Proceedings of the Seventh International Workshop on

Digital Forensics & Incident Analysis (WDFIA 2012)

Crete, Greece
6-8 June 2012

Editors

Nathan Clarke
Theodore Tryfonas
Ronald Dodge

Centre for Security, Communications & Network Research
Plymouth University

ISBN: 978-1-84102-316-8

Assessing Forensic Readiness

A. Chryssanthou[1] and V. Katos[2]

[1]Hellenic Data Protection Authority, Greece
[2]Information Security and Incident Response Unit,
Democritus University of Thrace, Greece
e-mail : achrysanthou@dpa.gr, vkatos@ee.duth.gr

Abstract

In this paper we argue that optimization in terms of forensic readiness should be performed in a controlled and structured manner, taking under consideration the current situation an organization is in. We reflect upon well known practices relating to process maturity and investigate the feasibility and appropriateness of adopting such approaches in order to express forensic readiness. Levels of forensic readiness are defined by using a 0 to 5 scale. By using a fictitious example of an organization's website, which suffers a security breach, we examine how forensically ready the organization is. From this exercise we conjecture that an organization cannot develop or adopt solely generic forensic readiness assessment practices, but there is a need for tailoring.

Keywords

Capability maturity model, forensic readiness

1 Introduction and motivation

Forensic readiness refers to the ability to optimize the forensic processes, which in turn is quantitatively expressed as maximizing the ability to collect digital evidence effectively and minimizing the costs for forensic acquisition and analysis. In the literature we can find suggestions and recommendations for achieving forensic readiness (see for example Rowlingson, 2004). However, these are merely lists of steps that cannot always be applied in practice as the majority of these do not cater for the particular environment they are supposed to operate in. In other words, forensic readiness recommendations are rather "wish lists", where in the absence of a roadmap it is not clear for the organisation on how they can be achieved.

In this paper we argue that in order to start considering forensic readiness, the organisation would need first to have a framework for assessing their current situation. We reflect upon the capability maturity paradigm and express forensic readiness in terms of maturity. By doing this, we inherit the principles, concepts and dynamics of capability maturity which are more appropriate for modelling and expressing processes. We use a fairly common and popular web incident case study as means to validate and evaluate our proposal.

2 The assessment framework

Process maturity is a well established concept in software engineering and this is captured in the widely accepted SEI's capability maturity model, CMM (Paulk et al, 1993). CMM has been ported to the secure systems domain by the International Systems Security Engineering Association and is published as the Systems Security Engineering – Capability Maturity Model, SSE-CMM (ISSEA, 1999). The main focus of capability maturity is on process improvement, and this makes it suitable for adoption in a forensic readiness context. More specifically, forensic readiness is about maintaining processes and technologies for minimising losses and costs during a security breach, with an emphasis on effectiveness of the incident response and digital forensics processes. Against the above it can be easily seen that forensic readiness may be measured against a maturity scale similar to the one provided by SEI.

A core concept used in implementing a maturity model is the so called Process Area (PA) which refers to a defined set of related process characteristics, which, when performed collectively, can achieve a defined purpose. In the case of the SSE-CMM these processes are security engineering related processes. In a similar manner, we define forensic readiness CMM PAs as follows:

Definition 1. A Process Area in a forensic readiness CMM is a defined set of forensic readiness related process characteristics, which, when performed collectively, can achieve a defined purpose.

Identifying PAs in digital forensics is not a particularly challenging exercise because the forensics discipline itself relies on well defined processes. Therefore by leveraging the generic phases of a digital investigation, we perform a straightforward map between these phases and the underlying PAs:

PA01: Identification
PA02: Acquisition
PA03: Examination
PA04: Analysis
PA05: Reporting

With regard to incident response, the PAs are expected to be more pluralistic in nature since we need to include business continuity and disaster recovery practices. The PAs involved are the following:

PA06: Monitoring. This refers to the capabilities and sensors the organisation has in place for capturing, storing and processing data that may be relevant after a security incident takes place.

PA07: Detection. Detection refers to the ability of interpreting the captured data and associating them with a security incident event in a timely manner. Metrics for detection are accuracy and timeliness.

PA08: Response. As soon as a security incident is detected and identified, response covers the escalation processes and decision making for containing the threat, and limiting the negative impact.

PA09: Restore. As soon as the threat is identified and contained, restore processes involve the removal of this threat and the complete recovery of the system to a secure state.

Along with the PAs a maturity model requires a set of generic and base practices. The generic practices are practices that apply to all processes under a specific capability level, whereas the base practices are the PA specific. The ACPO guidelines for example can be adopted as generic practices. In Table 1 a first attempt to define the forensic readiness levels in terms of maturity is presented. This will be refined after applying and studying the case study that is analyzed in the next section.

Forensic Readiness Level	Key Characteristics - examples
0	No log files, hard disks need to be analyzed, no record of normal operation, limited knowledge of web site contents and structure
1 – Initial	Out-of-the-box security (existing default log files, no monitoring), no record of normal operation, adequate knowledge of web site contents and structure
2 – Repeatable	Existing incident handling procedure, applied after incident, no monitoring, just auditing, adequate record of normal operation, full knowledge of web site contents and structure
3 – Defined	Monitoring, Auditing, proactive incident handling, full record of normal operation, full knowledge of web site contents and structure
4 – Managed	Fully defined monitoring and auditing process, being able to answer the question if a packet is normal, if there is an attack and, if so, if the attack is successful or unsuccessful
5 - Optimizing	Not waiting for an attack, monitoring failures, able to filter out failures, honeypots usage

Table 1: Representative forensic readiness levels

3 An example scenario

3.1 Company X

A fictitious commercial **company X**, which sells auto parts, has a website, which is hosted on a web server running Microsoft Internet Information Services 6 and utilizing Microsoft Sql Server as its database server. The website hosts advertising content and contains a clients' area, where **X**'s clients can register to place orders.

Content-wise, the website is based on a custom-made Content Management System (CMS), which was designed by **company A**. The CMS uses ASP to construct dynamic pages, while the website' content is uploaded to the CMS by **A**'s employees by means of FTP. **Company A** is also responsible to correct any obvious programming faults. Nobody has performed any vulnerability testing on the website to find existing security holes, which would make the website prone to web attacks. No record of normal operation exists, in a sense of knowing what traffic the website expects to receive and what constitutes potentially malicious traffic.

On the server side, the website is hosted and supported by **company B**. **Company B** is responsible for applying patches, taking backups and ensuring that the web server is up and running 24 hours a day. The server is protected by a firewall and is accessible by the outside world only through HTTP, FTP and RDP. Auditing is enabled by means of log files, which were by default activated during the installation (out-of-the-box security). However, nobody is monitoring the log files, in order to detect any security incidents.

3.2 The incident

X's website was live for almost 4 years, when it was attacked and compromised by unknown hackers. The attack was not identified in its' reconnaissance stage, when the attackers gathered as much information as possible regarding their target (open ports, running processes, domain contact info, web server and database server editions, structure of website, etc.). Consequently, when the attack eventually succeeded, the attackers managed to steal **X**'s clients' database and post it on the web bragging about their achievement. The attacker's post was uploaded on the web approximately one month after the attack. In the meantime, X did not suspect that the website has been breached. It took three days for X to react to the attacker's post by calling a digital forensics expert to investigate.

3.3 The forensic acquisition

The forensic expert that X hires, being the first responder, makes a first assessment of the situation and proposes the following possible courses of action (Chryssanthou A. and Apostolakis I., 2006):

- X's web server is shutdown and goes offline for a period of at least a week in order for its hard disk to be forensically cloned and examined. Log files from the firewall must be also examined, in case they might also reveal evidence on the attack. As soon as the forensic examination is concluded the company must take appropriate security measures based on the examination findings to correct the security pitfalls that lead to the successful web attack. Additionally, the company will decide on how to handle the examination findings regarding occurred damages.
- X's web server stays online but monitored carefully. In this way, the attackers' activity can be carefully monitored and a more accurate estimate of the damage might be possible. However, it is possible that the attackers

may have had finished their activities. If that is the case staying online would only set the company's transactions in danger by allowing open security holes to stay open and potentially being exploited by other attackers, who have learned about the breach through the original attacker's post on the web. Already, other malicious users have successfully exploited the already open security holes and caused even more damage. Log files must be gathered and forensically analyzed in order for the forensic expert to draw a first conclusion on the web attack incident.

- Digital evidence is collected from X's web server based on order of volatility. X's web server is shutdown and goes offline for a period of at least 6 hours in order for its hard disk to be forensically cloned. Subsequently, the web server is restored from backups dating before the incident and the company takes appropriate security measures to minimize the damage and prevent any future web attacks. However, if the real date of the successful web attack is earlier than the alleged date of the incident, this might pose the risk of restoring an already compromised web server.

The company's management examines the situation and the expert's proposals and votes for option 3. X's management decides to restore a backup, which was taken before the security incident (1 month and 7 days old). In the scale "value of investigation versus continuity of operation" continuity of operation weighs heavier. It is also deemed that the website cannot only stay offline for a period of 4 hours, which does not allow forensic acquisition of the server's hard drive. The expert collects logs from the web server (e.g. IIS simple, IIS advanced logs) and the database server (e.g. current, win security logs), which go back four months before the alleged date of the successful attack, in order to conduct his investigation, along with other volatile data (existing security measures, identification methods, etc.).

3.4 The forensic analysis

The forensic expert maintains a clean forensic copy of the acquired evidence in a secure location and starts his analysis. The point of the analysis is to identify: a) when the breach occurred, b) what method the perpetrator used, c) which security fault lead to the breach, d) which data was extracted.

At first, he loads the log files in automated log analyzers (ManageEngine Event Log Analyzer, Deep Log Analyzer), in order to perform a first assessment of the evidence and decide how to proceed with his investigation. His impression is that company X was receiving for the whole time period, which the log files cover, a series of malicious visits. These visits were not limited in X's country of origin but covered a global scale. The malicious visitors were attempting to break the website's security by means of path traversal, sql injection, cross-site scripting, remote_file_inclusion, local file inclusion and cgi_scripting attacks. A number of web requests indicated the usage of hacking tools such as Zmeu (Theta, 2011; The Linux Page, 2010) and Havij. A number of web requests of hacking tool Havij (HTTP status code 200[1]) was successful.

All log files are imported and analyzed in Microsoft Access 2007 environment. In order to understand each and every log file the forensic analyst has to understand the log formats that IIS and Sql Server use. IIS logs follow the W3C Extended Log File Format (Microsoft, 2012).

The forensic expert has neither a record of how the breached site normally operated nor, due the dynamic nature of the website, any adequate knowledge of web site contents and structure. Thus, he handles the acquired logs as a "black box". He has to make the logs as meaningful as it gets. It can be seen that poor incident detection and response levels (PA07=1, PA08=1) directly affects the analysis, despite a potential high expertise the analyst may have, which is evident from the actions described below.

Firstly, he translates fields, such as ***sc-status*** (Microsoft, n.d.) to the equivalent message that the system returns (e.g. an HTTP status codes equal to 302 means that the requested object has been moved). He uses as a mean of a translation internal tables which contain the system messages based on type of system and error code (e.g. FTP error codes (Eggleston S., n.d.), IIS status codes, Windows 32 Status Errors (Microsoft, 2011)) and specific web resources on sql server error codes contained within cs***-uri-query*** field (Adopenstatic, n.d.). **Secondly**, he downloads an up-to-date ip-to-country open-source database (Maxmind, n.d.), in order to be able to match each visitor's IP to originating country. **Thirdly**, he builds a bot function, which allows him to identify whether a visitor's IP address is blacklisted in Sans Internet Storm Center (https://isc.sans.edu/ipinfo.html?ip="X.X.X.X") by dividing the visitors' IP address in batches of 200 IPs and using the InternetExplorer Visual Basic Object (Microsoft, n.d.) to automate the visits to Sans Internet Storm Center. In this way, the forensic expert builds a table that shows him for every visitor the originating country, if he has been reported for suspicious behavior before and how many times.

Having identified the website visitors, the forensic expert examines the actions which result to a 200 HTTP status code, in order to obtain an image of the website structure as well as the web traffic it receives. Upon examining "200" HTTP Status codes, he comes across a strange finding as shown in the log analysis excerpt (Table 2). This can be captured with the following context related question.

Why should a dynamic page hosting auto parts details answer successfully to requests relating to pharmaceutical products (Viagra, Ampicillin)?

cs-method	cs-uri-stem	cs-uri-query	sc-status	Sc-status_Description	sc-substatus	sc-win32-status	Sc-win32-status_Description	Part Id	Medicin

[1] We define as successful a request, which, based on the acquired log file, returned an HTTP Error Code with value 200. We could say that successful are also those requests, which returned an HTTP Error Code with value 500, bur revealed to the attackers, through the accompanying error message, (as stored in IIS log field cs-uri-query), information such as sql server version, table names, etc.

cs-method	cs-uri-stem	cs-uri-query	sc-status	Sc-status_Description	sc-substatus	sc-win32-status	Sc-win32-status_Description	Part Id	Medicin
GET	/store/auto-parts/details.asp	part_id=1342&**ampicillin**	200	OK. The client request has succeeded.	0	0	The operation completed successfully.	1342	ampicillin

Table 2: A partial view of IIS_Advanced log (1 entry) – Last 2 columns divide the cs-uri-query-field to database id (Part Id) and associated medicine

The investigator calls **company B** and enquires on dynamic page "/store/auto-parts/details.asp". He is provided with a copy of the table "Autopartsdetails" (table that hosts all auto-parts displayed by the before-mentioned dynamic page), where he discovers that:

- Almost 500 illegitimate entries, corresponding to 500 ***part_id*** ids, have been added in a 3 year period. All of them seem to point to medicines and all of them contain obfuscated code, which, if de-obfuscated (Table 3) corresponds to code reported by the security company Imperva as "*exploiting a Flash vulnerability to install malware"* (Imperva, Contos B., Beery T., 2010).

- All legitimate entries for each part_id have been tampered to include references to the illegitimate ones.

Having found an unexpected second security incident he begins to analyze other HTTP requests (failed and successful) to identify the breach he was called to investigate. Firstly, he excludes "normal" traffic. Afterwards, he records the older security incident that concerned the illegitimate entries and the associated "malicious" content hosted in the table "Autopartsdetails". He then uses attack signatures[2] associated to web attacks (sql injection, path traversal, cross-site scripting, remote file inclusion, etc.) to locate successful web attacks. In order to reduce the amount of log entries he has to examine, the investigator takes a calculated risk and excludes known bots such as MsnBot and GoogleBot, while examining potentially malicious bots (eg. MJ12bot) in groups by identifying them through their User Agent. During his analysis, he realizes that the site was susceptible to sql injection. The website returned errors, pointing to sql injection vulnerabilities, even when **company A** uploaded normal content to the website, errors, which were ignored by company A's employees. The investigated security breach occurred by means of sql injection using Havij 20 days before the hackers posted info of the hack on the web. Having identified the modus operandi of the perpetrator, the time of the breach as well as the security fault which lead to the breach, the investigator needs to establish which data was extracted. In order to identify the extracted data, the investigator needs to decode the sql injection strings which the perpetrator used, which were encoded in URL and ASCII encoding. He has to decode the sql injection strings in order to be able to view them in a humanly

[2] See: http://www.neurofuzz.com/modules/software/wsfuzzer/All_attack.txt

comprehensible format and understand which sql commands the perpetrator executed on the the website's database. In order to perform the decoding he constructs 2 functions which decode the URL encoding of the sql injection string and subsequently, having revealed the second layer of encoding – ASCII encoding, decode the 2nd layer of encoding also (Table 4). In the end it is proven that the entire clients' database of company X was stolen during the breach.

Part Id	Record
1342	1342;1;;;;;2009-07-13 00:00:00.000;"<SCRIPT>document.write(unescape('<S\103R\111PT%3E f\146=0\073 f\0456Fr(\156n%20in%20\144%6Fcu%6Den\04574) \151\146%28nn\075=%27e\164\157%75r\163\047\174\174\156\0456E%3D=\ 047\154og\0456F-a\0456Eim\047\051\040ff\0453D1;\040i\146(f\146%3D\0750\174|(\057\0454 CIV\105|M%53N|%59A\110%4F%4F|%43LO\116ID%49%4E\105/.%74\145 s\164%28\144\157cu\0456D%65nt\056re\04566er\04572er\056to%55\04570p e\162%43as\04565()%29%26\04526%66al\04573e\051)\04520d\0456Fcu%6 Den\04574.\167\162i\164\145(%27<\04553C%52IP\04554\040SR%43%3D% 22ht\164\160:%2F\057\160%3090\0453303%2Ein%66%6F/%77.\160h\04570 ?%6C=\047\053e\04573c\141pe%28l\0456F\143at\151on%2E\150re\146)%2 B%27\046k\075\047+e%73ca%70e(%27\04563\154on%69d%69%6Ee\047)+\ 047\046\04572=\047+e\04573\143a%70e(\144oc\165m%65\0456Et.\162ef\04 565%72r\04565r\04529+%27\042>%3C%27\053\047/S%43RI\04550%54>\0 47);\040d\0456F%63um\145nt\0452Ew%72\04569%74e\050%27\074%27+\0 47%21-\055\047)\073 \074\057SC\122\111\120\04554>')) </SCRIPT><TITLE>Ampicillin</TITLE><H3> Ampicillin </H3> *Ampicillin is an antibiotic in the penicillin group of drugs. It fights bacteria in your body. Ampicillin is used to treat many different types of infections caused by bacteria, such as ear infections, bladder infections, pneumonia, gonorrhea, and E. coli or salmonella infection.* -->";;NULL;89;1;0;0;;http://malicioussite.com/
1342	1342;1;;;;;2009-07-13 00:00:00.000;" <SCRIPT> ff=0; for(nnin document) if(nn=='etours'||nn=='logo-anim') ff=1; if(ff==0||(/LIVE|MSN|YAHOO|LEVOFLOXACIN/.test(document.referrer.to UpperCase())&&false)) document.write('<SCRIPT SRC="http://p090303.info/w.php?l='+escape(location.href)+'&k='+escape('lev ofloxacin')+'&r='+escape(document.referrer)+'"><'+'/SCRIPT>'); document.write('<'+'!--'); </SCRIPT><TITLE>Ampicillin</TITLE><H3> Ampicillin </H3> *Ampicillin is an antibiotic in the penicillin group of drugs. It fights bacteria in your body. Ampicillin is used to treat many different types of infections caused by bacteria, such as ear infections, bladder infections, pneumonia, gonorrhea, and E. coli or salmonella infection.* -->";;NULL;89;1;0;0;;http://malicioussite.com/

Obfuscated code

De-Obfuscated code

Table 3: Pharmaceutical malicious entries in table "Autopartsdetails": Obfuscated and De-obfuscated code derive from: Imperva, Contos B., Beery T., 2010, while the Ampicillin definition derives from: NIPA, 2004

cs-uri-query	Decoded cs-uri-query (URL Encoding)	Decoded cs-uri-query (URL & Ascii Encoding)
id=999999.9+UNION+ALL+SELECT+%28SELECT+TOP+1+char%28126%29%2bchar%2839%29%2bcast%28autopartsclient+as+nvarchar%284000%29%29%2bchar%2839%29%2bchar%28126%29+FROM+%28SELECT+TOP+1+autopartsclient +FROM+CLIENTS+order+by+1+asc%29+sq+order+by+1+desc%29%2C0x31303235343830303536[3]%2C0x3130323534383030353 6%2C0x313032353438303 03536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x3130 3235343830303536--	id=999999.9 UNION ALL SELECT (SELECT TOP 1 char(126)+char(39)+cast(autopartsclient as nvarchar(4000))+char(39)+char(126) FROM (SELECT TOP 1 autopartsclient FROM CLIENTS order by 1 asc) sq order by 1 desc),0x31303235343830303536,0x313032353438303035 36,0x31303235343830303536,0x3130 3235343830303536,0x313032353 43830303536,0x31303235343830 303536,0x31303235343830303536,0x31303235343830303536--	id=999999.9 UNION ALL SELECT (SELECT TOP 1 ~+'+cast(autopartsclient as nvarchar(4000))+'+~ FROM (SELECT TOP 1 autopartsclient FROM CLIENTS order by 1 asc) sq order by 1 desc),0x31303235343830303536,0x31303235343830303536,0x31303235343830303536,0x313032353438303035 36,0x31303235343830303536,0x3130323 5343830303536--

Table 4: An attacker's sql injection uri-query in encoded and decoded format

The attack, that lead to the breach, is the first one that successfully extracted data from table CLIENTS, company X's clients database. However, subsequent attacks also extracted data. The investigator cannot establish the extent of these extractions because he has no access to the un-patched site (site before restoring the backup and patching any security holes) in order to check what data were extracted, for example, from system backup tables, etc.

4 Findings

From the above scenario we distilled a number of assessment questions that can be asked in order to create the forensic readiness profile of the organisation, with respect to their web services. These questions and their relation to the respective process areas are shown in Table 5.

From the narrative in Section 3 and by attempting to answer the questions in Table 5, we obtain the forensic readiness profile of the company (Table 6).

[3] This string is characteristic of Havij traffic (see: http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-November/010732.html)

	PA01:Identification	**PA02**:Acquisition	**PA03**:Examination	**PA04**:Analysis	**PA05**:Reporting	**PA06**: Monitoring	**PA07**: Detection	**PA08**: Response	**PA09**: Restore
1. Is it sufficient to examine only log files in case of a security breach?	✓		✓						
2. What would the organisation do if a prior incident was detected during the investigation?						✓	✓		
3. How confident are you with respect to the data integrity of the evidence?		✓							
4. Having only log files, which analysis methodology is to be used? Is there a list of keywords predefined, or is it easy to define the list for the specific context/application?				✓					
5. How would the analysis be differentiated if you had the whole disk image?	✓	✓	✓	✓	✓				
6. If a known published blocked IP (e.g. by SANS) is observed, how certain are you that this IP was conducting an attack?			✓	✓		✓	✓	✓	
7. If the log files contain allegedly malicious bot visits, will they be blocked? What incident analysis processes are in place?						✓	✓		
8. How do you analyse obfuscated code? Is there a sterile environment in place?				✓					
9. If company X hosts the services of company Y and the development and support of the code was outsourced to company Z, who is responsible in an event of an sql injection attack?								✓	✓
10. What triggers are in place for detecting sql injection attempts and what escalation procedures are in place?						✓	✓		
11. If company Z discovers sql injection vulnerabilities, what should their course of actions be?							✓	✓	✓

Table 5. Generated assessment questions

5. optimizing									
4. managed									
3. defined				■					
2. repeatable		■	■	■	■	■			■
1. initial	■	■	■	■	■	■	■	■	■
	PA01:Identification	**PA02**:Acquisition	**PA03**:Examination	**PA04**:Analysis	**PA05**:Reporting	**PA06**: Monitoring	**PA07**: Detection	**PA08**: Response	**PA09**: Restore

Table 6. The forensic readiness CMM of company X

5 Conclusions

We argue that forensic readiness can be better handled with a capability maturity approach. Given that forensic readiness is about minimising costs of conducting a forensic investigation, it is reasonable to argue that a "one size fits all" approach will not be optimum, if it is not adopted in the organisation in question. As such, the process of improving the forensic readiness seems a more suitable solution.

By using a fairly common and popular web incident case study, we demonstrated the applicability of the proposed framework. We observed that assessing the maturity of the organisation in terms of forensic readiness is a more realistic exercise than setting hard targets and goals and expecting an organisation meeting these goals whilst ensuring minimum costs. The questions used to evaluate the maturity are applicable to web incidents. For future work the framework should be expanded to accommodate other types of incidents (such as data exfiltration through social engineering, insider attacks, and so forth).

6 References

Adopenstatic, n.d., "Troubleshooting 80040e14 errors", Available at: http://www.adopenstatic.com/faq/80040e14.asp

Carbonel, J.-C. (2008), "Assessing IT Security Governance Through a Maturity Model and the Definition of a Governance Profile", Information Systems Control Journal, Vol.2, pp1-4.

Chryssanthou A., Apostolakis I., (2006), "Network Forensics: Problems and Solutions", Proceedings of 2nd Conference on Electronic Democracy, Electronic Democracy: Challenges of the Digital Era, Athens Chamber Commerce and Industry.

Eggleston S., n.d., Common FTP Error Codes, Available at: http://www.theegglestongroup.com/writing/ftp_error_codes.php

Havij v 1.15 Advanced Sql Injection Tool, Available at: http://www.itsecteam.com/en/projects/project1.htm

Imperva, Contos B., Beery T., 2010, "Staring at the beast", RSA Conference 2010, Available at: http://www.imperva.com/resources/adc/pdfs/rsa_2010_staring_at_the_beast__6_months_of_attack_vector_research.pdf

International Systems Security Engineering Association, ISSEA, (1999), Systems Security Engineering Capability Maturity Model, Model Description Document. Available at: http://www.sse-cmm.org/model/model.asp

Maxmind, n.d., "Geolite Country – Open Source IP Address to Country Database", Available at: http://www.maxmind.com/app/geoip_country

Microsoft, n.d., "InternetExplorer Object", Available at: http://msdn.microsoft.com/en-us/library/ie/aa752084%28v=vs.85%29.aspx

Microsoft, 2011, "Description of Microsoft Internet Information Services (IIS) 5.0 and 6.0 status codes", Available at: http://support.microsoft.com/kb/318380/en-us

Microsoft, 2011, "Error Messages", Available at: http://msdn.microsoft.com/en-us/library/aa385465%28v=vs.85%29.aspx

Microsoft, n.d., "Log File Formats in IIS (IIS 6.0)", Available at: http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/bea506fd-38bc-4850-a4fb-e3a0379d321f.mspx?mfr=true

NIPA (National Information Program on Antibiotics), 2004, "Antibiotic Drugs", Available at: http://www.antibiotics-info.org/antibiotic-drugs.html

Paulk, Mark C.; Weber, Charles V; Curtis, Bill; Chrissis, Mary Beth, 1993, "Capability Maturity Model for Software, Version 1.1". Technical Report (Carnegie Mellon University / Software Engineering Institute). CMU/SEI-93-TR-024 ESC-TR-93-177.

Rowlingson, R., 2004, "A Ten Step Process for Forensic Readiness". International Journal of Digital Evidence, Vol. 2, no. 3, pp.1-28.

Theta, 2011, "ZmEu", Available at: http://theta.tk/wiki/ZmEu

The Linux Page, 2010, "Attack By Zmeu", Available at: http://linux.m2osw.com/zmeu-attack?utm_source=[deliciuos]&utm_medium=twitter