolen the data would be useless after a set period of time. It appears that there is potential for this technology use with the three devices: (a) USB flash memory devices, (b) mobile smartphones, and (c) mobile tablets. The application of this technology will assist in data confidentiality and integrity. Unfortunately, availability of the data would be limited by time and device connections.

Theme 2 – Operations to Secure Data being Processed

Allam, S. & Flowerday, S. (2011, August 15). An adaptation of the awareness boundary model towards smartphone security. *Information Security South Africa (ISSA)*, 1-8.

Abstract. This paper addresses the increasing usage, functionality and risk that is associated with smartphone technologies. Noted through the paper is the concept that security features have not kept pace with the other device aspects. Suggested is a form of security risk assessment to deal with ever changing, dynamic issues. This paper examines the Awareness Boundary Model and its feasibility in reducing organizational risks introduced through increasing employee awareness of the information security risks of smartphone computing.

Credibility. Sean Allam is a PhD student in Information Systems at the University of Fort Hare in East London, South Africa. He also serves as the Head of Technology for the Public Sector Advisory Services BU at EOH Mthombo Ltd. EOH is a consulting, technology and outsourcing firm headquartered in Bruma, South Africa. Stephen Flowerday is a Professor of Information Systems at the University of Fort Hare. Information Security South Africa is an annual conference cosponsored by the IEEE.

Summary. The conference paper is primarily concerned with addressing risk in smartphone device usage. Risks are going to be changing as the technologies evolve. Their focus is on using an awareness boundary technique to adapt to these new risks. The techniques that are discussed could be applied to tablet devices; however the concepts would be ineffective in dealing with USB storage. The primary reason this seems to be true is that the paper is discussing the activities that are processed and the security features generated or enabled during the systems use. USB devices do not process information, whereas devices with an operating system can perform notification and security countermeasures.

Becher, M., Freiling, F., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. *IEEE Symposium on Security and Privacy*. (Vol. 0, pp. 96–111). Los Alamitos, CA, USA: IEEE Computer Society. doi:http://doi.ieeecomputersociety.org/10.1109/SP.2011.29

Abstract. The authors address the transition from the Internet society to a mobile society where more and more access to information is done by previously dumb phones. The number of mobile phones using a full blown OS has risen nearly 200% in a period of time from 1999 to 2000. They feel that mobile security has become an absolute necessity. This survey paper provides a concise overview of mobile network security, attack vectors using the back end system and the web browser, but also the hardware layer and the user as attack enabler. A distinction is drawn between "normal" security and mobile security. The paper attempts to draw conclusions that will lead towards additional research possibilities.

Credibility. Michel Becher was a lab member and PhD student at the University of Mannheim, Germany. He has published 9 times and is an employee working in the field of security in mobile communications at Deutsche Telekom AG. Felix Frieling was the head of Computer Science at University of Mannheim in Germany. During his employment he reviewed the thesis of Michael Becher. He currently serves as a professor at the University of Erlangen-Nurnberg. The IEEE Symposium on Security & Privacy has existed for more than 30 years highlighting developments in computer security and electronic privacy.

Summary. The paper addresses, to some extent, all three security areas of (a) confidentiality, (b) integrity and (c) availability. Definitions are provided for a mobile device within the text. It addresses specifically mobile devices as being controlled by an operating system. A statement is included that directly indicates USB devices are not considered. The paper defines security attack vectors and attack models that can be used to compromise a mobile device. Network communications are addresses, although considerable attention is paid to operating system protection and malicious software that would affect data processing.

Botha, R., Furnell, S. & Clarke, N. (2009). From desktop to mobile: Examining the security experience. *Computers & Security*, *28*(3–4), 130–137.

Abstract. Mobile devices have become more widely used, though the security capabilities are not as powerful or developed as those provided with full-fledged desktop operating system. This paper explores the availability of security mechanisms from the perspective of a user who is security-aware in the desktop environment and wishes to consider using similar protection in a mobile context. The authors are concerned with determining if the same functionality can be found in mobile devices, if it can be used in the same manner and is capable of producing the same results. The discussion is supported by an examination of the Windows XP and Windows Mobile environments, with specific consideration given to user authentication, secure connectivity, and content protection on the devices. The conclusion drawn is that the security features and user experience are less effective than that of a traditional computer.

Credibility. Reinhardt Botha is a professor at the Nelson Mandela Metropolitan University (NMMU) in South Africa. He holds a PhD in Computer Science from Rand Afrikaans University and a post-graduate certificate in higher education from NMMU. Steven Furnell acquired a PhD from the University of Plymouth in the United Kingdom. He is a fellow of the British Computer Society and a senior member of the IEEE. He currently is the head of the School of Computing and Mathematics at Plymouth University. Nathan Clarke is an Associate Professor in Information Security and Digital Forensics at Plymouth University. He has over 20 journal papers, 50 conference papers and 2 books to his credit. Computers & Security is peer-reviewed and the official journal of Technical Committee 11 of the Information Federation for Information Processing.

Summary. The paper addresses the security areas of user authentication, connectivity and content security. These areas could lend the paper useful in each theme of this bibliography: (a) operations that secure stored data on a mobile device, (b) operations that secure mobile device data being processed, and (c) operations that secure mobile device data while it is transferred to and from the device. The paper pertains most directly to the second theme because the analysis is examining the operating system and user experience. While the security technologies are different, the configuration of features is the most important element and the focus of the paper.

Distefano, A., Grillo, A., Lentini, A., & Italiano, G. F. (2010). SecureMyDroid: Enforcing security in the mobile devices lifecycle. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, CSIIRW ’10 (pp. 27:1–27:4). New York, NY, USA: ACM. doi:10.1145/1852666.1852696

Abstract. Mobile devices are now being widely used for both work and personal life. Due to the combination of circumstances there are newer and more serious threats to the security of devices. In this paper the authors provide a life cycle based approach to dealing with mobile devices and their unique security challenges. The approach proposed leverages on a customized release of the mobile device Operating System (OS). Presented is a prototype of a secure mobile device based on a customized release of the Google Android operating system. It is referred to as SecureMyDroid. One of the strong features of this prototype lies in the capability of fully customizing the operating environment of mobile devices. The concept hopes to prevent tampering and the need to configure malware and virus protection.

Credibility. Alessandro Distefano is a PhD student and holds a Masters of Computer Engineering from the University of Rome Tor Vergata. He currently works as a Computer Engineering Professional. Antonio Grillo is a PhD student in Computer science at the University of Rome Tor Vergata. Giuseppe Italiano is a Professor of Computer Science at the University of Rome Tor Vergata and the advisor of student Antonio Grillo. He received his PhD in Computer Science from Columbia University in 1991. Alessandro Lentini holds a Computer Science PhD from the University of Rome Tor Vergata. The Workshop on Cyber Security and Information Intelligence Research (CSIIRW) is published by the Association for Computing Machinery (ACM).

Summary. The paper provides a five phase life cycle format that would be utilized by the device operating system. The phases will include (a) a purchase phase, (b) a set-up phase, (c) a usage phase, (d) a shutdown phase and (e) a disposal phase. During the life cycle the device will move from states of untrusted, trusted and owned. The phases and states of the device are discussed as being capable to provide security for (a) data at rest, (b) processed on the device, and (c) transported or received across a network. All of these aspects of security would be handled by the processing power of the SecureMyDroid operating system.

Kostiainen, K., Reshetova, E., Ekberg, J.-E., & Asokan, N. (2011). Old, new, borrowed, blue –: a perspective on the evolution of mobile platform security architectures, 13–24. doi:10.1145/1943513.1943517

Abstract. The authors of this paper describe the business, regulatory and end-user requirements, which paved the way for this widespread deployment of mobile platform security architectures. Hardware based security mechanisms interact with the operating system and applications within these architectures. In some instances these mechanisms have been adopted from older security architectures. The authors highlight a number of problems in creating an effective mobile security platform. Used within the discussions are the four mobile platforms (a) Symbian, (b) Java ME (c) Android, and (d) MSSF.

Credibility. Karl Kostiainen is a postdoctoral researcher at System Security Group of ETH Zurich. Prior to ETH he worked at Nokia Research Center in Helsinki. He holds a PhD in Computer Science from Aalto University in Helsinki. Elena Reshetova is a doctoral student at the Helsinki University of Technology. Jan-Erik Ekberg works with Nokia Research and the On-Board Credentials open security framework. Asokan is a researcher and Professor of computer science at the University of Helsinki. Asokan holds a PhD from the University of Waterloo. The ACM conference on data and application security and privacy is focused on high-quality research in the development of secure, private, useful and cost efficient information technology systems. The conference is organized and managed by the ACM Special Interest Group on Security, Audit and Control (SIGSAC).

Summary. In order for data to process within a smartphone device operating systems must communicate with hardware. Within the mobile platforms addressed in this paper these security mechanisms include identities, certificates, and trusted roots. The combination of these creates an environment where applications can run and maintain integrity during system processing. The authors feel that many of these platforms were created off of concepts that have been utilized in prior laptop and computing environments. The security mechanisms presented could be utilized in both smartphone and tablet devices.

Schmidt, A.-D., Peters, F., Lamour, F., Scheel, C., Çamtepe, S., & Albayrak, Ş. (2009). Monitoring smartphones for anomaly detection. *Mobile Networks & Applications*, *14*(1), 92–106. doi:10.1007/s11036-008-0113-x

Abstract. The paper demonstrates how to monitor a smartphone running Symbian operating system and Windows Mobile in order to extract features for virus or malware detection. These features are sent to a remote server because running a complex intrusion detection system on this kind of mobile device still is not feasible due to capability and hardware limitations. The authors demonstrate the process of how usage is determined and monitored. Through a monitoring client the system behavior can be monitored. The results of public and self-written malwares are shown. For improving monitoring client performance, Principal Component Analysis was applied which lead to a decrease of about 80% of the amount of monitored features.

Credibility. Professor Sahin Albayrak is the Chief Executive Director of the Distributed Artificial Laboratory (DAI-Labor) at the Technische Universitat Berlin. Aubrey-Derrick Schmidt is a PhD student in Computer and Information Science at Technische Universitat Berlin – DAI-Labor in Berlin, Germany. The article is peer-reviewed in the journal Mobile Networks & Applications. The journal focuses on the symbiosis of portable computers and wireless networks, addressing mobility, computing organization and management.

Summary. The paper discusses a process for detecting malware and viruses on handheld and smartphone devices. The methods in use are focused on a narrow set of operating systems. The process could be expanded and applied to tablet device operating systems; however it would have no use on a USB memory device. Antivirus and malware is capable of affecting a mobile device by (a) slowing the devices processing speed, (b) corrupting information that is being processed, or (c) causing the system to be controlled in some way by another system. System performance is taken into consideration by offloading some of the detection tasks off the system. This provides more system resources to assist in quickening the availability to data. The solution assists in providing integrity of information being processed. The likelihood of system control or data corruption is minimized if antivirus and malware can be identified and mitigated.

Ugus, O., Westhoff, D., & Rajasekaran, H. (2012). A leaky bucket called smartphone. *Pervasive Computing and Communications Workshops, IEEE International Conference on* (Vol. 0, pp. 374–380). Los Alamitos, CA, USA: IEEE Computer Society. doi:http://doi.ieeecomputersociety.org/10.1109/PerComW.2012.6197513

Abstract. The paper presents a discussion of attacks on smartphones and defense countermeasures that can be utilized to protect the device and data. Attack vectors are categorized into three classes according to their characteristics as attacks via application layer, communication layer and operating system layer. This paper is not all encompassing, however it does provide numerous examples of attacks that have been documented and used.

Credibility. Osman Ugus is a research assistant in the Internet Technologies Group at the Hamburg University department of Computer Science. He is pursuing a PhD from HAW Hamburg. Dirk Westhoff holds a PhD in computer science from the University of Hagen. He is co-founder of the European Workshop on Security in Ad Hoc and Sensor Networks. Hariharan Rajasekaran is a Researcher at the AGT Group in Darmstadt, Germany. He is pursuing a MBA from ESSEC Business School and the Mannheim Business School. The IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom) provides presentations and technical forums regarding the fields of study of pervasive computing.

Summary. The paper is packed with examples of smartphone attacks and vulnerabilities. It provides the reader with examples of exploits via application stores, communication protocols and exploits at the operating system level. These exploits are able to jeopardize all three data characteristics of (a) confidentiality, (b) integrity and (c) availability. The majority of the exploits are focused on data while it is being processed in some way. Countermeasures are provided and segmented into three possible device locations: (a) on the smartphone, (b) through the Internet cloud, or (c) through a small internal cloud. The content provided in the paper is applicable to both smartphone and tablet devices.

Verma, I. (2011, August 23). A security analysis of smartphones. Retrieved from http://hdl.handle.net/1805/2630.

Abstract. This work analyzes and discusses the current security environment of today's smartphones, and proposes a security model which will reduce smartphone vulnerabilities, preserving privacy, integrity and availability of smartphone native applications to authorized parties. An overlook is conducted of current smartphone security standards, threats, vulnerabilities and attacks on them that have been uncovered so far with existing popular smartphones. Addressed are potential future uses of the smartphones, and the security threats that these newer applications would introduce. This knowledge is used to construct a mathematical model, which gives way to policies that should be followed to secure the smartphone under the model. Existing and proposed security mechanisms that can be incorporated in the smartphone architecture to meet the set policies are set as recommended security standards.

Credibility. Ishita Verma is employed as a Software Engineer for Symantec. She holds a Master's degree from Purdue University in Electrical and Computer Engineering. Verma has served as a research assistant at Carnegie Mellon and Integrated Nanosystems Development Institute in Indianapolis. Indiana University-Purdue University Indianapolis is Indiana's premier urban university. IUPUIScholarWorks is an institutional digital repository which employs the DSpace open source software (freeware) created by MIT and Hewlett Packard in 2000.

Summary. The thesis presented by Verma provides a thorough discussion of smartphone devices and security. It addresses four different smartphone platforms including the Android, iOS, Symbian and Windows Phone 7. While the focus of the document is an analysis of smartphones, two of the three of these operating system types are applicable to today's table devices. Considerable attention throughout the thesis is paid to the security of data and how it is handled within the phone by the operating system and applications. For each of the four smartphone platforms the author attempts to explain a trusted computing base, trusted computing environment, process capabilities, data confinement and installers. These areas are tied to concepts and security methods such as confidentiality through the Bell-LaPedula model and integrity through the Biba Integrity Model.

Wallach, D. (2011, February 17). Smartphone security: Trends and predictions. *Secure Application Development.* SecAppDev 2011. Leuven, Belgium.

Abstract. It's no exaggeration to say that smartphones, whether RIM's Blackberry, Apple's iPhone, Google's Android, or other models coming out every day, have become ubiquitous in government and in the population at large, and it's no wonder. For the worker on the move, everything from email to calendaring, as well as news and entertainment, is now available in a convenient pocketable device.

Credibility. Dan Wallach is a professor in the department of Computer Science at Rice University. He holds a PhD in computer science from Princeton University. Wallach serves as the associate director of the National Science Foundation's Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE). Secure Application Development (SecAppDev) is a non-profit organization focused on broadening security awareness within the application development community. Materials and courses are provided by leaders in both academia and private enterprise.

Summary. The author discusses the methods by which a number of mobile operating systems are handling applications and data that are being processed as a device is operating. Concepts include the isolation of tasks into separate operating areas that prevent applications and data from interacting with unwanted or malfunctioning software. This is a method for preventing the compromise of and integrity and confidentiality of data. The author addresses the concepts in terms of smartphones, however the concepts are applicable to operating systems that would control tablet devices.

Theme 3 – Operations to Secure Data in Transit

Ashford, W. (2012). Network security controls struggle to keep pace with wireless devices. *Computer Weekly*, 7.

Abstract. The article discusses the proliferation of mobile wireless devices accessing corporate networks and the accompanying security challenges presented to chief information officers. Data leakage is a possible occurrence through lax security efforts and the use of susceptible avenues of data transmission. The author addresses what problems may exist and basic adjustments that would be necessary to created more secure data transmission.

Credibility. Warwick Ashford holds the position as security editor at Computer Weekly. Previously he worked as a technical course developer and technical writer for South African Broadcasting Corporation (SABC). Computer Weekly is a leader in providing news, analysis, opinion, information and services for the United Kingdom IT community.

Summary. The article mainly addresses the concept of data confidentiality. The author discusses how information or data can be intercepted while in transit over wi-fi or unencrypted connections. The use of WPA2 and VPN connections are suggested in the case of Wi-Fi connections. Where possible corporate traffic should be segregated from open public or guest traffic. There should also exist a separation of computing devices traffic from other IP based traffic, such as video devices. This information could be utilized in both smartphone and tablet based computing devices.

Fjermestad, J., Passerini, K., Patten, K., Bartolacci, M., & Ullman, D. (2006). Moving towards mobile third generation telecommunications standards: The good and bad of the “anytime/anywhere” solutions. *Communications of the Association for Information Systems*, *17*(1). Retrieved from http://aisel.aisnet.org/cais/vol17/iss1/3

Abstract. The development of mobile communication and technologies has created a change in the borders between work-life and the workplace. Individuals are now capable of performing many of their tasks from home or outside of the office. Texting and voice conversations were the beginning, but now many organizations are deploying mobile applications that can be used by employees on the move. The authors discuss the evolution to Third Generation/Universal Mobile Telecommunication Systems (UMTS). IT departments need to change their systems, upgrade, and adapt their infrastructure and policies to support these mobile services. This progression may present issues that require answers to some fundamental questions related to privacy, security, and a new concept of work place and work space.

