A Dynamic Security Model for Addressing Hacking Risk Factors

Saad Abdullah Alsunbul[1,2] *ssunbul@kacst.edu.sa*
[1]Computer and Electronics Institute
King Abdullaziz City for Science and Technology
Riyadh, Saudi Arabia
[2]Faculty of Information Technology *saad.alsunbul@monash.edu*
Monash University
Melbourne, Australia
Phu Dung Le *Phu.Dung.le@monash.edu*
Faculty of Information Technology
Monash University
Melbourne, Australia
Jan Newmarch *j.newmarch@boxhill.edu.au*
School of IT, Computing and Mathematics
Charles Sturt University
Bathurst, Australia
Jefferson Tan *jeffetan@du1.ibm.com*
IBM Research Australia
Melbourne, Australia

Abstract

Communication technologies have a significant influence on the business industry. Exchanging information, storing and retrieving data, and cutting communication costs are prime reasons for relying heavily on these technologies. However, these technologies are significantly affected by hacking. Due to neglecting the behaviour of hackers during the initial design stage of common security solutions, including firewalls, Intrusion Detection Systems, Intrusion Detection and Prevention Systems, Honeypot and Honeynet, successful hacking attempts still exist. This paper aims to investigate pre-hacking steps (footprinting, scanning, and enumeration) and to highlight the risk factors that are not considered during the development of current security solutions. These risk factors are the common causes of the failures of current security solutions against many hacking attempts. Moreover, this paper proposes a dynamic security model to guide security researchers towards proposing security countermeasures that address these risk factors, which eventually lead to minimising hacking risks.

Keywords: pre-hacking steps, dynamic security model, hacking techniques, footprinting, scanning, enumeration.

1. Introduction

Communication technologies have brought significant advancement to the business industry, which has become a single interdependent system. Efficiency, speed, and reducing communication costs have made these technologies a necessity. Nevertheless, these technologies suffer significantly from hacking threats. Hacking is defined in [1] as 'the attitude and behavior of a group of people who are greatly involved in technical activities which, more commonly today than in previous years, result in gaining unauthorised access'. There are countless motivations for hacking, including political causes, such as the 2012 incident on Saudi Arabian Oil Company [2], or stealing, such as the 2014 incident with Sony Picture Entertainment [3].

There has been considerable effort made by security industry and researchers to minimise hacking risks, including firewalls, Intrusion Detection Systems, Intrusion Detection and Prevention Systems, Honeypot and Honeynet. However, the gap between the offered security countermeasures and successful hacking attempts is significant [4]. This is due to the difference between the methodologies of security researchers and hackers in pursuing their objectives. In addition, the lack of understanding the behaviour of hackers during the initial design stage of security countermeasures makes them defenceless against new forms of hacking techniques [4,5]. Therefore, studying hackers' methodologies have become a necessity to develop effective security countermeasures.

Therefore, this article aims to provide deep insight into the behaviour of hackers based on pre-hacking steps, including footprinting, scanning, and enumeration. Examining and understanding hacking methodology against current security solutions, allow us to draw conclusions on hacking risk factors listed as: being a static security solution, easing acquiring information about victims' systems and being single security responsibility. Furthermore, this paper introduces a dynamic security model to guide security researchers towards designing effective security countermeasures based on the concluded hacking risk factors.

This article is organised as follows: Section 2 investigates the behaviour of hackers. Section 3 highlights the risk factors which are associated with current security solutions. The dynamic security model is explained in Section 4. Section 5 summarises this article.

2. Background

Hacking is an overused term, and the differentiation between hacking and attacking is ambiguous. Attacking is a general term referring to all non-authorised activities directed towards technologies in general whether to cause damage or to break into systems. Hacking is the most sophisticated attack classified under the attack category aimed to study all technological aspects in most infrastructures and explore vulnerabilities associated with operating systems (OSs), networks, communication protocols, security postures, and applications [4].

Most hackers take considerable time and effort to investigate a victim's infrastructure with sophisticated adopted hacking techniques and broad knowledge of the technologies for one reason: seeking vulnerabilities. The prime reason for the existence of vulnerabilities is the initial design of existing technologies. There were designed to satisfy basic requirements: speed, performance, and efficiency. Utilising the technologies in an appropriate way was an assumption at the early stages of developing these technologies, and the security as a primary objective was neglected [1].

