Research on Newsroom Security Challenges

Rezza Moieni and Ikuesan R. Adeyemi, Information Security Department, Faculty of Computer Science and Information System,Universiti Teknologi, Malaysia

Newsroom play a very significant role in the modern day news production and broadcast, and a vast array of technological advancement is being introduced to improve communication efficiency but surprisingly, threats to the security of the network and communication channel, server systems, and work stations ; external and internal alike, of the newsroom are often overlooked/neglected. This threats if not mitigated could compromise the security of the newsroom and consequently jeopardize the integrity, reputation and even the safety of personnel. Test security will be enhanced by mitigating these threats. Few articles on the security of newsroom exist while it is of high importance. This survey studied the possible threats to newsroom and its possible effect, as well as possible mitigation to these threats.

Categories and Subject Descriptors: COMPUTING [**C.2**] COMPUTER-COMMUNICATION NETWORKS

General Terms: Networking

Additional Key Words and Phrases: Newsroom, Vulnerabilities, Intranet, Digital, Network, Security

ACM Reference Format:

R.Moieni and I.R.Adeyemi, **Research on Newsroom Security Challenges**, *International Journal of Computer Communications and Networks (IJCCN)*, 2(3), pp 14–26, 2012

1. INTRODUCTION

NEWS PRODUCTION is the process of planning, gathering, producing and communicating news content [Palmer 2008]. While this is primarily an editorial process these days, it is supported by sophisticated technical appliances and systems. A **newsroom** is the place where journalists–reporters and producers, along with other staffers–work to gather news to broadcast on television or radio. However, Newsrooms can be a separate production unit but usually they are part of large broadcasters as it needs a lot of technical and informational support.

Newsroom is an integrated, operational and information system in which 3 functional elements works together: Software, Hardware and human resources. Newsroom productions are high quality news in either news structure or content quality. Videos are the best possible qualities. Searching and retrieving data in such system is much easier. Transferring items from/to Archive is an important milestone due to traditional systems.

Journalists, super journalists, technicians, grapiest, editors, presenter, camera operator, audio engineers, light controllers and all other roles play as a team to produce high quality items in the fastest order. Time is a very important factor in news production. Owing to the relevance of newsroom to broadcasting organization, the need for secured news gathering, processing, dissemination and production cannot be overemphasized.

Threats to newsroom are not often reported, or even heard of, in the modern day digital world. They however exist nonetheless. Broadcast correspondents, [Baksh 2010; Schechter 2003] gave insight into the nature of newsroom and forms of threat/attacks targeted against it. Nowadays most newsrooms are

Corresponding Author: Rezza Moieni, Information Security Department, Faculty of Computer Science and Information System,Universiti Teknologi, Malaysia, Moieni@IRIB.Ir *or* MRezza3@Live.utm.my

© 2012 IJCCN /2012/12-ART2 $00.00 (FREE)

fully digitalized environments. Such networks may contain 100s of computers and sub-networks. These level of digitization has further introduce new vulnerabilities, and easier level of threats, ranging from an insider abuse, hackers, to planned corporate espionage.

This paper attempt to present the vulnerabilities attributed to newsroom, as well as describe the possible mitigation to these vulnerabilities. The rest of the paper is as follows: section 2 gives the architectural overview of newsroom. Section 3 elucidate on the various composition of newsroom. In section 4, the paper introduces the various vulnerabilities accredited to newsroom. A comprehensive summary of the possible mitigation to the vulnerabilities in newsroom is also given. Relevant discussion on the security of newsroom is given in section 5. Section 6 present the conclusion of this paper.

2. ARCHITECTURAL OVERVIEW OF NEWSROOM

2.1 Newsroom Workflow

New technology, added delivery channels and the increasingly unpredictable viewing habits of consumers are forcing today's news staffs to make significant changes. Today, station news teams need to be vigilant 24/7. In addition, they must not be dependent upon a linear storytelling model, and they must be able to distribute content across multiple platforms. Likewise, the production technology they deploy has to do more than simply present the daily television newscast. [Matics 2010] The role of broadcasting stations in news production workflow is primarily to promptly communicate accurate information. The changeover from tape media to file-based media usage, including that used in news coverage of on-air broadcasting can improve the workflow that used to impose a lengthy time longer than actual recording hours [Yasuharu and Masaki 2011]. In Traditional newsrooms, Journalists gathered news from news sources that were usually other news channels, reproduced them as a new news package that were as texts most of the time. Nowadays fully digitalized newsrooms could consist of hundreds of computers and servers. Journalists search via different news sources from tele-texts and satellites to websites and news-feeders. They benefit from automatic mechanisms and softwares, which help to make news.

In a newsroom system, news, monitored news programs and data from other sources store in a central storage attached to powerful servers and journalists have access to this central storage via their workstations. These workstations can be ordinary PCs. Journalists prepare news text and it is multimedia content with the help of editors and Monitors. The news will be sent to Super journalist for final checking. Super journalist will check the news structure and will put it in the conductor due to its subject and News Value. Playlist items will play in studio, the presenter will read the read-only parts of the news and audio/video parts will play automatically from central storage.

These systems are usually in a newsroom network:

- Archive network and systems
- Satellite- Tele-text receivers
- Internet feeders
- Journalists systems
- Graphic systems
- Narration systems
- Studio systems
- Monitoring systems
- Ingest systems
- Crawling systems and Character Generators(CG)

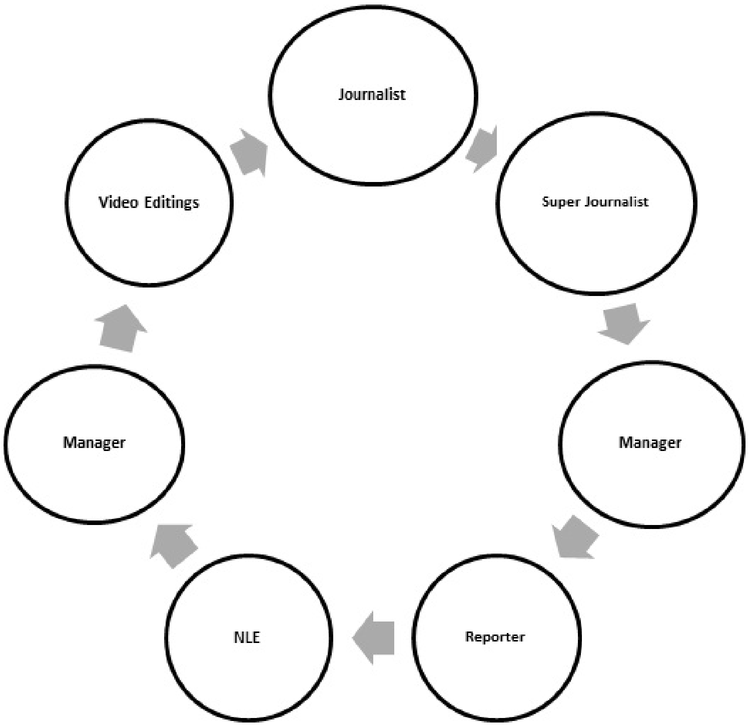


Fig. 1. News production workflow of human resources

—Reggie systems

—Server room systems

Sample architecture of these blocks and elements is introduced in Figure 2. Variety of architectures exist depends on the configuration of television equipment and applications [Viana et al. 2003].

3. WHAT CONSTITUTES THE NEWSROOM?

3.1 Archive Network and Systems

Current work in digital preservation (DP) is dominated by the Open Archival Information System (OAIS) reference framework specified by the international standard ISO 14721:2003[Nicholson and Dobreva 2009]. This is a useful aid to understanding the concepts, main functional components and the basic data flows within a DP system Archive probably is the heart of digital broadcast systems. While in analogue workflow it was usually in basements, but in digital era availability of archive and its services probably is the most critical part of the chain. Huge archives may contain PBs of data. Many archives or based on OAIS (Open Archival information system) model [Nguyen and Le 2010].

An AV archive network in a broadcast channel typically consists of these systems:

—Mass storage consist of:

- —Online like SAN-DAS-NAS (TB).It contains the materials that MUST be available always without a second of even one second. Example of such content can be titrages or Audio or video clips with the highest usage or the items of current playlist that are going to be on-air in few seconds or minutes

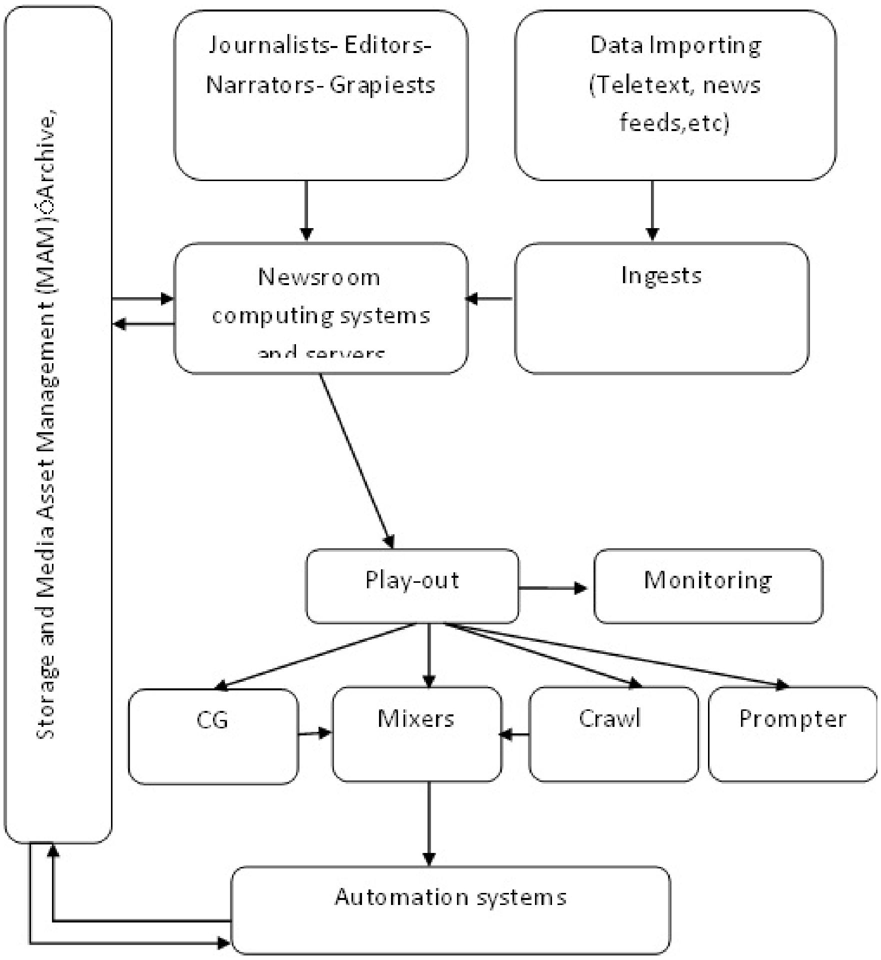


Fig. 2. A Sample Newsroom Architecture

- —Nearline like tape autoloaders or MAID (TB): A delay of 1 to 5 minutes are usually acceptable for retrieving of contents of this type of archive. For example items that will be on-air in near future can be kept in nearline archive until a reasonable time and then moved to online.
- —Offline (Like tape libraries) (PBs): Items that rarely are used like a special sport event are kept in offlines. Speed of service is not very important. Due to HSM policies using content of such archive usually needs it to be first moved to nearline and offline and then is ready to be used. Hierarchical Storage Management (HSM) architecture defines topology of these archives [Avrin et al. 2001; 2000].

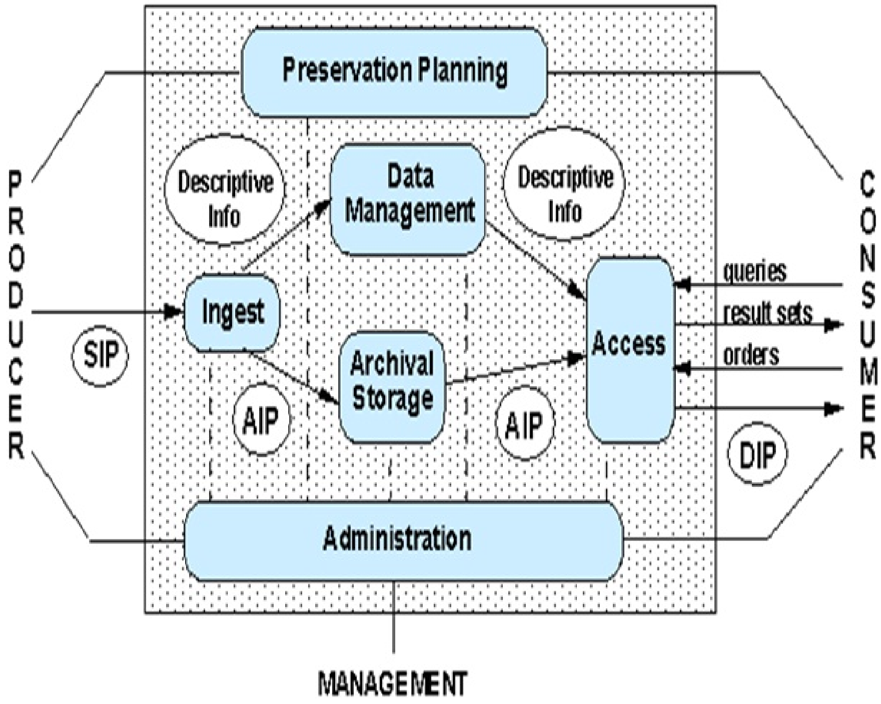
—Audio-Video Ingests : to ingest Audio/Video materials from external/internal sources

—A/D systems for transferring Analogue essences to digital

—Metadata systems (cataloging and others)

—Network management systems (DNS, Domain controllers)

—Editing systems : To remove noises like Pops, Hiss, from essences



Source: Procedures Manual for the Consultative Committee for Space Data Systems (2001)

Fig. 3. OAIS Archive model [CCSDS 2003]

—Backup systems

3.2 Satellite- Teletext Receivers

Broadcast teletext is a television information retrieval service developed in the United Kingdom in the early 1970s which offers a range of text-based information, typically including national, international and sporting news, weather and television schedules, Subtitle (or closed captioning) information is also transmitted in the teletext signal, It is usually used to receive latest raw essences (Audio-Video-Text) from satellite sources. These are always pay-services [Kawamoto et al. 2004].

3.3 Internet feeders

Nowadays internet is not just about emails and websites, more and more applications use internet as communication platform. Many broadcasters use internet to transfer data like Graphics including pictures and News Texts from internet sources. These are usually pay-services [Lee 2000].

3.4 Journalists Systems

To choose a text with the order of super journalist and find a suitable Video clip and make video cuts including Rough cut, Jump cut, fading,etc. It can be a simple PC. Usually all inputs like USB, CD-DVD and other disk drives in order to decrease the risk of possible security vulnerabilities.

