A Security Architecture to Protect against the Insider Threat from Damage, Fraud and Theft

Clive Blackwell
Information Security Group,
Royal Holloway, University of London,
Egham, Surrey. TW20 0EX. UK.
C.Blackwell@rhul.ac.uk

ABSTRACT
The insider threat poses a significant and increasing problem for organizations. This is shown by the regular stories of fraud and data loss reported daily in the media in the US and elsewhere. There is a need to provide systematic protection from insider attacks because of their privileged access. We have developed a three-layer security architecture containing the physical, logical and social levels that we use to analyze the insider threat holistically to prevent, detect and recover from attacks. We examine destructive insider attacks, but the same analysis can be straightforwardly applied to the other main classes of insider threat from financial fraud and information theft. Our practical security model appears to have widespread application to other problem domains such as critical infrastructure and financial systems, as it allows the analysis of systems in their entirety including human and physical factors, not just as technical systems.

Categories and Subject Descriptors
K.4.2 [Social issues]: Abuse and crime using computers
K.6.5 [Security and protection]: Unauthorized access, physical security

General Terms
Security, Design, Management, Human Factors

Keywords
Insider threat, security architecture, multilayered model, attack and defense classification, attack surface, impact zone

The insider threat is very serious as shown by the recent report showing that 68% of respondents said that it is the biggest threat to their intellectual property and other sensitive data [1].

We define an insider as one who has legitimate access to an organization, its systems, information or other resources. The insider threat is a risk that an insider can misuse their access or knowledge to cause harm to the organization. We also mention the insider weakness where an insider performs unsafe actions or fails to apply adequate protection that may expose the organization to accidental damage or malicious attack. We do not count outsiders that appear to be insiders because they have gained internal access by defeating system defenses.

1.2 Architectural Security Model
We believe that the insider threat is a difficult problem that requires systematic analysis to mitigate. We have designed a three-layer architectural security model to investigate and evaluate organizational security. The use of layers is a common structuring method used to decompose and analyze systems. We are influenced by Neumann’s practical classification system for attacks with eight layers [2], [3], which are, in descending order: the external environment, user, application, middleware, networking, operating system, hardware and internal environment.

Our new organizational criteria such as the separate spatial scope of entities at each layer allow us to achieve a simplified three-layer model, which includes the social layer (people and organizations) and physical layer along with the middle logical layer containing computers and networks. This allows a holistic representation and analysis of complex systems such as organizations in their entirety including human and physical factors rather than as technical systems alone.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. CSIRW '09, April 13-15, Oak Ridge, Tennessee, USA Copyright © 2009 ACM 978-1-60558-518-5 ... $5.00
The physical layer is the bottom layer that contains tangible objects including buildings, equipment, paper documents, and the physical aspects of computers and associated devices. In addition, it contains electromagnetic radiation such as radio waves, electricity and magnetism that are used to transmit and store data. All higher layer entities including people and information have a physical existence as well as a higher layer representation that must be considered when analyzing organizational security.

Technical measures alone are incomplete and cannot stop attacks that occur partially or totally at other layers. The social level controls such as policies and procedures can usually be evaded by employees, as they cannot cover every eventuality and are often weakly enforced. In addition, physical attacks to steal, damage or misuse equipment, computers and documents are common. We conclude that organizational security must involve all layers to provide comprehensive defense.

1.3 An Attack Classification Scheme

We investigate the attack phases with an extension of Howard and Longstaff’s taxonomy [4], [5] for network security incidents that show the different classes of entity involved in attacks and their relationships. The categories are attacker, tool, vulnerability, action, target, unauthorized result and objectives. The attacker uses a tool to perform an action that exploits a vulnerability on a target causing an unauthorized result that meets its objectives. This conceptual model is incomplete as it does not consider most social and physical attacks because of its focus on computer attacks, and does not investigate the corresponding defensive measures.

Our classification scheme extends Howard’s taxonomy to include the social and physical aspects of systems, which allows comprehensive system modeling of complex systems such as organizations. All attacks are initiated by people at the social layer and are only effective if they meet a social goal such as obtaining money, power, reputation or pleasure. However, people cannot operate directly at the logical layer, so they use agents to act on their behalf such as user accounts to issue commands, run programs and access services.

In the active stage of an attack, the attacker or their agent employs a method to perform an action that executes a threat to exploit a vulnerability with an immediate effect on a target. This ultimately achieves the attacker’s social layer goal at the expense of the organization. We distinguish between the immediate effect at the lower layer on the confidentiality, integrity and availability of organizational resources and the ultimate effect on the organization at the social layer. In addition, we include additional concepts to describe and classify defensive mechanisms.

1.4 Attack Surface

A Microsoft employee called Michael Howard [6] invented the idea of the attack surface, which is the set of available channels to access and use computer systems. For example, it is the set of commands offered by an application or the available links on a Web page. We extend the idea of attack surface to all three layers, which allows a complete determination and analysis of exploitable access paths.

In addition, we extend the attack surface to include boundaries that the attacker can move through to gain local access to the target rather than operating at a distance over a channel. Higher layers entities have a conceptual location that can describe their position, proximity and relationship to other entities at the same level. For example, every file has a logical position within the directory structure, programs and processes execute in memory, whereas people have a conceptual social-level location that can be taken over by an identity thief.

A complete attack surface can provide systematic defense by constraining remote access and movement to the target at every layer. The insider is not limited by the external system boundaries such as building entrances and firewalls that protect the organization from external attacks. The insider may instead be constrained by internal attack surfaces that partition the system with defensive controls, which must be breached to gain unauthorized access to the target. Many insider attacks, however, use authorized access such as using their own accounts to access the target directly, so there is no interposed attack surface. Authorized access should be limited as far as possible so that the impact of malicious activities is limited as we discuss now.

1.5 Impact Zone

We also need to limit the scope and impact of successful insider attacks, as they are very difficult to stop entirely. This includes limiting undesirable effects on the target, the compromise of other parts of the system, and stopping the attacker from causing additional damage. The impact zone is the set of resources affected within the organization that are unavailable, modified or disclosed illegitimately. This is a dual notion to the attack surface that constrains the inward movement and access to a system and its resources.

The idea of the impact zone is already used informally in defense at all three layers. Employees are trained not to reveal sensitive information about the organization to third parties on the phone. The term data leak prevention (DLP) refers to controlling the disclosure of sensitive information by searching the content of documents and messages for confidential information before release. Physical assets such as goods and paper documents can be tagged with transmitters such as RFIDs to stop their theft. Finally, it applies to the rule of least privilege that limits employees’ privileges to the minimum required for their jobs thus limiting the impact of attacks that can be launched using authorized access.

The impact must have an ultimate effect at the social layer to be effective, as lower-level resources only have value to the extent that they support organizational goals. We can attempt to stop or limit the organizational effect by providing redundant resources such as data backups to provide enough resilience, so that systems can continue to provide service after an attack.
2 PROTECTING AGAINST THE INSIDER THREAT

2.1 System Hardening
The aim is to stop the ultimate social level effect on the organization, so we can consider protective measures at multiple stages before, during and after the attack, which equate to attack surface reduction, hardening the target and limiting the impact zone. The target is part of both the attack surface and impact zone, but is considered separately for clarity. The defense may also attempt to reduce the motivation of the attacker, which we discuss later.

Systems and resources should be difficult to damage, remove, alter or use in undesirable ways, which requires comprehensive protection at all layers. There should be a complete attack surface to limit the access paths and operations allowed at all layers to stop unauthorized access and constrain authorized use. In general, we may locate defenses on the external system boundary, within the system and on the target to provide defense-in-depth.

The protection of resources needs a clear understanding of their functionality and weaknesses along with the powers of possible users that may be abused. Potential targets should be hardened to hinder damage, removal, change and undesirable use. We have already mentioned partitioning systems internally to stop uncontrolled access, as protecting system boundaries does not stop insiders already within the system.

The potential impact may be limited to the target, within its neighborhood or system wide. Resiliency can be provided using redundant capacity or spare resources within the system, acquiring additional resources or provisioning services in other ways. System activities should be monitored to detect problems and determine their causes and effects. This may enable undesirable changes to be fixed rapidly to limit the impact and pinpoint weaknesses that can be mitigated to stop similar attacks in the future.

The impact may be limited to the lower physical and logical layers or reach the social layer. Additional protection measures are required to stop or reduce damage to lower layer resources from causing the ultimate effect of stopping the organization carrying out its normal business activities. For example, damage to a computer providing a key service may not cause a major business impact if there is a straightforward repair or ready replacement.

2.2 Targeting the Attacker
We now consider how to dissuade attacks from employees and other insiders. We need to understand their goals to determine their likely actions, which allow the selection of appropriate measures to meet credible attacks as not everything can be protected equally. Every position has some degree of access that can be abused, but some positions such as technical, financial or managerial roles have higher risk because of the greater means and opportunities for exploitation. The class of attack and its execution is strongly influenced by insiders’ role and capabilities, as they usually attack easy and familiar targets using their existing knowledge and abilities.

Attacks are often prompted by the need to resolve or relieve personal and work problems. Personal issues include divorce, drug abuse, financial problems and emotional disturbance. Organizational issues include job dissatisfaction, workplace disputes and disciplinary sanctions. The main objectives are financial including acquiring money and assets, and psychological including enjoyment and revenge.

The motives, means and opportunity are key questions that need to be answered to prove a suspect guilty of a crime. These are considered necessary predisposing attributes of attackers with the corollary that the defense should be successful if it can circumvent at least one factor. The opportunities include employees’ system privileges and knowledge of weaknesses that enable them to commit the attack and escape detection. The means is the set of methods, tools and techniques at the attacker’s disposal. The means and opportunities are largely determined by the defensive controls discussed already that limit insiders’ powers.

The organization can attempt to persuade their employees not to attack by addressing their underlying personal and financial issues by offering professional advice and treatment, and reducing their workload and responsibilities. The organization may also encourage more loyalty and respect by good work conditions and pay, team-building exercises, fair treatment and addressing grievances.

The organization should also attempt to deter attacks with strong defensive measures that make the cost/benefit equation less favorable by increasing the risk or reducing the benefits. We propose a ‘carrot and stick’ approach using both persuasion and deterrence.

‘Trust, but verify.’ (Translation of an old Russian proverb ‘Doveray, no proveryay’, often quoted by former US president Ronald Reagan during discussions with the Soviet Union about nuclear disarmament.)

The attacker often lacks foresight of the possible repercussions for themselves and the organization. Employees’ obligations should be made clear by the explicit allocation of duties and responsibilities, and well-publicized understandable policies with disciplinary action for breaches. It is important to deal with unacceptable behavior early as minor abuses may escalate if they become accepted as part of the corporate culture. Deterrence includes the probability of detection and being held accountable after the event with disciplinary action and legal measures.

2.3 Insider Attack Classification
We classify attacks by their actions of sabotage, fraud and theft, which follows the classification used in the second CERT guide to insider threats [7]. This is slightly different from the classification used in the current third guide, where the three classes are sabotage, financial gain and business advantage, which focus on the purpose of the attack [8]. We also mention attacks motivated by curiosity or enjoyment without clearly defined goals that may inadvertently cause problems. The attacks cause these undesirable impacts indirectly by breaching the fundamental security services of confidentiality, integrity and availability usually at lower layers. These problems may
also be caused by accidental failure or external attack, which are allowed by internal weaknesses.

The main characteristics of the three classes of attack are:

- Damage and sabotage – causes the loss of availability and integrity of the targeted resources with possible consequential effects on the ability of the organization to perform its normal business activities
- Fraud – causes financial losses to the organization or their customers by interfering with internal financial records or making unauthorized transactions
- Theft – includes logical resources such as information and physical resources such as equipment. The disclosure of sensitive business information often has a much higher impact than the loss of physical assets

2.4 Brief Discussion of Destructive Attacks

The goal of an employee in sabotage is the psychological satisfaction obtained from causing damage to the organization motivated by a personal grudge for some perceived wrong. The aim is to destroy or damage physical resources such as buildings, equipment and computers, and logical resources such as programs and data. These attacks on the integrity and availability of organizational resources have the ultimate effect of harming its business activities. Possible attacks can be plotted in a table showing the active elements of our classification as columns in a grid with a row for each level. The progression of possible attacks through the various stages are shown as paths through the grid from left to right starting with access to the target before moving on to illustrate the subsequent damaging effects. Our model also has some extra categories for the concepts of attacker, ultimate effect and ultimate target outside the active attack that only have meaning at the social layer. We then consider defensive barriers to provide a complete and consistent defense at all layers to prevent or constrain the impact of attacks as we demonstrated elsewhere [9], [10], which can be plotted in a corresponding defensive table.

Conclusions

We believe that the insider threat poses a significant and increasing problem for organizations. Systematic defense is required as no single method can protect against employees with legitimate access to organizational resources. We proposed an architectural three-layer security model to analyze the insider threat systematically. We extended Howard’s classification model and introduced the attack surface and impact zone to investigate the different stages of insider attack. This enables a systematic analysis of defensive protection measures within the classes of hardening the system by limiting access, constraining the use of the target and limiting the impact of successful attacks. We also considered how to reduce the insider’s motivation to attack by persuasion or deterrence.

Our model has been used to demonstrate destructive attacks by disgruntled employees [10]. Attacks by terrorists should be considered separately as they launch more destructive attacks to cause widespread damage to other organizations and society in general. Similar tables can be used to analyze the other main types of insider threat from fraud and theft. The corresponding defense tables help to provide comprehensive protection against insiders that can attack at all three layers. In addition, it aids the provision of multiple supporting controls offering defense-in-depth, including recovery methods that limit the impact of attacks that are difficult to avoid.

Our security model appears to have widespread application in other areas such as critical infrastructure and financial systems, as it allows the analysis of systems in their entirety including human and physical factors, not just as technical systems. The model has been used to investigate critical infrastructure with its widespread scope and weaknesses at all layers [11]. In addition, it has application to complex financial systems such as banking networks where weak procedural and physical controls are usually exploited rather than the technical controls such as cryptography [12].

REFERENCES