Detecting insider fraud is rather like looking for a hay-coloured needle in a haystack. This is because the perpetrators of systematic, long-term fraud need to preserve the secrecy of their activities. They know the controls and how to bypass them, and are often well-versed in the investigative process and know how to hide any incriminating evidence.

A key benefit of the system described here is its efficient handling of the time dimension. This improves upon early attempts in this area that use simple rules for spotting single events and are poor at detecting subtle, longer-term patterns. Audit trail data can be viewed from any point in time and changes in data are more easily visible.

By better defining the needles using the time dimension we can then go one step further and better define the hay. End result: cut away the hay and see a needle-rich picture.

The second benefit is that this kind of system gathers data in from all sources rather than adopting a ‘silo-based’ approach. It can, therefore, cross-reference and link across organizational, procedural and transactional boundaries, identifying cross-silo fraud and collusion between employees and external accomplices.

**Bigger picture, lower risk**

Ultimately, it’s dangerous to try to put different kinds of criminal behaviour and threats in neat little boxes, without thinking about the interplay between them. To return to the recent DTI survey, we see a slower growth in ID fraud indicated, compared with viruses, for instance. This kind of analysis gives the impression they are separate from each other but, in reality, they are not. Fraudsters and other criminals will make use of all kinds of tricks and techniques in their armoury, including viruses and fake IDs.

Also, bear in mind that if ID fraud does not appear to be growing as quickly, then that’s probably down to the old adage - ‘What we don’t know, we don’t know’. Only the bad fraudsters get caught - the really good ones carry on, mostly undetected. As a parting thought, consider that perhaps most organizations don’t believe they have identity management problems … because they’re completely unaware of them in the first place.

---

**Enemies within: the problem of insider attacks**

*Steven Furnell, Network Research Group, School of Computing, Communications & Electronics, University of Plymouth, Plymouth, UK*

This article considers the problem of insider attacks, beginning with some survey-based evidence to illustrate the existence of the problem, before proceeding to classify types of internal attacker. By far the most difficult problem to address is that of misuse of legitimate access, and the discussion proceeds to consider approaches to prevention and detection, concluding that a combination of technical and personnel measures represents the most feasible solution.

A significant aspect of computer security will always involve protecting systems from attack. When confronting this reality, it is perhaps only natural that our first thoughts will typically turn to protection against external attackers. There is, after all, a wealth of evidence to suggest that hostile forces are in operation on the Internet, and organizations are now fairly attuned to the fact that they face threats from this source (particularly in relation to worm and virus problems). Indeed, the significance of the external threat is reinforced by many of the products and much of the literature in the security domain, and when computer crime has hit the headlines, it has typically done so as a result of hacker and malware incidents. However, it is important not to lose sight of the potential for problems much closer to home. Alongside the reports of external attacks, there is ample evidence to show that insiders are very often the cause of the most significant and costly security incidents, and a large proportion of what is commonly classed as cybercrime can consequently be attributed to them.
As with external attacks, insider incidents may be motivated by a range of different factors, including greed, revenge, stress, and espionage, as well as being exacerbated by factors occurring outside the workplace (e.g. family problems). However, the fact that insiders are already within the organization, with some level of legitimate IT access, often makes them ideally placed to misuse a system if they are inclined to do so. The fact that they already know the system(s) involved puts them in a better position to:

- Know what is of value.
- Know what parts of a system may be vulnerable.
- Hide evidence of their activities.

As such, their ability to commit and conceal significant activities is often better than that of outsiders.

**Evidence of the problem**

The problem of insider attacks is far from a new one, and for a long time, the received wisdom in security circles was that around 80% of the threat actually came from within a target organization. Widespread adoption of the Internet has significantly altered this in recent years, exposing organizations to a vastly increased range of externally sourced threats, such as network-borne worms and viruses, denial-of-service, Web defacements, and other forms of hacker attack. However, internal problems remain, and a variety of survey results can be cited to provide an illustration of the scale and type of the threats:

- Results from the Department of Trade & Industry’s *Information Security Breaches Survey* 2004 revealed that approximately one third of businesses considered their worst security incident to have been caused internally (with the proportion rising to 44% when considering large organizations, with over 250 employees).²
- A survey of 544 human resource managers from large UK companies, conducted by *Personnel Today* in 2002, revealed that 72% of respondents had encountered Internet misuse in some form (illustrating that the Internet can increase the internal threats as well as external ones). In addition, almost a quarter of them (23%) had felt obliged to dismiss employees in relation to this misconduct (with the vast majority of these cases, 69%, being linked to the downloading of pornographic materials).³
- A survey of 18 000 UK office workers, conducted by Yahoo! in 2003, showed how information could be at risk of snooping from employers or unscrupulous colleagues, with 45% suspecting their co-workers of invading their privacy by reading their emails when machines were left unattended.⁴

Although the problem is clearly recognised, an off-reported survey statistic in relation to insider versus outsider attacks comes from the CSI/FBI survey series, and in more recent years, the presentation of these results has been emphasizing that more respondents are citing their Internet connection as a more frequent point of attack than internal systems (e.g. the 2003 figures were 78% and 30% respectively).⁵ However, although the Internet has undoubtedly shifted the balance considerably, and has significantly increased our visibility and vulnerability to external threats, this does not mean that the insider threat has disappeared, or that it has become any less significant than it was in the past. In addition, the number of incidents is not necessarily the factor that is of most concern. Of more interest to CEOs, for example, may be the cost to the organization, and to assess this we need to compare the losses attributable to internal and external incidents. Although many of the CSI/FBI categories encompass incidents that could potentially have come from either source (e.g. theft of proprietary information, sabotage of data networks, and virus), three of them very clearly indicate the origin, and the associated annual losses are summarized in *Table 1*. It is quite evident from these figures that, although they relate to a period over which the proportion of externally sourced incidents had exceeded internal ones, the quantifiable losses in the latter case dwarf those attributable to external attackers.

**Types of insider attack**

There are, of course, different grades of insider, who may differ fairly significantly in terms of their status in the eyes of the organization (e.g. full and part time employees, contractors, consultants). At the core, however, all share the common characteristic of having some level of legitimate access to IT systems, and it is in this context that we are considering their potential to originate an attack. When defining what is actually meant by the term ‘insider attack’, there is an important distinction to be drawn between unauthorized access and misuse. In this respect, a useful top-level classification is provided by a widely cited report from Anderson.⁶

**Internal penetrators**

Authorized users of the system who access data, resources or programs to which they are not entitled. Sub-categorized into:

- Masqueraders - Users who operate under the identity of another user.
- Clandestine users. Users who evade access controls and auditing.

---

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

<table>
<thead>
<tr>
<th>Year</th>
<th>System penetration by outsider</th>
<th>Insider abuse of Net access</th>
<th>Unauthorised insider access</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>$7,104,000</td>
<td>$27,984,740</td>
<td>$22,554,500</td>
</tr>
<tr>
<td>2001</td>
<td>$19,066,600</td>
<td>$35,001,650</td>
<td>$6,064,000</td>
</tr>
<tr>
<td>2002</td>
<td>$13,055,000</td>
<td>$50,099,000</td>
<td>$4,503,000</td>
</tr>
<tr>
<td>2003</td>
<td>$2,754,400</td>
<td>$11,767,200</td>
<td>$406,300</td>
</tr>
<tr>
<td>2004</td>
<td>$801,500</td>
<td>$10,601,055</td>
<td>$4,278,205</td>
</tr>
<tr>
<td>Total</td>
<td>$42,881,500</td>
<td>$135,453,645</td>
<td>$37,806,005</td>
</tr>
</tbody>
</table>

---

² "Annual Breach Report 2004". The Department of Trade and Industry, 2004
³ "Half of Office Workers Suffer Internet Misuse". *Personnel Today*, 2002
⁴ "Less Than Half of Employees Monitor Emails". *Personnel Today*, 2003
⁵ "Internet as a Point of Attack". *CSINews*, 2003
Misfeasors

Users who are authorized to use the system and resources accessed, but misuse their privileges.

The internal penetrators can, in many ways, be considered to be practicing hacker-type activities, with the only distinction being that they are employees rather than external parties. Their activities in all cases are clearly unauthorized when related to the access they have been granted to the systems concerned. In contrast, misfeasar behaviour can encompass a whole range of different incidents, but vagueness is often introduced by the term misuse and what it means to different people or organizations. What is considered illegitimate in one particular organization can be perfectly acceptable for another. For example, activities such as personal Web browsing, personal email, and playing games are outlawed entirely in some companies, whereas others are somewhat more relaxed and may permit them within certain limits. This clearly has the potential to cause problems if employees move from one workplace to another, and the issue highlights the need to possess and promote policies on IT security and acceptable use. Without this, significant scope for ambiguity remains, and employees could legitimately claim that they did not know any better. Having said this, there are also some activities that would be regarded as misuse in almost all contexts, and some practical examples are reported below:

In 1996, US-based Omega Engineering experienced an insider attack motivated by revenge. Timothy Lloyd, an employee for 11 years, had become disillusioned with his status within the company, and decided to respond by planting a time bomb within a vital computer system. When it triggered, the bomb destroyed the manufacturing programs and left the company unable to produce further products. Omega claimed the resulting damages totaled $10 million, plus a further $2 million in reprogramming costs. 7

In 1998 a member of staff from the UK’s Defence Evaluation and Research Agency (DERA) was discovered to have amassed a stash of 170,000 pornographic images using the organization’s Internet connection. 8 Investigators discovered that a key system had been spending 70% of its online time downloading and distributing the material.

In 2003, the UK Inland Revenue issued a warning to its staff regarding “computer misuse,” following evidence that employees had been abusing their access to IT systems in order to look up the tax details of their friends and family, as well as those of celebrities. Although the motivation in most cases was found to be idle curiosity, there was also evidence that some were using the information for malicious purposes (e.g. looking up the salary of an ex-spouse, and then passing the information on to the Child Support Agency). The Inland Revenue was keen to point out that such misuse was extremely rare, but nonetheless, 2001 had seen 226 disciplinary cases as a consequence of computer misuse, with serious cases resulting in staff dismissal. 9

Such incidents portray the variety of forms that insider misuse may take, and some of the consequences that may result. From those above, the DERA and Omega cases can be considered to be fairly opposite ends of the scale. In the DERA case, the organization was not being attacked, and was not at risk of divulging or losing any data. Nonetheless, this incident (and many others like it) can still be clearly related to security. Most obviously, such misuse can introduce potential availability implications, because the activities are certainly consuming network resources (e.g. in this case, a system tied up for 70% of its time downloading porn). In addition, of course, the employees are doing all of this on company time (for which they are being paid), and bringing the possibility of embarrassment to their employers. Meanwhile, in the Omega case, there was a clear example of an insider attack causing direct and significant harm to the organization concerned.

All of the above share the characteristic that the individuals committed the abuse of their own volition. However, it is also important not to overlook the possibility for insiders’ privileged access to be targeted and leveraged by third parties (e.g. via blackmail or bribery). This point links into the desirability of appropriate supervision by line managers – one of the points flagged again in the next section.

Preventing and detecting insider attacks

Having outlined the problem, it is naturally relevant to consider what we can do about it. However, when compared to other aspects of security (e.g. detection of external attacks), it becomes apparent that there is a relatively limited body of prior work dedicated to the issue. There are, nonetheless, certain directions that can be pursued to aid prevention and detection.

One aspect of prevention can relate to predicting whom such attacks might arise from. In this respect, previous research has indicated that psychological characteristics, such as introversion, may make an individual a more likely candidate for committing misuse. 10 However, it is not necessarily easy to identify the danger signs from this perspective – particularly if we desire an automated solution. By contrast, other research activities have suggested some characteristics that could be measured and assessed at the system level, in order to yield a metric for the estimated potential threat posed by different users. 11 These findings could feed into other processes, such as assignment and review of access rights, as well as monitoring and supervision of user activity.

Perhaps unsurprisingly, appropriate technical measures begin with the fairly mundane and standard considerations, such as ensuring appropriate user authentication, and that subsequent user access rights and privileges are not excessive for their role. Attention to such details will significantly help to control the potential for unauthorized insider access via masquerade attacks and clandestine activities.

More problematic are the cases in
which insiders are operating in misfeasor mode, and making inappropriate use of legitimately assigned access rights. Certain elements of misuse can already be policed and controlled with existing technologies. For example, appropriate use of firewalls and filtering software can effectively restrict those users who spend their time accessing inappropriate sites and/or downloading undesirable materials. Furthermore, if the platform permits it, then careful application of access controls can be used to regulate access according to the role of the user. Roles for appropriate job functions should be created with the least privileges required to complete the relevant tasks, and users can then be assigned to the role(s) that reflect their responsibilities (thus inheriting the associated privileges). With such access control in place, the scope for misuse of privileges can be reduced by ensuring separation of duties. In this way, a single user is not in a position to commit the whole sequence of events necessary to achieve a malicious aim. For example, users may be given the right to issue transactions, but not to approve them. As such, a user wishing to commit misuse is forced to collude with others – thus hopefully complicating matters in many cases.

Unfortunately, while they can be used to tighten things up, none of these techniques will necessarily provide a complete solution. The user will still retain some level of legitimate access, and may still be able to find scope within this to cause damage if they desire to do so. Indeed, from a technical perspective, there is a notable difficulty in actually monitoring and detecting the insider problems, when compared to those that originate from outsiders. In the previous examples, for instance, 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. At this point, the type of control needs to move from preventative towards monitoring, and as a consequence some techniques traditionally associated with intrusion detection systems (IDS) can have a role to play. IDS can employ two main strategies to identify attacks, namely misuse-based detection and anomaly-based detection:

**Misuse-based detection:**
This approach relies upon knowing or predicting the scenario that the system is to detect. Signatures are created for attacks, 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 it can be anticipated they could attempt, based upon the privileges and resources available to them.

**Anomaly-based detection:**
This approach involves watching for things that appear abnormal when compared to typical activity within the system. In 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.

In terms of how and where such techniques could be applied, it is notable that different forms of misuse are likely to manifest themselves at different levels within the system. As such, monitoring activities can target a number of levels:

**Network level:**
Monitoring of activity at the network traffic level. Misuse activities visible at this level might include access to prohibited content, downloading of inappropriate material, spamming, and playing network games.

**System level:**
Monitoring at the operating system level, using events such as system calls, CPU usage, and file access, alongside data sources such as audit trails and event logs. Incidents discernable at this level may include breaches of privacy, installation of unauthorized software, and storage of inappropriate materials.

**Application level:**
Monitoring of interactions with the application, such as request-response, access patterns, user input, application output, and utilization of application functions. This would be the most appropriate level for determining misuse such as disclosure of confidential information, malicious data modification, and fraud.

For the purposes of detecting the most significant and damaging classes of insider misuse, it is likely that application level monitoring would provide most relevant data. However, this puts us into the realm of more application-specific measures, such that the controls introduced to combat misuse in one application (or type of application) will not provide any protection for other contexts. Examples of such approaches can be cited from the research community, with database applications proving to be popular candidates for attention due to the myriad misuse opportunities that present themselves within such environments. Previously published work in this respect has included:

**DEMIDS (Detection of Misuse In Database Systems)**
DEMIDS attempts to profile working scopes based upon user access patterns in relational databases. The approach assumes that a user will not typically access all attributes and data in a database schema, and therefore their access patterns will form some working scopes, which are sets of attributes usually referenced together with some values. Based upon this assumption, DEMIDS uses the notion of a distance measure between sets of attributes that consider both the structure of the data and user behaviour. This notion is then used to guide the search for regular patterns that describe user behaviour in a relational database.

**DIDAFIT (Detecting Database Intrusions Through Fingerprinting Transactions)**
DIDAFIT monitors anomalous SQL...
queries by generating fingerprints of authorized queries. These fingerprints are sequences of SQL queries, along with variables that the users should not change, ensuring that the queries are executed in proper order and only on the restricted range of records.

In addition to the above, related research is also in progress within my own group, again using database applications as the target environment. The approach here is based upon a combination of role-based access, separation of duties, and transaction profiling in order to provide a basis for specifying rules and identifying anomalies in relation to user activities within the database environment.

Given that the preceding paragraphs have been making reference to research activities, it should be apparent that some of the technological approaches in the domain of insider attack detection are not as mature as those relating to other aspects of security. However, it is worth noting that preventative measures need not be technical, and it is very likely that we will remain reliant upon a mixture of human and technological measures. In identifying the precautions that can be taken at the personnel level, it is relevant to observe that security guidelines, such as those provided by the ISO 17799 standard, typically suggest a number of measures that could dramatically reduce the likelihood of insider misuse being successful:

- Check references of prospective new employees before hiring them. Survey evidence suggests that the majority of organizations would prefer not to hire individuals such as ex-hackers, and taking up references is a good start in guarding against both this and other undesirable backgrounds.
- Ensure that employment contracts include a clause relating to the acceptable use of IT resources. In this way, employers can help guard against claims of ignorance by staff.
- 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. Appropriate use of informal monitoring, as well as more formal contexts such as appraisal, may help to identify disgruntled employees who may be at risk of causing problems.
- Provide a means by which staff can confidentially report misuse of IT systems, without fear of recrimination from colleagues.

Used in combination with appropriate technical measures, these procedures may well improve the prevention and detection of insider incidents.

**Blurring the boundaries**

The discussion in this article has intended to show that, while we have many good reasons for guarding our borders, there are also many good reasons for watching within them. Having said this, the issue needs to be approached with care. Creating a situation in which honest and well-behaved employees feel that they are not trusted will be counterproductive. Not only could it lower morale and create bad feeling – it could also increase the chance of misuse occurring as a result of staff becoming disillusioned.

At the end of the day, the vast majority of staff in most organizations will be honest and try their best to abide by the rules. However, even when they can be trusted not to be malicious, it is still worth remembering that insiders can cause problems purely by accident. For example, how many malware infections occur because our own users are simply careless (e.g. opening unsolicited email attachments)? How often are external attackers indirectly assisted by internal oversights that have left target systems vulnerable (e.g. unpatched software, weak passwords, etc)? Survey results would seem to suggest that the answers to these and other similar questions do not favour our own employees. At the same time, of course, much of the potential insider misuse can involve entities outside the organization. Although it may originate from within our systems, an incident involving access to the Internet has clear external links.

Such considerations bring us to a point at which the issues of internal and external threats become intertwined, and the required solutions become similarly inseparable. In this sense, we are not looking at a clear boundary at all, but rather a landscape in which security is required to address threats irrespective of their location.

**References**


Cisco source code stolen – but should we care?

Philip Hunter

It was clearly bad news for Cisco itself when a portion of its IOS software surfaced for a few days in May on a Russian website. But it was difficult to obtain a consensus within the security industry over the potential threat posed by the breach to the Internet as a whole or to the countless private IP networks. Given that IOS drives most of the world’s routers that direct traffic both through the Internet and private networks, theft of some of its source code clearly gives hackers the potential to exploit vulnerabilities that would be hard to identify otherwise. Naturally the Open Source community pounced on the issue, as they did earlier in the year when some Microsoft Windows source code was stolen, with the argument that any system relying on secrecy for security is fundamentally flawed and by definition insecure. Kerckhoff’s law that “a system should be designed to be secure if everything is known about it except the key information” was trotted out as an argument that closed source software such as IOS and Windows would soon be extinct, ushering in the golden age of open source.

Secrecy for security’s sake?

In truth this argument is rather disingenuous. Source code may be kept secret for commercial reasons, and doing so does not automatically imply that it is less secure. The test is whether the vendor is relying significantly on secrecy for security, in which case it is untrustworthy. But in the case of Cisco and Microsoft the situation is slightly ambiguous in that while intellectual property protection is the primary motive for source code secrecy, both vendors have relied to some extent on obscurity for their security. At any rate that has been the practical outcome of their efforts to maintain source code secrecy, for exposure even of portions of code usually leads to the discovery of previously unknown vulnerabilities.

Is the leak a threat?

The question is whether the newly exposed vulnerabilities pose a serious threat. In the case of Cisco it is too early to tell, although there are some pointers. In the case of Microsoft, exposure of the source code revealed a hole in Internet Explorer (IE), but this has yet to be exploited, and no further vulnerabilities have been discovered. Hackers continue to find ways of attacking Windows and IE without having to probe the source code.

About the author

Dr Steven Furnell is the head of the Network Research Group at the University of Plymouth, UK. He has been actively involved in security research for over 12 years, and has authored numerous papers on the topic, as well as the book ‘Cybercrime: Vandalizing the Information Society’, published by Addison Wesley. He is currently leading a project in relation to insider misuse detection, funded by the UK Engineering and Physical Sciences Research Council.

Contact
sfurnell@network-research-group.org

The theft reinforced...the futility of keeping source code secret

That being the case, Cisco should be in a still more comfortable position, at least with regard to the source code exposure. Hackers have hitherto concentrated most of their fire on the servers, hosts and private networks attached to the Internet, rather than on the underlying IP infrastructure. Whether the motive is notoriety, fraud or disruption, end systems constitute a more rewarding target.

On the other hand a successful large scale attack on the Internet itself could