Even with complete awareness nowadays of the importance of security, most services at some stage in their lifetime will contain vulnerabilities, and hundreds of them are discovered yearly. The current security practice regarding vulnerabilities is to patch a security hole after it has been discovered. The timeframe between exposing a vulnerability to the public and patching it is an absolute leverage for hackers, which gives them enough time and ease for breaching [1][4].

Minimising hacking risk is a broad and complex research area due to the countless number of hacking techniques and the appearance of new hacking techniques associated with advanced technology. However, most sophisticated hackers (the producers of hacking tools and scripts) perform three pre-hacking steps. This stage is related to information gathering, which is critical to escalate the success rate of hacking attempts. The pre-hacking steps consist of *footprinting*, *scanning*, and *enumeration* [1][4][5][6]. The following subsection describes in detail these pre-hacking steps and their relation to hacking techniques.

Pre-hacking steps

Hacking techniques comes in countless forms and recounting all techniques is impractical. Most hackers put considerable time and effort into ensuring the success of their hacking techniques.

Therefore, they devote their time to collecting information about their victims' systems and design the most appropriate hacking techniques. Pre-hacking steps are a sequential process for gathering information they need.

Sophisticated hackers start collecting information via footprinting. They start with a list of network blocks and try to understand how the targeted victim operates. They investigate the interrelation between their victims and external organisations to mark potential vulnerabilities. With the right tools and patience, hackers can end up with a detailed profile of the victim's system, which includes IP addresses, network blocks, employee names, phone numbers, mail server and DNS server [1][4][5][6].

The following step is scanning in which hackers start sending malicious packets to the victims to obtain necessary information. It requires continuous engagement with the victim's system. The main purpose of this stage is collection of necessary information, which includes the IP address of the victim's system, OS type and version, running services, and open ports. For instance, remote control attack is possible if the hacker obtained the following information:

- IP address: One system is listening to incoming traffic.
- OS type: Windows.
- Running services: SMB is running.
- Open ports: 139 and 445 ports are open.

The last step in information gathering is enumeration. Enumeration is the most intrusive step compared with footprinting and scanning. It is related to gathering information for known vulnerabilities and exploring new vulnerabilities in addition to identifying user, system, and admin accounts. What left for a hacker to perform a remote control attack is obtaining one account with high privileges. Nevertheless, hacking techniques have evolved to target end users using social media. Sophisticated hackers construct malicious messages and send them to end users in the victim's organisation via a phishing technique, using email or social media. This requires the spreading of malware in the victim's system via incorporation with a common program. Therefore, instead of performing scanning and enumeration manually, malware is embedded with scanning and enumeration operations to be part of the malware main objectives. These hacking strategies are called *advanced persistent threats* (APT) [5][7]. The following figure summarises the relation between hacking strategies and pre-hacking steps.

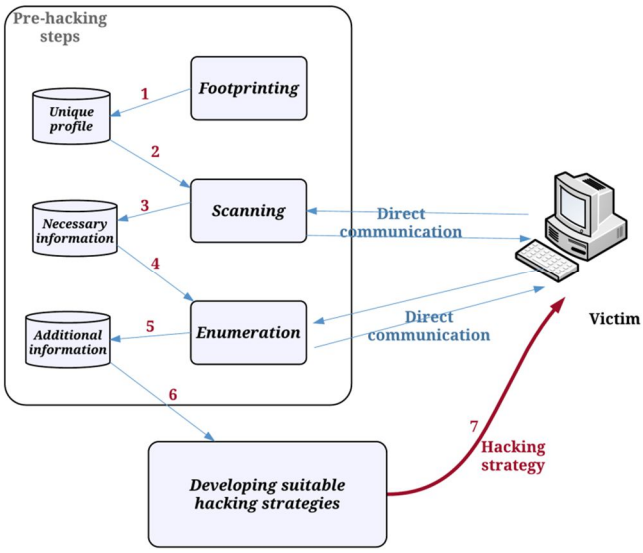

Fig. 1. Hacking techniques and pre-hacking steps.

