Internal Vs. External Penetrations: A Computer Security Dilemma

Pedro A. Diaz-Gomez, Gilberto ValleCarcamo, Douglas Jones
Computing & Technology Department, Cameron University, Lawton, OK, USA

Abstract— *In computer security it has been said that internal penetrations are the highest threat for data and information. This paper took the challenge to investigate if such a common belief is true. Various statistics are analyzed with the goal to give some light to the research community about internal and external penetrations. This paper highlights a weakness in computer security called "the unknown", which corresponds to intrusions to computers and network resources from which organizations do not know the cause.*

Keywords: computer security, data breach, external penetration, internal penetration.

1. Introduction

It is a common belief that most of all penetrations to computer resources come from within the organization [1], [4], [12], [17], [22], [24], [20] and, it is normal to think that computer users, who have rights and access to particular resources in the system, constitute the principal threat. *Anderson* [2] indicates that the internal penetrator has no barriers to surpass in order to have access to the computer, and that their intrusion activity could be difficult to track. Three categories of users are identified: the masquerader, the legitimate, and the clandestine user. The masquerader is a user that steals credentials to have access to computers, pretending to be a trusted party. The legitimate user is the user that has been granted access to computer resources by an organization, and uses his or her own credentials to use them. The clandestine user has or can get superuser privileges. All these intrusions constitute a security threat to computer resources [2].

The barrier that classifies insider from outsider is difficult to draw. *Anderson* [2], for example, defines an outsider as the one that has no permission to use computer resources. In this sense, an outsider could as well be an employee who has no rights to use the computer, as well as a hacker, that can seize security mechanisms in order to have access to it. *Pfleeger*, on the other hand, gives various definitions of the term insider: as an employee or other member of an organization who has permission to use the system, as customers who perform transactions with an organization as part of services or businesses, as anyone identified and authenticated by the system—could be a masquerader, as someone that executes actions on the system on behalf of an outsider, and as a former employee that uses privileges not revoked or that uses privileges secretly created while at work [20]. The CERT cybersecurity survey defines an insider, as a current or former employee, service provider or contractor; and outsider, as someone that has never been granted computer and network access privileges of an organization [9]. In this sense, a former employee with revoked privileges that is able to bypass security mechanisms will be considered an insider.

Some reports go against the common trend which says that insiders are the highest threat for computer resources. The *Data Breach Investigations Report* gives statistics which show the trend that outsiders are responsible for a higher number of intrusions and a higher number of records breached [25], [26].

A statement about what actors of computer penetrations are responsible for the majority and more devasting attacks could be difficult to demonstrate. Not only such statement could be biased by the observer—in particular if it is a vendor—the type of organizations that report or not report, but also for the data sample. Coming from inside, coming from outside or working in conjunction, computer penetrators are developing new techniques, like network sniffers and RAM scrapers, that allow them to perform sophisticated penetrations and avoid discovery [26]. Computer security countermeasures have been addressed to mitigate such threats, like intrusion detection systems, firewalls and anti-viruses; however, errors, misconfigurations and noncompliance with security policies have allowed some successful penetrations that could be avoided if those countermeasures are in place [26].

The order of this paper is as follows: Section 2 presents some basic definitions, Section 3 describes the penetration problem, Section 4 presents statistics about external vs. internal penetrations, Section 5 relates to the analysis of statistics presented, and Section 6 presents the conclusions and future work.

2. Basic Definitions

The following definitions are used in this paper:

- **Threat**: any potential danger to computers and network resources, like unauthorized access to confidential information, virus infection and system malfunction [3], [16]. There are external threats that originate from outside the organization, and internal threats that originate from within the organization [25].
- **Threat agent**: the actual penetrator or intruder that performs the threat, like outsiders, insiders, viruses and trojan horses [16].

