A Security Model for Mitigating Multifunction Network Printers Vulnerabilities

Conference Paper · May 2016

CITATION
1

READS
124

1 author:

Jean-Pierre Kabeya Lukusa
Botho University
5 PUBLICATIONS **1** CITATION

SEE PROFILE

Proceedings of the 1st International Conference on the Internet, Cyber Security, and Information Systems (ICICIS), Gaborone, 18-20 May 2016

A Security Model for Mitigating Multifunction Network Printers Vulnerabilities

Jean-Pierre Kabeya Lukusa
Department of Network and Infrastructure Management
Botho University
Jean-Pierre.Lukusa@bothouniversity.ac.bw

ABSTRACT

With the ability of incorporating a wide range of functions, Network Printers have not only become one of the most essential tools in today's businesses but also one of the most neglected component in network security defenses. An efficient network security architecture design therefore necessitates the integration of key security implementations by means of formal security models conceived with security policies that take into consideration multifunctional network printers (MNP) security liabilities. This paper, presents a novel approach aimed at enforcing policy constrained security mechanisms using a multilevel printer security architecture. The proposed security model ensures discretionary access control (DAC), and a secure flow of information to and from entities connected to the network, to provide a trusted computing base (TCB). Access to the printer by subjects is controlled by means of security clearance matrices that can then be applied to security classes under which network resources can be grouped. Lastly, a validation of the model is presented using simple set theoretic concepts to assess the resilience of the implemented security defense model.

Keywords: Printer security, access control matrices, security architecture design, information flow control, trusted computing base (TCB)

1. INTRODUCTION

1.1. Background

The modern printer has over the years evolved into an embedded device that is capable of incorporating a wide range of functionalities that go beyond what an otherwise conventional printer would be thought capable of doing. This unique ability of incorporating multiple functions into a single unit, has earned it the acronym Multi-function Printer (MFP). For generalization sake, the term Multifunction Network Printer (MNP) has been adopted in the text to better represent it as a network integratable embedded[1] device. MNP have, in spite of the commendable efforts made by the "go-green" (Bansal, 2000; Di Giuli, 2014) corporations[2], managed to become one of the most essential tools in today's businesses and homes

[1] An object containing a special purpose computing system.
[2] Encourage conservation of paper by advocating printing only when absolutely necessary (a.k.a. Green Computing).

ISBN 978-99968-0-430-4

(Infotrends, 2011). Due to this increasing market demand for a multipurpose printer and the need for incorporating a wide range of functionalities into a compact unit, most manufacturers have opted to integrate disk drives in their printer designs to record and store latent and/or residual data thus effectively turning, even the most secured printers, into a dormant security liability.

Nowadays, a typical MNP is capable of printing, scanning, copying or faxing documents from both electronic and hard sources. These documents would more often than not contain potentially sensitive information that if not properly secured may fall into the wrong hands (Forbes, 2013). Therefore, identified security flaws in mechanisms preventing unauthorized access to files residing within these printers and the illegal flows of information heighten the level of vulnerability to inter-process communications and thus potentially compromising the privacy and integrity across the network (Gonsalves, 2013; Vail, 2003).

1.2. Problem of Interest

In highlighting the problem of interest, this paper takes cognizance of the ISO/IEC 15408[3] standard (Chen, 2015) and it would thus be of consequence to clarify that the focus of the paper is not on the internal or architectural security design flaws (Cui, 2013; Forbes, 2013) in MNPs, that are otherwise conventionally addressed by the aforementioned standard, but rather on potential security loopholes born from complexities inherent to MNPs. These loopholes can be roughly grouped into risks linked with *(i) control security*, *(ii) data security*, and *(iii) network security*. Risk (Bishop, 2012; Pfleeger, 2011), in this sense, can then be viewed as a component that increases at the same rate as the resulting threats and vulnerabilities subjected to the MNP as presented by the following formula:

$$Risk = Threats \times Vulnerability \times MNP \quad (1)$$

1.3. Focus of this Paper

In order to best describe the proposed security architecture, a formal mathematical model (Landwehr, 1981) is presented to demonstrate its potential implementation. This paper primarily focuses on: *(i) devising a multilevel printer security[4] mechanism for controlling access by subjects with different security clearances*; *(ii) safeguarding privacy and integrity of data stored on the printers*; *(iii) providing audit trails for all transient inter-process communications*; and *(iv) providing protection against printer denial of service*. The goal is to attain optimum security without compromising the balance between *protection* and *usability* (Vail, 2003).