At the final stage, the hacker has effectively recognised points of entry. Before they form their hacking strategies, they intensely probe the spotted services looking for known weaknesses or discovering new vulnerabilities. Enumeration is a process that includes active engagement and direct queries with the target's systems, giving it a higher level of intrusiveness compared with scanning (see Figure 1) [1][4][5][6].

Studying hackers' methodologies provides us with a complete understanding of the way they launch their attacks. 'Think like a hacker' is the best way for security researchers and experts to develop a security system that minimises hacking risks. There are risk factors associated with current security solutions that make performing pre-hacking steps and developing hacking techniques successful in many cases. The following section discusses the risk factors.

3. Risk Factors

There has been considerable effort made by the security industry towards minimising hacking risks, such as firewalls, intrusion detection systems, intrusion detection, and prevention systems, honeypot and honeynet. However, successful hacking attempts still exist. Through investigating pre-hacking steps and current security solutions, there are noticeable risk factors. These risk factors make current security solutions defenceless against many hacking techniques. These risk factors include being a static security solution, ease of acquiring information by hackers, and single security responsibility.

Static Security Solution

Most current security solutions share one characteristic: being a static solution. A static security solution from a hackers' point of view is fine leverage for investigating and acquiring the information they need. It gives them sufficient time to perform scanning and enumeration. Hackers have time to investigate the rules set for most firewalls and direct their malicious packets to open ports, which is the case of directing their traffic to an authorised port (port 80) [8,9,10]. For instance, guessing authentication credentials on Windows systems which is accomplished through mounting print sharing service over Server Message Block (SMB) [6]. This method requires from hackers to utilize TCP protocol and intentionally deliver packets to authorized ports by firewalls through port direction attack where it is port 80 in the giving example [6][11][12].

Moreover, with intrusion detection systems and prevention systems, hackers can examine these systems and identify the detection threshold, at which they can launch their hacking technique on 'low strength mode' to pass undetected [13,14,15]. Also, guessing authentication credentials on Windows and brute force attack on Unix systems can be applied under threshold to avoid detection [6][11][14][16]. Nevertheless, with honeypot and honeynet, hackers can identify the type of operation (low interaction or high interaction) and device of these systems with complicated protocols and utilise them for their malicious purposes [12][17][18]. Therefore, a static security countermeasure is defenceless against well-crafted hacking techniques.

Acquiring Information

As highlighted in Section 2, the information-gathering stage is a critical component that defines the methodologies of hacking techniques. The absence of the information obtained from scanning will eventually make developing suitable hacking techniques nearly impossible. Scanning only provides hackers with IP addresses, OS type and version, running services, and open ports. Moreover, information about the security countermeasure is another key element for successful hacking techniques. Acquiring the authorised ports in firewalls (port 80; as shown in the previous subsection) will impose a great security risk to computer systems.

In addition, identifying the threshold for intrusion detection systems and prevention systems will cause the malicious activity to pass undetected which is the case with guessing

authentication credentials and brute force attacks. Nevertheless, hackers can acquire information about the protection scope of deployed Honeypot and Honeynet systems and develop appropriate hacking techniques to utilise these systems [12][17][18].

Single Security Responsibility

Common security systems share another common risk factor, which is single security responsibility. A single security responsibility means that most security features are deployed in one piece of hardware. When that hardware is compromised, the entire computer network is compromised (single-point failure). These risk factors impose significant challenges for security researchers towards developing advanced defence systems. The following section describes the dynamic security model for the communication that focuses on addressing these risk factors.

4. Dynamic Security Model

The dynamic security model is introduced to guide security researchers and experts towards designing security solutions that effectively minimise hacking risks. The security within a computer network can be affected by countless factors, and research towards addressing security issues has taken completely different paths. Through investigating pre-hacking steps and current security solutions, we have concluded the following key principles to be included in the security model, which must be embraced with current and new defence systems to address the risk factors described in Section 3. Alsunbul et al. [1,5] proposed an active defence system based on the following key principles. The evaluation of their proposed security system showed the effectiveness, high accuracy and speed in deterring many hacking techniques. The following subsection describes the key principles.

Design Principles

Security level

The security for computer networks is heavily related to the network security and intercommunication between all endpoints, whether internal or external. It is impossible to exclude the security of endpoints out of the design of the defence system, since they are crucial elements. Therefore, the security model focuses on intercommunication between endpoints. If the network is protected, endpoints are saved from hacking techniques. The intercommunication is based on communication protocols, which is the main focus of the security model.

Security responsibility

Common security solutions discussed previously tend to place the security responsibility on one server or specific endpoints. Such concepts would place tremendous computational cost on that specific endpoint. A single-point failure is an open issue for these security solutions. The security model assumes that the security responsibility is distributed to all endpoints within the protected network even for remote users. It is not a responsibility for one server or some endpoints. In fact, it is reflected to all elements involved in a protected computer network. In other words, if a single element becomes compromised, the entire network is at high risk and might suffer the consequences. This design principle addresses one of the risk factors, which is ‘single responsibility’.

Active and dynamic security system

In practical terms, providing any network with a well-known static security feature might fulfil the expectation of protecting the network; however, it is just for a short period. In fact, hackers perform such a painstaking job to analyse and explore vulnerabilities in deployed technologies and security postures. Thus, when a vulnerability is discovered and publicly available for hackers, that security posture will become a risk factor instead of a safety measure.

One of the main principles in the security model is that the intercommunication must be continuously updated, such as creating and updating a unique communication protocol, which is known only for legitimate users. Alsunbul et al. [5] presented a perfect example of a security solution based on a unique protocol for legitimate users. The idea does not provide enough clarity and time for hackers to investigate the protected system and extract the needed information for developing appropriate hacking techniques. This dynamic feature is applied on intercommunication aspects in order to provide ambiguity and obfuscation in communication. This design principle addresses two risk factors, which are the static security solution and acquiring information regarding the targeted victim. The following subsection describes the dynamic security model.

Dynamic Security Model Stages

The suggested security model consists of six stages. It is a relatively mature dynamic security model for a whole computer network with a complete protection against risk factors discussed in Section 3. It consists of modelling, enforcement, analysis, detection, response, and monitoring. Every stage perceives certain security fundamentals and functions. The security life cycle in the model starts with modelling as the initial step and ends with the monitoring stage in which the hacking attempts have been detected and a response to such a security breach is required. The following figure illustrates the dynamic security model.

