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

1 SYSTEM MODELING

1.1 What is the Insider Threat?

Insiders can cause great damage to organizations because of their privileged access, knowledge of weaknesses and the location of valuable targets that can be misused for their own purposes. Internal attacks are more difficult to discover and diagnose, because the controls can be evaded by employees.

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.

The social or organizational layer contains the abstract representation of organizations by their attributes including their goals, policies and procedures. It also includes people and their characteristics such as their goals, knowledge and beliefs. The logical layer is the intermediate layer that contains intangible computational entities including computers, networks, software and data. The logical layer is incorrectly the focus of most attention in security, because all layers need protection to provide comprehensive security.

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 '*Doveryay, 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

[1] McAfee (2009). Unsecured economies: protecting vital information, at http://resources.mcafee.com/content/NAUnsecuredEconomiesReport.

[2] Neumann PG and Parker D (1989). "A Summary of Computer Misuse Techniques". Proceedings of the 12th National Computer Security Conference.

[3] Neumann PG (2000). Practical Architectures for Survivable Systems and Networks. SRI International, at www.csl.sri.com/neumann/survivability.pdf.

[4] Howard JD (1997). An analysis of security incidents on the Internet 1989-1995. Carnegie Mellon University, at www.cert.org/archive/pdf/JHThesis.pdf.

[5] Howard JD and Longstaff TA (1998). A common language for computer security incidents. Sandia National Laboratories, at www.sandia.gov.

[6] Howard M (2004). "Attack surface: mitigate security risks by minimizing the code you expose to untrusted users". MSDN magazine (November 2004), at http://msdn.microsoft.com/en-us/magazine/cc163882.aspx.

[7] D Cappelli, A Moore, TJ Shimeall and R Trzeciak (2006). Common sense guide to prevention and detection of insider threats (version 2.1). Carnegie Mellon CyLab, at www.cylab.cmu.edu/pdfs/CommonSenseInsiderThreatsV2.1-1-070118-1.pdf.

[8] Cappelli D, Moore A, Shimeall TJ and Trzeciak R (2009). Common sense guide to prevention and detection of insider threats (version 3.1). CERT/Software Engineering Institute, at www.cert.org/archive/pdf/CSG-V3.pdf.

[9] Blackwell C (2009). The insider threat: Combating the enemy within. IT Governance at www.itgovernance.co.uk or www.27001.com.

[10] Blackwell C (2009). "A Security Architecture to Model Destructive Insider Attacks". 8th European conference on information warfare, Academic Publishing Ltd.

[11] Blackwell C (2008). "A Multi-layered Security Architecture for Modelling Complex Systems". 4th Cybersecurity Information Intelligence Research Workshop, ACM Press.

[12] Anderson R (1993). "Why cryptosystems fail". 1st ACM conference on computer and communications security, ACM Press.

Royal Holloway
University of London

Combating the Insider Threat with a Systematic Security Architecture

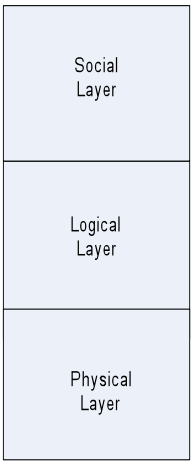
Clive Blackwell
Information Security Group
Royal Holloway, University of London
C.Blackwell@rhul.ac.uk

Royal Holloway
University of London

Neumann's 8-layer classification

- Neumann and Parker organised systems into eight layers for security analysis
  - External environment, user, application, middleware, networking, operating system, hardware and internal environment
- Neumann's model needs simplification to reason about systems
  - Want an executable model with a new process calculus called bigraphs that has the concepts of location and communication
- Our architectural model adds sub-layers and horizontal scope
  - Reduces the number of layers to three – Social, logical and physical
  - Some of Neumann's layers such as the internal and external environment are at the same layer with differing horizontal scope
  - Most of the others are considered as sub-layers of our logical layer

