Watching your own: The problem of insider IT misuse

Steven Furnell and Aung Htike Phyo

Network Research Group, University of Plymouth, Plymouth, United Kingdom

Email: sfurnell@network-research-group.org

Abstract

In recent years the Internet connection has become a frequent point of attack for most organisations. However, the loss due to insider misuse is far greater than the loss due to external abuse. This paper focuses on the problem of insider misuse, the scale of it, and how it has effected the organisations. The paper also discusses why access controls alone cannot be used to address the problem, and proceeds to consider how techniques currently associated with Intrusion Detection Systems can potentially be applied for insider misuse detection. General guidelines for countermeasures against insider misuse are also provided to protect data and systems.

Keywords: Insider misuse; misuse detection; misuse countermeasures.

Introduction

If one was to play a game of word association and use the terms ‘security breach’ or ‘cybercrime’ as the starting point, it is very likely that words like ‘hacker’ or ‘virus’ would be amongst the first responses. It is somewhat less likely that terms like ‘employees’ or ‘insiders’ would emerge as many peoples’ first choices. In reality, however, insiders are very often the cause of the most significant and costly security incidents, and a significant proportion of what is commonly classed as cybercrime can be attributed to them. Indeed, the fact that insiders are already within the organisation often puts them in an ideal position to misuse a system if they are inclined to do so.

Although the great majority of the people are familiar with the generic meaning of the word 'misuse', when we try to map it to an IT context, there is a need to clarify certain issues. Insider IT misuse can be a very subjective term, and one of the most challenging tasks is to draw a clear line that separates an IT misuser from a person who is using a system in an acceptable way and for an approved purpose. The word ‘misuse’ implies the presence of rules that specify the conditions of allowable usage for the resources concerned. These rules are often embodied within an IT usage policy. However, such a policy, and hence the definition of misuse, can differ from one organisation to the other. For example, where some would give priority to detecting data-theft and unsanctioned modification of data, others might want to detect denial of services and Internet access abuse. Thus no single definition of misuse is appropriate for all organisations.

The aims of this paper are to present evidence of the insider misuse problem, and suggest possible means by which it could be addressed. The discussion begins by examining the scale of the problem, based upon evidence from computer abuse surveys from recent years. This is followed by a more specific consideration of what can actually be considered to constitute IT

misuse in an organisational context, which then leads into a discussion of methods that could potentially be employed to combat the problem.

The scale of the insider misuse problem

If one takes a look back to computer crime literature and surveys dating up to the mid-90s, the evidence presented would certainly suggest that the main threat was to be found from one's own staff (with as much of 80% of computer crime believed to be the result of insider activity). In more recent years, however, many sources have indicated a significant rise in externally sourced incidents (principally in terms of Internet-based attacks such as website defacement and denial of service), with the consequence that although insider misuse is still significant, it now accounts for a far lesser proportion of raw incidents. For example, in the UK, results from the Department of Trade & Industry's Information Security Breaches Survey 2002 revealed that only 34% of businesses considered their worst security incident to have been caused by an insider (DTI 2002). This possibly accounts for why 60% of respondents in the same survey were either not very concerned or not at all concerned about threats originating from their own employees. Hackers were the most feared threat, particularly amongst large businesses (with over 250 employees) where 50% expressed some level of concern about them). However, when considering the large businesses only, it should be noted that the split between those experiencing their worst incident as a result of internal staff versus external parties was almost equal.

Another source that has monitored the changing trend regarding internal and external attack is the annual CSI/FBI Computer Crime and Security Survey. Looking back to 1995, a key observation from the CSI was that "the greatest threat comes from inside your own organisation" (Power 1995). In more recent years, however, the survey results have painted a rather different picture, and by 2002 it was reported that, for the fifth year running, more respondents had cited their Internet connection as a frequent point of attack (74%), than had cited internal systems (33%) (Power 2002.). This may well be the case, but presenting the information in this manner tends to create something of a false impression, because the raw number of incidents is not necessarily the factor that we should be most concerned about. Of more interest to most CEOs, for example, will be the effect that the incidents had on their bottom line.

Many of the categories used in the CSI/FBI results encompass incidents that could potentially have been both internally and externally sourced (e.g. theft of proprietary information, sabotage of data networks, and virus). However, three of the categories very clearly indicate the source, and it is interesting to see the level of the annual losses that were associated in each case. The relevant information is presented in Table 1 (Power 2002). It is quite evident from the results that, although they relate to a five-year period over which the proportion of externally sourced incidents had exceeded internal ones, the quantifiable losses in the latter case dwarf those attributable to outside hackers. It is therefore clear that, in real terms, the level of the insider threat is still much greater than that exhibited by external hackers.

