

# Combating the Insider Threat: What System Administrators need to know

Clive Blackwell

Information Security Group  
Royal Holloway, University of London  
✉: [C.Blackwell@rhul.ac.uk](mailto:C.Blackwell@rhul.ac.uk)

Advanced Computer Services  
Staines, Middlesex  
[Clive@advance.plus.com](mailto:Clive@advance.plus.com)

# Presentation outline

Layered security architecture components

Layers and attack step classification

Modelling insider threats

Destruction, fraud and theft

Sabotage on the electricity grid

Defensive controls – prevention, detection  
and reaction

Interactive exercises

# Modelling complex systems

## Problems with complex systems

- Sophisticated functionality and highly interconnected

- Difficult to manage or even understand

- Apply piecemeal defences to address limited technical problems

## Most security models are incomplete

- Focus on the technical aspects of systems

- Results in limited technical solutions

We require holistic system modelling to structure protection with multiple safeguards at many layers and locations to provide defence-in-depth.

# System layering

Common structuring method used in system design

Systems can be decomposed so that each layer can be analysed and implemented separately

Notable example is the OSI network model with seven layers to model communication

Layering aids comprehensive security modelling

Can consider security breaches separately at every layer

Including physical and organisational aspects

Allows the selection of a holistic set of controls based on the costs and benefits for the complete system

# Neumann's 8-layer classification

Layers are a common structuring method used in system design

Systems can be decomposed into layer that can be analysed and implemented separately

Notable example is the OSI network model with seven layers to model communication

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

Especially to construct an executable model

Our architectural model adds sub-layers and horizontal scope

Reduces the number of layers to three

Social, logical and physical

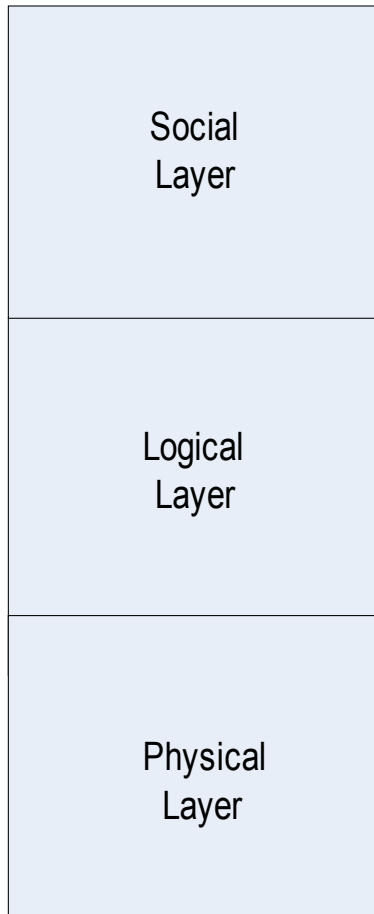
Some of Neumann's layers such as the internal and external environment are at the same layer, but with differing horizontal scope

Most of the others are considered as sub-layers of our logical layer

# Neumann's 8 layer model

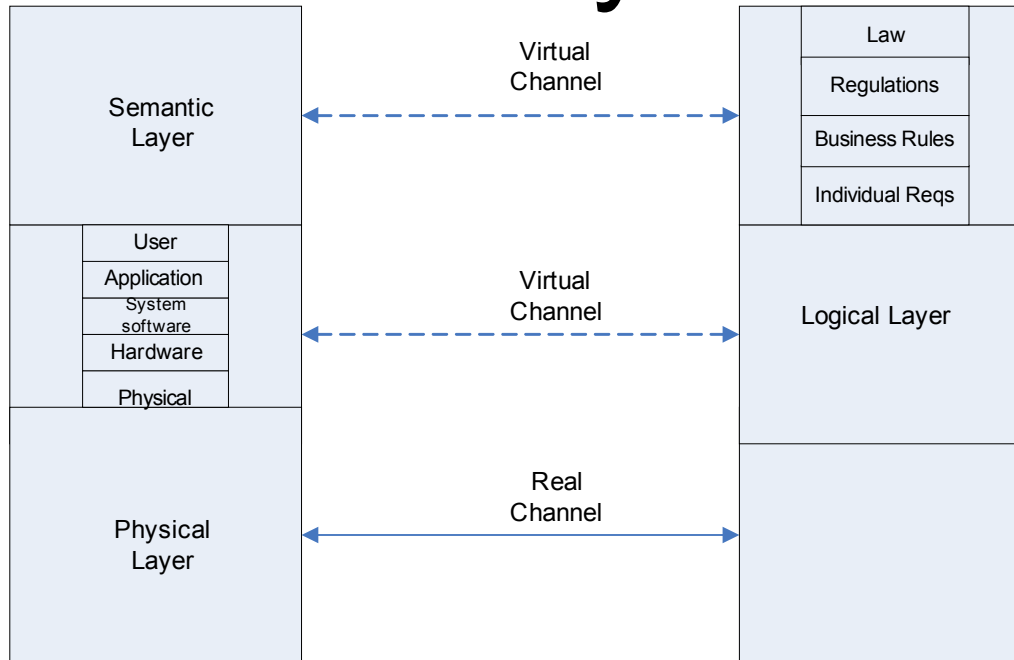
Layer	Compromise from Outside	Compromise from Within	Compromise from Below
Outside environment	NONE		
User			
Application			
Middleware			
Network			
Operating system			
Hardware			
Inside environment			NONE

# 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 entities 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

# Sub-layers



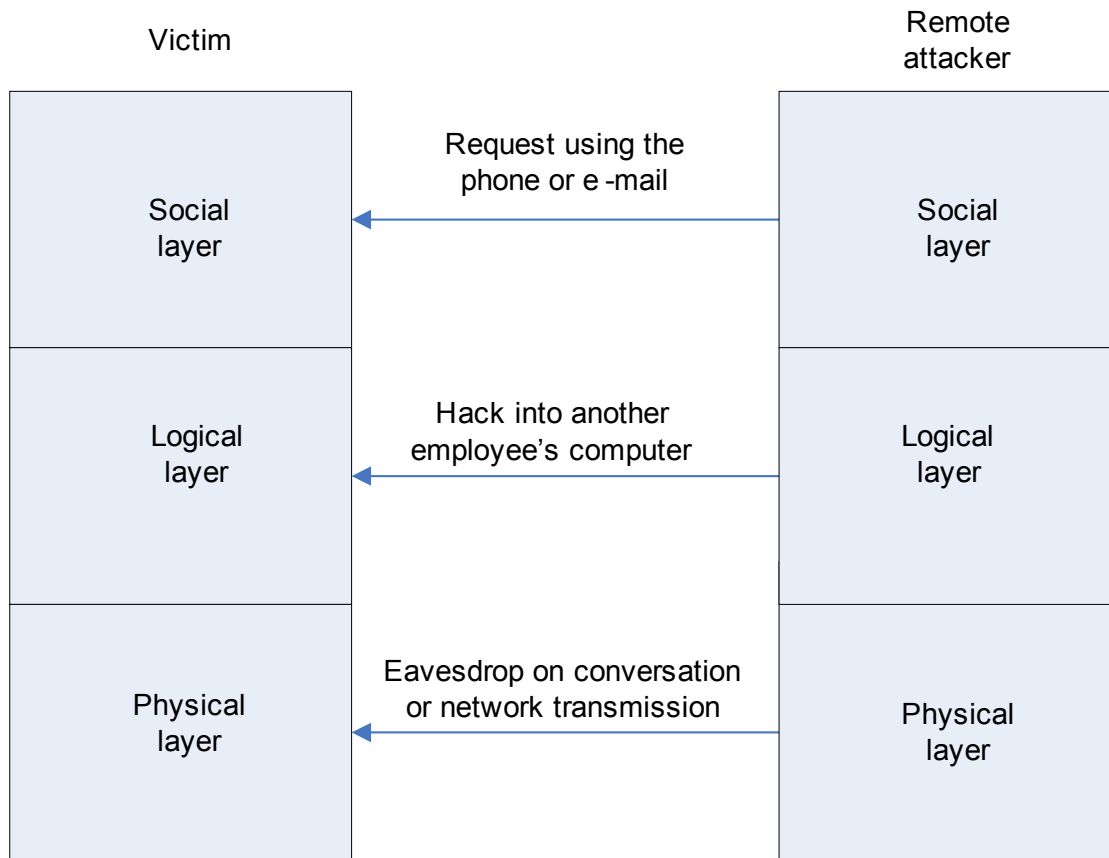
- Each layer can have sub-layers for detailed analysis
  - Can represent Neumann's eight layer model with the user, application, system software (OS) and hardware as sub-layers of our logical layer
  - The upper user and lower physical sub-layers interface to the social and physical layers of our model respectively
  - The social layer and physical layers can be divided into sub-layers as well
  - Communication is down through the layers, but is actually horizontal