[3] The Common Criteria for Information Technology Security Evaluation.

[4] *Multilevel security* deals with the protection of information to which different security level clearance classifications have been ascribed.

ISBN 978-99968-0-430-4

2. IDENTIFICATION OF TRUSTED COMPUTING BASE[5] FUNCTIONS IN MNPs

2.1. Definition of Terms Used

- A *Subject* – is an active network resource capable of exchanging data or control information with an MNP.
- A *Network User* – is a person authorised to use a given network.
- A *User Identifier* – is a unique character string used to identify a given network user.
- A *Security Class* – is a security attribute that can be assigned to all network resources to which a sensitivity level can be ascribed (e.g. ADMIN, POWER-USER, DOMAIN USER, etc…). It provides a basis for determining access from subject(s)-to-MNP(s). This allows us to define the set of security class S as a bounded[6] lattice of sensitivity levels $l_i$where $S = \{s_1, \dots, s_n\}$ such that $0 \leq i \leq n$. This is important as it defines the set of permissible information flow/transactions between subject(s) and MNP.
- A *Classification* – is a designation attached to an MNP used for a given security class that reflects its relative value and vulnerability levels as a network asset.
- An *I/O Interface* – is a point of transit for data/control located on an MNP. Each I/O interface belongs to a given classification.
- An *Operation* – is a unit function that can be assigned to a given MNP and performed by an authenticated subject. These include, but are not limited to, the following:
  a. *Print* – reproducing text and/or image from digital to hard-copy.
  b. *Scan* – capturing images from hard-copy onto a digital format.
  c. *Fax* – transmitting or receiving an electronic copy of a document.
  d. *Email* – an electronic transmission or reception of a document.
- A *Reference Monitor (RM)* – is used to mediate all information flows/transactions to a given MNP by subject(s).
- A *Reference Validation Mechanism (RVM)* – is used to represent an implementation of the RM concept.

2.2. MNP Security Mis-configurations: A Review of Possible Problem Areas

In order to best address possible problem areas inherent to MNP, it is necessary to look at security control management in terms of its access (Dohi, 2012), information flow (Denning, 1975; Stoughton, 1981), and cryptographic (Kahate, 2013) control. These are briefly discussed in the following sections as potential security sore spots leading to network threats and/or vulnerability in MNP.

i. Devising Generic MNP Based Security Mechanisms for Controlling Access by Subjects

When inspecting access control vulnerabilities areas, one needs to describe them in terms of configurable authentication[7], authorization[8], and accountability[9] features. For instance on a generic MNP these can be controlled through enabling, amongst others, features such as discretionary copy/print/scan/fax account

[5] A set of hardware, software, or firmware factory implemented protection mechanisms within a given MNP that are responsible for enforcing security policies (Bishop, 2003).
[6] An ordered set with both join *(i.e. least upper bound)* and meet *(i.e. greatest lower bound)* semi-lattices
[7] confirming subjects' *identity*
[8] determining *what* the subject can do
[9] *associating* subjects to its action

ISBN 978-99968-0-430-4

tracking, subjects authentication for both remote and local access, auto log off on idle processes, function restrictions, event log historic, printer driver user data encryption, non-business hours user account tracking, etc…

ii. Safeguarding Data Privacy and Integrity

While it is equally important to ensure confidentiality of data by taking simple measures such as not leaving personal documents lying in the MNP's output tray; the emphasis in this section is on the implementation of appropriate data security policies to safeguard latent and/or residual data stored on MNPs' resident drives. Amongst others, these can be controlled by enabling features such as disk-drive password protection, hard-disk data encryption, hard-disk data overwriting, temporary data deletion, timed data auto deletion, etc…

iii. Providing Audit Trails for Transient Inter-process Communications

Provision of audit trails for transient inter-process communications on MNP is often realized through the integration of *reference monitor* functions on the MNP. Control is achieved here by enabling features such as IP address filtering, port and protocol access control, SSL[10]/TLS[11] encryption, IPSec support for secured session tunneling, IEEE 802.1x support, NDS[12] authentication, etc…

iv. Protection Against Printer Denial of Service

Most MNPs denial of service attacks discussed in literature (Ormazabal, 2014a; Ormazabal, 2014b; Ormazabal, 2015) can be grouped into two broad categories. The first is often achieved by gaining unlawful access to the printer via unsecured ports (such as HTTP, or Telnet) with the intent of damaging or unlawfully restricting access to services or functionalities that were otherwise provisioned for authenticated subjects. The second type is achieved by flooding known printer interfaces/ports (such as port 9100) with random data with the intent of exhausting its resources and thus effectively preventing it from provisioning any further service. These are often circumvented by simply observing basic access control measures as discussed earlier and frequently applying printer firmware patches.

2.3. Security Requirements for Connecting Trusted and Untrusted Subject(s) to MNP(s)

This section presents some scenarios aimed at highlighting specific security requirements for connecting trusted *(t)* or untrusted *(u)* subject(s) to MNP(s). Before proceeding further, it is important to point out that creating a perfectly secured network is an ultimate, albeit unachievable goal as there would in some way always be an element of risk albeit minute (Suh-Lee, 2015). For instance, a *trusted* subject or MNP may be defined as one that is deemed to have provided sufficient credible evidence that it meets a finite set of security requirements (Bishop, 2003) and thus also making it in a way *trustworthy*. Consequently, a subject or MNP deemed as 'trusted' would remain in that state provided that the link between the 'credible evidence' and the finite set of 'security requirements' is maintained. For this reason, 'trust' within the context security should never be thought of as a given.

[10] Secure Socket Layer
[11] Transport Layer Security
[12] Novel Directory Services

ISBN 978-99968-0-430-4

Let X represent the set of security states for a given MNP such that $\{x_t|x_u\} \in X$ and Y represent those of its connecting subject(s) such that $\{y_t|y_u\} \in Y_j \mid j \in \aleph$ where $\{x_t, y_t\}$ represent trusted security states and $\{x_u, y_u\}$ untrusted security states. Figure 1, illustrates four partial ordered sets that can result from the interaction between given elements of X and those of Y using a Hasse diagram. From the diagram, the following four possible cases can be deduced, with the assumption that all involved MNP have a resident TCB:

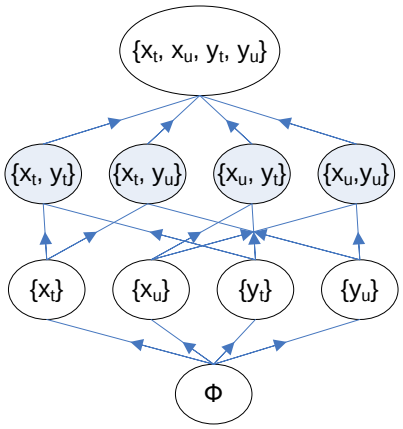

Figure 1: Hasse diagram of partial order ⊆ derived from X and Y

i. *Threat* T1:$\{x_t, y_t\}$ – A *trusted subject* connecting to a *trusted MNP*.
   a. *Requirement T1*-A: the subject is permitted to begin a session only if a unique user identifier[13] has been supplied to the MNP and if it has been successfully validated and authenticated by the MNP.
   b. *Requirement T1*-B: an active subject must belong to a classification that allows or prohibits access to both operations and/or I/O interfaces provided by the MNP.
   c. *Requirement T1*-C: an inactive session albeit authenticated must have a finite expiration period.
   d. *Requirement T1*-D: a valid subject identifier must have a finite print/copy quota in any given session.
   e. *Requirement T1*-E: Mandatory security policies and flow control functions must be implemented on both MNP and its subjects.