	System penetration by outsider	Inside abuse of Net access	Unauthorized insider access
1998	$1,637,000	$3,720,000	$50,565,000
1999	$2,885,000	$7,576,000	$3,567,000
2000	$7,104,000	$27,984,740	$22,554,500
2001	$19,066,600	$35,001,650	$6,064,000
2002	$13,055,000	$50,099,000	$4,503,000
Total	**$43,747,600**	**$124,381,390**	**$87,253,500**

Table 1 : Annual losses for selected incidents from CSI/FBI surveys

The CSI figures relating to insider abuse of network access clearly suggest that, as well as bringing considerable advantages in terms of web and email communication, Internet access has also ushered in a whole range of new problems. This can be further evidenced by a survey of 544 human resources managers, conducted in 2002 and targeting large UK companies (with 'large' in this case being defined as those employing an average of 2,500 people). The results revealed that almost a quarter of them (23%) had felt obliged to dismiss employees in relation to Internet misconduct (with the vast majority of these cases – 69% - being linked to the downloading of pornographic materials) (Leyden, 2002). Many other cases resulted in less severe courses of action, such as verbal warnings or a discreet word in the ear of the person concerned, and in total the results indicated that 72% of respondents had encountered Internet misuse in some form.

The nature of insider IT misuse

One of the CSI/FBI categories from Table 1 was that of 'unauthorised insider access'. However, one of the complicating aspects with insiders, and the aspect that differentiates this from the other insider category listed in the table, is that incidents will not always relate to something that is unauthorised. Indeed, the basic problem with insider misuse is that the person concerned has legitimate access to IT resources of the target organisation. This means that he/she does not need to bypass the authentication mechanisms of the IT infrastructure (no stealing or illegal reproduction of passwords and other forms of authentication tokens). Thus, in an IT context, insider misuse is the act of abusing granted privileges to cause harm. In this context, it can also be observed that users that know more about a system are more likely to abuse their privileges than users who are less knowledgeable.

Although this is not difficult to grasp, vagueness is introduced by the term misuse and what it means to different people or organisations. What is considered illegitimate use in one particular organisation can be perfectly acceptable for another. For example, browsing the web for personal use is outlawed entirely in some companies, whereas others are somewhat more relaxed about it and impose varying limits upon what is acceptable (e.g. some may permit up to 20 minutes per day, whereas others may allow twice this). In addition, there are myriad other activities that would likely be regarded as misuse in any organization, for example:

- Personal entertainment (e.g. playing games, writing personal email etc.)

- Downloading MP3s, pirated software, pornographic images, or other unsuitable material
- Fraud and theft (e.g. modifying payroll database to increase one's wages)
- Sending out inappropriate material using company computers
- Installing and using pirated software.
- Reading or modifying another user's files.

Although the computer security research community has created a plethora of taxonomies that describe computer intrusions in general (see Furnell et al. 2001 for an overview), little effort has been placed on the construction of a taxonomy that specialises in insider incidents. The earliest attempt to classify internal misuse of computer systems is presented by Anderson (1980) and discusses borders of distinction between *masqueraders*, *clandestine users*, and *misfeasors*. Masqueraders are insiders that exploit weaknesses of the authentication system, thus gaining the identity of other legitimate users. A clandestine user is related to authorised users and their capabilities to bypass audit, control and access resource mechanisms in a particular computer system. Finally, misfeasors are insiders who do not need to masquerade, but abuse the power of their privileges to misuse the system. However, as the small selection of examples above shows, the single category of 'misfeasor' can encompass a whole range of different incidents. As a result, other works have focused more specifically upon the issue of insider misuse, and indicative examples are given below:

- *Tuglular* (2000). This is the first comprehensive taxonomy of misfeasor incidents. The taxonomy classifies computer misuse incident in three dimensions: incidents, response and consequences. The entire taxonomy is orientated towards data collection for insider incident response.

- *Magklaras and Furnell* (2002). This taxonomy is human centric. Magklaras and Furnell perceived that all actions that constitute IT misuse lead back to human factors. The fundamental aspect for their taxonomy is classifying people in three basic dimensions: system role, reason of misuse and system consequences. This scheme is the most appropriate for threat prediction, but not suitable for detection.

Intentional misfeasor cases are performed for a variety of reasons. The best way to sub-divide them is to consider the motives in a way that could detect the ultimate goal of the abuser. It might be inferred, for example, that a legitimate user is trying to access sensitive data (data theft), take revenge against a particular person or an entire organisation (personal differences), cover indications of unprofessional behaviour, or deliberately ignore a particular regulation of the information security policy.

Unfortunately, despite evidence of the insider threat, there is no substantial effort devoted to addressing the problem of internal IT misuse. In fact, the great majority of misuse countermeasures address forms of abuse originating from external factors (i.e. the perceived threat from hackers). A significant reason for this is the difficulty in actually monitoring and detecting the problem in order to enable a response to be mounted. In the cases above, for example, it is clear that the misuse would have been very difficult to control or prevent, as the perpetrators concerned were not violating any system-side access rules.

Combating insider misuse

The problem with insider abuse is that, once a user is authenticated to use a system, what he does with the system or the objects he has access rights to is neither monitored nor logged most of the time. Considering the list of potential misuses in the previous section, it is possible that appropriate access controls could be used to prevent some of them, but even these will not be sufficient for all contexts (consider, for instance, the case in which the misfeasor has legitimately been granted administrator level privileges). This epitomizes the difficulty in implementing access controls that resembles organisational hierarchy onto the IT systems. It must also be remembered that one user/process/account having all the privileges can lead to serious misuse by exploiting the situation. Neumann's suggestion of multilevel systems and compartmentalization (Neumann 1999) should be given a serious consideration before we proceed with the insider misuse detection.

Today's commercial operating systems are based on the old systems developed years ago. At the time when the core components of these systems were developed, the users were expected to behave themselves. The problem of insider misuse was not an issue. However the research in the IT security over the years has proved that people do misbehave and that insider misuse is a serious problem. Since these systems were not developed with insider misuse in mind, the preventive mechanism and the logging present in today's commercial systems are not optimized for misuse detection. Existing access controls are not good enough to prevent insider misuse, making it more difficult to enforce insider misuse policies. For example, a user with administrator level privileges may not have the moral right to access confidential data on the system, but access controls present in today's systems cannot prevent such actions. As such, it is considered that some form of supervision system is required to monitor for misuse activity.

Such technologies are already available to some extent in the form of Intrusion Detection Systems (IDS) (Amoroso 1999), but as with many other mainstream security technologies, these are geared towards detecting attacks on the system rather than misuse of it by legitimate users. Nonetheless, some of the principles are transferable. For example, current IDS employ two main strategies to identify attacks namely misuse-based detection and anomaly-based detection, and it is possible to see how each of these could be applied to the insider problem.

- *Misuse-based detection*
  In a traditional IDS, this approach relies upon knowing or predicting the intrusion scenario that the system is to detect. Intrusions are specified as attack signatures, which can then be matched to current activity using a rule-based approach. A similar approach could potentially be incorporated for misfeasor incidents, based upon those methods that employees have been known to exploit in the past, or those that they can be anticipated to attempt based upon the privileges and resources available to them. For example, at a conceptual level, one such misuse signature might relate to a user who is identified as attempting to modify a record about him/herself in a database (e.g. the payroll example indicated earlier). The principle here would be that, although their database privileges may allow them to do so, users should probably not be modifying details relating to themselves without someone else's authority. Another example could be to watch for any sequence of events where a user accesses confidential information and then attaches it in an email destined for a recipient outside the organization. Neither of these rules would necessarily cause the user in

question to be locked out of the system (because in some contexts the actions could still be quite legitimate), but they could be used to flag the activity for closer scrutiny.

- *Anomaly-based detection*
  Rather than being based upon known or predicted patterns of misuse, this approach relies upon watching out for things that do not look normal when compared to typical user activity within the system. In a standard IDS, the principle is that any event that appears abnormal might be indicative of a security breach having occurred or being in progress. The assessment of abnormality is based upon a comparison of current activity against a historical profile of user (or system) behaviour that has been established over time. For example, past behaviour might suggest that a particular user typically downloads an average of 5MB of material from the web per week, and the nature of the attachments they assign to emails are normally documents. Therefore, if activity supervision detects a surge of download activity to 10MB in a single day, or a large number of email messages suddenly being sent with image attachments, then there would be reasonable grounds to investigate whether unsuitable activities might be in progress.

Although the above descriptions make the concepts sound relatively straightforward, it must be appreciated that neither technique can be considered 100% reliable, even in the context of traditional IDS. The consequence is that they can lead to false positives (where legitimate activity is believed to be intrusive) and false negatives (where genuine intrusive activities are misjudged as acceptable). The concept of applying the techniques for the detection of misfeasor activity / insider misuse makes the task more difficult, because we are dealing with legitimate users who are not violating access controls. From a misuse-based detection perspective, it is more difficult to identify the ways in which an insider might misuse the resources to which they have legitimate access, while from an anomaly detection perspective the level of behaviour profiling would need to be much more detailed and precise. When basing the assessment upon a comparison against their behaviour profile, a legitimate user misbehaving will almost certainly be more difficult to identify than a total impostor who is masquerading under the legitimate user's identity. In addition, in an adaptive system, the process of profile refinement might be exploited by wily misfeasors who gradually train the system to accept misuse behavior as normal. As such, this aspect is still an area of active research, as the technical approaches are not mature.

When considering how to protect systems now, it is worth noting that preventative measures need not be technical. Security guidelines, such as the recommendations provided by the ISO 17799 standard (BSI 2001), typically suggest a number of personnel-related measures, which if employed correctly could dramatically reduce the likelihood of insider misuse being successful:

- Check references of prospective new employees before hiring them;
- Ensure that employment contracts include a clause relating to the acceptable use of IT resources;
- Ensure that adequate reminders about the 'acceptable use' policy are encountered by staff during their day to day use of systems;
- Ensure adequate supervision of staff by line management;
- Provide a means by which staff can confidentially report misuse of IT systems, without fear of recrimination from colleagues.

- Concerning the access of data, make sure that access control policies resemble organisation's management hierarchy or rules.
- Security and access control policies need to be maintained to keep up with the change in organisation's management hierarchy.

In the absence of an automated supervision approach, it would still fall to line managers and the like to enforce and monitor these aspects.

Conclusion

Insider misuse poses a great threat to organizations. Even though the Internet connection is the most frequent point of attack, the loss due to insider misuse is far greater than the loss due to external attacks.

At the present time, the system level countermeasures that can be implemented are limited. Current access control systems, although well-suited to guarding against unauthorized activities, cannot prevent insider misuse effectively if the subject is doing something within their legitimately assigned privileges. More advanced mechanisms, in terms of activity monitoring and supervision systems may offer a potential solution in the future. The authors' ongoing research will design and evaluate approaches for realizing the latter approaches, and results will be detailed in future publications.

References

Amoroso, E. (1999). *Intrusion Detection: An Introduction to Internet, Surveillance,Correlation, Traceback, Traps and Response*, First Edition, Intrusion.Net books, NJ, ISBN: 0966670078

Anderson, J.P. (1980). *Computer Security Threat Monitoring and Surveillance*, 1980.

BSI. (2001). *Information technology. Code of practice for information security management*. BS ISO/IEC 17799:2000. British Standards Institution, 15 February 2001. ISBN 0 580 36958 7

DTI. (2002). *Information Security Breaches Survey 2002*. Department of Trade & Industry, April 2002. URN 02/318.

Furnell S.M., Magklaras G.B., Papadaki M. and Dowland P.S. (2001). A generic taxonomy for Intrusion Specification and Response, *Proceedings of Euromedia 2001*, Valencia, Spain, 18-20 April 2001: 125-131.

Leyden, J. (2002). P45s for Porn Surfers, *The Register*, 9 July 2002. http://www.theregister.co.uk/content/6/26098.html

Magklaras G.B and Furnell S.M. (2002). Insider Threat Prediction Tool: Evaluating the probability of IT misuse, *Computers & Security*, vol. 21, no 1, pp62-73.

Neumann, P.G. (1999). The challenges of Insider Misuse, SRI Computer Science Laboratory, *Paper prepared for the Workshop on Preventing, Detecting, and Responding to Malicious Insider Misuse*, 16-18 August 1999, at RAND, Santa Monica, CA.

Power, R. (1995). *Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare*, San Francisco, CA: Computer Security Institute.

Power, R. (2001). 2001 CSI/FBI Computer Crime and Security Survey, *Computer Security Issues & Trends*, vol. VII, no. 1. Computer Security Institute. Spring 2001.

Power, R. (2002). 2002 CSI/FBI Computer Crime and Security Survey, *Computer Security Issues & Trends*, vol. VIII, no. 1. Computer Security Institute. Spring 2002.

Tuglular, T. (2000). A preliminary Structural Approach to Insider Computer Misuse Incidents, *EICAR 2000 Best Paper Proceedings*, pp105-125.