# Attack surface

- Michael Howard invented the idea of attack surface
- Access to the available communication channels together with the possible impact
- We apply it to locations and well as communication channels
- We apply it to all layers for completeness
- Insider starts at an internal starting location
  - Within the external system attack surface, but may be controlled by internal attack surface

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

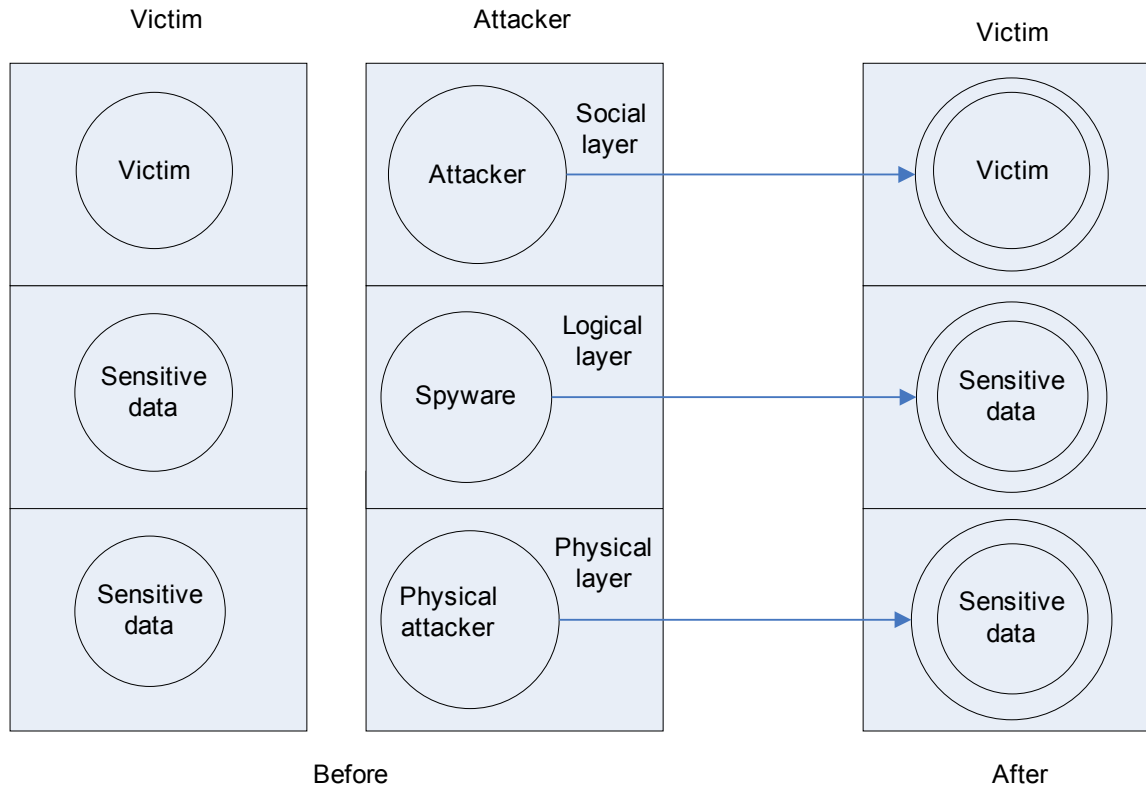


A social engineering attack occurs by email or over the phone to acquire confidential information

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



Can steal data physically from computers, memory sticks or paper documents

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 also 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

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

# Modelling protection requirements

- Neumann considers 3 conceptual locations for compromise at each layer
  - From below, internal, and external compromise
- We consider above and outside as separate classes
  - Conceptually different and are subject to different attacks and defences
  - Protection from external entities requires vertical boundaries
  - Protection from higher entities requires horizontal boundaries between the layers
  - Insiders should be constrained by limiting their powers and partitioning the system with additional internal boundaries
  - The underlying components that control the system must be protected and trustworthy
- All entities should be outsiders relative to some controls that mediate their use of the system

# SEARCHLIGHT model

Location Layer	Compromise from Above	Compromise from Outside	Compromise from Within	Compromise from Below
Social	NONE			
Logical				
Physical				NONE

Consider the location of the source and target

# SEARCHLIGHT model

Location Layer	Compromise from Above	Compromise from Outside	Compromise from Within	Compromise from Below
Social	NONE	Social engineering	Conspiracy	Eavesdrop
Logical	Unauthorised use	Hacking	Install malware	Keylogger
Physical	Command equipment	Physical access	Destroy equipment	NONE

# Howard'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, but incomplete, conceptual model

- Does not contain a comprehensive set of categories

- Focuses on computer attacks, not compromise at other layers

- Focuses on attacks and so does not consider defensive aspects very well

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

# Extended security taxonomy

- Extends Howard's classification scheme
- 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 goal* of the *attacker* against the *defender*.