- **Outsider**: an external threat agent, in other words, an agent from outside the organization [25], or an agent not authorized to use the system [3].
- **Insider**: internal threat agent, in other words, an agent that belong to the organization [25]. For example, this includes an authorized user that surpasses his or her legitimate access rights [3].
- **Penetration or intrusion**: all incidents involving the successful breach to computer software, computer systems or computer networks [2], [19]. There are internal penetrations and external penetrations depending if the penetrations were performed by an identified and authorized user, or by someone not identified, or not authorized to use the system [1].
- **Incident**: an event or set of events that affects an organization negatively. An incident can be observed, verified and documented [16], such as with a data breach.
- **Don't Know**: If organizations do not know whether there was any unauthorized use of their computer systems and networks [6].
- **Unknown**: All incidents involving an unknown cause [19].
- **None**: The organization reports no penetration.

3. The Penetration Problem

Anderson [2] studied the penetration problem from the prospective of whether an attacker is authorized to use the computer and whether an attacker is authorized to use data and programs. These two events give the following combinations: external penetration, internal penetration and misfeasance.

External penetration is considered from the prospective of access to the computer and its data/programs. Not just the case of an outsider, who is not part of an organization or its affiliates is considered, but the case of an employee or contractor who has no access to computer resources and data.

Internal penetration is considered for attackers that have access to a computer, but who are not authorized to use certain computer's data and programs. Anderson highlights that in some organizations, internal penetration is more frequent than external penetration, because internal penetrators already have authorization to use computers. An internal penetrator can be a masquerader that could be an outsider who has already gained access to the system, an employee without full access, or an employee that is using others' credentials. An internal penetrator could be a legitimate user of a computer who misuses his or her access permissions to use the system. The clandestine, is considered an internal penetrator, and is the attacker that is able to change in operating systems' parameters in order to hide tracks of the penetration.

Table 1: Percentage of incidents from inside reported by CSI/FBI.

year	*1-5*	*6-10*	*>10*	*Don't Know*
1997	47%	14%	3%	35%
1998	70%	20%	11%	–
1999	37%	16%	12%	35%
2000	38%	16%	9%	37%
2001	40%	12%	7%	41%
2002	42%	13%	9%	35%
2003	45%	11%	12%	33%
2004	52%	6%	8%	34%
2005	46%	7%	3%	44%

Table 2: Percentage of incidents from outside reported by CSI/FBI.

year	*1-5*	*6-10*	*>10*	*Don't Know*
1997	43%	10%	1%	45%
1998	74%	18%	9%	–
1999	43%	8%	9%	39%
2000	39%	11%	8%	42%
2001	41%	14%	7%	39%
2002	49%	14%	9%	27%
2003	46%	10%	13%	31%
2004	52%	9%	9%	30%
2005	47%	10%	8%	35%

Anderson's' study has been addressed elsewhere [3], [13], [24] and it certainly reached the goal of classification of penetrations, but it is important to have in mind that this seminal work was at a time where interconnecting networks were not a high threat. However, Anderson's' work posted the problem and gave the solution, of his time, to the difficulty of defining internal and external penetrations.

4. Statistics

Some difficulties were encountered in the goal of presenting the most complete and updated statistics available in free repositories of the internet. This research found a few places with reliable statistics. The presentation of statistics were different—some reported percentages, others raw data—the format changed within the same report making statistical inferences a challenging task. This paper tried to perform some statistical inferences on statistics available, and tried to motivate other researches in pursuing a more rigorous statistical analysis.

4.1 Statistics CSI/FBI

Tables 1–3 show totals corresponding to organizations—represented primarily by United States corporations, government agencies, financial institutions, educational institutions, medical institutions and other organizations [7]—that have between $1-5$, $6-10$ or more than 10 incidents per year. Each row is approximately 100% because numbers are rounded to the nearest integer.

Table 4 was calculated taking the corresponding proportion of *inside incidents* as in Table 1, *outside incidents* as in

Table 3: Total percentage of incidents reported by CSI/FBI.

year	*1-5*	*6-10*	*>10*	*Don't Know*
1996	46%	21%	12%	21%
1997	48%	23%	3%	27%
1998	61%	31%	9%	–
1999	34%	22%	14%	29%
2000	33%	23%	13%	31%
2001	33%	24%	11%	31%
2002	42%	20%	15%	23%
2003	38%	20%	16%	26%
2004	47%	20%	12%	22%
2005	43%	19%	9%	28%
2006	48%	15%	9%	28%
2007	41%	11%	26%	23%
2008	47%	14%	13%	26%