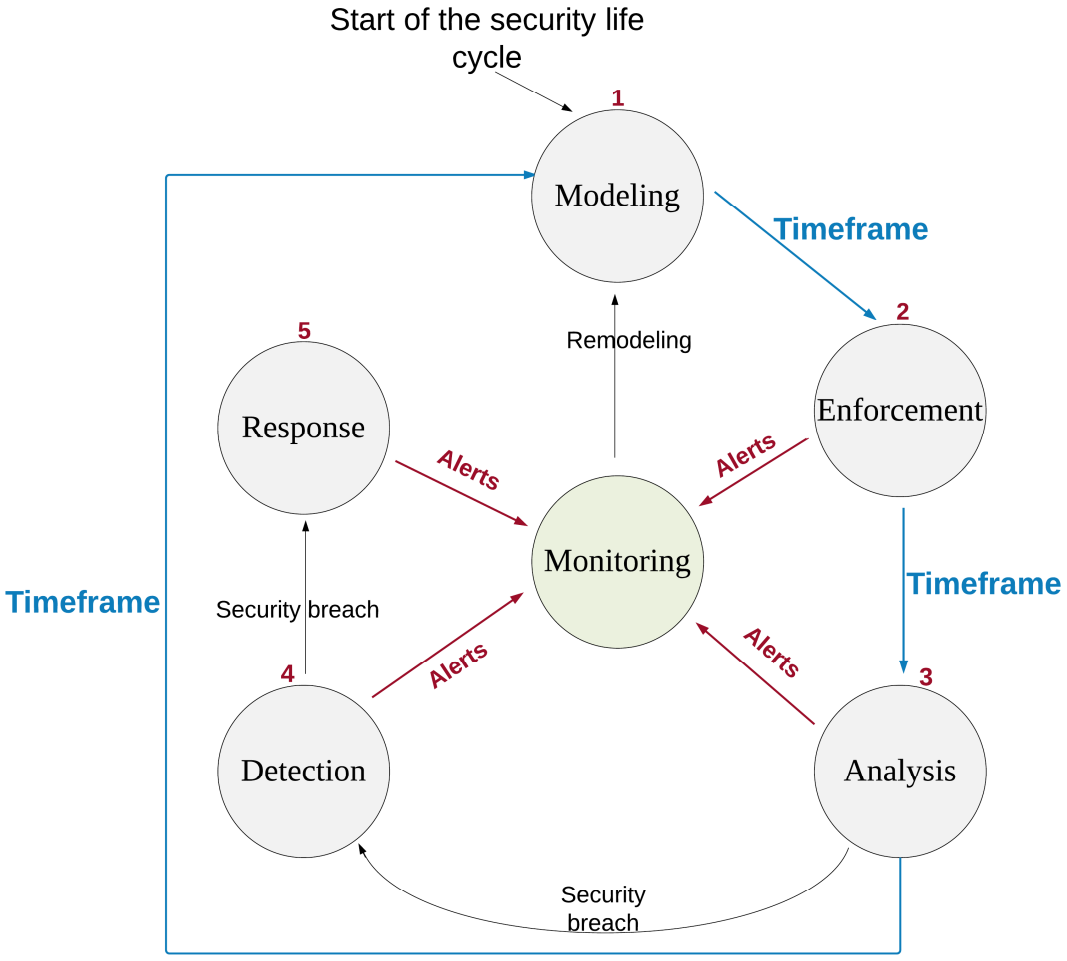

Fig. 2. The dynamic security model.

The life cycle in the security model is defined based on the timeframe instead of actions in which the condition of the security state moves to the following state. In other words, the lifecycle moves from analysis to modelling without the need for hacking-attempt recognition. In fact, the lifecycle starting with modelling might pass the detection and response stages if there are no detected hacking attempts. The core concept is to avoid providing a static security solution by updating the intercommunication procedure after specific timeframe (for instance: one day, one hour or ten minutes), which might ease the analysis and investigation of the proposed countermeasure by hackers. The following subsections explain the aspects of every component.

Modeling

Modeling is the first component in the lifecycle for our security model, and our security solution heavily relies on that stage. The main principle for that stage is to model a unique connection procedure between legitimate users. Modelling the intercommunication could be based on the protocol, where it was perfectly expressed by Alsunbul et al [5], or using cryptograph. This stage is responsible for forming and defining the behaviour for legitimate users within the computer network. The communication must be remodelled in every lifecycle based on the specified timeframe or hacking attempts. Alsunbul et al [1,5] used a specific hardware that automatically remodels the connection via changing the communication protocol.

Enforcement

The second stage in our suggested security model is enforcement. During the second step in the security lifecycle, the communication is already modelled. However, there must be assurance that the modelled communication is enforced by all endpoints in the protected network. This stage ensures that the security responsibility is distributed to all endpoints in the protected network. It could be a special hardware connected to every host as it has been suggested in [1,5] or developing network cards to suit the communication procedure.

Analysis and detection

Analysis as a conceptual idea is integrated with most security solutions. It is a method of studying and observing the intercommunication inside the protected computer network for detecting any hacking attempts. Cooperation between all endpoints appears in this stage where they monitor the communication based on the modelled communication in the first stage. The analysis in the security model is very efficient since the detection mechanism is based on spotting any communication request that is excluded from the modelled communication. For instance, a user requesting to communicate with the protected network using a TCP protocol when the modelled communication is not TCP protocol.

Response

The second important stage after spotting hacking attempts is the response. That stage includes all necessary functions and actions that must be performed when the assurance of hacking attempts has been granted. The response mechanism in our suggested security model forces remodelling of the communication procedure.

Monitoring

The core stage in the security model is to monitor all security stages via special hardware. Alsunbul et al. [5] proposed a monitor engine that receives alerts from all endpoints based on any request of communication excluded from the modelled communication. The excluded request of communication is considered a threat or error. This stage performs the decision making for the security defence system where faults and hacking attempts are detected. For instance, Alsunbul et al. [5] proposed a monitor engine that receives alerts from all endpoints. These alerts are generated when there are excluded communication requests from the modelled

connection or when a legitimate connection is not complying with the modelled communication.

5. Summary and Conclusion

Despites the considerable efforts by security researchers, successful hacking attempts exist. The main cause is the lack of understanding the behaviour of hackers during the initial design of current security solutions. This paper aims to direct the security researchers' attention to the behaviour of hackers, especially on the pre-hacking steps. Moreover, the risk factors have been highlighted in this paper, and a proper dynamic security model has been suggested to address these risk factors. The dynamic security model is suggested to guide security researchers during the design of new security countermeasures and to provide an effective defence system for most hacking techniques. Addressing these risk factors will eventually lead to minimising hacking risks.

References

1. Alsunbul, S. Le, P. Tan J. (2015). Deterring hacking strategies via targeting scanning properties. International Journal of Network Security & Its Applications (IJNSA). Vol.7. No.4.
2. Alsunbul, S. Le, P. Tan, J. (2013). A Defense Security Approach for Infrastructures against Hacking. In Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). p.1600. Melbourne, Australia.
3. Alsunbul, S. Le, P. Tan, J. Srinivasan. B. (2016). A Network Defense System for Detecting and Preventing Potential Hacking Attempts. In Proceedings of the 30th IEEE International Conference on Information Networking (ICOIN). p.449. Kota Kinabalu, Malaysia.
4. Appelt, D. Nguyen, C.D. Briand, L. (2015). Behind an Application Firewall, Are We Safe from SQL Injection Attacks?. In Proceedings of the 2015 IEEE 8th International Conference on Software Testing, Verification and Validation (ICST). p.1. 13-17 April.
5. Dehlawi, Z. Abokhodair, N. (2013). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. In Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics (ISI). p.73. 4-7 June.
6. Makiou, A. Begriche, Y. Serhrouchni, A. (2014). Improving Web Application Firewalls to detect advanced SQL injection attacks. In Proceedings of the 10th International Conference on Information Assurance and Security (IAS). p.35. 28-30 November.
7. McClure, S. Scambray, J. and Kurtz, G. (2012). Hacking Exposed: Network Security Secrets and Solutions, Seventh Edition: McGraw-Hill, Inc., 2012.
8. Mudzingwa, D. Agrawal, R. (2012). A study of methodologies used in intrusion detection and prevention systems (IDPS). In Proceedings of the IEEE Southeastcon. p.1. 15-18 March.
9. Najafabadi, M.M.; Khoshgoftaar, T.M.; Kemp, C.; Seliya, N.; Zuech, R. (2014). Machine Learning for Detecting Brute Force Attacks at the Network Level. IEEE

International Conference on Bioinformatics and Bioengineering (BIBE). pp.379,385, 10-12 Nov.
10. Pevny, T. Komon, M. Rehaky, M. (2013). Attacking the IDS learning processes. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). p.8687. May.
11. Rawlinson, K. (2014). Sony boss: 'No playbook' for dealing with hack attack. BBC. Viewed on 13 February 2016, http://www.bbc.com/news/technology-30744834
12. Saadaoui, A. Ben Souayeh, N.B.Y. Bouhoula, A. (2014). Formal approach for managing firewall misconfigurations. In Proceedings of the IEEE Eighth International Conference on Research Challenges in Information Science (RCIS). p.1. 28-30 May.
13. Mike, S. Johnson, B. (2006). Anti-hacker tool kit. New York: McGraw-Hill/Osborne.
14. Song L. Qian Z. Wei H. (2014). A new type of intrusion prevention system.). In Proceedings of the International Conference on Information Science, Electronics and Electrical Engineering (ISEEE). pp.361. 26-28 April.
15. Spitzner, L. (2003). The Honeynet Project: trapping the hackers. Security & Privacy, IEEE, vol. 1, pp. 15-23.
16. Vukalovic, J. Delija, D. (2015). Advanced Persistent Threats - detection and defense. In Proceedings of the 38th International Convention Information and Communication Technology, Electronics and Microelectronics (MIPRO), p.1324. 25-29 May.
17. Wattanapongsakorn, N. Srakaew, S. Wonghirunsombat, E. Sribavonmongkol, C. Junhom, T. Jongsubsook, P. Charnsripinyo, C. (2012). A Practical Network-Based Intrusion Detection and Prevention System. In Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCome), pp.109-214, 25-27 June.
18. Yang, Y. Bao, F. (2010). Password Protected Credentials. International Conference on Multimedia Information Networking and Security (MINES), pp.541,545, 4-6 Nov.