The security analysis mapping for T1 can be defined as: T1 ↦ {T1-A, T1-B, T1-C, T1-D, T1-E}. The set {T1-A, T1-B, T1-C, T1-D, T1-E} is known as a *security target reference* mapping to threat T1.

ii. *Threat* T2:$\{x_t, y_u\}$ – An *untrusted subject* connecting to a *trusted MNP*.
   a. *Requirement T2-A:* a valid justification of the security analysis mapping for T1 must be presented in accordance to ITSEC (Commission of the European Communities, 1991).
   b. *Requirement T2-B:* the classification of each untrusted subject must fall within the range of sensitivity levels that the MNP is trusted.
   c. *Requirement T2*-C: the MNP must provide an audit trail (i.e. maintaining an event log) for all past actions performed on behalf of subject(s).
   d. *Requirement T2*-D: an appropriate user classification with matching sensitivity level must be defined for all subjects connecting to an MNP during non-business hours.
   e. *Requirements T2*-E: appropriate network level security must be enforced to ensure discretionary access control[14] as well as port and protocol access control is observed at all network layers.

The security analysis mapping for T2 can be defined as: T2 ↦ {T1, T2-A, T2-B, T2-C, T2-D}.

[13] May be presented as a user id and password, biometric inputs such as finger vein scan, smart card, etc…
[14] Also known as an *identity-based access control (IBAC)* – Granting restricted access to subjects on the basis of their identity and/or groups to which they belong.

ISBN 978-99968-0-430-4

iii. *Threat* T3:$\{x_u, y_u\}$ – An *untrusted subject* connecting to an *untrusted MNP*.
   a. *Assumption T3-A:* due to lack of discretionary access control trust association with subject(s) cannot be reciprocated by the MNP and vice-versa.
   b. *Assumption T3-B:* as a result of T3-A, no security policy may be effected. This also means that the presence of a TCB on the MNP is symbolic (i.e. not functional).

The security analysis mapping for T3 can be defined as: T3 ↦ { T3-A, T3-B}.

iv. *Threat* T4:$\{x_u, y_t\}$ – A *trusted subject* connecting to an *untrusted MNP*.
   a. *Requirement T4-A:* a valid justification of the security analysis for T2 must be validated in accordance to ITSEC (Commission of the European Communities, 1991).
   b. *Requirement T4*-B: upon initiation of an active session, subject need to secure their transaction using either data protection mechanisms[15] or printer job locking[16].

3. MEASURING SECURITY AS A RESULT OF THE INTERACTION BETWEEN SUBJECTS AND MNP

3.1. Preamble:

This section presents an adaptation of the method for quantifying security risk presented by Suh-Lee and Jo (2015). Before proceeding to the calculations, there is need to define the following terms:

i. *A Danger Zone* – is a network segment where trusted members belonging to the set $(X_i \cup Y_j)$attached to the segment have frequent interactions with an untrusted host belonging to the set $(X_i \cup Y_j)$. The set of nodes belonging to a given Danger Zone is defined as:

$$DZ_k = \{H |\ H\ \in trusted\ (X_i \cup Y_j)_j\ is\ a\ node\ in\ a\ Danger\ Zone\ k\ where\ 1 \leq k \leq n\ and\ n\ \in \aleph\} \quad (2)$$

ii. *A Zone Proximity Value* – is an integer value $Px(DZ_k)\ \in \beth \mid Px(DZ_k) \geq 1$ that indicates the proximity of a trusted members of DZ_k to the untrusted member of $(X_i \cup Y_j)$. The smaller the value of $Px(DZ_k)$, the closer the member is to the untrusted node, and therefore, the higher the risk in the zone (Suh-Lee, 2015).

iii. *The Proximity value Px of a node H from DZ_k* - is defined as:

$$Px(H) = \min(Px(H, DZ_k)\ \forall\ DZ_k\ in\ the\ network \quad (3)$$

iv. *The Proximity-adjusted Vulnerability Score of a Host H* (Suh-Lee, 2015) – is defined as:

$$PVS(H) = \sum_{k=1}^{n} PVS(v_k) \quad (4)$$

Where v_k is a given vulnerability found in the host Hv and

$$PVS(v) = CVSS(v) \times {}^{1}/_{2^{Px(Hv)}} \quad (5)[17]$$

[15] Includes – hard-disk password protection, disk data encryption, hard-disk data overwrite, latent data auto deletion, etc…
[16] Ensuring that jobs from an authenticated subject is put on hold until a matching identifier is provided physically at the machine.
[17] The Common Vulnerability Scoring System v3 (CVSS): is a measurable vulnerability severity score ranging from 0 to 10, with 7.0 to 10.0 being the highest, often used to prioritize responses and resources according to threat.

