Security Controls or Countermeasures: Vunerabilities Prevention

Frank Appiah

October 17, 2020

SECURITY CONTROLS OR COUNTERMEASURES: VUNERABILITIES PREVENTION.

FRANK APPIAH.

KING' COLLEGE LONDON, CENTRE OF DOCTORAL STUDIES, ENGLAND, UNITED KINGDOM.

frank.appiah@kcl.ac.uk

appiahnsiahfrank@gmail.com.

Extended Abstract^{+}. This looks at the security control abstracts (i) concerning creation of secret Ceil to attempt prevent paper un-ruin (ii) deflecting by choosing stamp over a digital watermarking or the vice versa (iii) detecting by validating in space-time of stamp or watermarking. (iv) recovering from counterfeits information and it's behavioral effects. Vulnerabilities prevention measures are addressed as a second look at more digitized image watermarking.

Keywords. security control, secret Ceil, stamp, watermarking, vulnerabilities prevention, recovery, document, counterfeits, countermeasures.

Year of Study: 2016 **Year of Publication: 2020**

***AFFILIATE. UNIVERSITY OF LONDON, KING'S COLLEGE LONDON, DEPARTMENT OF INFORMATICS, LONDON, UK.**

1 INTRODUCTION

Ghana is an international country and the international dimensions of decentralized network[1, 3] of watermarking image can be an exploitation. This treats risk of un-ceiled secret information dealt with by a two point statement. The conception of creation of secret Ceil to attempt prevent paper un-ruin is discussed to bring fort the ideas of thought. The ways of document processing a more digitized image watermarking will be look at in addressing the counterfeit information in computer crime. There, three ways of addressing counterfeit information in computer crime will be looked at detail. A board of storytelling in the castle of fortress is approved. This is so because in the castle of counterfeiting by duplication, one can insert an image quickly in the document processing of the watermarking paper. How should it be address? Counterfeiting by duplication[2] has a creation in risky information and it is looked at by 8 bulletins of security characteristics. Vulnerability is a weakness in the security system[2]. A threat is blocked by control of vulnerability. A control is a protective measure used as an action, procedure or technique.

Simply, this is security measure research report is addressing the following:

- Creation of security controls in un-ceiled secret information
- Laying out risk of un-ceiled secret information and ways of dealing with it.
- Certain on ways of document processing with digitized image watermarking
- Middle aging of counterfeiting by duplication with deletion-replacement and insertion-replacement.
- A decentralized network with marginal error on control printing with watermarking process.
- A counter-attack measure in validating and verification of authentic documents and

- Delegating to the fortress of counterfeiting by duplication to characterize risky information by security means.

Section 2 is about attempts in preventing un-ruin secret paper. Then in section 3, watermarking process is looked at. Section 4 is a discussion on counterfeiting by duplication characteristics.

An unauthorized person or party can create *fabrication[2]* of counterfeit object or information on a computing system. *Confidentiality* is a measure to ensure that information is only accessed by an authorized parties. *Integrity* is a measure to ensure modification of information by authorized means only. The third measure of security goal is *Availability*. It is a measure to ensure accessibility at appropriate times exponentially. A secure system has measure of balance in secure goals for building an authentic and authorize information access.

3 CREATION OF SECRET CEIL

In the creation of secret Ceil to attempt prevent paper un-ruin, vulnerabilities prevention is established. Un-ceiled secret can cause haste behavior to the attacker and will definitely leave the vulnerable room. If it is possible or necessary watermarking secret Ceil should be used to prevent ruining access control. Security agents chasing a person out of a room because counterfeit ceiled can cause embarrassment or dismissal. Sometimes, control can prevent or mitigate attacks. Computer crime can be the exploit of digital watermarking[2] a document or paper. This is an imminent attack on the secrecy of information passed through a document. A method of defense needs to neutralize the threat in order of proper protection against harmful data or information.

The risk of unceil secret information can be dealt with by:

1. *preventing* counterfeit ceiled or watermarking by blocking access to stamp(cal-marker) or digitizing the watermarking on a certain algorithm,
2. *deterring* by making the watermarking color has a color profile that can be analyzed to validate its exploits,
3. *deflecting* by choosing stamp (cal-marker) over a digital watermarking or the vice-versa,
4. *Detecting* by validating in space-time of stamp or watermarking Each room at the secure site can be time-stamped at certain intervals of operation. Digitally, it is quite easy to do this but hard in physical time-stamp process.
5. *recovering* from counterfeit information and its behavioral effects can be placed under incident response procedure. A careful loot at controls that can institute confidentiality, integrity and availability can be done. A measure can be a counter on incidents of dirty, bad or ruin documents or papers. A threshold placed on certain cases of ruin incidents can raise an alarm of need to attend to the incident and recover.

3 WATERMAKING PROCESS

A second look at the more digitized image watermarking will address certain ways of document processing:

1. The watermarking image will be placed on authorized document marker and a printer control software will count the number of documents printed with the watermarking. The printer control software will authenticate before it can be accessed at operating systems level. The technique of authentication can be password or biometry (fingers, iris, height etc). A time-stamped key-pass can be created and maintained for

availability. This can be public key infrastructure or ACL (Access Control List). It blocks the counterfeiter from having a watermarking document to print fake information on it.

2. The image is placed at secure ftp (file transfer protocol) in a decentralized manner. In the decentralized scenario, the document marker will still need to be authenticated as usual to able to have access to the digital document to make a copy for further processing. The network printer control software will still be able to keep record of the total number of watermarking print outs. It is impossible to make a copy without being seen or getting noticed. Counterfeiting a watermarking document is still deterred and deflected. It is deflected in that sense because the decentra-lised approach made it attractive for counterfeit exploitations. It is a natural hierarchy of main document access to a more decentralized document accesses.
3. A security officer or engineer addressing duplication copy in cases an attacker deletes and insert a counterfeit copy to be used by the document marker thereby making information lose confidentiality or integrity. In the middle ages of counterfeiting by duplication, a copy of existing image is kept with the security officer or engineer on deletion-replacement or insertion-replacement. In the castle of counterfeiting by duplication, a different but approved image is quickly inserted into the document processing of the watermarking paper. Then it is casted into decentralized networks with a marginal error on the previous information dissemination from the control printer software. The fortress of counterfeiting by duplication a security officer will counter-attack with an invalid document fight in the sense of seizing and requesting a re-print of information to process a new.

4 COUNTERFEITING BY DUPLICATION

Counterfeiting by duplication creates a methods of recovery in risky information. The fortress of counterfeiting by duplication can look at these security characteristics:

(1) A strong gate or door has been broken into and this make the document/ paper incorrect.

(2) A heavy wall to withstand paper theft is broken into pieces.

(3) A guard on access-bridge is wounded and at hospital.

(4) There was a cancellation at the main entrance and it is impossible to have a paper of such at that time. Possibility of paper theft on vacations.

(5) A control system is not responding to access code entered.

(6) There was a fight between some officer and pass-by: thus a moment to grab a copy of paper.

(7) Acknowledgment of vulnerabilities on the Internet, it is possible for an attacker to hack or crack into secure site and can cause a theft of document.

(8) An intern replaces a security personnel at job and his/her access code cannot verify correct information.

5 CONCLUSION

Ghana is an international country and the international dimensions of counterfeiting by duplication, thefting by delection-replacement or insertion-replacement, cyberattacking, hacking/cracking on internet/ decentralized networks

, strong gating with incorrect measure, ungaurding on access-breach, unlawful entry, uncontrolling access system codes, momenting by pass-by fights, intern replacement unverifiables and unvalidating information are exploitations that needs to be addressed.

If it is possible or necessary watermarking secret Ceil should be used to prevent ruining access control. Then it should be used. If counterfeiting by duplication creates a methods of recovery in risky information. Then, it should be recover after incident. If a security officer or engineer can address duplication copy in cases an attacker deletes and insert a counterfeit copy to be used by the document marker thereby making information lose confidentiality or integrity. Then, it should be engineered for counter measuring.

If in a decentralized scenario, the document marker will be able to authenticate as usual to able to have access to the digital document to make a copy for further processing. Then, it should create authenticated access. If the technique of authentication and authorization can be by password or biometry (fingers, iris, height etc). Then it should create technology for culturing and socializing the security process of characterization.

If file-transfer protocol gives the decentralized manner of network access with secure means. Then it should create confidentiality and availability in the security process.

If Unceil secret paper creates vulnerabilities and embarrassment in ruining the authenticity of document. Then it should leave the security room of vulnerabilities.

If security agents unchase theft document in a vulnerable situation. Then it should be way to dismissal from the work place.

If it is hard and difficult to physically time-stamp all documents at a security site. Then watermarking by stamping should be the way to countermeasure.

If vulnerabilities prevention is a means to countermeasure a counterfeit information. Then finally a Ceil by watermarking should be used.

Compliance with Ethical Standards

(In case of funding) Funding: This is research is funded by King's Alumni Group, Association of Engineering with ISAreference grant number: 204424 20821845.

Conflict of Interest:

Author, Dr. Frank Appiah declares that he has no conflict of interest .

REFERENCES

1. Stallings W. (1999), Cryptography and Network Security: Principles and Practice, Prentice Hall. 2nd Edition.
2. Pfleeger Charles P. and Pfleeger Shari L.(2003), Security in Computing. Prentice Hall.
3. Coulouris G., Dollimore J. and Kindberg T. (2005). Distributed System. Addison Wesley. Fourth Edition.