Credibility. Jerry Fjermestad is a Professor of Information Management at the New Jersey Institute of Technology. He holds a PhD in management information systems from Rutgers University. Katia Passerini is an Associate Professor of Management Information Systems at the New Jersey Institute of Technology. She graduated from the George Washington University with a PhD in Information Systems. Karen Patten is an Assistant Professor of Integrated Information Technology at the University of South Carolina and a PhD candidate at the New Jersey Institute of Technology. Michael Bartolacci is an Associate Professor of Information Sciences and Technology at Penn State University. He graduated in 1995 with a PhD in Industrial Engineering and in 1988 with a MBA from Lehigh University. David Ullman is the Associate Provost for Information Services & Technology at the New Jersey Institute of Technology. Communications of the Association for Information Systems (CAIS) has existed for over 10 years and serves to provide new ideas within the IS community through case studies, survey articles and tutorials.

Summary. Within the paper broadband wireless standards are defined and discussed. Addressed are the concepts of availability to information and applications through wireless and cellular connections. Confidentiality issues comprise the majority of the security related issues with these technologies. Discussed are weak password efforts leading to unauthorized access and the interception of data in transit. The authors recommend (a) 2 factor authentication, (b) use of VPN technologies and (c) monitoring of rogue access points and unauthorized traffic.

Goodman, S., & Harris, A. (2010). The coming African tsunami of information insecurity. *Communications of the ACM*, *53*(12), 24–27. doi:10.1145/1859204.1859215

Abstract. The article presents a discussion of the rapid adoption of mobile phone technologies across the African continent, as of December 2010, and predicts that the use of smart phones to facilitate commerce will lead to significant challenges in terms of data security. The potentially revolutionary and beneficial implications of mobile electronic banking for African populations are discussed in terms of personal finance and electronic commerce. However, the associated risks include identity theft, malign electronic surveillance, and the susceptibility of cell phones to both physical and software-based attacks.

Credibility. Seymour Goodman is a Professor of International Affairs and Computing at the Georgia Institute of Technology. Dr. Goodman obtained his PhD from the California Institute of Technology. Andrew Harris is a researcher at the school of International Affairs at Georgia Tech. The Communications of the ACM is a print and online publication for the computing and information technology field. The publication is peer reviewed and has a readership of over 100,000 ACM members.

Summary. The article discusses at a very high level the rapid growth of mobile phones that are capable of data transmission in Africa. The security discussion surrounds data transmission and the basic vulnerabilities that exist based on economic conditions. Currently the devices used are more limited than other higher cost devices found in the developed world. Data confidentiality is addressed through highlight of data in transit during common basic financial transactions. The article focuses on smartphone devices and does not address USB or tablets.

Hafiz, M., & Johnson, R. E. (2006). Security patterns and their classification schemes. *University of Illinois at Urbana-Champaign Department of Computer Science, Tech. Rep*. Retrieved from http://www.munawarhafiz.com/research/patterns/secpatclassify.pdf

Abstract. This paper indicates that solving security problems needs to be assisted by a classification scheme that can be used to group security patterns. A proper scheme can help efficient storage and retrieval of information. There are five schemes that are discussed within the paper which include: (a) the CIA model, (b) application context, (c) the security wheel, (d) the McCumber Cube, (e) threat modeling and (f) hierarchical classification.

Credibility. Munawar Hafiz is a tenure track Assistant Professor working in the Department of Computer Science and Software Engineering at Auburn University. Hafiz studied with Ralph Johnson at the University of Illinois at Urbana-Champaign, earning his PhD in 2010. He is currently the head of the Software Analysis, Transformation and Security research group. His research is funded in part by grants provided by the National Science Foundation (NSF). Ralph Johnson is an Associate Professor at the University of Illinois at Urbana-Champaign. He has co-authored a book on programming design, which was the winner of the 1994 Software Productivity Award.

Summary. The McCumber Cube is presented in the discussion of this paper. A high level conceptual view of the scheme defines how security vulnerabilities and safeguards are mapped in a three- dimensional cube structure. The value of the paper is for this scheme description and its comparison to other methods of classification. Use of the McCumber Cube can be utilized with all three themes that are presented within this bibliography.

Jaha, A. A., Ben Shatwan, F., & Ashibani, M. (2008). Proper virtual private network (VPN) solution. In *The Second International Conference on Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08* (pp. 309 –314). Presented at the Second International Conference on Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08. doi:10.1109/NGMAST.2008.18

Abstract. A virtual private network (VPN) can be defined as a way to provide secure communication between members of a group through use of public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. There are many different VPN solutions out there, and just deciding which one to choose can be difficult since they all have advantages and disadvantages. VPNs can be categorized as Secure or Trusted VPNs, Client-based or Web-based VPNs, Customer Edge-based or Provider Edge-based VPNs, or Outsourced or In-house VPNs. These categories often overlap each other. In order to decide what VPN solutions to choose for different parts of the enterprise infrastructure, the chosen solution should be the one that best meets the requirements of the enterprise. The purpose of this paper is to serve as a basis when creating an enterprise WAN which connects sites and users together using VPN technology. The purpose of creating such a WAN is to allow the resources of a company to be remotely accessed.

Credibility. Ahmed Jaha is an engineer for the Organization for Development of Administrative Centers in Lybia. Majdi Ashibani is the Chairman at Libyan Post, a telecommunication and information technology holding company. The Higher Institute of Industry, Misurata, Libya was founded in 1989 by the Lybian Minstry of Industry. The school is a member of the Association of African Universities. The Second International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST) focuses on technology, application and service development within the mobile and wireless communication industry. The conference brings together experts from the fields of government, industry and academia

Summary. The authors detail and summarize a variety of methods for securing information as it travels to and from a computing device. They do not specifically address devices as being smartphones or tablets, but the concepts can be readily applied to both categories. A virtual private network solution provides confidentiality of data traffic by creating an encrypted secured tunnel where data can pass. This tunnel can be created through the public internet, leased lines or through internal networks. The authors point to the fact that hybrid schemes for VPN setups can be readily used. Their conclusion focuses on a wide area network solution, however the specific information contained within the article can be applied to individual devices.

Kumar Madria, S., Mohania, M., Bhowmick, S. S., & Bhargava, B. (2002). Mobile data and transaction management. *Information Sciences*, *141*(3–4), 279–309. doi:10.1016/S0020-0255(02)00178-0

Abstract. A strong shift to mobile computing has occurred due to advances in wireless or cellular networking technology. This rapidly expanding technology poses many challenging research problems in the area of mobile database systems. The mobile users can access information independent of their physical location through wireless connections. However, accessing and manipulating information without restricting users to specific locations complicates data processing activities. There are computing constraints that make mobile database processing different from the wired distributed database computing. Discussed are the fundamental research challenges particular to mobile database computing, proposed solutions are introduced and challenges are identified. The research areas include mobile location data management, transaction processing and broadcast, cache management and replication and query processing.

Credibility. Sanjay Kumar Madria is a Professor of Computer Science at the Missouri University of Science and Technology. He holds a PhD from the Indian Institute of Technology in Delhi. He has taught at Purdue University, Nanyang Technical University and University Sains Malaysia. He has served as a reviewer of journals including IEEE, IEEE Computer and ACM Internet Computing. Mukesh Mohania holds a PhD in Computer Science and Engineering from Indian Institute of Technology, Bombay. He is employed as a STSM and IBM Master Inventor in the IBM India Software Lab. He has published more than 100 papers and filed more than 30 patents in the areas of distributed databases, data warehousing, data integration and autonomic computing. Sourav S. Bhowmick is an Associate Professor at the Nanyang Technological University's School of

Computer Engineering. He holds a PhD in computer engineering from Nanyang Technological University. Bharat Bhargava is a Professor of Computer Science at Purdue University. He obtained a PhD in Electrical Engineering from Purdue in 1974. This peer-reviewed article is published within Information Sciences. The journal publishes articles that serve researchers, developers and managers in the fields of information, knowledge engineering and intelligent systems.

Summary. The paper addresses the concern of (a) confidentiality, (b) integrity, and (c) availability of data as those pertain to the transmission of database information. The authors approach security and data transfer with the concept that wireless traffic suffers from slower speeds, connection and reliability issues. Instead of storing all database information locally, systems should be configured to pass far fewer amounts of information than would be the case with physical wire connected databases and applications. Detailed data would be transmitted from mobile service stations (MSS) which would contain the detailed data. Much lighter metadata would be used to request the information. The security of the transmission of the data would have to take into account the message origin, destination and path.

Kushchu, I., & Kuscu, H. (2003). From e-government to m-government: Facing the inevitable. In *The 3rd European Conference on e-Government* (pp. 253–260). Retrieved from http://www.mgovservice.ru/upload/uploadfiles/From%20eGov%20to%20mGov.pdf

Abstract: The changes in the Internet and World Wide Web technologies and services lead to new developments in the way e-government efforts provide services to citizens and businesses, and in the way governments handles their internal operations. One of the revolutionary developments comes from adoption of wireless mobile technologies in government related activities: m-government. In this paper technological drivers of m-government are presented through cases where these technologies are in use.

Credibility. Ibrahim Kushchu is an Assistant Professor of eBusiness at the GISM, International University of Japan. He holds a PhD in Cognitive Science and Artificial Intelligence from the University of Sussex, UK. Mehmet Halid Kuscu is the Chief Executive Officer of the Mobile Government Consortium International. He also is an adjunct professor at Southwestern College in the School of Business and Information Systems. The paper was presented at the European Conference on e-Government (ECEG). The ECEG offers a forum for academics, practitioners and researches to discuss, explore and develop theoretical and practical aspects of e-Government.

Summary. Kushchu and Kuscu discuss trends involving mobile technologies within government. They specifically address cases within the realm of public safety, including firefighting and law enforcement. Movement towards services provided outside of the office continues to grow. Productivity increases using these technologies are driving continued adoption. The concern of security of agency information and public information is highlighted. Security issues surround the transmission of data across wireless methods that are more prone to leakage of confidential information.

Mancini, F., Gejibo, S., Mughal, K. A., Valvik, R. A. B., & Klungsoyr, J. (2012). *Secure mobile* *data collection systems for low-budget settings.* Presented at the 2012 Seventh International Conference on Availability, Reliability and Security (ARES). doi:10.1109/ARES.2012.23

Abstract. Lack of infrastructures in health care and transportation, combined with the demand for low cost health services and shortage of medical professionals, are some of the known causes for loss of life in low income countries. Mobile Health (a.k.a. mHealth) is an emerging and promising health service delivery concept that utilizes mobile communication technology to bridge the gap between remotely and sparsely populated communities and health care providers. As sensitive information is stored, exchanged and processed in these systems, issues like privacy, confidentiality, integrity, availability and authentication must be dealt with accordingly. Addressed in this paper are the challenges in securing Mobile Data Collection Systems deployed in remote areas and in low-budget settings.

Credibility. Federerico Mancini is an Associate Professor in the Programming Theory group at the University of Bergen in Norway. He holds a PhD from the Universita degli studi Roma Tre in Computer Engineering. Khalid Azim Mughal is an Associate Professor in the Department of Informatics at the University of Bergen. Samson Hussien Gejibo is a PhD candidate in the Department of Informatics at the University of Bergen. Jorn Klungsoyr is a PhD candidate in the Centre for International Health at the University of Bergen. Remi Andre B. Valvik is a Masters Student at the University of Bergen. The International Conference on Availability, Reliability and Security (ARES) is ranked 17th on the

Google Scholar list of all Computer Security and Cryptography publications. The conference brings together researchers and practitioners in the area of digital dependability.

Summary. The paper discusses less than traditional methods for creating secure transmission of information within a medical data application. The authors discuss how many web-based applications utilize https technology to create an encrypted communication of data. The problem they attempt to address is when this solution is unacceptable due to certificate availability and device limitations. Mobile device certificate authorities are preinstalled on the phones and may not be standardized. Alternative keyed encryption methods are considered and presented. The solutions presented address all three concerns of (a) confidentiality, (b) integrity, and (c) availability of data that must be transmitted through cell or wireless connections.

Milligan, P. M., & Hutcheson, D. (2007). Business risks and security assessment for mobile devices. In *Proceedings of the 8th Conference on 8th WSEAS Int. Conference on Mathematics and Computers in Business and Economics - Volume 8* (pp. 189–193). Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS). Retrieved from http://dl.acm.org/citation.cfm?id=1347862.1347873

Abstract. Technology advances over the past decade have elevated business risk from mobile devices to an unparalleled high. The relationships between security, business risks, and their corresponding costs are increasingly complex. Corporate security measures have lagged behind the need for protection. Bottom line security relies on the individual business professional is ethics and diligence in protecting confidential corporate, market, and customer information. This paper identifies and compares the various business risks, assesses prevalent security solutions, and analyzes the total cost of corporate mobile technology.

Credibility. Patricia Mayer Milligan is an Associate Professor at Baylor University in the Department of Information Systems. Dr. Milligan holds a PhD in Computer Science from the University of North Texas. Donna Hutcheson is the Director of IT Audit at TXU Corporation in Dallas, Texas. The World Scientific and Engineering Academy and Society is an international organization that promotes the development of computational techniques and mathematical methods in science and engineering. Collaboration is conducted with universities and scientific organizations throughout the world at their annual conferences.

Summary. The authors examine all three sets of devices addressed within this annotated bibliography. The devices include (a) smartphones, (b) tablets, and (c) USB flash memory. The paper provides a high level, but well-rounded examination of potential risks and security issues that exist for mobile devices. Possible security improvements are divided into categories and provided for the reader. Network-based issues are provided as one of the category headings. The authors indicate four improvements that will assist in securing the transfer of data which include (a) tracking rogue wireless devices, (b) disallowing peer-to-peer wireless connection, (c) implementing controls for ad-hoc services, and (d) conducting real time network audits.

O’Neal, M. R., Dixon, J. S., Naval Postgraduate School (U.S.), & Naval Postgraduate School

(U.S.). Graduate School of Business and Public Policy (GSBPP). (2011). *Department of Defense Strategic and Business case analyses for commercial products in secure mobile computing*. Naval Postgraduate School, Monterey, California.

Abstract. The Department of Defense (DoD) lags behind commercial entities in terms of adopting mobile computing technologies. Commercial smartphones offer scalable solutions to meet requirements ranging from business functions to tactical operations; however, these solutions require considerations beyond those applicable to the commercial sector. This research identifies whether potential solutions may contribute to three objectives: 1) reduce the DoD’s currently high device and service costs; 2) increase the DoD’s smartphone functionality; 3) maintain or increase the level of security functionality available in commercial devices for DoD.

A strategic analysis of the commercial mobile communications industry highlights the business drivers and motivations of industry participants. This information is used to identify the DoD’s strategic options, which, in turn, serve as the basis of business cases for adopting future smartphone capabilities. Business case analyses compare proposed cost models with the cost models for current smartphone implementations.

Credibility. Matthew R. O’Neal holds a Master of Science in Physics from the Naval Postgraduate School in Monterey, California. He is currently employed as a Physicist at the Naval Surface Warfare Center in Washington, D.C. Joshua Dixon holds a Master of Business Administration and a Master of Science in Computer Science from the United States Naval Postgraduate School. He currently serves as a Captain in the United States Marine Corps. The Naval Postgraduate School is a fully accredited graduate school focused on providing advanced education and research programs that increase the combat effectiveness of the United States Naval Services.

Summary. The report details in considerable length the consideration of using custom off the shelf commercial smartphones for military application. As one of the research questions the authors attempt to answer the benefits and risks associated with the use of these devices. A secure mobile encrypted portable electronic device (SME PED) is a device that exists in the military and incorporates security features such as anti-tamper design, end-to-end cryptography and hardware separation. The authors believe that these devices exist due to the inability to acquire commercial products. Trustchip, created and sold by the company Koolspan, is an interface solution that is addressed to secure data while it is in transit. These types of technologies have been used by corporations, government and law enforcement to provide some of the same security features available in a SME PED. The report addresses the three areas of (a) confidentiality, (b) integrity, and (c) availability in its discussion of risk, threat and vulnerability assessment. The report is focused on smartphone devices that communicate with cellular networks. USB and tablets are not addressed.

Straus, S., Bikson, T., Balkovich, E., & Pane, J. (2010). Mobile technology and action teams: Assessing BlackBerry use in law enforcement units. *Computer Supported Cooperative Work (CSCW), 19*(1), 45–71.

Abstract. A research study was conducted using RIM BlackBerries for approximately 650 squad members for a law enforcement agency within the state of California. The researchers were primarily interested in the effectiveness of the devices in providing communication and information for sets of law enforcement teams. The trials provided an opportunity to assess acceptance, use, and perceived performance benefits of the technology. Data was collected from semi-structured interviews, user surveys, and system logs.

Credibility. Dr. Susan Straus holds a PhD from the University of Illinois at Urbana-Champaign. She is a senior behavioral scientist at the RAND Corporation. Tora Bikson is the chair of the Human Subjects Protection Committee at the RAND Corporation. She holds a PhD in Psychology form the University of California, Los Angeles and a PhD in philosophy from the University of Missouri. Edward Balkovich has a doctorate in electrical engineering and computer science from the University of California, Santa Barbara. He is a senior information scientist at the RAND Corporation. Dr. John Pane is also a Senior Information Scientist at the RAND Corporation. He holds a PhD in computer science from Carnegie Mellon University. Computer Supported Cooperative Work is an ACM Conference focused on presenting research in the field of technology design and its effects on organizations and networks.

Summary. The security concerns that are addressed within the study pertain to the interception of information while in transit. Noted within the research results is concern that the sensitive law enforcement information transmitted from device to device could lose its data confidentiality. The researchers note that security is implemented through the use of complex and lengthy passwords for device authentication. Data traffic is also segmented from internal agency computer traffic to provide an extra layer of security while information is in transit. Only one type of device, the RIM Blackberry smartphone, is addressed within the study.

US Department of Commerce, N. (2011, February 17). Glossary of key information security terms. Retrieved December 5, 2012, from http://www.nist.gov/manuscript-publication-search.cfm?pub_id=907638

Abstract. This glossary of key information security terms has been extracted from NIST Federal Information Processing Standards (FIPS), Special Publication (SP) 800 series, NIST Interagency Report (NIST IR) series, and the Committee for National Security Systems Instruction (CNSSI) 4009 (Information Assurance Glossary). The terms included are not all inclusive of terms found in these publications, but are a subset of those most frequently used. The purpose of this glossary is to provide a central resource of definitions most commonly used in NIST and CNSS publications. Each entry in the glossary points to one or more source NIST or CNSS publications, and in addition, other supplemental sources where appropriate. As we are continually refreshing out publication site, terms included in the glossary come from out more recent publications.

Credibility. The U.S. Department of Commerce promotes job creation, economic growth, sustainable development and improved standards of living for all Americans by working in partnership with businesses, universities, communities and our nation’s workers. The department manages a wide range of responsibilities in the areas of trade, economic development, technology, entrepreneurship and business development, environmental stewardship, and statistical research and analysis. The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Summary. The publication provides a reference document that defines terms and concepts associated with security practices, devices, and technologies securing data. Many of the terms can be applied within the three themes of the annotated bibliography. Terms such as encryption, Wi-Fi, VPN and certificate management clarify discussions involved with security while data is in transit. Definitions are supported by and linked to other United States federal standards documents.

Violino, B. (2012). A calculated risk. *Computerworld, 46*(17), 31-32.

Abstract. The article discusses how information technology (IT) executives are making strategies to manage the risk associated with the increasing number of mobile devices at companies. Several companies have launched mobile strategies to handle the risks. Chicopee Savings Bank in Massachusetts is planning to adopt a bring-your-own-device (BYOD) program to minimize the cost of providing smartphones. HomeTown Bank is planning to use a software-as-a-service mobile device management tool.

Credibility. Bob Violino is a freelance writer and editor that has covered information technology for more than 25 years. He was employed as the senior editor at CMP for 11 years and has written as a freelance writer for the past 11 years. He has written for industry publications such as CFO Magazine, CIO magazine, Computerworld, Eweek, InformationWeek and Secured magazine. Computerworld is a leading source of technology news and information. The magazine has existed for more than 40 years and is a subsidiary of Thompson Reuters.

Summary. The article discusses the effort to manage risk associated with mobile devices. Several internal organizational policies regarding the devices are addressed. Bring your own device (BYOD) is highlighted as a use policy that is being implemented at banks and healthcare providers. The specifics of the policies address data that may be stored within the device. In an effort to maintain confidentiality of information, policies are developed to allow the organization to ensure password protection, encryption and remote wiping of devices. Employees of organizations must commit to these restrictions and sign documentation that indicates there has been agreement of understanding and acknowledgement.

Wang, Y., Streff, K., & Raman, S. (2011). Security threats and analysis of security challenges in smartphones. *Computer, 99*(1), 1.

Abstract. A smartphone carries a substantial amount of sensitive data and thus is very attractive to hackers, making it an easy target. For these reasons, ensuring smartphone security is extremely important. While there are many similarities between smartphone security and regular security, distinct differences exist between these two. The unique characteristics of smartphones make securing them very challenging. In this paper, we summarize smartphone threats and attacks, reveal the unique characteristics of smartphones, evaluate their impact on smartphone security, and explore the countermeasures to overcome these challenges. Many enterprises have started to look into security issues in smartphones. However, these solutions must correspond with the unique characteristics in smartphones. New business models are highly desired to solve security issues in smartphones.

Credibility. Yong Wang is an Assistant Professor and senior researcher in the Information Assurance department at Dakota State University. He holds a PhD in computer science from the University of Nebraska, Lincoln. Dr. Kevin Streff is an Associate Professor and Director of the Center for Information Assurance at Dakota State University. Sonell Raman is a graduate student at Dakota State University majoring in Database Management. Computer is a peer-reviewed publication that provides technical content of all aspects of computer science. It is the flagship publication of the IEEE Computer Society.

Summary. Wang, Streff and Raman provide a wide and high level analysis of dangers and security issues associated with smartphones. The focus of their discussion within the article is on smartphone devices; however a number of the attacks, impacts and features could pertain to tablet devices. The authors use a model to divide the smartphone into three separate layers consisting of an application layer, communication layer and a resource layer. Nine separate forms of device attacks are described for the reader. The article directly addresses the need for any security features implemented to provide either (a) confidentiality, (b) integrity or (c) availability.

Weier, M. (2009). What goes mobile? *Informationweek*, 20-26.

Abstract. The article reports on the use of iPhone's application on businesses and different fields. It talks on the way General Motors Corp. uses smartphone's application to complete sale or lease transaction for its Chevrolet Cruze without coming to a dealership. Oklahoma Heart hospital uses a Blackberry to monitor the patient's heart by sending a visual image of it. The police at Los Angeles Sheriff's Department utilize the Blackberry to take photos of gang-related graffiti and search for fingerprints.

Credibility. Weier is the Senior Managing Editor of Corporate Content at Workday. She assumed this position after working for InformationWeek from 1994 to 2010. She is an award-winning journalist with over 20 years’ experience writing about business and information technology. InformationWeek has existed for more than 30 years and is a leading industry provider of information for industry professionals. Content is provided through website, blogs and magazine covering current technologies and strategies in the field of information technology.

Summary. The article addresses four distinct situations where smartphones are being utilized to conduct business. One scenario addresses the use of Blackberry devices within a criminal justice agency. The devices are utilized to capture photographs, fingerprints and access warrant information regarding suspects. Within the article are high level discussions of methods used to update devices and provide reliable communications with back-end servers. These situational descriptions provide a reference for real world applications that should assist in data availability. The situations highlight both the use of cellular and Wi-Fi connections being used by smartphone devices. The concepts could also be applied to tablet devices.

Conclusion

The annotated bibliography contains 32 references that support an analysis of operations that could serve to develop secure mobile data policies within a US criminal justice agency. The organization of information within this annotated bibliography is driven by how information contained within the references serves to answer the central research question: How can a criminal justice agency establish confidentiality, integrity and availability (i.e., security) of information that is stored, processed, or transmitted on a mobile device (USB flash memory device, mobile smartphone, and mobile tablet)?

The model developed by John McCumber, referred to as the McCumber Cube, is used to determine and organize appropriate security policies based on the intersection of information states with information characteristics (Myers, 2010). Information states are defined as the concepts of data (a) while in storage (Lee, Yim, & Lee, 2010), (b) while being processed (Wang, Streff, & Raman, 2011) or (c) while in transmission (Milligan & Hutcheson, 2007). Information characteristics are organized by three security concepts of (a) confidentiality, (b) integrity, and (c) availability (McCumber, 2005, p. 103). The goal is to identify industry-recognized operations that could best help information technology personnel avoid vulnerabilities and risks when developing procedures for securing mobile data.

Confidentiality. This information security characteristic is defined by McCumber (2005) as the effort of "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information" (2005, p. 18). Criminal justice information and personally identifiable information used within a law enforcement agency is considered sensitive (CJIS Security Policy Resource Center, 2012). The distribution of information to unauthorized parties can lead to difficulties in investigations and the decrease in security of criminal justice personnel.

Integrity. This information security characteristic refers to the ability to guard against "improper modification or destruction and includes ensuring information nonrepudiation and authenticity" (McCumber, 2005, p. 18). In other words, data should remain in its original or intended state. Unauthorized adjustments or corruption to data causes the integrity of the data to become compromised. According to Wallach (2011), policies must be developed and implemented that ensure that data is correct and remains uncorrupted.

Availability. This information security characteristic is involved in "ensuring timely and reliable access to and use of information" (US Department of Commerce, 2011, p. 18). Systems are intended to access data efficiently and on demand. Straus, Bikson, Balkovich, & Pane (2010) state that downtime or inaccessibility to data at any state that it currently exists hampers the availability of criminal justice agencies in locating suspects and solving crimes.

Three distinct mobile data devices are addressed within this study: (a) USB flash memory devices (Lee, Yim, & Lee, 2010), (b) mobile smartphones (Wang, Streff, & Raman, 2011) and (c) mobile tablets (United States Government Accountability Office, 2012). Universal Serial Bus (USB) flash memory devices are very light storage devices weighting about 30g and small enough to easily into a person's hand (Lee, Yim, & Lee, 2010). Emerging in around the year 2000, USB devices became popular as a personal storage device due to their relatively small size and large data capacity (Tetmeyer & Saiedian, 2010). Mobile smartphones can be defined as "a category of mobile device that provides advanced capabilities beyond a typical mobile phone; running complete operating system software that provides a standardized interface and platform for application developers" (Verma, 2011, p. 1). The ever-increasing popularity of these devices is staggering with a nearly 200% increase in sales during one year alone (Becher et. al., 2011). Mobile tablets can be considered a personal computer with a touch screen that is smaller than a laptop computer while a bit larger than a smartphone (United States Government Accountability Office, 2012). The popularity of these devices is noted by the fact that 19% of American adults owned a tablet as of 2012 (United States Government Accountability Office, 2012).

The rapid proliferation of devices that enable data and information to be utilized outside of the traditional workspace or office brings with it an increase in security issues (Violino, 2012). As an example, malware intended for use on mobile devices has risen 185% in less than one year's time (United States Government Accountability Office, 2012). There exists considerable pressure on agency management and information management departments to embrace and utilize these devices (Wallach, 2011). Security risks must be understood and thoughtful security policies must be used to prevent leakage, destruction or corruption of sensitive criminal justice information (McCumber, 2005).

Operations to Secure Data at Rest

USB flash memory mobile devices. References cited in the bibliography support the notion that significant risk is incurred in USB devices when the data is at rest (Kleidermacher, 2010). The operations that can assist in the mitigation of risks are highlighted in Table 1 (see below). One risk that arises with any mobile device is the physical loss of the device because the potential exists for an unauthorized individual who acquires the device to extract the data at will (Tetmeyer & Saiedian, 2010). To prevent that occurrence a form of encryption can be implemented on the device or the data contained within. Kleidermacher (2010) proposes several distinct types of encryption which include (a) full-disk encryption, (b) a self-encrypting drive, (c) block layer manager encryption, or (d) encryption at the file system layer. In the situation where a device is provided or acquired by another individual there should exist a proper policy to ensure previous information is completely removed from the device. Sun et al. (2008) provide an examination of the use of block cleaning and zero overwriting to achieve proper data deletion. Security regarding integrity of data on a USB device is assisted by a form of user authentication (Tetmeyer & Saiedian, 2010). System logging can also be enabled to gain an understanding of who and when the device was accessed (Tetmeyer & Saiedian, 2010). This provides the owner an understanding of whether or not the data contained within the device has maintained its original integrity or if it has been changed (Mislan, Casey & Kessler, 2010). Concern over the introduction of viruses that would corrupt or alter data can be prevented at some level by a policy that would prevent auto-run or auto-mounting of a USB device when it is plugged into a system (Tetmeyer & Saiedian, 2010).

Lee, Yim and Lee (2010) suggest that user convenience should be taken into consideration when securing the USB device. Their paper highlights a method for a simple form of user authentication, taking into consideration the need for password recovery and rapid availability to data.

Table 1

USB operations that can secure stored data.

USB flash memory devices	**Data Stored at Rest**
Confidentiality	• Hardware layer: Full-disk encryption (FDE) • FDE self-encrypting drive (SED) • Block layer manager encryption • File system layer encryption • User authentication

	- Blocking of auto-run - Proper deletion of flash memory
Integrity	- User authentication - Device logging
Availability	- Password recovery

Mobile smartphones. Many of the considerations addressed for USB flash memory mobile devices are also pertinent to smartphones. A summary of the security operations is contained in Table 2 (see below). Encryption should be enabled in some form to prevent the extraction of data if the device falls into the possession of an untrusted party. User authentication and device logging are still needed to ensure that the data stored within the device remains with its original integrity (Mislan, Casey & Kessler, 2010).

Additional concepts that are addressed in references selected for use in this study, only in regard to smartphones, include self-destructing data (Yue, Wang & Liu, 2010), data separation (Seifert et al., 2010) and the ability to triage (Mislan, Casey & Kessler, 2010). Within the realm of criminal justice efforts there exists the need to extract information from mobile devices (Mislan, Casey & Kessler, 2010). Organizations need to have the proper equipment that is capable of extracting data from devices through a process known as on-scene triage (Mislan, Casey & Kessler, 2010). However, while criminal justice agencies are interested in extracting criminal information from devices, it is not desirable for criminals to be able to extract their information. Yue, Wang and Liu (2010) present a method by which sensitive data can be set to self-destruct and prevent theft in case encryption methods are breached. Devices are being developed that provide the ability to separate data stores and usage (Seifert et al., 2010). By separating data stores through secure methods the potential exists to use a single device for criminal justice activities as well as personal use. This ability provides confidentiality through the denial of access to sensitive information. It also provides availability to data that would otherwise require two devices or the intermixing of secure and insecure data.

Table 2

Smartphone operations that can secure stored data.

Mobile smartphones	Data Stored at Rest
Confidentiality	• Hardware layer: Full-disk encryption (FDE) • FDE self-encrypting drive (SED) • Block layer manager encryption • File system layer encryption • User authentication • Self-destructing data • Data separation
Integrity	• User authentication • Device audit logging
Availability	• Triage • Data separation

Mobile tablets. None of the materials included in this annotated bibliography directly address mobile tablets in the discussion of security techniques or methods. However, many of the methods described for USB and mobile phone devices are applicable to tablets and are addressed in Table 3 (see below). A number of operating systems and file systems of smartphones and tablet devices are extremely similar (O’Neal & Dixon, 2011). Hardware devices, such as hard drives, are also similar. These devices can be secured through many of the same techniques including encryption (Kleidermacher, 2010), user authentication (Mislan, Casey & Kessler, 2010, and audit logging (Tetmeyer & Saiedian, 2010).

Table 3

Mobile tablet operations that can secure stored data.

Mobile tablets	Data Stored at Rest
Confidentiality	• FDE self-encrypting drive (SED) • Block layer manager encryption • File system layer encryption • User authentication • Self-destructing data
Integrity	• User authentication • Device audit logging
Availability	• Not addressed in the bibliography

Operations to Secure Data Being Processed

USB flash memory devices. USB flash memory devices remain outside of the scope of operations to secure data being processed because these types of devices do not have built in processing capabilities and are not capable of such tasks (Tetmeyer & Saiedian, 2010). Due to the nature of these devices they are not addressed in this theme of the bibliography.

Mobile smartphones. Included in Table 4 (see below) are security operations that are capable of securing smartphone data while it is being processed. Allam and Flowerday (2010) discuss the security awareness boundary model that assists in understanding a balance between the effort involved in securing a device and an individual’s awareness of how the device functions. The use of security settings to secure data processing requires knowledge of how to configure them within an operating system. Security settings assist in data confidentiality of any data processing through the device. According to Allam and Flowerday (2010), if a security setting is preventing access to legitimate data then the level of availability is less than acceptable. If it is extremely difficult to configure security settings then the user will not likely enable those settings. A properly self-configuring device with user feedback will most appropriately create the balance that is needed (Allam & Flowerday, 2010).

Smartphone devices utilize operating systems that are capable of isolating the processing involved in the use of applications (Wallach, 2011). Unfortunately applications may be installed on a device that has either vulnerabilities allowing malware to enter the system or malware that is embedded within the application (Becher et al., 2011). Policies should exist that require that applications are provided by a reputable creator and include a signed source to limit the exposure to incidents of confidentiality loss (Verma, 2011). Traditional malware detection is difficult on a smartphone device, even if properly designed, due to the limited processing power of the devices (Becher et al., 2011). It is possible to offload the processing of these tasks to other centralized servers or cloud technologies (Ugus, Westhoff, & Rajasekaran, 2012). If offloading services to an offsite cloud provider is considered infeasible from a security perspective, antivirus and rootkit detection can be performed in a local small cloud configuration (Ugus, Westhoff, & Rajasekaran, 2012).

Authentication into mobile device operating systems must deal with the balance between efficiency and confidentiality (Botha, Furnell, & Clarke, 2009). Traditional user passwords are inefficient on these smaller form factor devices and shortened logins consisting of only numbers are more susceptible to attack (Botha, Furnell, & Clarke, 2009). Operating system and application logons should involve multiple forms of authentication to provide access to these areas of data.

It is apparent that smartphone security bugs will continue to proliferate and be eventually discovered (Becher et al., 2011). Proper update procedures should be considered and evaluated. Operations that effectively update devices are able to assist confidentiality by removing vulnerabilities exposed during data processing. These same operations would increase availability if the installation process is efficient and free from errors. Becher et al. (2011) feel that these exact procedures are still a focus for future research.

Table 4

Smartphone operations that can secure data being processed.

Mobile smartphones	Data being processed
Confidentiality	• Self-regulatory system and feedback • Application signatures • Proper browser design • Malware detection • Update procedures • Process isolation • Limited privileges • Device security phases • Multiple authentication methods
Integrity	• Malware detection • Process isolation • Limited privileges • Security integrity patterns
Availability	• Self-regulatory system and feedback • Proper system design • Malware detection • Update procedures • Process isolation • Limited privleges

Mobile tablets. The processing of data is similar between smartphones and mobile tablets; in many cases the operating systems are identical and hardware does not differ drastically (O’Neal & Dixon, 2011). Due to the basic similarities, all of the security operations associated with data being processing are identical between smartphones and mobile tablet devices. These operations are summarized in Table 5 below.

Table 5

Mobile tablet operations that can secure data being processed.

Mobile tablets	Data being processed
Confidentiality	• Self-regulatory system and feedback • Application signatures • Proper browser design • Malware detection • Update procedures • Process isolation • Limited privileges • Device security phases • Multiple authentication methods
Integrity	• Malware detection • Process isolation • Limited privileges • Security integrity patterns
Availability	• Self-regulatory system and feedback • Proper system design • Malware detection • Update procedures • Process isolation • Limited privileges

Operations to Secure Data in Transit.

USB flash memory devices. USB device data is transmitted through a physical connection to another system. The transfer of information does not occur through Ethernet cables, cellular or Wi-Fi connection. The references selected for use within the bibliography address only these forms of data traffic. Therefore, the connection scenario utilized by USB devices is not addressed.

Mobile smartphones. Data transferring to or from a smartphone device is capable of traveling through either a cellular connection or through a wireless Wi-Fi connection. In any wireless transmission scenario there exists the potential for data leakage (Kushchu & Kuscu, 2003). Operations that secure the data while traveling should address a form of authentication and encryption, as noted in Table 6 below. Authentication when possible should be implemented with multiple factors (Fjermestad et al., 2006). Encryption can be accomplished through a variety of methods and does not necessarily require a high cost for implementation and utilization (Mancini, Gejibo, Mughal, Valvik, & Klungsoyr, 2012). Use of both of these techniques, proper encryption and authentication, will assist in insuring all three information characteristics (a) confidentiality, (b) integrity and (c) availability. Smartphones utilizing Wi-Fi should utilize at a minimum WPA2 to encrypt each wireless session (Ashford, 2012). Wi-Fi Protected Access 2 is a wireless security implementation that meets the IEEE 802.11i security standard (US Department of Commerce, 2011).

One efficient method for creating a secure encrypted wireless connection is the use of a Virtual Private Network (VPN) (Ashford, 2012). A VPN connection provides an encrypted tunnel between two devices where data can securely be transmitted in both directions (Fjermestad et al., 2006). Jaha, Shatwan, and Ashibani (2009) provide a variety of forms of VPN systems, which include secure, trusted, client-based, web-based, customer edge-based or provider edge-based. The selection of a VPN depends on the scenario and connection type (Jaha, Shatwan, & Ashibani, 2009).

Table 6

Smartphone operations that can secure data in transit.

Mobile smartphones	Data in transit
Confidentiality	• Authentication • Virtual Private Networks • Monitor for rogue access points • Wi-Fi Encryption • End-to-end cellular encryption

Integrity	• Two factor authentication • Wi-Fi Encryption • End-to-end cellular encryption
Availability	• Monitor for rogue access points • Database traffic transfer • Wi-Fi Encryption • End-to-end cellular encryption

Mobile tablets. A cellphone is defined as having the ability to make and receive phone calls through a radio network (United States Government Accountability Office, 2012). Some mobile tablets utilize cellular technologies for data transfer; however they are defined as a portable computer between the sizes of smartphones and laptop computers (United States Government Accountability Office, 2012). Within the operations addressed in this theme only Wi-Fi capabilities are presented (see Table 7 below). The Wi-Fi security operations applied to smartphones (see Table 6 above) are the same and are applied in the same methods.

Table 7

Mobile tablet operations that can secure stored data.

Mobile tablets	Data in transit
Confidentiality	• Authentication • Virtual Private Networks • Monitor for rogue access points • Wi-Fi Encryption
Integrity	• Two factor authentication • Wi-Fi Encryption
Availability	• Monitor for rogue access points • Database traffic transfer • Wi-Fi Encryption

References

About Us | Orange County Gov FL. (2012). Retrieved November 6, 2012, from http://www.ocfl.net/AboutUs.aspx

Allam, S. & Flowerday, S. (2011, August 15). An adaptation of the awareness boundary model towards smartphone security. *Information Security South Africa (ISSA)*, 1-8.

Ashford, W. (2012). Network security controls struggle to keep pace with wireless devices. *Computer Weekly*, 7.

Becher, M., Freiling, F., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. *IEEE Symposium on Security and Privacy*. (Vol. 0, pp. 96–111). Los Alamitos, CA, USA: IEEE Computer Society. doi:http://doi.ieeecomputersociety.org/10.1109/SP.2011.29

Botha, R., Furnell, S. & Clarke, N. (2009). From desktop to mobile: Examining the security experience. *Computers & Security*, *28*(3–4), 130–137.

Brown, E. (2012, October 31). NIST provides draft guidelines to secure mobile devices. *NIST Tech Beat.* Retrieved from http://www.nist.gov/itl/csd/mobile-103112.cfm.

Brown-Syed C. (2010). Keeping tabs: The potential of tablet computers during crises. *Library and Archival Security*, *23*(2), 141–142.

Busch, C., Mare, P. S., Flynn, T., Kellum, R., Le, S., Meyers, B., & Palmquist, M. (2013). *Content Analysis. Writing@CSU*. Retrieved from Colorado State University: http://writing.colostate.edu/guides/guide.cfm?guideid=61.

Corbin, K. (2012, August 23). BYOD security demands mobile data protection strategy. *CIO.*

Retrieved from http://www.cio.com/article/714550/BYOD_Security_Demands_Mobile_Data_Protection_Strategy?page=2&taxonomyId=3095.

CJIS Security Policy Resource Center. (2012). *FBI*. Retrieved November 6, 2012, from http://www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy

Creswell, J. (2009). *Research design: Qualitative, quantitative and mixed methods approaches.* (3rd ed.). Los Angeles: Sage.

Daunt, M. (2007). Security protection is needed when using USB sticks. *BMJ: British Medical Journal (International Edition)*, *335*(7611).

Distefano, A., Grillo, A., Lentini, A., & Italiano, G. F. (2010). SecureMyDroid: Enforcing security in the mobile devices lifecycle. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, CSIIRW '10 (pp. 27:1–27:4). New York, NY, USA: ACM. doi:10.1145/1852666.1852696

Dreger, R., & Moerschel, G. (2008). Inside smartphone security. *Informationweek*, *1062008*(1205).

Finneran, M. (2012). Mobile security gaps abound. *Informationweek*, *5142012*(1333).

Fjermestad, J., Passerini, K., Patten, K., Bartolacci, M., & Ullman, D. (2006). Moving towards mobile third generation telecommunications standards: The good and bad of the "Anytime/Anywhere" solutions. *Communications of the Association for Information Systems*, *17*(1). Retrieved from http://aisel.aisnet.org/cais/vol17/iss1/3

Florida Department of Law Enforcement. (2012). Retrieved November 6, 2012, from http://www.fdle.state.fl.us/Content/getdoc/cec8518d-db81-437b-8b7d-821dc8c28cda/CJIS-Home-Page.aspx

Goodman, S., & Harris, A. (2010). The coming African tsunami of information insecurity. *Communications of the ACM*, *53*(12), 24–27. doi:10.1145/1859204.1859215

Goth G. (2012). Mobile security issues come to the forefront. *IEEE Internet Comput IEEE Internet Computing*, *16*(3), 7–9.

Hafiz, M., & Johnson, R. E. (2006). Security patterns and their classification schemes. *University of Illinois at Urbana-Champaign Department of Computer Science, Tech. Rep*. Retrieved from http://www.munawarhafiz.com/research/patterns/secpatclassify.pdf

iPad in the enterprise tablets are unleashing new mobile apps but require IT support and updated security policies, too. (2010). *Informationweek.*, (1286), 49.

Jaha, A. A., Ben Shatwan, F., & Ashibani, M. (2008). Proper virtual private network (VPN) solution. In *The Second International Conference on Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST ’08* (pp. 309 –314). Presented at the Second International Conference on Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST ’08. doi:10.1109/NGMAST.2008.18

Kleidermacher, D. (2012). Enhance system security with better data-at-rest encryption. *Embedded Systems Design*, *25*(3), 19-23.