The Layered Security Model



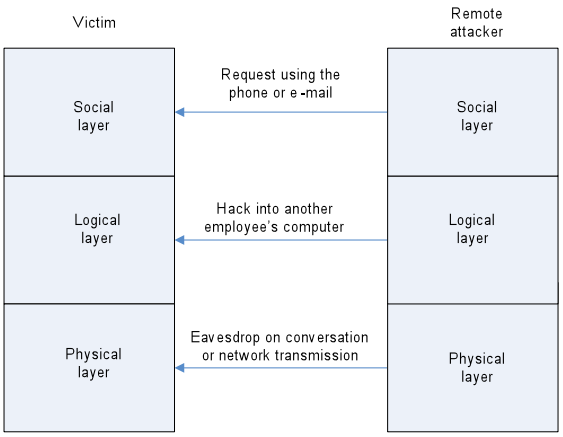
- We have achieved a simplified three-layer model
  - Introduce the concept of sub-layer to Neumann's model
- Social layer at the top includes people and organisations along with their goals
- Logical layer in the middle contains computers, networks and software
- Physical layer at the bottom represents the physical existence that all entities have in the real world
- Every layer has a different concept of location
  - Represents the separate conceptual scope and connectivity of systems and objects at each layer
- Allows a holistic representation and analysis of systems in their entirety including human and physical factors
  - Rather than as technical systems alone

Attack surface

- Michael Howard invented the idea of attack surface
- Is the set of accessible input channels together with the possible impact from access
- We apply it to all layers for completeness
- Apply it to locations and well as communication channels
- Insider starts at an internal starting location
  - Within the external system attack surface
  - May be controlled by internal attack surfaces

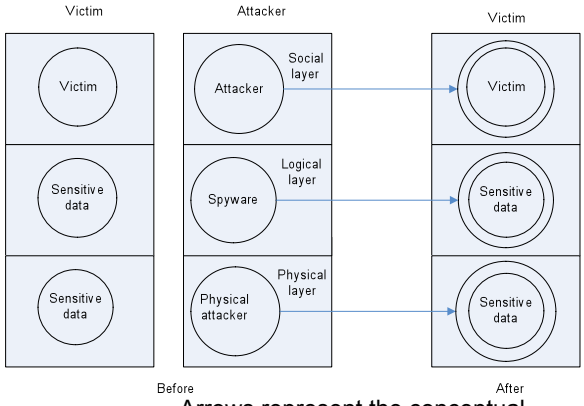
M Howard (2004), "Attack surface: mitigate security risks by minimizing the code you expose to untrusted users", MSDN magazine (November 2004), at http://msdn.microsoft.com/en-us/magazine/cc163882.aspx

Remote attacks using channels to acquire data



- A social engineering attack occurs by email or over the phone to acquire confidential information
- A logical attack occurs by hacking into a computer to search for valuable information
- Physical attacks can occur by eavesdropping on private conversations or on network communication

Remote attacks using movement to acquire sensitive data



Arrows represent the conceptual movement of the thief or its agents to control the victim or their data.

- Can impersonate other people and misuse their privileges to obtain access to sensitive information, which can be considered as occupying or controlling the victim's personal space at the social layer
- Spyware can be installed on computers to search for valuable information, which occupies a logical location within the spyware when it has been compromised
- Can steal data physically from computers, memory sticks or paper documents

Escape surface

- The escape surface is the set of accessible output channels together with their possible impact from misuse
  - Dual to the attack surface
- Applied to all layers, and to movement between locations as well as communication channels, as with the attack surface
- Includes the misuse of system resources in situ using channels, and the movement of resources through security boundaries
  - Attacker usually needs to exit system as well
- Successful attacks affect the target
  - Need to stop passage through the external system escape surface
  - Need internal escapes surfaces to limit impact within system
  - Escape surfaces can be at lower layers or limit the ultimate impact at the social level
- Only helps attacks that need outgoing access
  - Some attacks that interfere with the integrity or availability of the target do not need outgoing access

Howard and Longstaff's security classification

John Howard invented a classification system for network security incidents

Shows the different types of entity involved in attacks and their relationships

Includes the categories of attacker, tool, vulnerability, action, target, unauthorised result and objectives

Attacker uses a tool to exploit a vulnerability performing an action on a target resulting in an unauthorised result that meets its objectives

A useful conceptual model that we extend

- Include a comprehensive set of categories
- Include compromise at all layers
- Include defensive classification very well

Howard JD and Longstaff TA, "A Common Language for Computer Security Incidents", Sandia National Laboratories (1998), at www.sandia.gov.

Extended attack taxonomy

- Includes additional categories and elaborates others
  - Separates *Attacker* (social layer) and their *Agent* (lower layer proxy)
  - *Method* (more general classification encapsulating the tool category)
  - Elaborates the specific *Vulnerability* exploited rather than just the stage of the system cycle when it was introduced
  - Separates *Immediate effect* (lower layer) and *Social goal* (ultimate effect)
  - Immediate effect on confidentiality, integrity and availability
  - Social goal of money, pleasure, reputation, power
  - *Threat*, *Action* and *Target* are the same in both models

The *agent* uses a *method* that results in an *action* of executing a *threat* that exploits a *vulnerability* with an *immediate effect* against a *target.*

This ultimately achieves a *social level goal* of the *attacker* against the *defender.*

Insider threat definition

- Insider – A *person* who has the *legitimate* right to use an organisation's infrastructure, systems, controls, information, name or other resources
- Insider threat – A risk that an insider can misuse their rights to cause *deliberate* harm to the organisation
- Insider attack – The execution of a latent insider threat
- Insider weakness – An action or failing of an insider that may expose the organisation to malicious attack or accidental damage
- Do not include *external* entities that illegitimately gain internal access and *masquerade* as insiders
- Our model can analyse these last two possibilities, but are not the focus of the presentation

Royal Holloway University of London

Main insider threats

- Damage and sabotage
  - Affects system and resource integrity and availability
  - Purpose is usually to damage the organisation because of a grudge
- Fraud
  - Affects integrity and availability of monetary resources and other intangibles such as identity
  - Targets the organisation, its customers and other employees
  - Use confidential information to breach security controls
- Information and physical resource theft
  - Usually for financial motives or business advantage
  - Information can be sold to third parties
  - Used for personal advancement as when moving company
  - Includes product information, business plans and customer lists

D Cappelli et al, "Common sense guide to prevention and detection of insider threats, version 2.1", CERT (2006).

Focuses on actions, whereas new version 3 (2009) focuses on effects

Sabotage, financial gain and business advantage

Royal Holloway University of London

Destructive attack analysis

- Investigate the main characteristics of attacks in a table
  - In practice, we investigate each threat in a separate table
- Attacks follow a logical progression through stages from left to right
- All attacks are ultimately caused by people and have a social impact
  - Ultimate goal is to inflict damage to the organisational goals
  - Attacker attributes such as motives and abilities should be considered
- Attack execution usually employs lower layer methods to interfere with lower layer targets
  - Immediate effect is to destroy or damage organisational resources
  - Active attack steps are in the middle of the attack table
- Some attacks act in stages by gaining access and then misusing it
  - Annotate the table with a separate path for each intermediate stage
- Attacks may move between layers so that cells in different rows may be part of the same attack
- Attacks passing through vertical or horizontal boundaries are modelled by attack surfaces shown in the corresponding defence table

Destructive attacks

Motivation	Method	Action	Target	Immediate effect	Ultimate effect
Revenge, psychological satisf action	*Social engineering*, threats ♠	*Persuade or trick to act incorrectly in person*	*Security guards, system administrators*, colleagues ♦	*Unauthorized physical or logical access*, fear	*Failure of business activities, satisf ying contracts*
	Misuse authority, gain illegitimate access (exploit weaknesses, compromised accounts), install malware	*Illegitimate requests, damaging commands*, destroy or alter data ♣	*Control systems*, operating systems, applications, accounts, fi les, business processes and information (databases, documents)	*Lost production*, unusable computers or applications, loss of business services or documents	
	Exploit allowed access, illegitimate access to equipment and resources	*Physical damage* ♥ and destruction, theft	*Equipment*, computers, networks, data (documents, *backups*, disks)	*Damaged systems and outages, unavailable resources, lost production*	

Hybrid attacks

- Can model single layer attacks simply with our model
- Hybrid attacks demonstrate the utility of our model where the access, attack and effect may be at different layers
- Allows systematic investigation of different methods of achieving the same goal by consideration of all paths to the target
- Paths through the grid from left to right can make vertical layer crossings
  - Forward within a single stage (♣)
  - Back to the start when the results of one stage enable a subsequent stage (♦)
- Access may occur at a different layer from the subsequent attack
  - Illegitimate access to the target by persuasion can lead to interfering with a computer network or physical equipment (♥)
  - Social engineering attacks may be caused by logical actions (♠)
- Attack may occur at a different layer from the subsequent effect
  - Access to a control computer may lead to damaging commands with physical effects of closing down or damaging equipment (♣)

Cross functional attacks

- Cross functional attacks are also represented in our model by a third dimension in our tabular representation
  - Each separate domain can have its own plane parallel to the 2-D grid
- Attacks can be shown as a path through the grid from left to right making horizontal movements in the third dimension
  - Crossing different types of physical system, computer network or organisational domains
- Access, attack and effect may cross different system types
- Access may occur on a different system type from the subsequent attack
  - Access to telecoms equipment can affect control of the power grid and vice versa
- Attack may occur on a different system type from the effect
  - Damage to a computer may affect organisational workflows if business documents are lost

Defence

- An analogous defensive grid can show possible defences
- Allows analysis of the interaction between attack and defence
  - Shows where defensive mechanisms can be deployed, the components protected, attack steps targeted, and effects mitigated
- The defender should ensure the completeness of measures by providing comprehensive and consistent protection at all layers
  - Should be no uncontrolled paths to the target at any layer
  - Defence-in-depth required to cope with failure of defensive mechanisms
- Determine defences at different stages to limit access, harden the target or reduce impact corresponding to columns in the attack table
- Limiting access is ideal, but difficult with insiders
  - Attack surfaces should provide complete barriers with no exploitable gaps
- Hardening the target limits functionality and interferes with goals
- Constraining the impact of successful attacks can limit the immediate effect or the ultimate goal
  - Escape surface should be limited to aid recovery from successful attacks
- Also reduce adversarial motivation by persuasion and deterrence

Defensive table

Persuasion	Deterrence	Limit access	Harden target	Limit immediate effect	Fix ultimate effect
Good work conditions, address personal issues, clear policies	Increase prob of detection, zero tolerance, clear responsibilities, disciplinary procedures, prosecute, sue	Vigilant observation, identify odd behavior, limit activities (use roles, limited privileges)	Security awareness and training, strict policy enforcement, double-check critical systems	Incident response, use spares, contingency plans, acquire new resources, repair critical problems, stop attacker's access	Alternative services, disaster recovery, contract, fi x weaknesses, insurance
		Roles, dual control, strong authentication, password policies, limited accounts, prevent damaging commands, partition systems, intrusion prevention, network access control	Hardwired controls, secure confi guration (checklists), limited interfaces, read-only fi les, integrity checks, antivirus, anomaly detection, network scans, apply patches	Intrusion detection, audit logs, reboot systems, fi le versioning, data leak prevention, disable accounts, change passwords, restore backups, rollback database	
		Alarms, CCTV, key management, accompany, sign in/out, movement detection, open plan offi ces, badges, secure areas	Toughen or shield equipment, attach to fi xed objects, connect transmitters, tag, put documents/valuables in safes, clean desk policy, locked cabinets/desks	Resilience (run in degraded mode, use spares, secure offsite backups) shut down and repair systems, fi nd and stop attacker	

Limiting access

- The limit access column corresponds to both action and method in the attack table
- Access controls can be applied at multiple locations and levels
  - Consider access to the system and target separately (next slide)
  - Constrained attack surfaces limits user domain providing least privilege
- Physical access to buildings, secure areas, equipment and computers controlled using keys, CCTV and security guards
- Isolate networks physically and logically
  - Limited physical channels
  - Network access control (NAC) ensures access only to hosts that are properly secured with latest updates and AV protection
- Host controls should include strong authentication, limited privilege accounts and role-based access controls
- Encrypt sensitive data at rest and in transmission
- Use security awareness training to detect access attempts and unusual behaviour

Royal Holloway University of London

Harden target

- Target has aspects of the attack surface and impact zone
  - Hardening limits access to and undesirable effects on the target
- Limit employee discretion by policies to constrain behaviour
  - Stop unnecessary storage or transmission of sensitive information
- Use checklists eg from NIST to remove unneeded functions
  - Remove default system accounts, change known passwords and insecure security parameters when the system is initially configured
  - Install latest updates and test them adequately
  - Stop execution of untrusted content, which may allow malware to run, such as email attachments, JavaScript and ActiveX controls
- Control change using virtualisation, System Restore to undo corruption, and making files such as executables read only
- Limit physical attacks by constraining system functionality
  - Smart agents controlling the power grid can be arbitrarily modified, whereas hardwired controllers are fixed

Royal Holloway University of London

Limiting impact

- The impact zone of successful attacks should be constrained by limited escape surfaces
- Escape surfaces should limit the scope of the attack, and hinder exit of the attacker and resources
  - Sandbox in Java
  - Outgoing controls on firewall
  - Data leak prevention (DLP)
  - Physical checks on exit from buildings and secure areas
- May stop the loss of confidentiality and attacks on other systems that need to traverse the escape surface
- Does not stop attacks on the integrity and availability of the target, except for specific target hardening controls
- Attacker may not need to escape if accepts being caught or uses disposable agents such as malware

Conclusions

- We demonstrated a three-layer model for modelling security architecture
  - Simplifying and extending Neumann's eight-layer model
- Extended the attack surface and introduced the dual concept of escape surface
- Extended Howard and Longstaff's attack taxonomy and introduced a corresponding defensive classification
- Applied our model to insider attacks
  - Showed how to reason about destructive attacks
  - Indicated how our defensive classification could aid systematic defence
- We plan to elaborate the model so it can be used by organisations to plan systematic defence against all threats
- Develop a security ontology to support automation of attack discovery and classification
  - Formalise the meaning of attack components and their interrelationships

References

Blackwell C, "A Multi-layered Security Architecture for Modelling Complex Systems", CSIIRW (2008), ACM Press.

Blackwell C, "A Multi-layered Security Architecture for Modelling Critical Infrastructure", 7th ECIW (2008), Academic Conferences Ltd, Reading, UK.

C Blackwell, "The insider threat: Combating the enemy within ", IT Governance (April 2009) available at www.itgovernance.co.uk or www.27001.com.

C Blackwell, "A Security Architecture to Model Destructive Insider Attacks", 8th European conference on information warfare, Academic Publishing Ltd (2009).

Neumann, PG, "Practical Architectures for Survivable Systems and Networks", (2000), at www.csl.sri.com/neumann.

Howard JD and Longstaff TA, "A Common Language for Computer Security Incidents", Sandia National Laboratories (1998), at www.sandia.gov.

M Howard, "Attack surface: mitigate security risks by minimizing the code you expose to untrusted users", MSDN magazine (November 2004), at http://msdn.microsoft.com/en-us/magazine/cc163882.aspx.

D Cappelli, A Moore, TJ Shimeall and R Trzeciak, "Common sense guide to prevention and detection of insider threats", version 3 (Jan 2009), Carnegie Mellon University CyLab available at www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf.