# A State-of-the-Art Survey on Computer Security Incident Handling

Parves Kamal, Saad Mustafiz

**Abstract—** Interconnection of the computers worldwide has enabled efficient transfer of files from one location to another freely. It has also made communication efficient through the world. Despite all the advantages the interconnection of computer has security related issues. . Since the invention of computer systems security handlings has all along been issue of public concern. However there are significantly important trends that have been recently established to cope with the challenge. The security of any organizational information is vital for economic progress. Information within the organization determines the management and organization of different aspects regarding it .The gist of this paper is to abbreviate the latest trends and techniques used in today's computer security incident handling world and how To reduce the impact of this incident.

**Index Terms—** Computer security incident response team (CSIRT), Computer security incident, wireless network sensors, DNS, Firewall, MySQL, Tripwire, Wormholes, Flooding, Sybil attacks

## 1. Introduction

Bern, et al Security incident handling, an integral part of security management, treats detection and analysis of security incidents as well as the subsequent response (i.e., containment, eradication, and recovery.)[1]Incidents are and unfortunate fact in any systems environment and they can be extremely damaging if goes unnoticed. Also if there is no expert response team in place the company will struggle to cope in the event of security incident occurs therefore having proper incident handling methods with well-trained computer security incident response team (CSIRT) is crucial to control and minimize any damage, preserve evidence, provide quick and efficient recovery, prevent similar future events, and gain insight into threats against the organization. [2]

## II. Information Security Breaches

Over the years many computer security related incident happened which often go unnoticed. Just how much this information security breaches cost is quite staggering.

according to the survey done by the Symantec in their 2010 Annual Study: U.S. Cost of a Data Breach report The average organizational cost of a data breach this year increased to $7.2 million, up 7 percent from $6.8 million in 2009 and 9 percent from $6.7 million in our 2008 study. Data breaches in 2010 cost their companies an average of $214 per compromised record, up $10 (5 percent) from last year and $12 (6 percent) from 2008.In UK if we look at the survey conducted by the INFOSEC in their INFORMATION SECURITY BREACHES SURVEY 2010 | technical report 63% of large respondents were attacked in the last year, compared with only 39% two years ago and if we see the figure shown below we can see the security breaches suffered by the different organizations. [3]

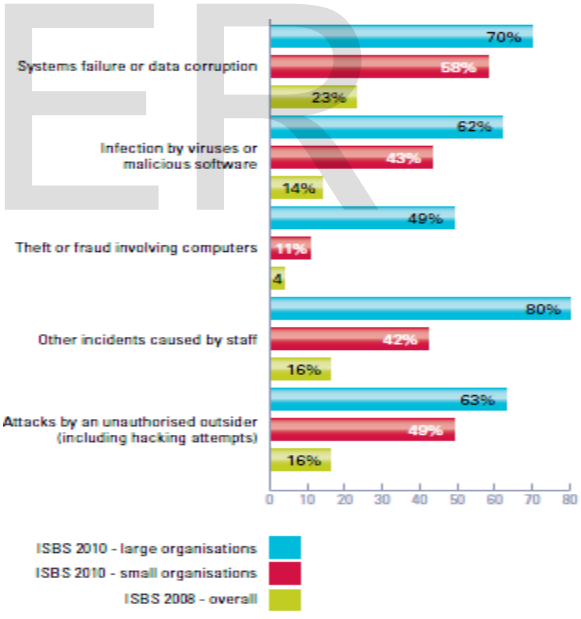


Figure 1: What type of breaches did respondents suffer? [3]

The average total cost of a small respondent's worst incident is between£27,500 and £55,000, up significantly on 2008. A similar trend is seen amongst large respondents; with the average total cost of the worst incident now up to between

£280,000 and £690,000 according to the survey. [3]

| | ISBS 2010 small organisations | ISBS 2010 large organisations |
|---|---|---|
| Business disruption | £15,000 - £30,000 *over 2-4 days* | £200,000 - £380,000 *over 2-5 days* |
| Time spent responding to incident | £600 - £1,500 *2-5 man-days* | £6,000 - £12,000 *15-30 man-days* |
| Direct cash spent responding to incident | £4,000 - £7,000 | £25,000 - £40,000 |
| Direct financial loss (e.g. loss of assets, fines etc.) | £3,000 - £5,000 | £25,000 - £40,000 |
| Indirect financial loss (e.g. theft of intellectual property) | £5,000 - £10,000 | £15,000 - £20,000 |
| Damage to reputation | £100 - £1,000 | £15,000 - £200,000 |
| Total cost of worst incident on average | £27,500 - £55,000 | £280,000 - £690,000 |
| *2008 comparative* | *£10,000 - £20,000* | *£90,000 - £170,000* |

Figure 2: What was the overall cost of an organisation's worst incident in the last year? [3]

So it is undeniable to emphasise the importance of Computer security incident handling in today's world.

## III. Latest Techniques in Computer security Handling

There has been several incident of attacks been carrying out in DNS servers recent years. According to recent studies there are nearly11.7 million public DNS servers on the Internet. It is estimated that nearly 52% of them allow arbitrary queries (thus allowing denial of service attacks or "poisoning" of the cache). About 31.1% of the servers also allow for the transfer of their areas of DNS.[5] João Afonso, et al in their paper proposed idea on Protecting Top level domain infrastructure with dynamic firewalling and network sensors. Their proposed systems comprised of firewall, Database, Web portal, Integrated Operation.

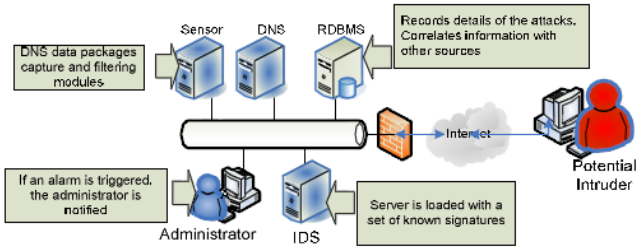


Figure 3: Diagram of proposed solution [4]

The way it works is the network sensor engine that analyzes the traffic from the DNS servers in the form of valid or invalid queries which then saved in the MySQL database. In case security incidents in real time. It also adds the advantage of operating in a distributed way, allowing the exchange of information between probes, and the reinforcement of its own security, even before it is threatened. [4] Wireless sensor network is new filed in the industry and Attacks in wireless sensor network are also on the rise. Wireless sensors are used in the field of monitoring, military procedure, remote surveillance etc. Habib, A in his paper mentioned the amount of possibilities of malicious activity exist in sensor networks. The most important vulnerabilities in sensor network routing are: [6]

- Spoofing or replaying information
- Selective forwarding or black holes
- Sink holes
- Sybil attacks
- Node replication attacks
- Wormholes
- Flooding
- Attacks against privacy

For protecting the wireless sensor networks authentication protocol like Security Aware Routing (SAR) protocol, to address the security issues in the wireless ad hoc networks, Sensor Network Encryption Protocol (SNEP) to provide confidentiality and two-party data authentication, µTESLA to provide authentication in broadcast messages, SPINS. This is a combination of the SNEP and µTESLA, with SNEP providing confidentiality s mentioned.[6]For managing key distribution LEAP protocol and PIKE are two of the more modern techniques of key establishment between the communicating parties. RC5 and TEA (Tiny Encryption Algorithm) have very good efficiency for the sensor nodes for encrypting data. [6] Prof Dhananjay, et al mentioned the use of open source tripwire in his paper which is used in Linux environment for detecting unauthorized activity in the computer. It creates baseline database of all the files that are created by the programme and with their size and modification date. So at any point user can check the state if the system against the baseline and thus finding any alteration. Tripwire runs in one of four modes: Database Generation, Database Update, Integrity Checking, or Interactive Update mode. [7]

Database Generation
$ tripwire --init
The /usr/local/lib/tripwire directory contains the Tripwire Database of your system's files (*.twd) named as host.twd, Where host is the host-name of the Linux machine and a report directory where Tripwire reports are stored.

Database Update
$ tripwire --update
Integrity check
$ tripwire --check > /tmp/report.txt
It will then proceed to check your file system against the Database and will create a file called report.txt in /tmp which Will contain information on what Tripwire discovered [7]

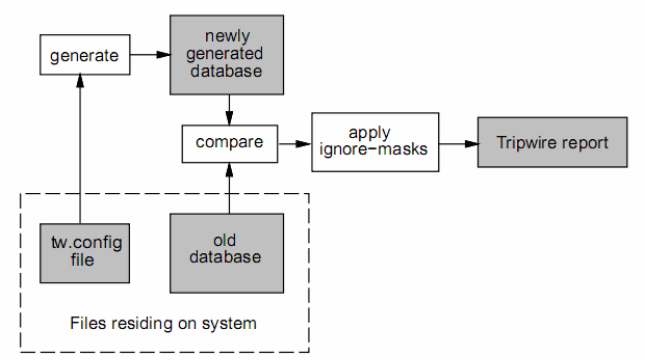


Figure 4: Working of Tripwire

Advantages of tripwire are it increases the security used with the intrusion detection system. Tripwire software reduces troubleshooting time, enabling rapid discovery and recovery. Disadvantages of being hard to install and maintain as well as it can be difficult to apply to frequently changing files. Wireless data communication has evolved rapidly and it's used in residential and enterprise network.

The growth of wireless networks and access devices have created more security vulnerabilities and resulted in more incidents and threats to both enterprise and consumers, this is mainly due to the exploitation of hackers of several inherent issues in wireless communication protocols and devices [9]. Tracing back to the intruders or wireless hackers is very hard as most of the tine it traces back to the ISP and the hacker's Identity remains undiscovered. H. Achi, et al mentioned Two Digital Forensics approaches: Tracing and Locating Wireless Hackers and Wireless Network Scanning and Identification.

1) Tracing and Locating Wireless Hackers:

Locating the wireless intruders within the omnidirectional antenna range used by the WLAN devices believed to be accurate is no more as expert hackers' use directional antennas having more powers often make it difficult to pinpoint the intruders locations within the range.[9] (Fig-5)

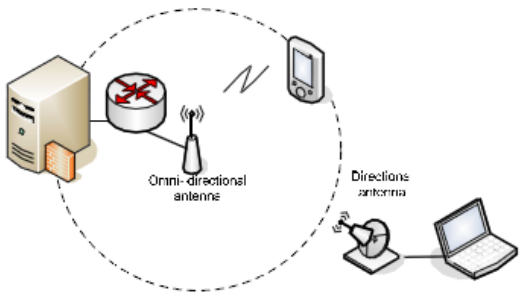


Figure 5: Access with Directional Antenna into Omni-directional AP

Of an abnormal behavior is detected it will be blocked from the firewall. [4] The advantages of this the ability to detect and control

Several techniques are proposed to narrow down the

Discovery of the location of the WLANs intruders [9]

Closet Access Point: Based on the closest AP intruder associated with. [9]

Triangulation: This is based on picking up the user Signal strength by three APs and finding the power Intersection to represent the corresponding location. [9]

RF Finger Printing: This is based on calibrating the system and taking measurements of received signal strength at specified locations and use them as reference finger print data to trace users locations. [9]

2) Wireless Network Scanning and Identification:

In the event of legal authorities confiscating the wireless devices it is important to find out the all the interconnected devices to get the data from. A good practise will be to scan passively to ensure all the elements are monitored.

## Iv. COMPUTER SECURITY RESPONSE TEAM

A computer security incident response team (CSIRT) needs to be formed and operated. This team helps an organization define and document the nature and scope of computer security incident. Where security controls are not adequate, high volumes of incidents may occur. This occurrence may overwhelm the resources and response capacity. In this case, there would be a delayed or incomplete recovery. There are instances where possible extensive damages and longer service periods and data unavailability happens. By complementing their incident response capability with resources, organizations are in a position to perform more effectively to maintain the security of networks, systems, and applications. This in turn leads to effective performance of incidence handling. In case of an incidence, communication would be required both within the organization and outside. The occurrence of communication need to be quick enough with predetermined communication guidelines which ensure only the relevant information is shared with the concerned parties. Poorly released information may lead to loses than the incident itself. Priority should be accorded to handling of individual incidences in an incidence process. Priority should be based on the following; how critical is the affected resources and Potential and Current technical effects of the incidence. These will determine the impact of the incidence at large on

the business. By prioritising incidence, the handlers would not be under immense pressure in the event of an incidence [10]

## V. NEED FOR INCIDENCE RESPONSE

Incident response is necessary because attacks cause a compromise of personal and business data. Incidents such as viruses, worms, Trojan horses, spyware and malicious code have disrupted or permanently damaged numerous systems and networks. National security and exposure of personal information raise the awareness for possible outcome of computer-based attacks. The concept of computer security incident response has gained wide acceptance due to the above threats from all spheres ranging from government, academia and the private sector [10]

## VI. BENEFITS OF INCIDENCE RESPONSE.

Benefits accrued from an incidence response capability include; information from past incident handling is used to prepare handling of future incidents. This also provides protection for systems and data. Assist in legal issues arising during the incidence [10]

Some of security techniques applied to computers include; labelling of files with authorized users list only, verification of the identity of user through a password. Shielding of computers to protect them from electromagnetic radiations, encipher information sent on telephone lines.

For physical security of computers, lock the room. Personnel who have the authority to alter the system should be controlled. It's important to certify that hardware and software are implemented as required. At times, use redundant circuits or programmed cross- checks to maintain security in the event of system failure [11]

## VII HOW TO REDUCE THE GENERAL IMPACT AND SEVERITY OF AN INCIDENT

- Establish and enforce policies and procedures that offer appropriate level of security.
- Management involvement on security policies and incident handling is required.
- Assess vulnerabilities regularly. Security specialist can done this vulnerabilities check.
- Latest patches should be installed and routinely checked.
- Security training program for staff and users need to be established.
- Users should be reminded of their responsibilities and restrictions through banners with strong messages.
- A strong passwords requirement policy should be developed, implemented and enforced.
- Monitoring and analyzing network traffic routinely.
- Regular check of logs and logging mechanisms.
- Verification of back-ups and restore procedures.
- Creation of a Computer Security Incident Response Team (CSIRT).

## CONCLUSION

Computer security is an integral part of any organization that's why the growing need of incident response technique and the computer incident response (CSIRT) team are ever so prevalent. There are various reasons why incident response teams are unable to effectively respond to the challenge from the attackers. This can be due to the lack of resources it possess or inadequate find that it has. Poor management and policies as well as inadequate knowledge on the latest threats can contribute to the failure of the CSIRT team.



## REFERENCES:

1. Bernd, Grobauer and Thomas Schreck. 2010. towards incident handling in the cloud: challenges and approaches. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW '10). ACM, New York, NY, USA, 77-86. DOI=10.1145/1866835.1866850 http://doi.acm.org/10.1145/1866835.1866850

2. G. Killcrece, K. Kossakowski, R. Ruefle, and M. Zajicek, "Organizational Models for Computer Security Incident Response Teams (CSIRTs)," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Handbook CMU/SEI-2003-HB-002003. http://www.sei.cmu.edu/library/abstracts/reports/03hb001.cfm

3. www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf

4. Afonso, J.; Veiga, P.; "Protecting the DNS Infrastructure of a Top Level Domain: Dynamic Firewalling with Network Sensors," Systems and Networks Communications, 2008. ICSNC '08. 3rd International Conference on , vol., no., pp.173-178, 26-31 Oct. 2008 doi: 10.1109/ICSNC.2008.68

   URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4693665&isnumber=4693626

5. D. Wessel's, "A Recent DNS Survey", DNS-OARC, November 2007.

6. Habib, A.; "Sensor network security issues at network layer," Advances in Space Technologies, 2008. ICAST 2008. 2nd International Conference on , vol., no., pp.58-63, 29-30 Nov. 2008 doi: 10.1109/ICAST.2008.4747687

   URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4747687

&isnumber=4747669

7. Prof Dhananja;Mr Manish Singh ; Prof Dr G.T. Thampi, "Incidence Handling and Response System" International Journal of Computer Science and Information Security, Vol. 2, No. 1, 2009

8. Achi, H.; Hellany, A.; Nagrial, M.; , "Digital forensics of wireless systems and devices technical and legal challenges," High-Capacity Optical Networks and Enabling Technologies (HONET), 2009 6th International Symposium on , vol., no., pp.43-46, 28-30 Dec. 2009 doi: 10.1109/HONET.2009.5423057 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5423057&isnumber=5423051

9. H. Achi, A. Hellany & M. Nagrial , "An overview of Digital Security Forensics Approach and Modelling", International Conference on Computer Engineering & Systems ICCES'08, Nov 2008

10. Scarfone, Karen, Tim Grance, and Kelly Masone. "Computer Security Incident Handling Guide." Computer Security. National Institute of Standards and Technology, Mar. 2008. Web. 24 Apr. 2012. <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>.

11. Jerome H. Saltzer and Michael D. Schroeder. The Protection of Information in Computer Systems. Communications of the ACM, 17(7), July 1974.



## AUTHORS BIOGRAPHY

**PARVES KAMAL:** Parves Kamal Has Completed BSc With honor's in Computer Security & Forensics from University of Bedfordshire (U.K), Cisco CCNA & COMPTIA SECURITY+ Certified.

EMAIL: Parves.kamal@outlook.com

**SAAD MUSTAFIZ :** Saad Mustafiz has completed BSc in Computer Science & Engineering from Ahsanullah University of Science & Technology, OCA: Oracle Certified Associate & Red Hat Certified Engineer (RHCE).
EMAIL: saadmustafiz@gmail.com