Kostiainen, K., Reshetova, E., Ekberg, J.-E., & Asokan, N. (2011). Old, new, borrowed, blue –: a perspective on the evolution of mobile platform security architectures, 13–24. doi:10.1145/1943513.1943517

Kumar Madria, S., Mohania, M., Bhowmick, S. S., & Bhargava, B. (2002). Mobile data and transaction management. *Information Sciences*, *141*(3–4), 279–309. doi:10.1016/S0020-0255(02)00178-0

Kushchu, I., & Kuscu, H. (2003). From E-government to M-government: Facing the inevitable.

In *The 3rd European Conference on e-Government* (pp. 253–260). Retrieved from http://www.mgovservice.ru/upload/uploadfiles/From%20eGov%20to%20mGov.pdf

Labaree, R. (2012). LibGuides. Organizing your social sciences research paper. The literature review. Retrieved from http://libguides.usc.edu/content.php?pid=83009&sid=615851.

Leavitt N. (2011). Mobile security: Finally a serious problem? *Computer, 44*(6), 11–14.

Lee, S.-H., Yim, K.-B., & Lee, I.-Y. (2010). A secure solution for USB flash drives using FAT file system structure. *Network-Based Information Systems, International Conference on* (Vol. 0, pp. 487–492). Los Alamitos, CA, USA: IEEE Computer Society. doi:http://doi.ieeecomputersociety.org/10.1109/NBiS.2010.30

Lemos, R. (2010). Security's gaping hole: USB flash drives. *Informationweek*, 14.

LSU Libraries. (2012). *Evaluation of information sources part II, evaluation criteria.* Retrieved from http://www.lib.lsu.edu/instruction/evaluation/evaluation20.html.

Mancini, F., Gejibo, S., Mughal, K. A., Valvik, R. A. B., & Klungsoyr, J. (2012). *Secure mobile data collection systems for low-budget settings.* Presented at the 2012 Seventh International Conference on Availability, Reliability and Security (ARES). doi:10.1109/ARES.2012.23

McCumber, J. (2005). *Assessing and managing security risks in IT systems.* Boca Raton, FL: Aurebach Publications.

Myers Jr, J. P., & Riela, S. (2008). Taming the diversity of information assurance & security. *Journal of Computing Sciences in Colleges*, *23*(4), 173–179.

Milligan, P. M., & Hutcheson, D. (2007). Business risks and security assessment for mobile devices. In *Proceedings of the 8th Conference on 8th WSEAS Int. Conference on Mathematics and Computers in Business and Economics - Volume 8* (pp. 189–193).

Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS). Retrieved from http://dl.acm.org/citation.cfm?id=1347862.1347873

Mislan, R. P., Casey, E., & Kessler, G. C. (2010). The growing need for on-scene triage of mobile devices. *Digital Investigation*, *6*(3–4), 112–124. doi:10.1016/j.diin.2010.03.001

National Institute of Standards and Technology. (2011, March) *Managing Information Security Risk: Organization, Mission, and Information System View.* Special Publication 800-39. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

National Institute of Standards and Technology. (2012, July 10). *DRAFT Guidelines for Managing and Securing Mobile Devices in the Enterprise.* Special Publication 800-124 Revision 1. Retrieved from http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf.

NCJRS Abstract - National Criminal Justice Reference Service. (n.d.). Retrieved November 14, 2012, from https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=252153

NSTISSI. (1994, June 20) *National training standard for information systems security (INFOSEC) professionals.* No. 4011. Retrieved November 26, 2012, from http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf.

O'Neal, M. R., Dixon, J. S., Naval Postgraduate School (U.S.), & Naval Postgraduate School (U.S.). Graduate School of Business and Public Policy (GSBPP). (2011). *Department of Defense Strategic and Business case analyses for commercial products in secure mobile computing*. Naval Postgraduate School, Monterey, California.

Pentland, A., Fletcher, R., & Hasson, A. (2004). DakNet: rethinking connectivity in developing nations. *Computer*, *37*(1), 78 – 83. doi:10.1109/MC.2004.1260729

Rajamäki, J., Holmström, J., & Knuuttila, J. (2010). Robust mobile multichannel data communication for Rescue and Law Enforcement Authorities. In *2010 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)* (pp. 1 –6). Presented at the 2010 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT). doi:10.1109/SCVT.2010.5720457

The SANS Institute. (2012). About the SANS institute. Retrieved from http://www.sans.org/about/sans.php.

Schmidt, A.-D., Peters, F., Lamour, F., Scheel, C., Çamtepe, S., & Albayrak, Ş. (2009). Monitoring smartphones for anomaly detection. *Mobile Networks & Applications*, *14*(1), 92–106. doi:10.1007/s11036-008-0113-x

Seifert, J., De Luca, A., Conradi, B., & Hussmann, H. (2010). TreasurePhone: Context-sensitive user data protection on mobile phones. In P. Floréen, A. Krüger, & M. Spasojevic (Eds.), *Pervasive Computing* (Vol. 6030, pp. 130–137). Springer Berlin / Heidelberg. Retrieved from http://www.springerlink.com/content/n12l6hqj22j30435/abstract/

Sørensen, C., & Pica, D. (2005). Tales from the police: Rhythms of interaction with mobile technologies. *Information and Organization*, *15*(2), 125–149. doi:10.1016/j.infoandorg.2005.02.007

Straus, S., Bikson,T., Balkovich,E., & Pane, J. (2010). Mobile technology and action teams: Assessing BlackBerry use in law enforcement units. *Computer Supported Cooperative Work (CSCW), 19*(1), 45–71.

Sun, K., Choi, J., Lee, D., & Noh, S. H. (2008**).** Models and design of an adaptive hybrid scheme for secure deletion of data in consumer electronics. *IEEE Transactions on Consumer Electronics*, *54*(1), 100 –104. doi:10.1109/TCE.2008.4470030

Tabourin, P. (2010, February). Security, control & management: Mobile data in a multiagency/jurisdiction environment. *Law Enforcement Technology, 37*(2), 72-76.

Tetmeyer, A., & Saiedian, H. (2010). Security threats and mitigating risk for USB devices. *IEEE Technology & Society Magazine*, *29*(4).

Tschersich, M., Kahl, C., Heim, S., Crane, S., Böttcher, K., Krontiris, I., & Rannenberg, K. (2011). Towards privacy-enhanced mobile communities—Architecture, concepts and user trials. *Journal of Systems and Software*, *84*(11), 1947–1960. doi:10.1016/j.jss.2011.06.048

Ugus, O., Westhoff, D., & Rajasekaran, H. (2012). A leaky bucket called smartphone. *Pervasive Computing and Communications Workshops, IEEE International Conference on* (Vol. 0, pp. 374–380). Los Alamitos, CA, USA: IEEE Computer Society. doi:http://doi.ieeecomputersociety.org/10.1109/PerComW.2012.6197513

University of Oregon (2012). Managing IT/IS security course materials. Retrieved from http://aim.uoregon.edu/current/courses/course_desc.php?CourseKey=654948.

United States Government Accountability Office. (2012, September). Information security: Better implementation of controls for mobile devices should be encouraged. *Report to Congressional Committees*. Retrieved November 19, 2012 from http://www.gao.gov/products/GAO-12-757.

US Department of Commerce, N. (2011, February 17). Glossary of key information security terms. Retrieved December 5, 2012, from http://www.nist.gov/manuscript-publication-search.cfm?pub_id=907638

US Department of Commerce, N. (2012). NIST updates guidelines for mobile device security. Retrieved November 2, 2012, from http://www.nist.gov/itl/csd/mobile-071112.cfm

Verma, I. (2011, August 23). A security analysis of smartphones. Retrieved from http://hdl.handle.net/1805/2630.

Violino, B. (2012). A calculated risk. *Computerworld*, *46*(17), 31-32.

Wallach, D. (2011, February 17). Smartphone security: Trends and predictions. *Secure Application Development.* SecAppDev 2011. Leuven, Belgium.

Wang, Y., Streff, K., & Raman, S. (2011). Security threats and analysis of security challenges in smartphones. *Computer*, *99*(1), 1.

Wawro, A. (2011). The smartphone data theft threat. *PC World*, *29*(5), 38–38.

Weier, M. (2009). What goes mobile? *Informationweek*, 20-26.

White, G., Conklin, W. A., Williams, D., Davis, R., & Cothren, C. (2008). *CompTIA Security+ all-in-one exam guide, second edition* (2nd ed.). McGraw-Hill Osborne Media.

Whitman, M. E., & Mattord, H. J. (2005). *Principles of information security*. (2nd ed.). Boston, Mass: Thomson Course Technology.

Yuan, Y., & Detlor, B. (2005). Intelligent mobile crisis response systems. *Commun. ACM*, *48*(2), 95–98. doi:10.1145/1042091.1042097

Yue, F., Wang, G., & Liu, Q. (2010). A secure self-destructing scheme for electronic data. In *2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC)* (pp. 651 –658). Presented at the 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC). doi:10.1109/EUC.2010.104