Table 4: Proportional percentage of incidents from inside, outside and don't know, *calculated* from CSI/FBI Reports.

year	*Respondents*	*Inside*	*Outside*	*Don't Know*
1997	48%	40%	33%	27%
1998	45%	50%	50%	–
1999	63%	38%	32%	29%
2000	61%	37%	32%	31%
2001	65%	33%	35%	31%
2002	64%	36%	41%	23%
2003	67%	37%	37%	26%
2004	57%	37%	42%	22%
2005	65%	32%	40%	28%

Table 2, as well as the *don't know* proportion from Tables 1 and 2, with respect to the total presented in Table 3. No data was found in public repositories of the internet, from years 1996, and 2006 – 2009 that give the classification of insiders, outsiders and don't know.

Average of the percentages for inside incidents (37.7%), outside incidents (37.9%), and don't know (24.1%) were calculated from Table 4. These averages were corroborated with the bootstrap technique [14]. One thousand samples of size nine taken randomly with repetition from Table 4 gives 37.77 for the mean of averages of percentages of inside incidents, 37.99 for the mean of averages of percentages of outside incidents, and 24.16 for the mean of averages of percentages of don't know, with an estimated error of 1.606, 1.829 and 3.044 respectively.

As all reports from the CSI/FBI reviewed present statistics in percentages [5], [6], [7], this paper tried to infer the number of incidents. For doing that, over 100 random samples averages of $1-5$, $6-10$, $11-30$, and $31-60$ incidents were drawn using Tables 1, 2, and Table 3. Table 5 as well as Figure 1 give the corresponding results.

The Pearson Coefficient [18] calculated for the Number of inside incidents and outside incidents, as in Table 5, gives a value of 0.624, which does not show a strong linear correlation between these two variables. The Fisher's coefficient ρ [15] corroborates such statement with the range $-0.069 < \rho < 0.910$ that includes the value 0. There is not a linear correlation between the number of inside incidents and the number of outside incidents.

Table 5: Number of incidents from inside and outside. *inferred* from 1997 – 2005 CSI/FBI reports.

year	*Inside Incidents*			*Outside Incidents*		
	Respondents	*Ave.*	*Std.*	*Respondents*	*Ave.*	*Std.*
1997	218	841.0	53.47	212	562.9	36.09
1998	184	1244.9	33.77	142	948.1	23.30
1999	308	1809.7	43.90	280	1439.0	30.28
2000	359	2092.3	36.83	341	2014.7	62.66
2001	348	1200.2	26.36	316	1614.2	30.23
2002	289	1473.3	36.09	301	1815.5	28.83
2003	328	1537.2	46.96	336	1635.0	39.93
2004	280	1022.2	33.33	280	1152.0	33.23
2005	453	1164.8	30.57	453	1740.9	40.17

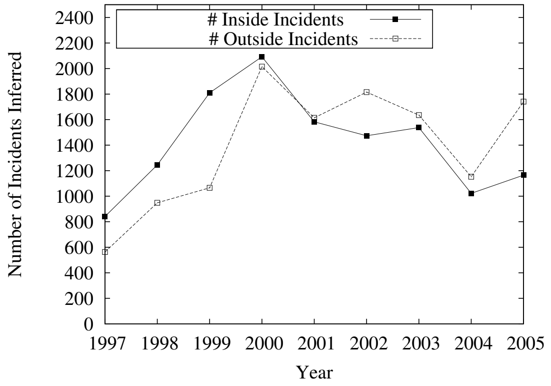

Fig. 1: Mean number of inside and outside incidents. Inferred from 1997 – 2005 CSI/FBI reports.

4.2 Statistics DataLossDB

Table 6 reports the findings in the database *DataLossDB.org* [11] which records security breaches from a variety of institutions like government, finantial, education and medical institutions. Three *categories of inside* are outlined: *inside incident* that corresponds to someone from inside the company, such as a disgruntled employee, *inside malicious* that is someone who eavesdrops, steals, or damages information, uses information in a fraudulent manner, or denies access to other authorized users, and *inside accidental* that is the result of carelessness or lack of knowledge from an employee [23]. The averages of inside incident, inside malicious and inside accidental are 6.0, 19.5 and 56.3, with percentages of 7.33%, 23.83% and 68.82%.