# Extended scope of taxonomy

- Extend classification of attacks to the physical and social layers
  - Allows more complete modelling of systems
- All attacks are initiated at the social layer
  - Malware arguably has a life of its own even though it is originally written and distributed by a person
- Attacks are only effective if they meet a social goal
  - Money, power, reputation or pleasure
- Attacks usually act at a lower layer
  - Social engineering attacks occur directly at the social layer
    - Normally use lower layer services such as the phone or email
  - Most attacks are carried out using lower-layer logical proxies such as programs and accounts
    - Issue commands, run programs, execute processes and access services
  - Physical attacks include destruction of objects, theft of hardware and documents, and eavesdropping on communications

# 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 weakness – An action or failing of an insider that may expose the organisation to malicious attack or accidental damage
- Insider attack – The execution of a latent insider threat
- Masquerade – Do not include *external* entities that illegitimately gain internal access and appear as insiders
- Our model can analyse these possibilities, but are not the focus of the presentation

# Types of insider

- Three categories of insider – trusted insider, regular insider and partial insider
- A trusted insider is someone with special privileges within the entire organisation or within some particular domain
  - Can usually do immense damage to the organisation
  - Includes management, financial staff and system administrators that need privileged access to perform their work
  - Often use their privileged access to subvert or avoid the controls
- A regular insider, (henceforth insider), is an employee of the organisation or someone with similar access to an employee
- A partial insider is someone with limited access to the organisation and its resources
  - Includes security guards, maintenance and cleaning staff and other building occupants at the physical layer
  - Outsourcers, collaborating partners, guests and contractors have limited access at all layers

# Location and scope

- The insider has a location and scope within the organisation at all layers
- Powers of insiders can be determined by the spatial and temporal scope of their access at all layers
- There may be internal and adjoining boundaries as well as external boundaries to control the insider
  - Internal boundaries control access to more privileged resources
  - Adjoining boundaries control access to different functionality
- The insider is in the same domain as the target if there no security boundary between them
- The insider may be able to can exploit weak, misplaced or incomplete controls to move to the target domain
  - Possibly using an agent such as malware

# 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 money and other targeted resources
  - Targets the organisation, customers and other employees
  - May access personal data and interfere with organisational controls
  - Use confidential information to breach authentication and authorisation controls
- Personal privacy and organisational confidentiality breaches
  - Usually have financial motives, but may have ideological motivation
  - Information can be sold to third parties
  - Information can be used for personal advancement as when moving company
  - Includes product information, business plans and customer lists that are valuable to competitors

# Sabotage

- Most sabotage is carried out by employees with a personal grudge against the organisation
- Usually by technical staff with privileged access
- Many have been terminated but retain partial insider access because not all access has been removed
- Some degree of sophistication involved
  - Often use remote access, malware such as logic bombs, backdoors or other users' or system accounts
- Investigate sabotage against critical infrastructure acting indirectly to affect external systems and people

# The electricity grid

‘Electric power systems constitute the fundamental infrastructure of modern society. A successful terrorist attempt to disrupt electricity supplies could have devastating effects on national security, the economy, and the lives of every citizen. Yet power systems have widely dispersed assets that can never be absolutely defended against a determined attack’

Massoud Amin

Consequences of a successful attack are potentially devastating as nearly all aspects of modern life are dependent on power

Investigate how terrorists can breach the security controls to access critical assets in violation of organisational requirements and social need

System requirements are met by lower layer physical and logical components  
Ultimately by the power lines and substations that are managed with a supervisory control and data acquisition (SCADA) network from a distance

The grid has a large horizontal extent with multiple social, logical and physical weaknesses

We are going to analyse the insider threats posed by terrorists to the electricity grid

# Electricity grid characteristics

Very complex systems that cannot be analysed manually

- Impractical to protect against or even discover all possible threats

- Large and unmitigated number of weaknesses

Large numbers of people and physical and computational components

- Numerous people and other subjects such as software with various powers and rights

- Extended horizontal scope allowing pervasive access at all layers

- Subject to social, logical and physical attacks on processing, resources, communication channels and control components

Need to continue operation and succeed in mission in face of an attack

- Failures will occur by accident or malice

- Need to limit the impact and provide recovery measures

- Continue to provide core services and avoid catastrophic failure

We need holistic system modelling enabling us to structure protection with multiple safeguards at many layers and locations to provide defence-in-depth.

# Terrorist motivation

- Terrorist goal is to cause fear and economic damage in pursuance of ideological motives
- Act indirectly to harm the organisation by affecting system and resource integrity and availability so that it cannot provide services
- Aspects of the Critical National Infrastructure (CNI) such as the electricity grid are especially vulnerable
- Immediate purpose is to destroy or damage physical or logical resources so that the organisation cannot provide service
  - Physical – people, buildings, machinery, control systems, computers
  - Logical – control systems, computers, programs and data
- The effects must link back to the terrorists' goal, which are on the people, economy and government
- Effects on organisation are a method of attacking the ultimate target
- Ultimate impact of an attack on the grid include business stoppages, price increases, fear and social disorder

# Insider terrorist threats

- We consider possible insider attacks at all layers
  - Against the physical power system and buildings, the SCADA control network and people
- Focus is on system integrity and availability
  - Confidentiality helps to provide these services
- Attacker may not have authorised access to the target
  - Could be classed as a partial or regular insider, but may easily gain elevated physical or logical access
  - Internal controls rarely stop employees from gaining additional privileges if they are determined enough
  - Easier to obtain partial insider status as they undergo fewer checks
    - Need proper checks and controls on business partners, outsourcers, temps, maintenance people, cleaners, security guards, other employees and organisations in the same building etc etc

# Physical attacks

- The access to the system and action on the target and the effects may be purely physical
- Includes attacks on physical structures such as buildings, control centre and components
- Can often attack resources in insecure locations with same effects as highly protected critical assets
  - Many essential components such as water or communication may be easier to compromise with similar effects
- Many physical attacks contain some higher-level aspect
  - Gain physical access to unprotected network components
  - Use the control network to affect the power transmission network

# Higher-layer attacks

- Logical attacks on the power transmission network, SCADA control network, people and other essential components
  - Logical attacks by insiders directly issuing damaging commands
  - Future use of smart agents in the SCADA network may allow installation of malware to control the grid
- Remote logical attacks
  - Use of the Internet and unprotected physical communication media for remote administration of power lines and electricity substations
  - Internal attacks from partial insiders on other organisational networks or can control the SCADA network remotely or install malware
- Social engineering to convince operators to act incorrectly
  - Controllers may be tricked by spoofed email or telephone calls on private network as they are implicitly authenticated by the medium
  - Threats and bribes to interfere with system

# Terrorist 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
  - Can convert to an attack tree
  - Can consider attacks as templates that are filled in with allowed values to constrain the paths between attacker and target
- Attack on grid is an attack vector used to affect terrorists' enemies
- Attacker attributes such as motives and abilities should be considered
  - Detection is the main weapon used against insiders which may also deter
  - Irrelevant if attacker does not mind being caught or is not going to be around to suffer the consequences

# Terrorist attacks on the electricity grid

Taxonomic Class	Attacker Motivation	Method	Action	Target	Immediate Effect	Semantic goal	Ultimate target
Layer							
<b>Social</b>	Political change, power	Trickery, social engineering, impersonation, threats, bribes	Persuade insiders to act incorrectly or insecurely	Operators, security guards	Loss of trust in system, unauthorised access	Fear, loss of money, social disorder	People, organisations, economy, government
<b>Logical</b>		Steal or fake credentials, bypass incomplete or non-existent controls, use hacking tools, scripts and commands, or install malware	Change control data or software, override safety controls, overload control system	Control System	System instability, loss of integrity, unavailability of controls		
<b>Physical</b>		Violence, forced entry, bomb	Close system down, physical damage, overload	Control room	Power outage		

# Attack modelling

- The execution of the attack nearly always uses a lower layer method to access and affect a lower layer target
  - Direct intention is to destroy or damage part of the grid
- However, all attacks are ultimately caused by people and must have a social impact on the target
  - Ultimate terrorist goal is to inflict overwhelming damage on the government, economy, organisations and people of their enemies
  - Effects include fear and social disorder, energy shortages, economic consequences, and government instability
- Some attacks act in stages by first gaining internal access and then using these elevated privileges
  - May 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
  - Needs to be a connected path through the table for a successful attack passing through any attack surfaces

# Gaining access

- Attack often needs to pass through several vertical or horizontal boundaries modelled by various attack surfaces
- The first step in an attack is usually to gain access to the system and then the target
  - Insiders may already have sufficient access, but partial insiders may need to acquire access first
- Insiders can pass through or bypass external boundaries at all layers without checks or inadequate checks
- Very hard to stop attacks from regular and privileged insiders
  - May limit the impact from early detection and recovery
- Terrorists may use extreme force and be happy to die to achieve their objectives
  - Plausible defences depend on the attacker, their motivation and goals
  - Detective controls may be irrelevant

# Hybrid attacks

- Hybrid attacks demonstrate the utility of our model where the access, attack and effect are at different layers
  - Can be shown as a path through the grid from left to right making vertical layer crossings
  - Allows systematic investigation of different methods of achieving the same goal by consideration of all paths to the target
- Access may occur at a different layer from the subsequent attack
  - Access to the control centre by persuasion (social) or force (physical) can lead to commanding the control network (logical)
- Attack may occur at a different layer from the subsequent effect
  - Controlling the SCADA network may lead to the physical effect of closing down part of the grid possibly causing power outages

# Defence

- An analogous defensive grid can show the complete set of defensive mechanisms
  - Each attack along with the corresponding defences can be shown in a separate table for a comprehensive analysis
  - Allows analysis of the interaction between attack and defence
- Defensive table shows where the set of defensive mechanisms can be deployed, the components protected, the attack steps targeted, and the actions mitigated
- The defender should ensure the consistency of measures at all layers by providing complete and consistent attack surfaces
  - Attack surfaces should provide a comprehensive vertical barrier
  - Should be no path from the attacker to the target at any layer
- Need to consider holistic protection at all layers as logical controls are incomplete
  - Attacks can happen from multiple locations at any layer
  - Defence-in-depth required by providing multiple controls at different stages to overcome the failure defensive mechanism failure

# Defensive classification

- The defensive classification is dual to the attack taxonomy
- Includes the *Defender* and *Control* that controls the system at different locations or layers on defender's behalf, *Vulnerability* (dual to threat), *Target* (in both lists), *Countermeasures* to avoid or limit system access and misuse, and *Aim* to mitigate the *Immediate effect* or ultimate impact on the *Defender* to ensure its *ultimate goals* are still achieved
- Defence aims to interfere with the logical progression of the attack through stages from left to right
- Can consider how each square in the defensive grid relates to the corresponding square in the attack grid
- Possible defensive countermeasures can be linked to the attack stages they stop

# Types of defence

- We focus on defence at different stages to limit access, harden the target, reduce impact
  - Roughly comparable to prevention, detection and reaction
  - Correspond to columns in the attack table
  - Action and method in the attack table correspond to the limit access column in the defence table
- Limiting access is ideal, but difficult with insider attack
  - Insiders have authorised access or can easily evade controls
- Hardening the target may limit functionality and cause interference with organisational goals
- Limiting the impact of successful attacks can aim to limit the immediate effect or stop the ultimate goal
- Should also consider the adversary
  - Aim to reduce the attacker's motivation, means and opportunities
  - Reduce motivation by persuasion and deterrence

# Defensive table for disgruntled employees (not terrorists)

Persuasion	Deterrence	Limit access	Harden target	Limit immediate effect	Limit ultimate effect
Good work conditions, address personal and financial issues, clear policies	Increase probability or perception of detection, zero tolerance, clear responsibilities, enforce disciplinary procedures, prosecute, sue	Vigilant observation, identify odd behaviour, limit activities (use roles, limited privileges)	Security awareness and training, strict policy enforcement double-check critical systems	Incident response, contingency plans, use spares, acquire new resources, repair critical problems, stop attacker's access	Alternative services, disaster recovery, business continuity, repair weaknesses, contract, insurance
		Roles, dual control, prevent damaging commands, partition systems, intrusion prevention, network access controls, strong authentication	Hardwired controls, secure configuration (use checklists), limited interfaces, read-only files, integrity checks, antivirus, anomaly detection, network scans, strong authentication, password change policy, limited accounts, delete unused and default accounts, apply patches	Intrusion detection, audit logs, reboot systems, reinstall software, restore backups, rollback databases, file versioning, disable accounts, change passwords	
		Alarms, CCTV, key management, accompany, sign in and out, movement detection, open plan offices, badges, place resources in secure areas or enclosures	Toughened or shielded equipment, attach to immovable objects, tag, connect transmitters, put documents and valuables in safes, locked filing cabinets and desks, clean desk policy	Continue in degraded mode, resilience (spare resources, secure offsite backups) shut down and repair systems, find and stop attacker	

# Prevention

- Prevention limits or constrains access, stops actions or its effects
  - Corresponding to the stages of the attack in the attack grid
- Prevention is problematic against the insider
  - Attacks may use authorised activities
  - May exploit system weaknesses to conduct an attack invisibly
- Prevention may stop access of partial insiders to the target by partitioning the system using internal controls
- Prevention may stop actions or effects on the system
  - Limited functionality providing a reduced attack surface
- Prevention may target the attacker
  - Deterrence reduces the motivation or rewards from a successful attack, raises cost or the probability of failure
  - May be warning signs from behavioural problems and policy breaches that are detected and reacted to before any damage is done
  - Example of reaction at an early stage possibly preventing a future attack

# Detection and reaction

- Detection and reaction considered together as they are not useful in isolation
- Detect the effect on the target and other system resources by monitoring for unauthorised or unusual system events and states, as well as the behaviour of the insider
- Detection is an observation that does nothing in itself that prompts reaction to stop the attack
  - Observation may see side effects or normal activities only, or the effect on the system after the event
- Reaction occurs after an observation has been made and its cause ascribed
  - Occurs usually at later attacks stages, but can undo earlier stages if detected and there is enough redundancy in system
  - Targets different logical stages in attack
  - Reaction may interfere with active attack or recover from unauthorised access, behaviour or effect

# Detection and reaction (2)

- Detection and reaction in a timely manner is very important to avoid a large or permanent impact for successful attacks
  - If we detect the effect on the target after an undesirable change of system state, it may be too late to recover the system
- Detection is easier later in the attack when there are more observations, but reaction becomes more difficult as the impact increases
- Temporal gap between the start of the attack and its detection
  - Needs to be limited and attacks that have large immediate impact must receive special consideration
- Temporal gap between detection and reaction
  - Should not react too early, which may incorrectly stop or interfere with legitimate activity
  - Allow suspicious activity if low impact or commonly performed legitimately as well

# Pervasive measures

- Encompass all layers and locations and influence all types of defence (preventive, detective and reactive controls)
- Must be relevant and not interfere with organisational goals
- Measures that do nothing by themselves
  - Need to be implemented and enforced
- Risk assessment and management
- Policy
- Security awareness
- Security architecture
  - Uses heuristics such as attack surface, defence-in-depth and least privilege
- Control and visibility of system
- Robustness and resiliency

# Heuristics

- Keep it simple. Simple defences are likely to work and be enforceable and not interfere with the functioning of the organisation. Reduce the attack surface to the minimum necessary
- Consider every layer. Controls must be complete and consistent at each layer in parallel. Attack surface must encapsulate all resources
- Defence in depth. Defence-in-depth should be applied with multiple boundaries in series in case one fails. Consider multiple attack surfaces backing each other up
- Consider evolution. Consider the temporal dimension to deal with how the systems are likely to evolve over time to become more complex and difficult to manage
- Least privilege and separation of duties. Reduce scope of user domains and impact zone
- Limit impact of successful attacks. Partition and isolate systems internally so user are limited and systems are partitioned internally
- Visibility and control. Need to communicate between layers and locations over trustworthy channels to obtain correct state of system and control it adequately
- Respect for organisational goals. Should not unnecessarily interfere with productive activities
- Need effective recovery procedures. Redundant components outside adversarial control

Need a coherent organisational structure and system architecture to meet these goals

# Security architecture

- The insider threat can be dealt with through the development of a systematic security architecture
- Provides defence-in-depth with several complete attack surfaces in series providing a complete and comprehensive set of controls
- Operate at every layer including policies and procedures, technical and physical controls
- Systematic defensive methods include partitioning and isolation, and redundancy
- Includes preventive and detective measures at multiple layers, locations and scope
- Must have communication between the layers as attacks may only be detectable with complete knowledge of system

Failures will happen with complex systems, but a comprehensive security architecture should limit the ultimate impact

# Protection against insiders

- Attacks are usually detected at the social layer or by chance at the logical layer by some irregular behaviour or change
  - Logical effects are invisible to people and automated checks can be avoided
- Actions may be correct or unavoidable at the logical layer, although incorrect or unauthorised at the social layer
- Actions often fall within the scope of legitimate behaviour
  - Will set off too many false alarms and damage productivity if their behaviour is strictly enforced
- Measures that limit the impact are crucial so confine effects within a limited impact zone
- The impact zone must reach the social layer to be an effective attack
- The impact zone may affect other levels in other locations
- Insiders could damage the recovery methods such as backups, which may makes the impact zone permanent

# Controlling access

- Consider access to system and access to target separately
  - Insiders already have some degree of system access so may be only one protection location on target
- Opportunity limited by reducing attack surface to confine user domain
- User domain = set of available resources and functions to the person at all layers
- User domain is a connected space within the system confined by the security controls, which provide the attack surface
- Attack surface is composed from the numbers of paths, their use and possible impact
- Reduce attack surface at all layers and locations to reduce user domain to its smallest scope possible
- Partition off unneeded functionality and protect needed functionality by limiting attack surface

# Limiting access

- Several locations and levels where access controls can be applied
- Physical access to buildings and secure areas using keys, CCTV and security guards
- Limit physical input and output devices to computers
- Isolate networks physically and logically from rest of organisation and other building occupants
  - Use encryption and host authentication if the network is physically insecure
  - Use network access control (NAC) to ensure access only to hosts that are properly secured with latest updates and AV
- Use strong authentication measures for computer access and limit privileged accounts
- Encrypt sensitive data

# Controlling social layer access

- Use strict enforceable policies to deter actions at social layer
  - May be partially enforced at logical layers
- Security awareness
  - Employees should not give out information to others without strictly defined need-to-know
- Use strong credentials to link person to their lower layer activities
- Only allow system changes with proper procedures, which are also enforced logically

# Harden target

Stop access to or an effect on the target

- Remove the defaults for system passwords and other security parameters when the system is initially configured
- Use checklists such as from NIST to remove unnecessary functionality that reduces the potential attack surface
- Stop persistent change using virtualisation
- Use policy enforcement to constrain allowed changes
  - Do not save sensitive data such as credit card data unnecessarily
  - Making files read only
- Install latest updates and apply procedures to test them adequately
- Do not allow the execution of untrusted executable content, which may allow malware to run
  - Email attachments, JavaScript, ActiveX controls, Trojan horses

# Limiting impact

- Impact zone of successful attacks should be limited
- Escape surface should avoid or hinder exit of attacker or resources, or extending the scope to other components
  - Sandbox in Java
  - Outgoing controls on firewall
  - Data leak prevention (DLP)
- Stops loss of confidentiality, but not integrity and availability
  - Impact may be within system and does not need to traverse escape surface
- Attacker may not need to exit boundary if acceptable to be caught or uses disposable agent such as malware

# Detection

- Provide system-wide observations
- CCTV and employee awareness
- Network and host intrusion detection and prevention
- Log access and change to computers, applications and data
- Use up-to-date antivirus and anti-spyware software
- Stop or detect modification of critical data or programs using integrity checks

# Redundancy and resiliency

Recover from effects by providing services or resources in other ways or providing effective recovery procedures

- Disaster recovery and business continuity, contingency plans
  - These scenarios should be tested and should consider deliberate interference by insiders
- Recover from loss of place in process
  - Reboot system, start process again, use checkpoints, backups
- Critical services can be provided in multiple ways
  - Ability to perform procedures manually is being lost because of complexity in the name of efficiency
- Secure backup and recovery procedures should be implemented
  - Should be controlled by different people and should be tested periodically
- Critical data must be backed up and properly protected in different physical locations otherwise an insider could compromise them all at the same time
- Need independent tests of the controls to make sure they work and do not reduce organisational efficiency

# Conclusions

We demonstrated a three-layer model for modelling security architecture

Introduced an attack taxonomy that has a corresponding defensive classification

Applied it to model insider attacks

- Showed how to reason about attacks on the electricity grid

- Indicated how an analogous defensive classification could aid the defender

Plan to elaborate the model so it can be used by organisations to plan systematic defence against all threats

# Insider threat references

- C Blackwell, “The insider threat: Combating the enemy within ”, IT Governance (April 2009).
- C Blackwell, “A Security Architecture for Modelling the Insider Threat”, The malicious exploitation of information systems conference (2008).
- 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/CommonSenseInsiderThreatsV3.pdf](http://www.cert.org/archive/pdf/CommonSenseInsiderThreatsV3.pdf).
- E Cole and S Ring, “Insider threat: Protecting the enterprise from sabotage, spying and theft”, Syngress (2005).

# Model References

Neumann, PG, “Practical Architectures for Survivable Systems and Networks”, (2000), at [www.csl.sri.com/neumann](http://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](http://www.sandia.gov).

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>.

Blackwell C, “A Multi-layered Security Architecture for Modelling Complex Systems”, CSIRW (2008), ACM Press.

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

Blackwell C, “A Security Architecture for Modelling the Resilience of Complex Systems”, ARCS (2008).