Incident Response: the road from a Security Policy to automated trace-back mechanisms

Sarandis Mitropoulos[1], Dimitrios Patsos[1], Christos Douligeris[1]

[1] Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str., Piraeus 185 34, Greece.

sarandis@students.unipi.gr, dpat@space.gr, cdoulig@unipi.gr

Abstract. Incident Response has always been perceived as a very important issue in every Corporate Security Policy. Every security incident has to be treated differently according to many different factors that define its significance, magnitude and effects. In this context, many Incident Response best practices were developed and adopted in corporate or legal frameworks and standards. On the other hand, Digital Forensics and trace-back mechanisms are considered to be the ultimate technical solution for holding attackers accountable for their actions. This paper presents a complete management framework and a structured methodology for efficiently respond to security incidents. Furthermore, it proposes an approach to effectively mirror specific management and policy issues to certain technical mechanisms in order to reach to the actual attacker. Finally, new challenges, open issues and the changing focus from corporate environments to ordinary users are presented, hoping to drive heavy research in this very prosperous field in Information Security.

1 Introduction

During the last few years we are witnessing the most important advances of technology, considering the fact that nearly one billion computing systems in our planet are already interconnected [1]. Under these circumstances, the new challenge for Information Technology (IT) is to provide a common ground for application development at all possible layers of infrastructures, services and devices. Today, many organization are providing access to their corporate systems to a number of different persons: employers, partners, contractors etc. A security incident in a corporate environment can affect lots of interconnected systems outside an organization's boundaries, therefore resulting to a huge number of side-effects. A security incident is defined as any related activity with negative security implications [2]. Traditionally, Incident Response Capability, within a corporate IT environment, is the process that aims to minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents [3]. Following the trends of Internet attacks and the progress made in international computer law, there are many instances where the actual attacker must be found in order to be held accountable for his actions. An effi-

cient Incident Response Capability has many important factors, each one introducing several features as well as limitations. One of the most important factor of an efficient Incident Response Capability is the clarification of the various management issues arising by incorporating a flexible Computer Incident Response Team, customized specifically to meet the organization's needs. On the other hand, a technical methodology combined with strong management commitment is necessary to coordinate a response and gain the utmost of the security technologies used. Finally, automated trace-back techniques and mechanisms (or semi automated Digital Forensics analysis) provide the reactive features of Incident Response, thus identifying the actual attacker. Most of incident response methodologies are strongly combined with the science of digital forensics, i.e. the processes of unearthing data of probative value from computer and information systems [4]. Forensics, in other words, include the necessary actions to trace back a security incident to its actual source and, in most cases, the physical person(s) that caused it and require strong understanding of network protocols and operating systems, while demanding patience and ability to follow law-related rules and procedures. Forensics is more centered in law enforcement agencies than research or practitioners [5].

Our approach is to identify and propose various schemas and artifacts in every critical factor that comprise a Corporate Incident Response Capability (also known as Incident Response Policy). Therefore, we present a detailed management framework including the key-players (contacts) that have to cooperate inside and outside the corporate environment. In turn, we present a structured methodology in order to assist the Incident Response Capability players choose from a selection of specific roles and responsibilities by applying certain security measures and techniques. Finally, we present the state-of-the art deployments in automated-trace back mechanisms that can help an organization to automatically reach to the actual attacker. Until now, little information is publicly available concerning the existence of an international de jure, either as a unique one or as part of larger, enterprise-wide information security standard. For example, all US Federal Agencies are obliged to provide an Incident Response capability to comply with OMB's Circular No. A-130, Appendix III [6], as well as the Federal Information Security Management Act (FISMA) of 2002 [7]. On the other hand, ISO/IEC 17799:2000 (Section 7.3), denotes that Incident Reporting and handling is essential for an organization but does not provide specific information on this [8][1]. With this context in mind, the need to address and solve the long-lasting issues on Incident Response is more than critical.

[1] This Section refers to non-existing sections on the same Standard (12.1.7), while the Introduction of the Standard that describes security incident reporting refers also to a non-existing section (6.1.3) of the same version. Finally, in this revision of the Standard, Incident Reporting (in the Index) is referring also to a non-existing section (Section 6.3.1).