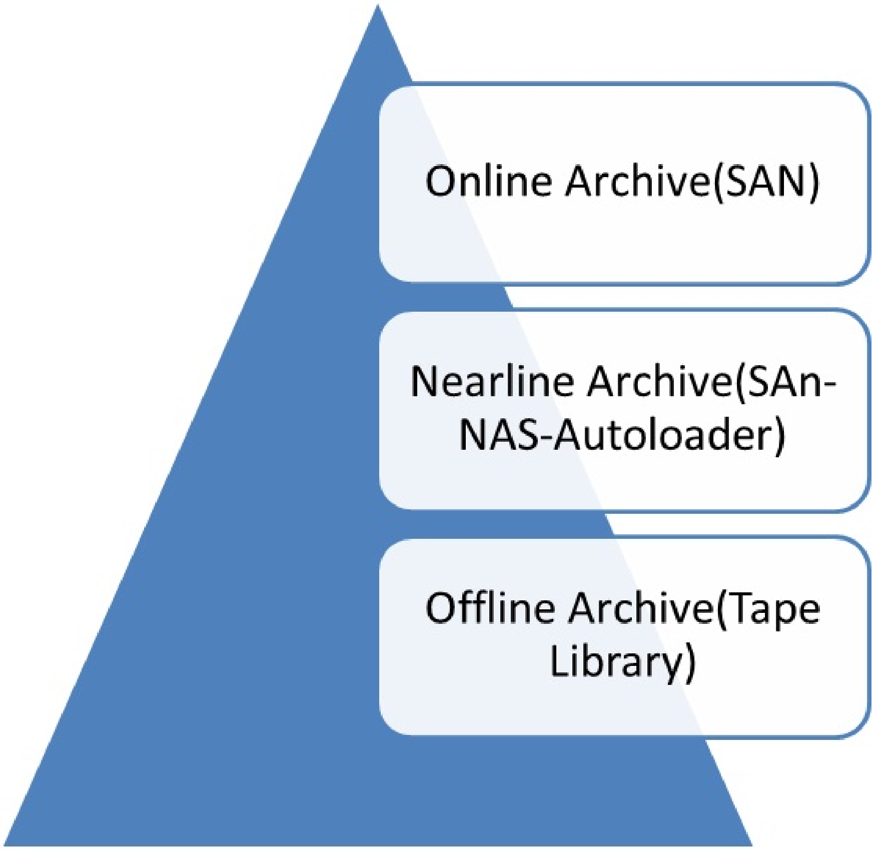

Online Archive(SAN)
Nearline Archive(SAn-NAS-Autoloader)
Offline Archive(Tape Library)

Fig. 4. HSM architecture of archive

3.5 Monitoring Systems

Due to the extension of satellite TV channels, using the technologies for streaming TV over LAN networks seems to be inevitable. A sampled Monitoring Network consists of many computers, ingests and video servers that are connected to the central storage

3.6 Graphic systems

The attractiveness of current news and productions highly depends on graphics and visual effects. These systems are used to add Subtitles ,Logos and etc to videos or captions or even making 2D-3D images for weather news and etc [Whitaker 2005].

3.7 Narration systems

Many videos and still images do not contain voice and need a narrator to ass narration on the file. A narrator is a person who tells the story of the still or moving image [Ranjbar 2011]. To add voice or reports to a clip to make a news package, there are narration systems in newsroom which are located in studios or acoustic rooms to record voice and adding it to the video.

3.8 Studio systems

Studio systems usually located at the end of newsroom workflow. Contents from workstations and journalists are sent to studio for broadcast, these systems usually contain followings [Whitaker 2005]:

—Autoque(Prompter)

—Lightings

—Video Mixers

—Audio Mixers

—Microphones

—Cameras

—Telephony systems

—Character Generators(CG)

3.9 Monitoring Systems

The quality and content of what has been broadcasted should be monitored at all times. These systems capture and store contents to monitor input/output content and its quality.

3.10 Ingest Systems

Ingest system captures video programs or news items and route them to the Tapeless workflow. This system can work as a Standalone system or be connected to other automation systems [Whitaker 2005].

3.11 Crawling Systems

It is usually located at lower one fifth of the screen to present headlines and latest news in text format. It also called thicker news [News 2011b]. The content prepared by journalists and added to video by video mixers.

3.12 Playouts

Audio/Video Playouts are the e outer layer of the newsroom that send the final video and content to the signaling department and/or antenna for broadcasting [Whitaker 2005]. Playouts are very important systems that if any vulnerability of them may threaten the whole newsroom process. They are connected to central storage usually by high speed connections like Fiber Optic. In many cases and scenarios currently using, technicians make a backup of each playlist contents on the local storage of playlist in order if any malfunctioning of network happened, there will not happen anything to the air.

Another threat is that like any other systems play out are consist of hardware. As they work 24/7 any problem to them may happen while in 99.999(five 9) of times they have to be on load.

These problems may be power consumption failures or processor or memory damage. Problems caused by operating system failure may happen as well. To guaranty the safety of our put signal there usually a redundancy configuration is used as Fig. 5.

In this structure, both play-outs act exactly the same operation at the same time simultaneously. The change over system is a switch that always sense the line and if detect any malfunctioning with play-out 1 then will move the output line to number 2. The process is usually controlled by RS232 port controller. There exists another structure for play outs that the changeover switch divides the tasks between both play outs, so each of them play one item at each time and the other one will rest. This minimizes the threats but still is risky. However a combination of above solutions may be ideal for highest security.

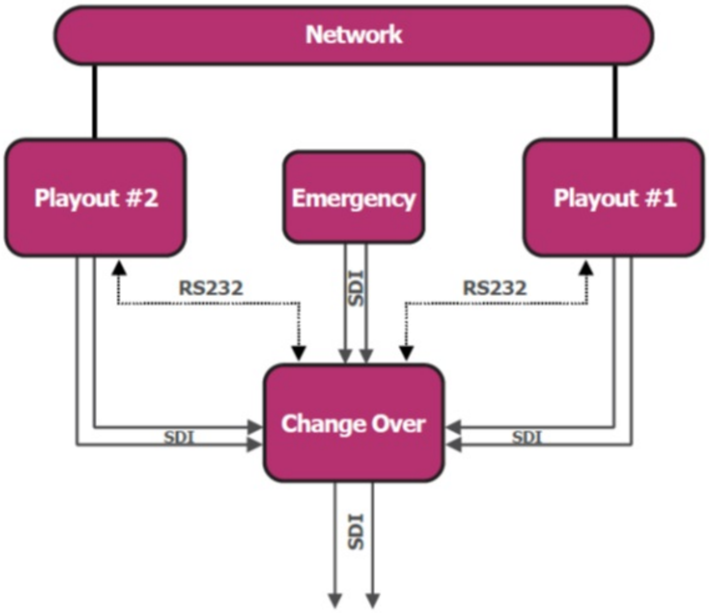


Fig. 5. Current Solution for Reducing Risks of Play Out Servers

3.13 Server Room Systems

All computing systems and communication between all systems in newsroom is managed and controlled with servers in server room [News 2011a]. It is a small data center to store and retrieve data. Administrators of the newsroom who work at server room are responsible for the integrity, confidentiality and availability of the systems all over the newsroom. Systems of a sample newsroom may contain followings [Warner 2008]:

- Data backups
- Antivirus
- Domain controllers
- Firewalls
- Routers and switches
- Monitor systems
- Webmail servers
- Internet feeder servers
- Teletext servers
- Proxy servers

4. NEWSROOM VULNERABILITIES

Typical newsroom architecture can be described as a group of inter-connected host forming an intranet [Kent 1981] which comprises PC stations, and servers. Being an Ethernet system, all security challenges associated with the Ethernet can also be exploited in a newsroom. Peculiar to a newsroom is the complication generated through the various phases of operation: negotiation, connection and transmission. Active or passive wiretapping could be a major threat to the intranet system. In [Jamieson and Low 1989], other risks associated with the intranet are elaborated. Attack could either be internal or external, and with differing motivation, capability, accessibility, and opportunity [King 2007]. Moreover, the weakest link into an intranet network is the human factor -journalist and network administrator- whose attitude towards security and threat varies significantly [King 2007].

4.1 Internal Threats

Features such as network latency, throughput, and availability of network are major factors of concern to a security analysis in newsroom architecture; with availability considered the quintessential [Huynh et al. 2010]. DOS/DDOS are the major threats to this quintessential factor. A malicious internal intruder who may otherwise be a legitimate user could be a major source to these threats. Generally, internal threats to intranet could either be as a result of un-authorization or un-authentication [Rao 2003]. Such internal threats could include but not limited to; illegal internet connection, unauthorized intranet connection, mobile storage equipment/device, and system vulnerabilities.

4.2 Illegal Internet Connection

While firewalls dictates the permeability of internal user to internet servers, it may not be able to prevent against newly discovered vulnerabilities in access control [Khoussainov and Patel 2000], and once an illegal access is gained, both active and passive eavesdropping can occur on data being transmitted. Additionally, an internal intruder can bypass border network protection through unprotected internal LAN, thus creating a backdoor access. In a newsroom, where gathering of international news is the hallmark, illegal access to internet can result to various security compromises. More so, since all station in a LAN share a single physical channel, compromising one station could be lead to attacks such as DOS, and even a DDOS. Segmenting the LAN using bridges as network filters could minimize the effect of a single compromised station [Khoussainov and Patel 2000]. Adopting the crypto-Ethernet NIC proposed by [Khoussainov and Patel 2000] could also be a feasible solution owing to the fact that a newsroom network could be managed using same types of station, and dual NIC cards.

4.3 Unauthorized Intranet Access

Authorization is simply an access control system for resources on the intranet. A station not belonging to the intranet initially could be easily plugged (though some network systems use Static IPs, and well defined IP look up tables, so simple plugging cannot occur.) into the intranet, without due authorization from the network administrator. If such a scenario occurs, other possible attacks could be embedded/launched into the network- Trojan horse being a very common backdoor- leading to system compromise[Haiyan et al. 2010]. Access control system such as access control list (ACL), discretionary access control (DAC), mandatory access control (MAC), and role based access control system (RBAC) could be a very useful tool in preventing this type of vulnerability exploitation [Rao 2003]. Also [Rao 2003] proposed a flexible access control model as an intrusion detection system, as well as an intrusion alarming system against system misuse. Similarly, [Khoussainov and Patel 2000] describes a practical requirement for unauthorized intranet access, with special consideration on integrating improvement into existing infrastructure. Also, the use of static IPs augmented with well defined look-up tables could mitigate this threat.

4.4 System Vulnerabilities

Working with the axiom that no system is perfect, especially in conjunction with human resources- the weakest security link [Wood and Banks 1993], there are always some vulnerabilities in any system [Haiyan et al. 2010] which could range from improper/wrong configuration, factory inaccuracy, to inherent weakness of the system. An internal intruder could be a source of the inclusion of Trojan-horse and or botnets. Attacks like botnets could lead to unauthorized information disclosure [King 2007].

Proper and adequate configuration is a prerequisite for adequate security. This implies that other function of stations which are not needed for a newsroom operation should be disabled, such as TELNET; remote access to intranet switches, routers and servers [King 2007]. This could prevent exploitation of system vulnerabilities. Additionally, the use of audit trail log system could also be considered as a pro-active measure, especially when combined with staffs (journalists, technical units, and management team), staff education, training and awareness (SETA) programs are proactive way of addressing some system vulnerabilities, coupled with network intrusion detection system (NIDS), and host intrusion prevention system (HIPS).

4.5 Mobile Storage Equipment

It is an easier way of transferring malicious codes. Famous auto-run class of virus and ferry-class can also be distributed through devices [Haiyan et al. 2010] such as flash drive, CD ROM, e.t.c. Such an intrusion can cause station (Station and server alike) compromise. Furthermore, a single station compromise can cause a DDOS since intranet functions on host-host interaction. Disabling port of movable devices, exclusion of disk drive unit on a station, station clustering, and access control could be a preventive ways for this types of threat. HIPS could also be used to address these types of threat/attack vector [King 2007].

4.6 External Threats

The process of newsfeed, gathering information and information dissemination are links to and fro the intranet. This could also be the channel of entrance for an external intruder. In [Haiyan et al. 2010], a logical structure of newsroom intranet was depicted. Additional, some necessary aggregates and predicates for predicting attacks attempts were also elaborated. However, attacks targeted at such network, depending on the motivation, resources and proficiency of the intruder; could bypass the rules of normal attack pattern [Jeong et al. 2007]. [Jeong et al. 2007] demonstrated attack scenarios on intranet using various risk analysis. Attacks such as dispersed/ distributed DOS, IP address embezzlement, e-mail hijacking, man-in-the-middle attack, network flooding, IP spoofing, eavesdropping, social engineering e.t.c are frequently experienced on intranet[Jamieson and Low 1989; King 2007], but peculiar to the newsroom is the DOS, DDOS, network traffic interception [Cheung and Mišić 2002]. These threats can however be mitigated using a virtual LAN/VPN (layer-2 & 3 security) either the IP-sec or non-IP sec based [Cheung and Mišić 2002; Arbaugh et al. 1998].

4.7 Network Vulnerabilities

The internet being a conglomeration of heterogeneous network (trusted and un-trusted) environment and also being an open system (OSI Model) forms the basic idea of the network vulnerability. A network whose constituent device and interconnection are physically secure, and its initial configuration are securely controlled could be termed a trusted network, since authenticating a single device over the network is equivalently the same as authenticating all devices on the network [Syngress et al. 2006]. Contrary to this is the Un-trusted network. An ideal VPN could guarantee secure (security triad-confidentiality, integrity, availability), connectivity, good quality of service (QoS), and network monitoring [Cheung and Mišić 2002]. A hardened configuration of network device can also reduce threat level [King 2007], while processes such as secure remote shell (SSH), secure www connection (SSL), and secure electronic mail such as encrypted PGP/MIMI [Khoussainov and Patel 2000; Hoffman 1998]; could be employed as measures against threats [Garfinke 2003].

Table I. Newsroom Vulnerability, Possible Type of attack, and its Mitigation

Newsroom Vulnerability	Possible Type of Attack	Possible Mitigation
Internal threats	Corporate espionage, data theft, data corruption, information leakage, logic bombs, Trojan horse	Continuous threat assessment evaluation and implementation, implementation of threat analysis & prediction tools
Illegal internet connection	Poor network performance, network disruption, data leakage	Regular network on-site evaluation and maintenance, regular update of IT infrastructure
System Vulnerability	Illicit data disclosure, system failure, poor network throughput	Regular maintenance, regular software/hardware updates
Unauthorized network access	Data theft, data disruption, unauthorized disclosure and dissemination of information, corporate espionage	Use of strong and secure password, regular training of staff, awareness on the need for ethical practice, strict adherence to information security policy
External threats/attacks	DoS, DDoS, website defacement,	System hardening, adequate network configuration, updating software patches, perimeter security system
Network vulnerability	DoS, DDos, news hijacking, untimely information leakage	Proper configuration of network infrastructure, regular penetration testing, regular update of patches
Mobile storage device	Data corruption, system disruption, data theft, classified information leakage	Total prohibition of the use of mobile storage device, removal of USB connection ports, disabling of wireless communication

4.7.1 *MAC Flooding.* This is a limitation caused switches and bridges inherent capability- characterized by limited hardware look-up table capacity- for storage of source address of received packet [King 2007]. When this look-up table is totally used up, further traffic directed to its address cannot be learned resulting in an overflow or permanently flooded. VLAN can be used to address such vulnerability [King 2007].

4.7.2 *IP Spoofing.* This is known as impersonation attack. It occurs at the IP-layer of the network [Harris and Hunt 1999]. Further exploitation of this attack could lead to TCP session hijacking [Harris and Hunt 1999]. Adopting a VPN could be a way to prevent such attack. Moreover, hardened router setting, filter and bridges [Jeong et al. 2007] and firewall [Harris and Hunt 1999] could also be used to prevent and or limit threats. For a newsroom broadcast scenario, this could result into QoS trade-off since VPN does not guarantee QoS [Arbaugh et al. 1998]. A more general way could be to connect only a trusted device to a trusted port [King 2007]. While this could be considered adequate against external attacks, it does little or no protection against internal attacks. If a trusted device is compromised, then all device connected sharing same port could as well be compromised. Table 1 gives a summary of the vulnerabilities in newsroom.

5. DISCUSSION

As elucidated in Table 1, newsroom vulnerabilities can be mitigated before any form of exploitation is experienced. However, the priority placed on security determines the level of mitigation implementation. In[Roy Sarkar 2010], detailed surgical analysis on insider motivation, misuse detection, misuse prediction as well as insider threat prevention is presented. Newsroom is a human centric organizational setting, which requires more on psychosocial behaviour analysis for threat prevention. Therefore, the security of any newsroom largely depends on the perceived relevance, from the management of the broadcasting institution. While more attacks that are sophisticated are not targeted at broadcasting institution today, it is not a yardstick however, to neglect the return on investment that adequate security can yield in the event of occurrence of an attack. Additionally, the possibilities of disgruntled staffs, or even laid off staffs, to attempt to carry out attack on newsroom cannot be ruled-out.

6. CONCLUSION

In this study, we examined the architecture of a typical newsroom from the security perspective. Communication processes between each components of the architecture were also considered. We further analyze the possible threats to the newsroom taking view from the inherent vulnerabilities identified from the architecture. Moreover, possible mitigation processes were also suggested. Further research on how to strengthen the security of the newsroom could be a feasible focus, in line with the business continuity plan of the organization.

REFERENCES

W.A. Arbaugh, J.R. Davin, D.J. Farber, and J.M. Smith. 1998. Security for virtual private intranets. *Computer* 31, 9 (1998), 48–55. DOI:http://dx.doi.org/10.1109/2.708450

D E Avrin, K P Andriole, L Yin, R Gould, and R L Arenson. 2000. Simulation of disaster recovery of a picture archiving and communications system using off-site hierarchal storage management. *Journal of digital imaging : the official journal of the Society for Computer Applications in Radiology* 13, 2 Suppl 1 (May 2000), 168–70. http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3453250\&tool=pmcentrez\&rendertype=abstract

D E Avrin, K P Andriole, L Yin, R G Gould, and R L Arenson. 2001. A hierarchical storage management (HSM) scheme for cost-effective on-line archival using lossy compression. *Journal of digital imaging : the official journal of the Society for Computer Applications in Radiology* 14, 1 (March 2001), 18–23. http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3489194\&tool=pmcentrez\&rendertype=abstract

Nazim Baksh. 2010. *Beyond Flak Attack: A New Engagement with the Newsroom*. Technical Report. Tabah Fundation.

CCSDS. 2003. *Consultative Committee for Space Data Systems*. Technical Report.

K.H. Cheung and J. Mišić. 2002. On virtual private networks security design issues. *Computer Networks* 38, 2 (Feb. 2002), 165–179. DOI:http://dx.doi.org/10.1016/S1389-1286(01)00256-0

Simson L. Garfinke. 2003. Enabling email confidentiality through the use of opportunistic encryption. In *dg.o '03 Proceedings of the 2003 annual national conference on Digital government research*. 1–4.