ISBN 978-99968-0-430-4

v. *The Relative Cumulative Risk (RCR) of the vulnerability* – is defined as:

$$RCR = PVS(v) \times NPVS(v) \quad (6)$$

3.2. Evaluating the Relative Cumulative Risk of the Interaction between Members of the set $(X_i \cup Y_j)$

To demonstrate the effect of the interactions between subjects and MNPs located in various sections of the network and estimate their relative risk, an emulation of a typical deployment environment is used as represented in figure 2.

Under the assumption that the internal network is adequately policed and fulfills security requirements as stated in the previous section; the three Multifunction Network Printers (MNP) have been placed in three different segments of the network. From figure 2, the following two danger zones (i.e. $DZ_1, DZ_2 \in DZ_i$) can be identified.

The first zone is directly positioned behind inbound connections originating from the internet via the ISP supplied gateway router inbound through FW1 and onto the DMZ segment containing the employees e-mail server (EMS), the public hall printer (MNP2) and the webserver (WS) that also has a backend connection to the database server(DS).

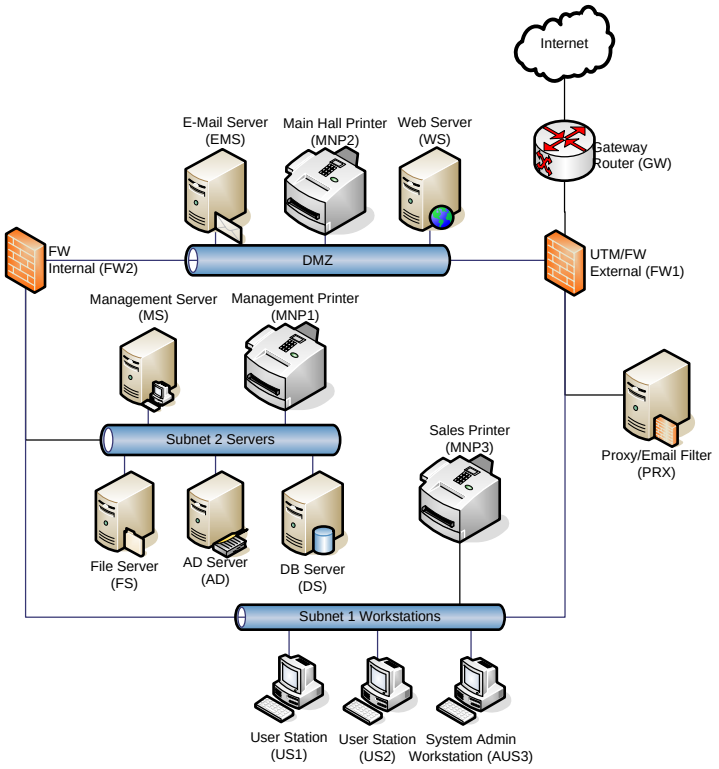

Figure 2: The Test Network Diagram

Excluding all none printing resources our zone definition and proximity value assignment would be:
$Px(MNP2, DZ_1) = 1 \; and \; Px(MNP2, DZ_2) = 5$

$\therefore DZ_1 = \{MNP2\}, and \; Px(DZ_1) = 2$

The second zone comprises of subnet 1 and 2. The first subnet has an outbound connectivity to the Internet through the proxy server via FW1. Similar to the above representation of zone 1, our zone definition and proximity assignment in this case is:

ISBN 978-99968-0-430-4

$Px(MNP1, DZ_1) = 2\ and\ Px(MNP1, DZ_2) = 5$

$Px(MNP3, DZ_1) = \infty\ and\ Px(MNP3, DZ_2) = 4$

$DZ_2 = \{MNP1, MNP3\}, and\ Px(DZ_2) = 4$

Determining proximity values for the printers relative to the danger zones, using (3) and (5) generates the following proximity map.