2. Managing Incident Response

Responding to security incidents requires a lot of international efforts, since the Internet is nearly entirely linking whole of our planet. During the last 15 years, Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie Melon University is providing a central location for the reporting of such incidents as well as the appropriate solutions. Similar efforts also exist in Europe (Forum of Incident Response and Security Teams - FIRST), Australia (Australian Computer Emergency Response Team - AusCERT) and in various other countries. Computer Security Incident Response Teams (CSIRTs) comprise an essential part of modern Information Security Standards (like ISO/IEC 17799:2000), while their expectations are fully described in RFC 2350 [8],[9]. CSIRTs can be categorized by their magnitude within a specific constituency (internal, external, commercial, vendor, governmental, academic etc.) or by their type of existence (formal, ad-hoc etc) [10]. These types of teams can be also members of international efforts or can even be part of transnational agreements [11]. In [12] the various kinds of Computer Security Incident Response Teams Organizational Models are detailed.

The key-person in a corporate Incident Response Capability is *Incident Response Capability Leader*. He is cooperating with all other managers that should be aware of the occurrence of a security incident and ask for management decisions. This person can, in some cases, direct the *Computer Security Incident Response Team* (CSIRT), the people responsible for designing, implementing and updating the technical solution, the procedures and all the necessary guidelines for maintaining the Incident Response Capability. Furthermore, the systems and network administrator(s), are the people with the most technical knowledge within the organization, as their everyday jobs include design, installation and fine-tuning of systems and networks. In case of a security incident, they can provide a very useful feedback. They could either belong to the CISRT or alarmed only if there is a significant need. However, they have to be aware of any instance regarding a security breach. Last, but not least, The *Help Desk* personnel should participate in the program, since there could be cases where the organization should answer relevant enquiries.

Apart from IT-related sections of an organization, there is emerging need for cooperation with other corporate departments. For example, the Public relations department should be responsible for handling the corporate public image after a security breach. This task involves communication with 3rd parties (e.g. contractors, media agencies etc). Furthermore, the *Human Resource* department should participate in the Strategy in order to take the appropriate actions when an internal incident (caused by an employee) happens. The role of the *Corporate Investigations Group* is also important since, among other duties, it has to keep the fact secret for as long as it is needed, facilitating the tracing of the incident to the responsible party and not allowing information flow outside the organization that could affect its public image. This Group is often in close cooperation with the *Security Officer* and other security Personnel. These people are responsible for investigating security incidents and communicate with the *Law Enforcement Agencies*, in case a serious incident happens

(e.g. theft of IT equipment, unauthorized copying of proprietary software or data, etc). The *Legal advisor* of the organization is also essential in an Incident Response Capability, being the person in charge of compliance and providing legal advises during the various phases of Incident Response. Finally, the *Corporate Users* should be trained to react as the Incident Response Capability indicates in its policies, procedures and guidelines. In some cases, ordinary users discover incidents; therefore, they must know how to react in the first place and whom to communicate with when such an incident occurs.

Finally, according to the severity of a security incident there may be the need to cooperate with external parties that can play an important role to the discovery and response phases of a security incident. As an obvious example, the *Internet Service Provider (ISP*) can provide useful information when trying to trace a network connection for it provides the link of the corporate systems and networks with the outside world (be it the Internet, Extranets etc.). In some cases, the Law Enforcement Agencies should be contacted, especially when an incident corresponds to a computer-related crime. Cooperation with the Agencies is within the duties of the Security Officer and the Legal Advisor, as mentioned above. Finally, other Computer Security Incident Response Teams (CSIRTs) and/or external security experts can provide extremely useful services when an incident is beyond the reach of an organization's CSIRT. The key-players and their interactions are depicted in figure 1 [16]:

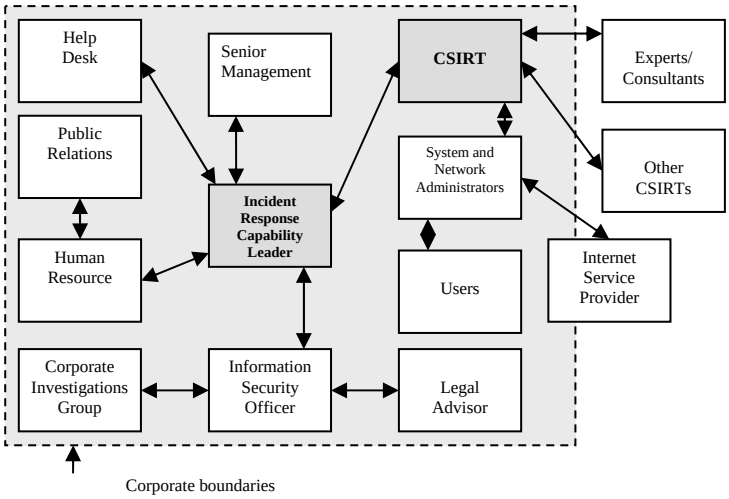

Figure 1 – The Incident Response Contacts

Summing up, the preparation, formulation, education, operation and maintenance of this framework is rather a management issue, considering the fact that management comprises an essential part of any Information Security program [8].

Both the literature and the commercial world are providing well-structured methodologies, most of them comprising of several distinct phases in order to effectively

handle its magnitude and efficiently respond to this. Important milestones are the "Framework for Incident Response" by the Information Security Team of DePaul University in US [13], the "HandBook For Computer Security Incident Response Teams" by Carnegie Mellon Software Engineering Institute [14] and "Computer Security Incident Handling Guide" published by NIST in January 2004 [15].

3 Structuring an Incident Response Capability within an organization

Trying to contrast appropriate actions when a security incident occurs we present the sketch of an Incident Response methodology in Figure 2, based upon the phases contained in [15] and [16]. We briefly explain the most important issues of every phase in the following.

3.1 Preparation Phase

Security mechanisms that protect both the corporate network perimeter (firewalls, strong authentication mechanisms etc.) and critical internal parts (Host-Based and Network-Based Intrusion Detection Systems – IDS) are to be found in nearly every modern corporate IT environment. For the purposes of Incident Response Capability, specific countermeasures have to be installed as well (e.g. sniffers, antivirus software, audit log consolidation software, backup software, etc) to gather and correlate as much information possible regarding a security incident.

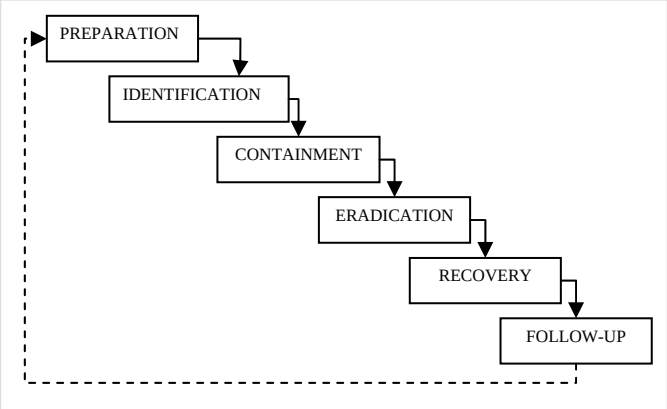

Figure 2– Incident Response Methodology Model

3.2 Identification Phase

The identification phase is of crucial significance, since it is the starting point of an incoming attack and critical decisions have to be made to categorize an event and respond accordingly (i.e. the beginning of evidence collection should start from that point onwards). The decision whether abnormal activity corresponds to an actual attack or an attack pattern is quite tricky and this is where audit log correlation information from the Preparation Phase is used. Nowadays, security technology offers a variety of methods via Intrusion Detection and (Near) Real Time Threat Management Systems that require a wide deployment into corporate networks. Apart from technology, the human factor also poses knowledge on what abnormal activity to a corporate environment is and decides global response strategies. For example, there are two main approaches regarding network incidents depending on the severity of them:

- Immediately identify close the attacker's point of entry and eliminate all possible access means or
- Remain 'open', as long as possible, and gather information to be used as evidence.

3.3 Containment Phase

Following identification, the next step is to apply immediate solutions, thus limiting the extent of the incident and driving the attack to the desirable extent. Not all attacks should be immediately stopped, since –for certain- reasons digital forensics analysis may be needed afterwards in order to identify the actual attacker(s).

3.4 Eradication Phase

This stage is primarily dealing with the mid and long-term solutions that have to be applied on the affected system(s) in order to eliminate any possible means for the specific attack recurrence. Possible actions taking place at that stage include policy compliance checks, independent security audits, policy updates, etc.

3.5 Recovery Phase

The recovery phase handle the procedures for systems restoration and security mechanisms enhancements in order to bring the whole system back to production and eliminate residual risk. Possible actions include complete systems rebuild, data recovery from backup media, installation of extra security mechanisms, etc. A vulnerability

assessment or a penetration test is advised to take place before putting compromised systems into production again.

3.6 Follow-Up Phase

Finally, it is of great importance that all actions and information regarding a security incident should be documented and electronic evidence should be disseminated to experts for analysis in a forensically sound manner. A post mortem meeting with senior management should also take place in order to assess the damage done and get the management commitment to strengthen the security policies and procedures following. Last but not least, the complete analysis of the incident, changes in systems configuration must be documented and the inventory of systems and network assets has to be updated to reflect them.

4 Network Forensics: Tracing back a security incident

Apart from effectively handling a security incident, there are many cases where the original source of an attack has to be found and, in yet more cases, the actual attacker(s) has to be identified so that be held accountable for his actions. We briefly present the problems of holding attackers accountable in the following.

During a security incident, many masquerade techniques can be used in order for an attacker to hide his/her original identity. Masquerade (aka impersonation) attacks are nothing new to Information Security and can be reproduced in various ways by the attackers, mostly using the following techniques:

- Link Layer spoofing, also known as MAC address spoofing (e.g. using a different MAC address than the original) [17]
- Internet Layer spoofing, also known as IP Source address spoofing (e.g. using a different source IP address than the original) [18]
- Transportation layer spoofing, also known as port spoofing/port forwarding (e.g. using a different TCP/IP port than the original one)
- Application layer spoofing (e.g. using a different email address than the original)

Following the numerous effects from Distributed DoS attacks [19], we can conceptually suppose that a number of attackers use some intermediate hosts and networks (i.e. different routing paths) in order to launch an attack to a victim machine(s). Apart from this straightforward attack scenario, an attacker may use many intermediate compromised hosts (known as stepping-stones) in order to hide his original identity along with launching a distributed attack [20]. In this scenario, the attacker uses another intermediate host before reaching to a “zombie” machine. This compromised host, called stepping-stone acts as a conduit for the attacker’s communication and is used to change the essence of the attack process. For example, an attacker can use

encryption resulting in hiding his actual identity. The reverse process of an attack (i.e. reconstruction of the attack path back to the originating attacker) that has used one of the previously mentioned masquerade techniques, though, is not straightforward. There are numerous reasons to prevent the correct reconstruction of the attack path (from the victim machine back to the attacker machine) including the effects of spoofing as well as security functions performed by security countermeasures that are already in place. In general, if $C = h_1h_2.. h_i h_{i+1} \ldots h_n$ is defined as the connection path between hosts h_i (i=1,..n), then the trace-back problem is, given the actual IP address of host h_n to recursively identify the actual IP addresses of $h_{n-1}, \ldots h_1$.

The issue of network tracing is of major importance for network engineers, especially when designing and implementing routing functions and protocols. The Internet Protocol [21] proposes the *Record Route* option for network tracing provisioning in the protocol header. The *Record Route* option mandates routing devices along a path to append their addresses to the IP options field. The protocol header has a fixed part of 20 bytes and a variable part, corresponding to the IP Options Field. However, the total length of every IP packet (in 32-bit words) is mandated by the value of the 4-bit IHL (IP Header Length), which is 15 (1111 in binary), thus resulting to a maximum of 60 bytes (and therefore leaving 40 bytes for IP Options). Considering the size of the Internet along with the heavy routing information used in current networks the *Record Route* field appears rather limited to withstand recording in every hop a packet traverses. First of all, there would be a tremendous amount of processing overhead in routing devices, since at least 32-bit information (at least for one hop) has to be appended to data in flight in every routing device. In addition to this, a wily attacker can use another option in the IP header options field (e.g. the *Loose Source Routing* that mandatory defines a list of routers that should not be missed during routing), "invent" additional hops in the path and fill the 40 bytes available for IP options with false or misleading information.

5 Automating the trace-back process

In this context, many IP marking techniques have been developed in order to enable routers to probabilistically mark packets and therefore reconstruct the complete path [22], [23], [24]. The term "marking" lies to appending data with partial path information so that trace-back can be completed. IP Marking approaches use quite complicated mathematical algorithms to identify the origins of sequential IP packets, especially when the source IP addresses are false (i.e. spoofed). So far, IP marking techniques have proved robustness, high probability rates and scalable deployment. On the other hand, marking techniques require that all network traffic is in cleartext while in transit. An obvious issue arising is the compatibility with IPSec [25], especially when operations are performed in Tunnel mode. In this case the original IP packet is encapsulated in another IP packet and therefore certain portions of the original IP header are cryptographically protected by the Authentication Header of the encapsulating IP packet, so routing devices cannot append marking information in order to achieve trace-back. Apart from IP marking techniques, there are some series

of ICMP-based mechanisms evaluated by the research community. Perhaps the most accredited of them is the *iTrace* scheme [26], proposed by Bellovin and currently being the IETF standard. This approach is based upon the capability of routing devices to generate a "trace" packet for every packet they forward and is marked for tracing. At the destination host, the original packet and the “trace” packet are collected and the route is reconstructed. This framework uses HMAC [27], as well as supporting the use of X.509 Digital Certificates for authenticating and evaluating the *iTrace* messages [28]. Under the current *iTrace* proposal, the number of *iTrace* packets generated by a router is small, which implies a low overhead (statistically, around 0.005%) to the Internet [29]. However, it is mainly addressing attacks where a significant amount of traffic is coming from a rather small number of sources, due to the lower probability of generating *iTrace* packets [23]. A fair enhancement to the Bellovin’s approach is the Intention-driven *iTrace* schema [29], which is based upon the addition of one extra bit (called intention-bit) in the routing and forwarding process and the functionality provided by the Border Gateway Protocol – BGP [30].

The *CenterTrack* approach is based onto an overlay network by introducing the concept of special types of routers, called tracking routers [31]. Tracking routers have a conceptual (physical or virtual) adjacency with edge routers in an autonomous system. The core of this model is a central tracking system. All edge routers are linked to a central tracking router (or a simple network of tracking routers) via IP tunnels and therefore an overlay network is created. A necessity for the model to perform is that all edge and tracking routers must perform input debugging functions. If no such option is available, the model supports the use of network sniffers for traffic analysis and attack pattern recognition. The malicious traffic destined for the victim is routed through the overlay network via dynamic routing protocols, therefore a hop-by-hop tracking is initiated, starting from the tracking router closest to the victim. Static routes, both in the egress and ingress routers closest to the victim must be configured in a way for attack traffic flows only through the overlay network, allowing at the same time the reception of legitimate traffic to the victim. The last function is non-trivial because -generally speaking- it is very difficult to filter and reroute only volumes of traffic that match certain attack patterns. In order to succeed in this, *CenterTrack* suggests that attack pattern matching must be done during the input debugging process either at edge or tracking routers. An important drawback of this model is that a wily attacker can detect the presence of tracking systems by statistically measuring the latency via fragmented packets sent to the victim during the information gathering phase of an attack [32]. In addition to this, similar techniques with that used for detection and evasion of IDS systems could be used from an attacker to cause a DoS either to the *CenterTrack* (actually a single-point-of-failure) or the overlay network itself. Finally, if the attack target is the edge router itself then the system would try to reroute traffic destined to the edge router through this specific edge router. This could have either tunnel collapse or routing loops . Baba and Matsuda proposed an alternate suggestion using the concept of an overlay network along with an innovative logging approach [33]. This network is built of sensors that detect attack traffic, along tracing agents (tracers) that log the attack packets and managing agents that coordinate the

communication between the sensors and tracers. This approach allows for increased speed as well as less storage requirements by performing selective logging traffic.

Apart from network-based techniques that exploit the functions provided by the Internet Protocol as well as features of active networking capabilities, there are also some host-based trace-back techniques that have been proposed in the first research efforts of the trace-back problem. Perhaps the most well-known of them are the *Caller Identification System (CIS)* and the *Caller ID* approach that are briefly explained in the following. The CIS is a fully distributed trace-back system that aims to identify the attacker through the login process [34]. The concept of this system relies on the login information exchanges through the systems involved in a connection chain. When a user from host h_1 connects to the system h_n (n>2) through intermediate hosts h_2,..h_{n-1} the h_n system recursively queries the hn-1 host about the login information. In simple words, for every system where a user requires access all previous login information are checked before access is granted. Apart from being a rather outdated method since it is primarily based on authentication techniques that introduce their own vulnerabilities, it adds an important overhead in the login process so that attackers could be possibly alerted. Apart from *CIS*, another interesting host-based identification approach has been proposed by Chen [35]. The *Caller ID* introduces a manual trace-back in every intermediate host of the connection chain. That is, when an attacker connects from h_1 to h_2, h_3, .., h_{n-1}, h_n, the system owner or security personnel break-into h_{n-1} to verify the origin of the connection, possibly using hacking techniques. He later breaks into h_{n-2} until he reaches h_1 which could potentially be the attacker's machine. Despite the ethics and legal complications of this technique, it does not introduce important overhead like *CIS* and could be scalable augmented to cross-administration domains or even the Internet. The most important limiting factor is the manual processes that have to be performed for every host traced that make this approach rather not-applicable in today's high-speed networks. Despite this limitations, it is said to be used by US Air Force [36].

Finally, a very recent research in automated intrusion response, sponsored by Network Associates and Boeing Phantom Works has resulted in the development of the *Intruder Detection and Isolation Protocol* [37],[38], currently being scaled to multiple administration domains across the Internet. This protocol supports low cost integration with the most common intrusion detection techniques but is featuring new response mechanisms as well as new response algorithms. The core of the response mechanisms is the Common Intrusion Specification Language (CISL), originally developed by the Common Intrusion Detection Framework (CIDF) as the language providing a unified explanation of a security incident [38], currently supporting a minimal set ("block" and "allow"). Considering that these actions can be performed against a variety of different objects (e.g. users, applications, processes, connections, states, systems etc.) the combination of the responses provides a significant number allowing for a granular policy development. Recent results indicate that the protocol is performing sound in integrating with IDS systems within the DARPA research community [37].

6 Summary

Incident Response has always been perceived as a very important issue in every Corporate Security Policy. Every security incident has to be treated differently according to many different factors that define its significance, magnitude and effects. In this context, many Incident Response best practices were developed and adopted in corporate or legal frameworks and standards. On the other hand, Digital Forensics and trace-back mechanisms are considered to be the ultimate technical solution for holding attackers accountable for their actions. The new challenging objective is to mirror high-level business requirements to specific technical controls through a well-defined and structured corporate Incident Response Capability.

Acknowledgements

This paper has been partially supported by GSRT under a PENED grant and by the IST FET Coordination Action ACCA (006475).

References

1. Global Reach, “Global Internet Statistics”, Available at http://www.glreach.com/globstats/
2. CERT/CC, Security Of The Internet, Available at: http://www.cert.org/
3. BSI, “Information Security Management, BS7799, Part 1: Code of Practice for Information Security Management”
4. Mandia, K., and Procise, C., Incident Response: Investigating Computer Crime, Osborne/McGraw-Hill, NY, 2002
5. Yasincac, and Y. Manzano, “Policies to Enhance Computer and Network Forensics”, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June 2001
6. OMB’s Circular No. A-130, Appendix III Online, Available http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
7. United States Code, Chapter 35 of Title 44, Subchapter III – Information Security, Federal Information Security Management Act (FISMA) of 2002
8. International Standards Organization, “Code of Practice for Information Security Management”, ISO/IEC 17799:2000
9. Internet Engineering Task Force, Request for Comments (RFC) 2350, “Expectations for Computer Security Incident Response”, June 1998
10. Van Wyk, K., and Forno, R., Incident Response, O’Reilly, NY, 2001
11. Council of Europe, “Convention on Cyber Crime”, European Treaty Series – No. 185, Budapest, 2001
12. Killcrece, G., Kossakowski, K.P., Ruefle R., and Zajicek M., “Organizational Models for Computer Incident Response Teams (CSIRTs)”, Report: CMU/SEI-2003-HB-001, Carnegie Melon University/Software Engineering Institute, December 2003
13. Information Security Team, DePaul University, “A Framework for Incident Response (Draft)”, 13th December 2002

14.West-Brown, M. J., Stikvoort, D., and Kossakowski K.P., “Handbook for Computer Security Incident Response Teams (CSIRTs)”, Report: CMU/SEI-98-HB-001, Carnegie Melon University/Software Engineering Institute, December 1998
15.National Institute of Standards and Technology, “Computer Security Incident Handling Guide”, NIST Special Publication 800-61, January 2004
16.Patsos, D., “A Strategic Approach to Incident Response”, M.Sc. Thesis, Department of Mathematics/Information Security Group, Royal Holloway University of London, 2002
17.Whalen, S., An Introduction to ARP Spoofing, (White Paper), Available at: http://www.gmx.net
18.Bellovin, S.M., Security Problems in the TCP/IP Protocol Suite, *Computer Communication Review, Vol. 19, No. 2, pp. 32-48*, April 1989
19.Lemos, R., Study: Sites attacked 4,000 times a week, CNET News, 22 May 2001, Available at: http://news.com.com/2100-1001-258093.html?legacy=cnet
20.Zhang, Y., and Paxson, V., Detecting Stepping Stones, *Proceedings of the 9th USENIX Security Symposium*, Denver Colorado, August 14-17, 2000
21.Postel, J., Internet Protocol, RFC 791, September, 1981, Available at: http://www.ietf.org/
22.Savage, S., Wetherall, D., Karlin A., and Anderson, T., Practical Network Support for IP Traceback, *Proceedings of SIGCOMM'00*, Stockholm, Sweden
23.Song, D. X., and Perrig, A., Advanced and Authenticated Marking Schemes for IP Traceback, *Proceedings of the IEEE INFOCOM01*, April 2001, Anchorage, Alaska
24.Park, K. and Lee, H., On the Effectiveness of Probabilistic Packet Marking for IP Traceback, *In proceedings of 2001 Conference on Applications*, Technologies, Architectures and Protocols for Computer Communication (ACM SIGCOMM), San Diego, 2001
25.Kent, S. and Atkinson, R., Security Architecture for the Internet Protocol, RFC 2401, Nov. 1998, available at: http://www.ietf.org/
26.Bellovin S.M., ICMP Traceback Messages, Internet Draft (work in progress), February 2003
27.US Department of Commerce, Federal Information Processing Standards Publication 198, The Keyed-Hash Message Authentication Code (HMAC), March 6, 2002
28.Adams, C., Internet X.509 Public Key Infrastructure Certificate Management Protocols, RFC 2510, Available at:http://www.ietf.org/rfc
29.Mankin, A., et. al, On Design and Evaluation of Intention-Driven ICMP Traceback, *In Proceedings of IEEE International Conference on Computer Communications and Networks*, October 15-17 2001, Scottsdale, Arizona
30.Rekhter, Y. and Watson, T.J., A Border Gateway Protocol 4 (BGP-4), Available at: http://www.ietf.org
31.Stone, R., CenterTrack: An IP Overlay Network for Tracking DoS Floods, *In Proceedings of 9th Usenix Security Symposium*, Aug. 14-17, 2000, Denver, Colorado
32.McClure, S., Scambray, J., and Kurtz, G., “Hacking Exposed”, McGraw-Hill. 2001
33.Baba, T. and Matsuda, S., “Tracing Network Attacks to Their Sources,” *IEEE Internet Computing, vol. 6, no. 3*, 2002
34.Jung, H., et al. Caller Identification System in the Internet Environment, *In Proceedings of 4th USENIX Security Symposium*, 1993
35.Staniford-Chen, S., and Heberlein, L. T., Holding Intruders Accountable on the Internet. *In Proceedings of IEEE Symposium on Security and Privacy*, 1995
36. X. Y. Wang, D. S. Reeves, S. F. Wu and J. Yuill. “Sleepy Watermark Tracing: An Active Intrusion Response Framework”, *In Proceedings of the 16th International Information Security Conference (IFIP/Sec’01)*, June 11-13, 2001, Paris, France
37.Schnackenberg D., Djahandari K., Reid T., and Wilson B., Cooperative Intrusion Traceback and Response Architecture (CITRA), Boeing Phantom Works and NAI Labs, Prepared Un-

der Contract N66001-01-C-8048 for Space and Naval Warfare System Center (SSC), San Diego, February 2002
38. Feiertag R., Kahn C., Porras P., Schnackenberg D., Staniford-Chen S. and Tung B., “A Common Intrusion Specification Language”, June 1999, Available at http://people.emich.edu/pstephen/other_papers/CISL-Original.PDF