Liu Haiyan, Yang Zhaohong, and Zhang Zhanjun. 2010. Study on the Detection and Analysis Technique of Intranet Security. In *2010 International Forum on Information Technology and Applications*. IEEE, 134–137. DOI:http://dx.doi.org/10.1109/IFITA.2010.218

B. Harris and R. Hunt. 1999. TCP/IP security threats and attack methods. *Computer Communications* 22, 10 (June 1999), 885–897. DOI:http://dx.doi.org/10.1016/S0140-3664(99)00064-X

Paul Hoffman. 1998. Putting it together: designs on Internet mail. *netWorker* 2, 1 (March 1998), 19–23. DOI:http://dx.doi.org/10.1145/280437.280444

Minh Huynh, Stuart Goose, and Prasant Mohapatra. 2010. Resilience technologies in Ethernet. *Computer Networks* 54, 1 (Jan. 2010), 57–78. DOI:http://dx.doi.org/10.1016/j.comnet.2009.08.012

Rodger Jamieson and Graham Low. 1989. Security and control issues in local area network design. *Computers & Security* 8, 4 (June 1989), 283–290. DOI:http://dx.doi.org/10.1016/0167-4048(89)90087-4

Gyoo-Yeong Jeong, Dong-il Seo, Soo-Gab Kwon, and Jeong-Ho Kim. 2007. Intranet Security Evaluation Using Hacking Techniques. In *The 9th International Conference on Advanced Communication Technology*. IEEE, 810–814. DOI:http://dx.doi.org/10.1109/ICACT.2007.358473

Kevin Kawamoto, David Carlson, Cheryl Diaz Meyer, Rich Gordon, John Pavlik, Adam Clayton Powell III, Patricia M. Radin, Paul W. Taylor, and Melissa A. Wall. 2004. *Digital Journalism: Emerging Media & the Changing Horizons of Journalism*. Rowman & Littlefield Publishers.

S. Kent. 1981. Security Requirements and Protocols for a Broadcast Scenario. *IEEE Transactions on Communications* 29, 6 (June 1981), 778–786. DOI:http://dx.doi.org/10.1109/TCOM.1981.1095068

Rinat Khoussainov and Ahmed Patel. 2000. LAN security: problems and solutions for Ethernet networks. *Computer Standards & Interfaces* 22, 3 (Aug. 2000), 191–202. DOI:http://dx.doi.org/10.1016/S0920-5489(00)00047-7

Paul King. 2007. In the new converged world are we secure enough? *Information Security Technical Report* 12, 2 (Jan. 2007), 90–97. DOI:http://dx.doi.org/10.1016/j.istr.2007.04.004

Chin-Chuan Lee. 2000. *Power, Money, and Media: Communication Patterns and Bureaucratic Control in Cultural China (Media Topographies)*. Northwestern University Press.

Scott Matics. 2010. Automating newsroom workflow. *Broadcast Engineering* (2010).

BBC News. 2011a. Behind the scenes at the cradle of TV. (2011).

BBC News. 2011b. Closing the BBC News Desktop Alert and Ticker. (2011).

Quyen L. Nguyen and Dyung Le. 2010. Archival asset package design concept for an OAIS system. In *Proceedings of the 2010 Roadmap for Digital Preservation Interoperability Framework Workshop on - US-DPIF '10*. ACM Press, New York, New York, USA, 1–10. DOI:http://dx.doi.org/10.1145/2039274.2039278

Dennis Nicholson and Milena Dobreva. 2009. Beyond OAIS: towards a reliable and consistent digital preservation implementation framework. In *DSP'09 Proceedings of the 16th international conference on Digital Signal Processing*. IEEE Press Piscataway, 104–111.

Mike Palmer. 2008. Newsroom Workflow. *News Operations / Whitepaper* (2008), 52–54.

Vahid Ranjbar. 2011. The Narrator, Iran:Baqney. (2011).

H.R. Rao. 2003. Intrusion countermeasures security model based on prioritization scheme for intranet access security (emerging concepts category). In *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.* IEEE, 174–181. DOI:http://dx.doi.org/10.1109/SMCSIA.2003.1232418

Kuheli Roy Sarkar. 2010. Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report* 15, 3 (Aug. 2010), 112–133. DOI:http://dx.doi.org/10.1016/j.istr.2010.11.002

Danny Schechter. 2003. *How Media Has Changed Since the Day that 'Changed Everything'*. Technical Report. CommonDreams.org.

Syngress, Dale Liu, Stephanie Miller, Mark Lucas, Abhishek Singh, and Jennifer Davis. 2006. *Firewall Policies and VPN Configurations*. Syngress.

Paula Viana, Mario Cordeiro, Vitor Rodrigues, Damien Bommart, Giullia Ferrari, Massimo Starmbini, Ingo Hoentsch, Tobias Marx, Wlater Bernet, Edgar Muller, Bernard Cousin, Mathurin Body, Serge Daulard, Bernard Algayres, Marc Laurentin, and Inesc Porto Isep. 2003. *A Unified Solution for the Integration of Media Applications and Products in Broadcaster Environments - The ASSET Architecture*. Technical Report.

Mark Warner. 2008. *IP-based centralcasting*. Technical Report. Broadcast Engineering.

Jerry Whitaker. 2005. *Standard Handbook of Broadcast Engineering*. McGraw-Hill Professional.

Charles Cresson Wood and William W. Banks. 1993. Human error: an overlooked but significant information security problem. *Computers & Security* 12, 1 (Feb. 1993), 51–60. DOI:http://dx.doi.org/10.1016/0167-4048(93)90012-T

KISO Yasuharu and FUKASAKU Masaki. 2011. Total Nonlinear Editing Solution that Supports News Production Workflow. *NEC Technical Journal* 6, 3 (2011), 38–41.