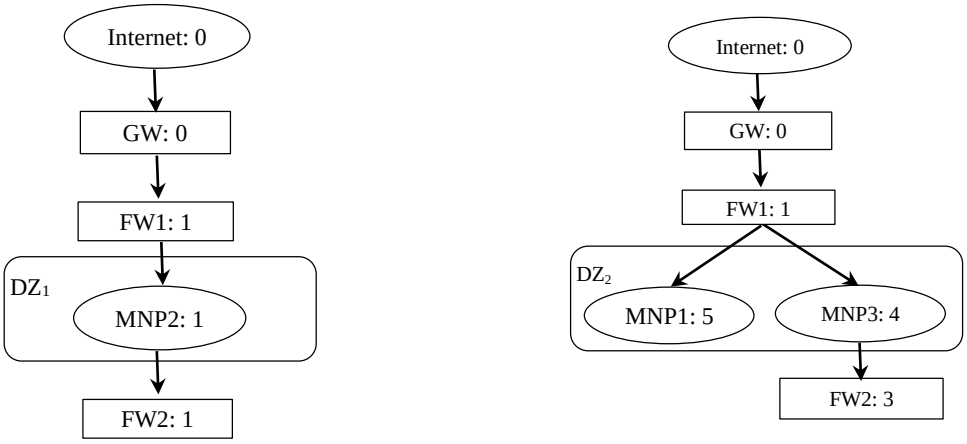

Figure 3: Proximity Map for Test Network

The proximity adjusted vulnerability scores for MNP1, MNP2, and MNP3 can be calculated as follows:

For MNP1:

$$PVS(v) = CVSS(v) \times {}^{1}/_{2^{Px(Hv)}} = 4.3 \times {}^{1}/_{2^{5}} \cong 0.134$$
$$RCR = PVS(v) \times NPVS(v) = 0.134 \times 17.365 \cong 2.\overline{33}$$

For MNP2:

$$PVS(v) = CVSS(v) \times {}^{1}/_{2^{Px(Hv)}} = 5.8 \times {}^{1}/_{2^{1}} \cong 2.9$$
$$RCR = PVS(v) \times NPVS(v) = 2.9 \times 15.687 \cong 45.49$$

For MNP3:

$$PVS(v) = CVSS(v) \times {}^{1}/_{2^{Px(Hv)}} = 7.5 \times {}^{1}/_{2^{4}} \cong 0.469$$
$$RCR = PVS(v) \times NPVS(v) = 0.469 \times 61.297 \cong 28.73$$

From the above calculation, we can conclude that MNP2 has the highest risk rank (i.e. RCR=45.49) of the three printers; followed by MNP3 (i.e. RCR=28.73). MNP1 is found to be the least at risk resource (i.e. RCR=2.33).

This conclusively demonstrates how exposure to different vulnerability levels can elevate the relative risk rankings of resources that may otherwise be assumed to have been properly secured.

ISBN 978-99968-0-430-4

The presented method (Suh-Lee, 2015) therefore establishes that while accurate configuration of printers is important, it is equally important to remedy existing network vulnerabilities to ensure that risks are kept at their lowest.

4. CONCLUSION

The paper presented a multi-level network printer security architecture that relied on robust policy constrained security mechanisms for discretionary control of both trusted and untrusted entities by means of the TCB. The developed model further demonstrates the need for a secured and trustworthy network environment since the nature of such an environment tends to measurably reduce the risk ranking ascribed to a given MNP regardless of how well it is thought to have enforced access and information flow control mechanisms. It is hoped that by focusing on accurate configuration, good use of discretionary security policy implementations, and strategic placement of MNPs; one can greatly improve both the security and trustworthiness of MNPs while still maintaining the balance between protection and usability.

5. ACKNOWLEDGEMENTS

I would like to thank Botho University for sponsoring this paper's presentation costs. I would also like to thank colleagues, and friends who have taken time to review and provide much needed feedback.

6. REFERENCES

Bansal, P., & Roth, K. (2000). "Why companies go green: A model of ecological responsiveness." *Academy of Management Journal* 43 (4): 717-736.

Bishop, M. (2012). "An Overview of Computer Security." In *Computer Security: Art and Science*, 3-24. Capetown: Addison-Wesley.

Bishop, M. (2003). "Assurance." In *Computer Security: Art and Science*, 475-544. Capetown: Addison-Wesley.

Chen, H., Bao, D., Goto, Y., & Cheng, J. (2015). "A Supporting Environment for IT System Security Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045." *Computer Science and its Applications* 1359-1366.

Commission of the European Communities. (1991). *Information Technology Security Evaluation Criteria.* Brussels: Commission of the European Communities.

Cui, A., Costello, M., & Stolfo, S. J. (2013). "When Firmware Modifications Attack: A Case Study of Embedded Exploitation." *NDSS.*

Denning, D. E. R. 1975. "Secure Information Flow in Computer Systems." *Ph. D. Dissertation. Purdue Univ.*

Di Giuli, A., & Kostovetsky, L. (2014). "Are red or blue companies more likely to go green? Politics and corporate social responsibility." *Journal of Financial Economics* 111 (1): 158-180.

ISBN 978-99968-0-430-4

Dohi, M. 2012. Printing system, information processing apparatus, printing apparatus, print management method, and storage medium. Washington, DC: U.S. Patent 8,161,297. April 17.

Forbes. (2013). "The Hidden IT Security Threat Multifunction Printers." February 7. Accessed December 26, 2015. http://www.forbes.com/sites/ciocentral/2013/02/07/the-hidden-it-security-treat-multifunction-printers/?sf9393024=1.

Gonsalves, A.,. (2013). "Printers Join Fray in Network Vulnerability Landscape." *CSO Online.* January 29. Accessed December 26, 2015. http://www.csoonline.com/article/2132861/access-control/printers-join-fray-in-network-vulnerability-landscape.html.

Grubb, B.,. (2013). "Security Fears over Exposure of Web-accessible Printers." January 29. Accessed December 26, 2015. http://www.theage.com.au/it-pro/security-it/security-fears-over-exposure-of-webaccessible-printers-20130129-2dhxo.html.

Infotrends. (2011). "Placements of Printers & MFP Devices Grew In U.S. and Western Europe Despite Challenging Economy." May 24. Accessed December 26, 2015. http://www.infotrends.com/public/content/press/2011/05.24.2011c.html.

Kahate, A. (2013). *Cryptography and network security.* New Delhi: Tata McGraw-Hill Education.

Landwehr, C. E. (1981). "Formal models for computer security." *Computer Surveys* 13 (3): 247-275.

Ormazabal, G. S., & Schulzrinne, H. G. (2014b). Denial of service detection and prevention using dialog level filtering. DC: USA Patent 8,719,926. May 6.

Ormazabal, G. S., & Schulzrinne, H. G. (2014a). Maliciouis user agent detection and denial of service (DOS) detection and prevention using fingerprinting. DC: U.S Patent 8,689,328. Apr 1.

Ormazabal, G. S., Schulzrinne, H. G., Yardeni, E., & Patnaik, S. B. (2015). Prevention of denial of service (DoS) attacks on session initiation protocol (SIP)-based systems using return routability check filtering. DC: U.S Patent 8,966,619. Feb 24.

Pfleeger, C. P., & Pfleeger, S. L. (2011). "Administering Security." In *Security in Computing*, 524-545. Boston: Prentice Hall Professional Technical Reference.

Savage, C., Petro, C., & Goldsmith, S. (2015). System for Providing Session-based Network Privacy, Private, Persistent Storage, and Discretionary Access Control for Sharing Private Data. Washington, DC: U.S. Patent 20,150,333,917. November 19.

Stoughton, A. (1981). "Access Flow: Protection model which integrates access control and information flow." *IEEE Symp. Security and Privacy.* 9-9.

Suh-Lee, C., & Jo, J. (2015). "Quantifying security risk by measuring network risk conditions." *2015 IEEE/ACIS 14th International Conference.* Las Vegas. 9-14.

Vail, V. T. (2003). "Printer Insecurity: Is it Really an Issue?" *SANS Institute InfoSec Reading Room*, May 28: 1-12.

ISBN 978-99968-0-430-4