Table 7, left side, sum the three categories of *inside incident* from table 6, rewrite the number of *outside incidents* and the number of *unknown*. The right side calculates percentages of inside, outside and unknown from 2000 to 2009. Figure 2 shows the number of inside and the number of outside as the left part of table 7. A Pearson coefficient of 0.922 shows a strong correlation between these two data sets. To corroborate previous statement, the Fisher's coefficient

Table 6: Incidents per year found on DataLossDB.org.

Year	*Inside*			*# Outside*	*# Unk.*	*Total*
	# Inc.	*# Mal.*	*# Acc.*			
2000	0	0	2	6	1	9
2001	0	2	6	10	0	18
2002	0	2	2	2	0	6
2003	1	2	0	11	0	14
2004	1	1	3	18	0	23
2005	1	9	22	104	5	141
2006	8	32	134	338	24	536
2007	13	24	76	382	9	504
2008	29	70	141	499	49	780
2009	7	53	177	306	48	591

Table 7: Total number & percentage of incidents per year found on DataLossDB.org.

Year	*Number*			*Percentage*		
	Inside	*Outside*	*Unknown*	*Inside*	*Outside*	*Unknown*
2000	**2**	6	1	**22**%	67%	11%
2001	8	10	0	44%	56%	0%
2002	4	2	0	67%	33%	0%
2003	3	11	0	21%	79%	0%
2004	**5**	18	0	**22**%	78%	0%
2005	32	104	5	23%	74%	4%
2006	174	338	24	32%	63%	4%
2007	**113**	382	9	**22**%	76%	2%
2008	240	491	49	31%	63%	6%
2009	237	306	48	40%	52%	8%

was calculated giving the range $0.698 < \rho < 0.981$ that does not include the zero (0) value.

Small values in Table 7 suggest the possibility of outliers. The Quartiles corresponding to the number of inside and outside incidents were calculated. For the data set *Inside*, second column in Table 7, $Q1 = 3.75$, $Median = 20$ and $Q3 = 190$, no outliers were found; and for the data set *Outside*, third column in Table 7, $Q1 = 9$, $Median = 61$ and $Q3 = 349$, no outliers were found. The *p-value* of 0.313 shows that the two data sets are not significant different at the 95% confidence level.

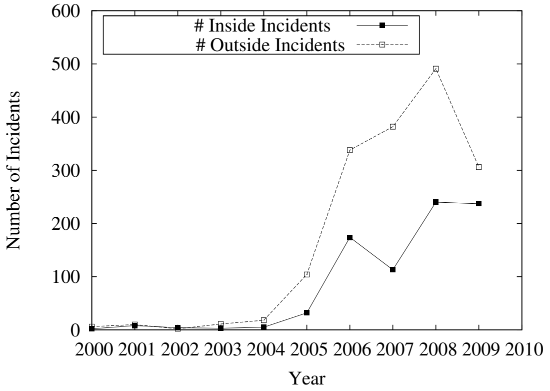

Fig. 2: Number of inside and outside incidents. DataLossDB.org reports at September 2010.

The average of the number of inside, outside and unknown is 81.8, 166.8, and 13.6, which gives the percentages of 31.19% for insiders, 63.61% for outsiders, and 5.18% for unknown. The raw averages were tested with the bootstrap technique as described in Section 4.1, and the corresponding values obtained were 81.77, 163.96, and 13.53 for inside, outside and don't know, with errors of 31.23, 55.09, and 5.88 correspondingly.

4.3 Statistics CSO/CERT

Table 8 includes statistics reported by business and government executives, as well as professionals and consultants [9]. This table needs some explanation. The years 2004 and 2005 sums approximately 200%, and this is because the report counts *Outsiders* as 100%, as well as *Insiders* [8]. For example, *don't know* has a value of 30% in the side of *Outsiders*, and 30% in the side of *Insiders*, in other words, it counts as 60%. Year 2006, as well as 2007, sums 300%, because this time the presentation of statistics changed; a new sections reports independently *unknown* adding an additional 100% to the statistics [10]. The report corresponding for 2010 is a little bit more difficult to handle, because it is now giving the mean and median for outsiders, insiders, and unknown that counts for 100% [9]. In *Section Two, numeral 1*, the *CERT* report describes the question about organizations that have experienced a cybersecurity event during the last 12 months—August 2008-July 2009—40% answered *none*, and 60% answered *any*. This is the 40% that appears in Table 8, year 2010, column *None*.

Table 8 shows a new column *None* that is not present in previous statistics—*FBI,DataLossDB.org*. *None* is different from *unknown* that indicates that the organization reports an intrusion but it does not know where it comes from—from inside, outside or unknown.

Finding some statistical inferences this time is more difficult. Table 9 shows the actual percentages used in order to find an average from the years at hand. Now *unknown* is 30% for year 2004, because it was considered as counted twice, one time with the outsiders report and another time for the insiders report—See Table 8. Same case is considered for year 2005, but for the rest of the years, *unknown* is reported independently, not in conjunction with insiders and outsiders. With these assumptions, in average for the years reported by *CERT* as in Table 9, 31.0% for insiders, 48.7% for outsiders, and 20.4% for unknown. The averages were tested with the bootstrap technique as describes in Section 4.1, and the corresponding values obtained were 30.96, 48.62, and 20.33 for insiders, outsiders and don't know, with errors of 0.59, 1.93, and 1.45 correspondingly.

4.4 Statistics Verizon

Verizon reports *confirmed breaches* that are representative of all breaches in all organizations [25], represented

Table 8: Percentage of incidents reported by CERT.

year	*# Resp.*	*Ins.*	*Out.*	***None***	*Don't Know*	*Total*
2004	342	41%	64%	37%	**60%**	202%
2005	554	39%	77%	47%	38%	201%
2006	328	55%	80%	128%	37%	300%
2007	443	49%	76%	142%	33%	300%
2010	523	34%	46%	40%	24%	144%

Table 9: Percentage of incidents inferred from CERT reports.

year	*Percentage Used*			*Proportion*			*Total*
	Inside	*Outside*	*Unknown*	*Inside*	*Outside*	*Unknown*	*Total*
2004	41%	64%	30%	30.4%	47.4%	22.2%	1
2005	39%	77%	19%	28.9%	57.0%	14.1%	1
2006	55%	80%	37%	32.0%	46.5%	21.5%	1
2007	49%	76%	33%	31.0%	48.1%	20.9%	1
2010	34%	46%	24%	32.6%	44.2%	23.2%	1

primarily by retail, financial services, food and beverages, manufacturing, business services and hospitality.

Table 10 estimates are from Figure 6 of the 2009 report [25]. Totals are greater than 100% because of the participation of external and internal with partner associations.

The proportion of internal (22.14), external (71.57) and partner (30.57) were calculated as an average from Table 10, having in mind that outsiders, insiders, and partners included not only themselves but possibly intersections between themselves [1]. As in previous reports, the bootstrap technique was applied to corroborate the averages calculated. The values of 22.08, 71.75, and 30.28 were obtained for insiders, outsiders and partners, with errors of 4.03, 3.81, and 5.28 respectively.

5. Analysis

As the focus of this paper is to address the inside vs. the outside threat, it is clear from the *FBI* reports recorded from 1997 to 2005—See Table 4 Section 4.1—that the averages of percentages are approximately of equal proportion for inside incidents (37.7%) and outside incidents (37.9%) with similar estimated errors of 1.606 and 1.829. The number of incidents derived shows a dominant number of inside incidents over outside incidents from the period 1997−2000, and a dominant number of outside incidents over inside incidents from 2001 – 2005—See Figure 1. There was not a linear correlation between the number of inside incidents and the number of outside incidents inferred from the period 1997 – 2005.

Table 10: Percentage of incidents reported by Verizon.

year	*Inside*	*Outside*	*Partner*	*Total*
2004	12%	92%	8%	112%
2005	28%	60%	41%	129%
2006	15%	75%	40%	130%
2007	16%	65%	44%	125%
2008	18%	73%	39%	130%
2009	20%	74%	32%	126%
2010	46%	62%	10%	118%

The database *DataLossDB.org* shows the categorization of insiders as inside incident (7.33%), inside malicious (23.83%) and inside accidental that is the bigger threat in this category with 68.82%. These percentages are taken from the averages of data from 2000 – 2009—See Table 6. Including these three categories makes inside incidents 31.2% under outside incidents 63.6%. The two data sets show a positive trend from 2000 – 2009 and a $p - value = 0.313$ shows that the two data sets are not significantly different at the 95% confidence level. There is a strong linear correlation between the number of inside incidents and outside incidents ($pearson - coefficent = 0.922$), but as the data is left skewed, averages of incidents give high errors. The average of inside incidents is 81.77 with an estimated error of 31.23. The average of number of outside incidents is 163.96 with an estimated error of 55.09, and the average of number of unknown is 13.53 with an estimated error of 5.88. However, there is no doubt that the number in outside incidents outperformed the number of inside incidents in all years except 2002. The right part of Table 7 was built in order to show how percentages give some general ideas, but they do not present the real picture. For example, two inside incidents, five inside incidents and 113 inside incidents correspond to the same percentage of 22%.

Making statistical inferences with the data reported from *CERT* is difficult, not only because reports change the way of presenting statistics every two years or so, but because with the data available, it is difficult to derive statistics more useful as the number of penetrations. Given the percentages inferred as in the right part of table 9, outside incidents with 48.7% outperformed inside incidents with 31.0% from 2004 – 2007 and 2010 reports [2]. Taking the percentages as presented by *CERT*—See Table 8, every year the percentage of outsiders outperformed the percentage of insiders.

Verizon reports confirmed breaches, so the source of the threat is known. Averages obtained give a proportion of 71.57 of outsiders over 22.14 of insiders, and as Table 10 shows, every year the percentage of outside incidents outperformed the percentage of inside incidents. This time, data was not normalized to 100%, which means that the proportions inferred have some intersections. This is an interesting fact that is shown in Figure 3 inferred from the 2009 report that indicates 43% only by external, 11% only by internal, 7% only by partner and 39% multiple sources [25].

FBI, *DatalossDB.org* and *CERT* reported *unknown* or *don't know* incidents. *FBI* reported an average of 24.2% of *don't know* from 1996 – 2008, *DatalossDB.org* reported on average 5.18% of *unknown* from 2000 – 2009—with four years reporting 0, and *CERT* reported an average 20.4% of

[1] Values shown do not sum 100% as per intersections to be addressed on Section 5

[2] 2010 reports from August 2008 to July 2009 [9].

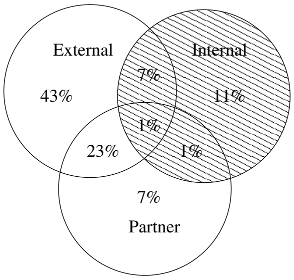

Fig. 3: Percentages of external, internal and partner data breaches as in Table 10. Year 2009. Intersections are inferred.

don't know/unknown from 2004 – 2007 and 2010.

DatalossDB.org and *Verizon* reported significant errors as a cause of data breaches; of the inside incidents reported by *DatalossDB.org* on average 68.8% corresponds to inside accidental—See Section 4.2, and *Verizon's* 2009 report gives 67% of cause of breaches due to significant errors [25].

6. Conclusions and Future Work

This paper presented and analyzed some statistics about the number/percentage of penetrations coming from inside, or outside organizations or from unknown sources. With this data, the reader could, at least partially, conclude if the general statement says that the highest threat for computers and its resources come from within organizations is true. However, computer security is complex [21] and making such a statement has the likelihood of not being true in some situations. Other variables not considered in this study, like the number of records breached, and the amount of money companies are losing, will improve this research and are part of future work.

Coming from inside the organization, or coming from outside, or coming as a partnership, could help security managers by setting appropriate security mechanisms in place, but coming from unknown sources, or reporting no penetration, should make organizations realize that current security mechanisms are not valid any more, and/or security policies, procedures and standards are not applied as they should be. *Verizon* reported that more than 60% of data breaches were discovered by third parties, and that more than 86% of breaches were avoidable through simple or intermediate controls [25], [26].

The perimeter to secure has been expanded, or maybe there is no perimeter at all [7].

References

[1] J. P. Anderson, "Computer security technology planning study," Deputy For Command and Management Systems. HQ Electronic Systems Division (AFSC), Fort Washington, PA, Tech. Rep., 1972.

[2] ——, "Computer security threat monitoring and surveillance," James P. Anderson Co., Fort Washington, PA, Tech. Rep., 1980.

[3] R. G. Bace, *Intrusion Detection*. USA: MacMillan Technical Publishing, 2000.

[4] T. Bengtson, "Shazam secure to help bankers with it security," 2005, accessed October 2010. [Online]. Available: http://www.allbusiness.com/financeinsurance/933194.html

[5] CSI Computer Crime and Security Survey Report, "CSI/FBI Computer Crime and Security Survey," 2000, accessed November 2010. [Online]. Available: http://www.

[6] ——, "8th CSI/FBI Computer Crime and Security Survey," 2003, accessed November 2010. [Online]. Available: http://www.citadel-information.com/library/4/2003-fbi-csi-survey.pdf

[7] ——, "14th CSI Computer Crime and Security Survey," 2009, accessed November 2010. [Online]. Available: http://www.personal.utulsa.edu/ james-childress/cs5493/CSISurvey/CSISurvey2009.pdf

[8] CSO magazine, U.S. Secret Service, CERT Coordination Center, "2004 Cybersecurity Watch Survey — Survey Results," 2004, accessed November 2010. [Online]. Available: http://www.cert.org/insider_threat/

[9] CSO magazine, U.S. Secret Service, CERT Program, Deloitte, "2010 Cybersecurity Watch Survey — Survey Results," 2010, accessed November 2010. [Online]. Available: http://www.cert.org/insider_threat/

[10] CSO magazine, U.S. Secret Service, CERT Program, Microsoft Corp., "2007 Cybersecurity Watch Survey — Survey Results," 2007, accessed November 2010. [Online]. Available: http://www.cert.org/insider_threat/

[11] DATALOSSDB, 2009, accessed July 19/2010. [Online]. Available: www.datalossdb.org

[12] D. Denning, "Cyber security as an emergent infrastructure," 2003, accessed October 2010. [Online]. Available: http://faculty.nps.edu/dedennin

[13] P. A. Diaz-Gomez and D. F. Hougen, "Improved off-line intrusion detection using a genetic algorithm," in *Proceedings of the 7th International Conference on Enterprise Information Systems*, 2005, pp. 66–73.

[14] B. Efron and R. J. Tibshirani, *An Introduction to the Bootstrap*. USA: Chapman & Hall/CRC, 1998.

[15] GISS, "GISS Goddard Institute for Space Studies." 2009, accessed December 2009. [Online]. Available: http://icp.giss.nasa.gov/education/statistics/page-3.html

[16] S. Harris, *All in One CISSP*. USA: MacGraw Hill, 2008.

[17] P. Hupston, "How to enhance computer network security," 2009, accessed July 19/2010. [Online]. Available: http://computeraccessories.suite101.com/article.cfm/how to enhance computer network security#ixzz0t3e7q2Yq

[18] D. D. Jensen and P. R. Cohen, "Multiple comparisons in induction algorithms," *Machine Learning*, vol. 38, no. 3, pp. 309–338, 2000.

[19] M. E. Kabay, "Educational security incidents (esi) year in review," 2009, accessed July 19/2010.

[20] Salvatore J. Stolfo et. all, *Insider Attack and Cyber Security Beyond the Hacker*. Springer, 2008.

[21] B. Schneier, *Secrets & Lies*. USA: Wiley Computer Publishing, 2000.

[22] C. Schou and D. Shoemaker, *Information Assurance for the Enterprise. A Roadmap to Information Security*. USA: McGraw Hill, 2007.

[23] J. Shah, "The threat within: Protecting information assets from well-meaning employees," 2009, accessed September 2010. [Online]. Available: www.net-security.org/article.php?id=1289

[24] W. Stallings, *Network Security Essentials. Fourth Edition*. USA: Pearson Prentice Hall, 2011.

[25] Verizon Business Risk Team, "2009 Data Breach Investigations Report," 2009, accessed November 2010. [Online]. Available: http://www. verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

[26] ——, "2010 Data Breach Investigations Report," 2010, accessed November 2010. [Online]. Available: http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf