A Network Black Box with Splunk for Forensic Analysis of Attack Patterns

Clive Blackwell
Oxford Brookes University
Oxford, United Kingdom
CBlackwell@brookes.ac.uk

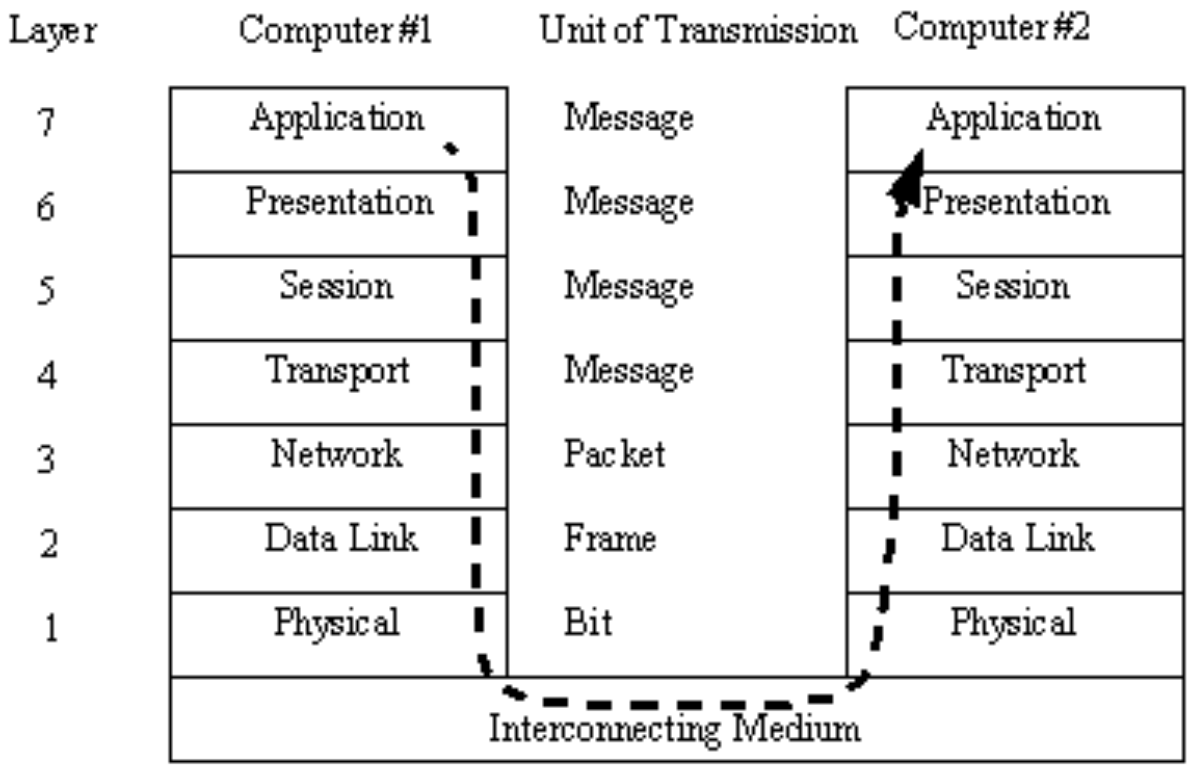
Roadmap

- Three layer architectural security model
  - Influenced by OSI 7-layer network model and Neumann's 8-layer security model
- Formalising attack patterns in predicate logic
  - Extending existing work on design patterns
  - Determine corresponding security and forensic patterns
- Beyond signatures
  - Abductive techniques for discovering incident causes
- Lab experiments in forensic analysis
  - Collecting and merging incident data with Splunk
- A network black box with Splunk

* Skip to slide 22 if not interested in the conceptual model *

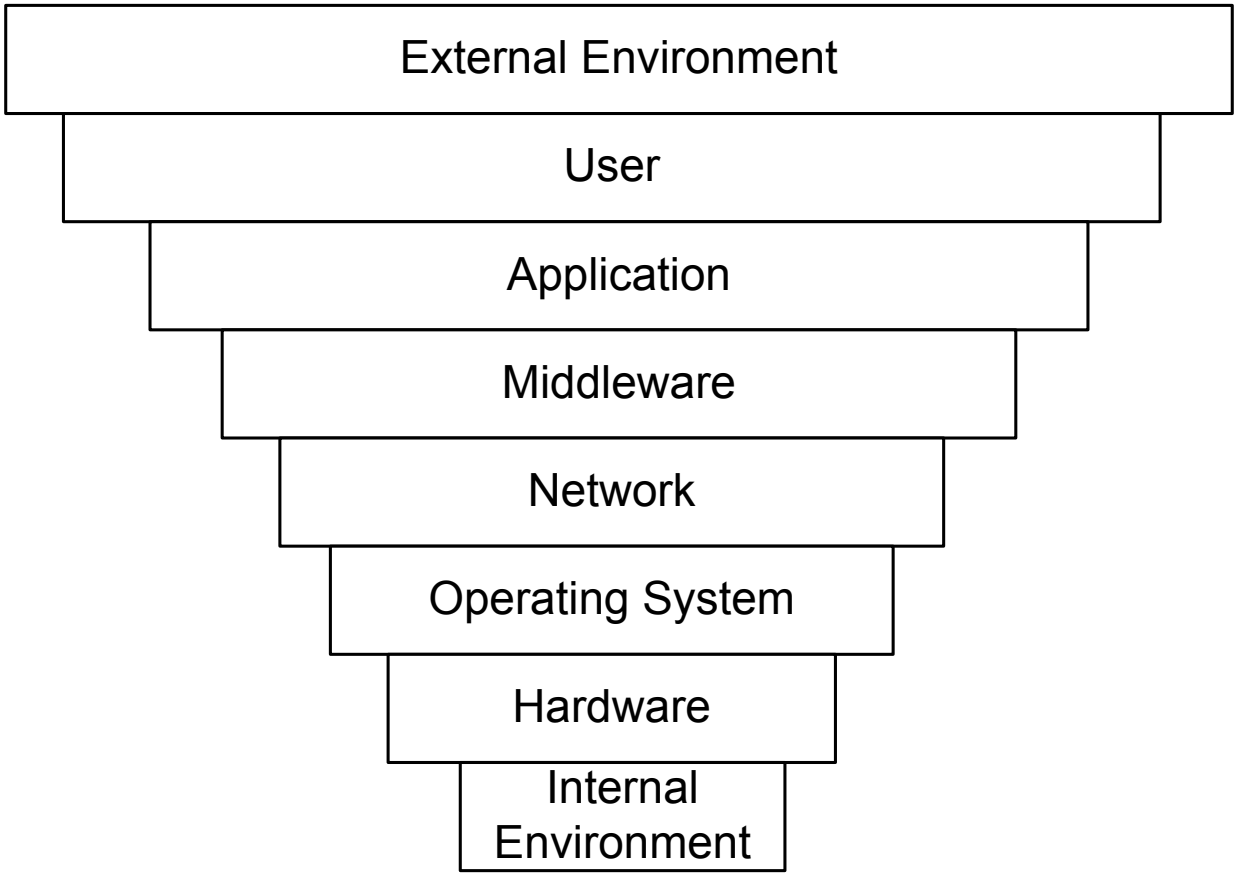
7-layer OSI network model

Strong influence on my multilayered model
Paths are down through the levels and transmission occurs physically
Physical medium is out-of-scope
My model explicitly includes people and the physical world



Neumann's 8-layer model

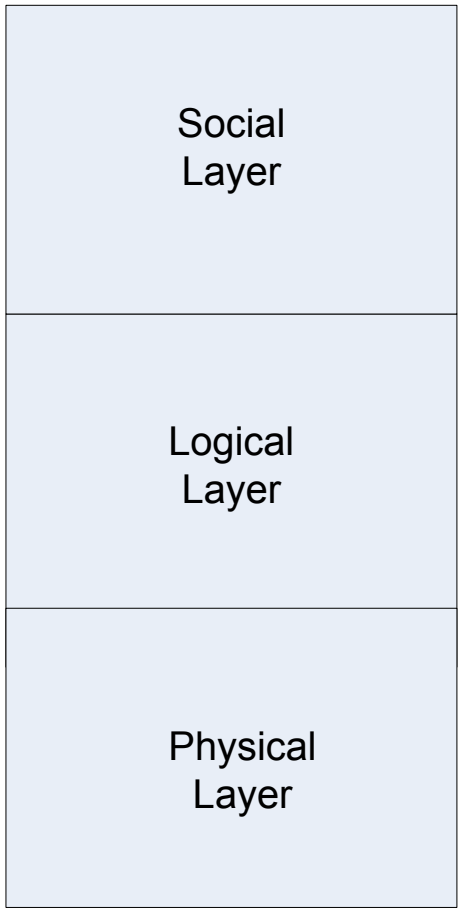
Scope reduces as the layers are descended
Confuses scope and level
External and internal environment are one level with differing scopes
Network is not a separate level, but has extended scope at multiple levels
Middle layers are part of our logical level
Environment is physical
User is social level
Has too many levels for analysis
Scope is infinite at all levels in my model



Digital forensic framework purpose

- We consider incidents within a wider context and from multiple perspectives to aid a broader and deeper investigation
- The focus is extended from misused computer systems to their wider social, legal, organizational and physical contexts
- The system interaction with the external environment and people provides the wider investigative context to
  - Examine incident progression and effects
  - Enable the goals of holding the perpetrator accountable, and
  - Repairing the damaged system and resources
- Purpose of the investigation differs depending on the circumstances
  - In a legal, regulatory or disciplinary process, it is to collect sufficient reliable evidence to discover the perpetrator and hold them accountable
  - In incident response, the purpose may be to discover the cause and extent of damage to determine effective system repair measures, fix the exploited weaknesses, limit further harm, and remediate external effects on third party victims and the environment

The Layered Security Model



- We have a simplified three-layer model
  - Add sub-layers to recover the greater number of layers in the OSI 7-layer network and other models
- Social layer at the top includes people and organisations along with their goals and intentions
  - Legal, organisational, economic, philosophical, political, sociological, and psychological aspects
- Logical layer in the middle contains computers, networks, software and data
  - Has multiple sublevels to recapture the layers of other mainly logical models
- Physical layer at the bottom represents the physical existence of all entities in world
  - Contains tangible objects including buildings, equipment, paper documents and computers
  - Also contains physical phenomena such as electromagnetic radiation, electricity and magnetism

Social layer

- The *social* or *conceptual layer* is the top layer
- Active subjects are abstract representations of organisations, systems and people, including their attributes and behaviour
- People's characteristics include their goals, knowledge and beliefs
- Can analyze using Parker's SKRAM classification (skills, knowledge, resources, authority and motivation)
  - D Parker, *Fighting Computer Crime, a New Framework for Protecting Information*, Wiley, 1998.
- The passive objects are abstract representations of lower-layer objects inhabiting the real world, and
- Concepts that only make sense at this layer such as trust, motivation, knowledge and information
  - Information is not understood by computers (Searle's Chinese room)
  - Evidence is a special type of information and therefore at the social level
- Higher layer entities like people and data have a physical existence as well as a higher layer form
  - Mind-body duality is extended to logical entities

Social layer in our framework

- Crucial in incident analysis, as people are ultimately responsible for causing and responding to incidents
- Conceptualizes the essential characteristics of people
  - Their skills, motivation, knowledge, weaknesses and other traits
- All deliberate incidents are initiated by people at the social layer and are only effective if they meet a social-level goal
  - Obtaining money, power, prestige or pleasure
- Ultimate effects are also on people and organisations at the social layer
  - Computers and other logical resources such as information are means to an end, and are not valuable in their own right
- Incidents are always executed using lower levels
  - Interaction between social entities at this level is only conceptual
  - People cannot operate directly at the logical layer, but use agents such as accounts to act for them
- All social and logical actions are ultimately executed at the physical level
- Therefore, effective investigation should involve complete analysis spanning all three levels

Social layer in investigation

- Scope of the incident analysis is at the social level
  - Within an organization for disciplinary action, industrial sector for regulatory breaches, or legal jurisdiction for criminal activities
- Evidence is contained within the social level and forms judgments on activities that happen at lower levels
  - Social level aspects such as intent must be inferred from lower level actions
- Evidence must be relevant and reliable, which requires lifting information about events and states at lower levels
  - Must use dependable and accepted investigatory processes to give a satisfactory argument within the particular domain
  - Such as rules of evidence for the law
  - But, evidence may be incomplete, incorrect or inconsistent
- Effective investigation must involve comprehensive analysis at all levels and the relationships between levels

Logical layer in our framework

- People cannot operate directly at the logical layer, but use agents to act on their behalf
  - User accounts to issue commands, run programs, execute processes and use resources
- This leads to the issue of proving responsibility
  - Agent may be initiated or taken over by others, or
  - Act outside its authority if faulty or has been modified
- Investigator also cannot directly observe logical functions and data
  - Examines them indirectly using software
  - Serious issues regarding its adequacy in collecting, interpreting and presenting digital data as evidence

- National Research Council, *Strengthening Forensic Science in the United States: A Path Forward*, National Academies Press (2009).
  - A compelling account of the failure to justify scientifically the vast majority of the physical forensic sciences
  - Analogous questions apply to digital forensics in spades

Physical layer in our framework

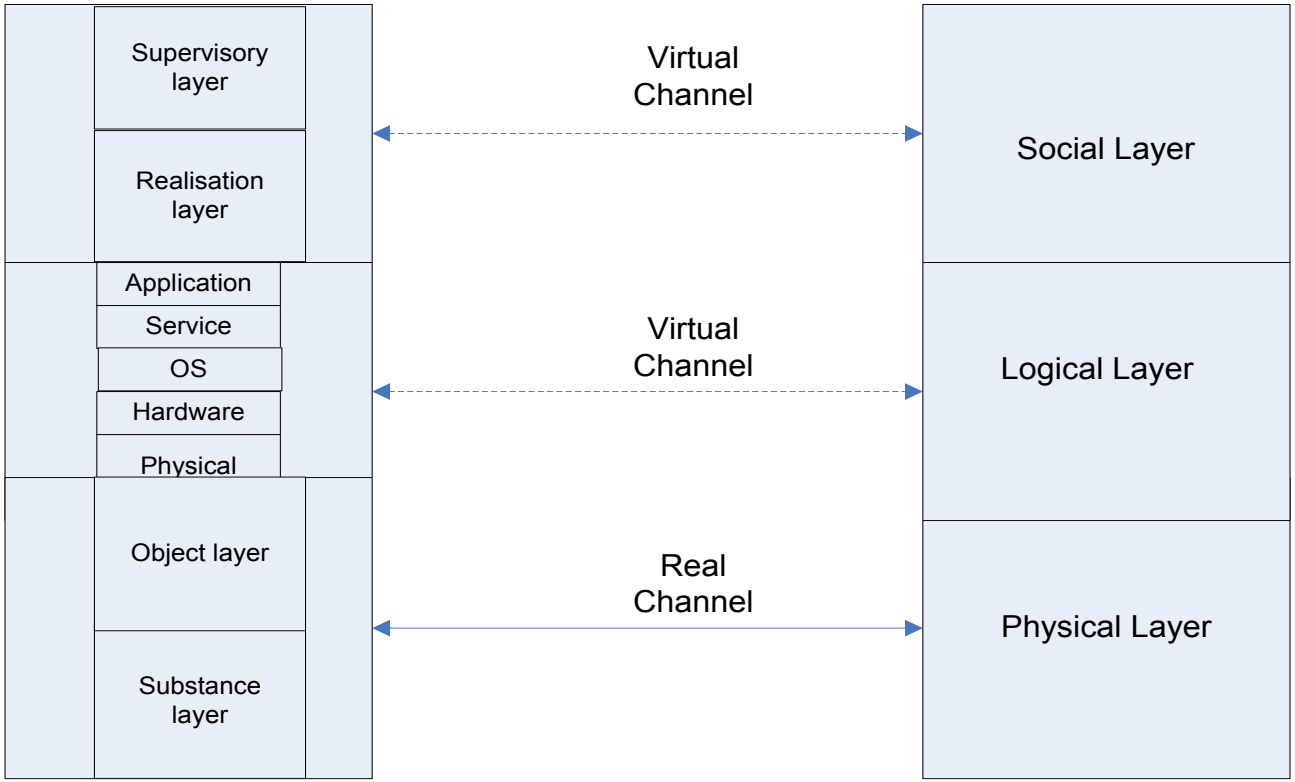
- Higher layer social and logical entities, have a physical existence as well as a higher layer representation
  - Except pure abstract entities like trust (influenced indirectly by real actions)
- Logical entities such as accounts and keys have a different physical existence to the people they represent (key distinction)
- But, higher layer entities cannot be understood at the physical layer
  - Information is ultimately stored physically
  - But understanding involves knowing its meaning and purpose, which can only be fully appreciated at a higher layer
- Effective investigation requires raising data about physical incident events into high-level evidence at the social level
- Must also link the physical and digital crime scene evidence
  - B Carrier and E Spafford, “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, Volume 2, Issue 2, 2003.
- Divide physical layer into upper object and lower substance sublevels
  - Contains intangible wave phenomena such as electromagnetic radiation, as well as material objects with differing size and scope

The Multilayered Architecture

Our model is more comprehensive

Also considers processing, storage and control

Incorporates physical actions



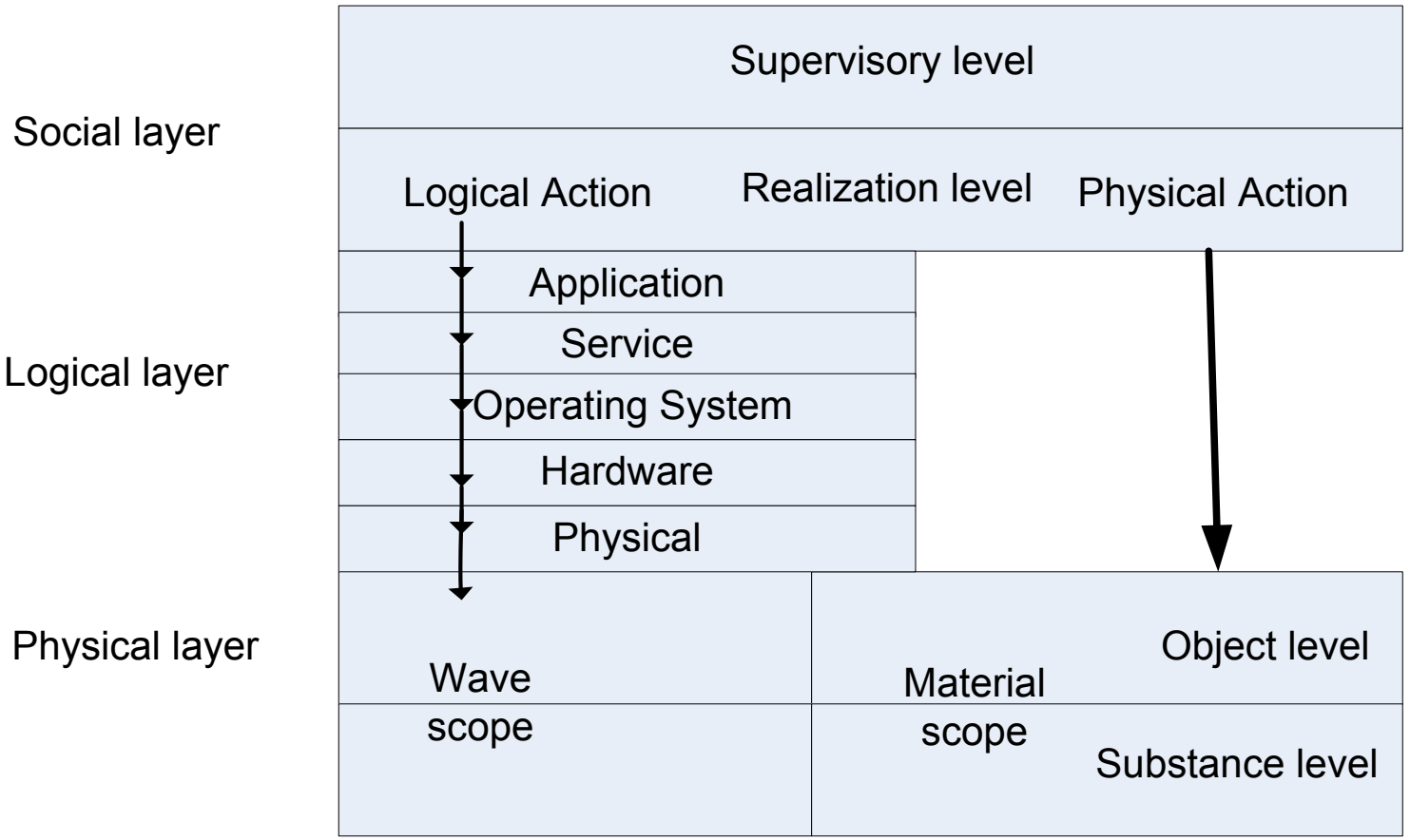
Sublevels – OSI network model

- For modelling logical communication only
  - Link, network and transport, session and presentation levels are contained in our intermediate logical layers
  - The upper application and lower physical sublevels interface to people and the physical world respectively
  - Our hardware level contains the OSI link layer
  - OS level contains network and transport layers in a wider scope
    - May have sub-sublevels of the OS level for detailed modelling
  - Service level contains the session and presentation layers
- People are represented implicitly by their logical agents
- The physical world is underneath and out-of-scope of the purely logical OSI network model
  - Physical level translates digital information to analogue signals
  - The physical world is abstracted away in the network model
  - Actions in the physical world are made explicit in our model
- Our logical layers are also more abstract and general
  - Incorporate all computational entities, not just networking

Sublevels – Neumann's model

- Simplified Neumann's eight-layer model to end up with three layers
  - Use of sublevels recovers all of Neumann's layers
- Many of Neumann's layers are sublevels of our logical layer
  - Application, operating system and hardware
- Neumann's user level is overloaded because it contains physical as well as logical actions
  - We distinguish the person from their application-level proxy as a user
  - Neumann also does not separate logical analogue functionality from the underlying real physical phenomena
- Explicit inclusion of horizontal scope at each layer as a first-class concept in our model
  - Some of Neumann's layers are better understood as an extended horizontal scope
  - Middleware is part of the service layer, and networking is within our operating system level
  - Our physical layer is one layer by including scope explicitly, rather than two layers in Neumann's model

The layered model



The layered model

- Many incidents involve a combination of logical and physical actions
- Relationship between digital and physical events needs to be understood for comprehensive incident investigation
  - An insider perpetrating sabotage may gain physical access to a machine and then execute damaging commands to delete critical data
  - Conversely, may gain remote logical access to a computer from the Internet to issue commands to shut down or overload critical equipment
- Digital forensics framework integrates the relationships and interactions at and between levels (some implicit and indirect)
- Can define, categorize and analyse incident characteristics
  - Following through from the initial motivation at the social level to the performance using lower layer resources
  - Analysing incident progression allows organisation of incident response
- Organizing constructs of vertical layer and horizontal scope help to model the incident structure and context within a wider setting
- Allows the analysis of incidents in their entirety including human and physical factors, not just from a technical viewpoint

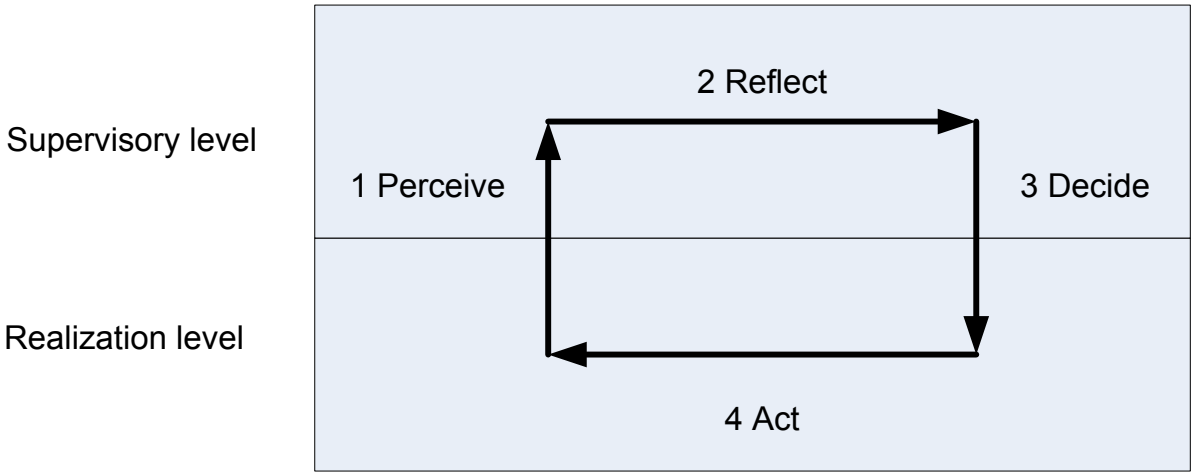
The five logical layers

- Application level interfaces to the social layer to provide a logical representation of users' identities
  - Provides logical services and resources (including data) to users
- Service layer provides generic services such as databases, middleware and cryptographic services
  - Do not directly satisfy people's goals, but offer complex services to applications beyond what the operating system provides
  - Services may actually be provided by the application or operating system, but it is useful to partition services conceptually for analysis
- Operating system provides lower level services such as processing, and resources such as files
  - Often initiated indirectly by people through the upper layers, by providing a virtual machine on top of the bare hardware
- Hardware provides the medium for logical services
  - Abstracts away from the underlying analogue world to provide complex functionality from simple digital components
- Physical sublevel interfaces with the physical layer to convert digital data to and from physical phenomena
  - Domain of transistors and cables using electricity and em waves

Physical sublevels

- Contains two aspects: the material aspect of substantial objects and the wave aspect of intangible phenomena such as em radiation
  - Likely best representation of object is determined by spatial size
- Contains the two sublevels of object and substance
  - All physical objects are composed of substances that make up the universe
  - Many aspects of physical forensic analysis have a microscopic scope when analysing properties of substances
- Investigation must raise physical incident information into evidence
- Physical evidence at a crime scene and the logical evidence from devices should be investigated together to form the complete picture
  - Carrier and Spafford produced the Integrated Digital Investigation Process (IDIP) to unite digital and physical crime scene investigation
- Analysis of logical events should consider the physical environment
  - Logging physical access to buildings, eyewitness accounts, CCTV, telephone records and fingerprints
- Logical access to a computer may be inferred from the physical context
  - Proximate printouts, written documents and notes (including passwords) or being observed at the keyboard

Dynamics of social-level activity



- Our elements can be combined in pairs to construct events
- 4 pairs: perceive (R→S), reflect (S→S), decide (S→R) and act (R→R)
  - Arrows indicate operations in the source domain with the outcome in the destination domain
- We use the cycle to observe the world (perceive), determine its state (reflect), form a conclusion about the necessary actions to reach the goal state (decide), and then act in the real world (act)
- Reality may be different from perception and impossible to determine

Conceptual incident modelling

- The progression of the entire incident and corresponding investigation can be modelled conceptually using our four-stage model
  - Abstract away from its lower level execution to only contain relevant actions and their meaning modelled conceptually at the social level
- Investigative process lifts, transforms, filters and possibly misrepresents data collected from the actual world at lower levels
  - Evidence is modelled conceptually at the realisation level to capture the relevant incident events
  - Missing arrows to/from lower levels in last diagram to model real process
- The supervisory sublevel is used to reason about the incident
  - Skills, knowledge, motivation and objectives are in the supervisory layer
- Investigative goals are at the supervisory level
  - But, met by a consistent, comprehensive and compelling narrative at the realisation level without any significant rebutting or undercutting arguments
- Realisation level contains the entities and processes involved the incident considered conceptually
  - Includes the actions, resources used, interaction between the involved parties and changes to the system

Evidential issues

- Motivation is at the supervisory level as it is psychologically based
  - Therefore, need to infer motivation from actions
  - Including indirect actions performed by agents on the perpetrator's behalf
- The ultimate outcome at the social level of gaining power, money, prestige or satisfaction needs to be linked to the underlying events
  - Perpetrators use low-layer entities to meet their goals
- Activities at lower levels are the focus of investigation, but raise several issues
  - Investigator needs to establish the link to a person from the activities indirectly carried out on its behalf by its agents
- Need a systematic account of the link between lower level events and their ultimate human cause and effects
  - Especially logical actions on compromised computers
- Logical evidence need special tools to analyse low level data and existing tools are not adequately validated
- Must also link evidence from different sources for coherent analysis
  - Including consolidating and connecting physical and digital evidence

Attack patterns

- Based on design patterns
  - A design pattern is a general reusable solution to a commonly occurring problem in software design
  - Represents desirable intentional anticipated system behaviour
- Attack patterns specified from the attacker's viewpoint
  - Describes how an attack is performed
  - Represent undesirable unintentional operational system behaviour
- We also describe how to trace and remediate attacks in incident response and forensic investigation
  - Using security or forensic patterns
  - Including specifying the different types of evidence and where it may be found
- Not much new compared to design patterns
  - A couple of new sections to cater for defensive reaction and evidence collection
  - Some sections amended to correspond to the attacker's viewpoint

Attack pattern template

- **Name:** Generic name for attack
- **Intent:** Short description of the intended purpose for the attacker
- **Context:** Description of the conditions where the attack may occur, including system defences and vulnerabilities
- **Problem:** Defines the goal of the attack pattern, including overcoming defensive mechanisms
- **Solution:** Describes how the attack is performed and its expected results
- **Known Uses:** Specific incidents using the attack method
- **Consequences:** Describes the benefits and drawbacks of the attack from the attacker's viewpoint
- **Related Patterns:** Patterns with different objectives that are performed in a similar way, and patterns with similar objectives that are performed in a different way

Attack pattern template (2)

- **Countermeasures:** This new section describes the measures taken to stop or mitigate the attack, which includes the list of possible deployable security patterns
- **Forensics:** This new section describes the forensic patterns of data collection to identify and trace the incident that supports forensic analysis to repair the system and hold the responsible party accountable
- **Evidence Locations:** Another new field that contains the relevant defensive entities for incident response and subsequent investigation. Includes primary sources such as firewalls, IDSs and applications where logs are collected. Also includes secondary sources such as caches and registry keys possibly containing additional evidence. Incorporates physical locations monitored by eyewitnesses, building access controls, CCTV, sensors and Internet of things

‘Proofs of security’

- ‘Proofs of security’ make a number of assumptions using unrealistic system models
  - Compare with ‘proofs’ that financial system was sound
- We cannot prove any system is secure
  - Meaningless statement that needs a context
- We can only say a system is secure against certain types of attack
  - That we model by logical predicates for the possible attack patterns
  - Then, transform into the corresponding security or forensic patterns intended to detect and respond to these incidents
- Analysis should take account of all relevant system factors and not make invalid assumptions
  - Need to consider the disposition of the system, its organisation, critical assets, weaknesses, goals and adversarial threats
  - All included in our security incident framework (not discussed here)

Formalising attack patterns

- Extend Zhu and Bayley's work on formalising design patterns to attack patterns
- Attack patterns form a specification for behaviour that must be recognised, understood and countered on network devices and hosts
- Intersect the attack pattern with the network and host model to create security or forensic patterns for their observations and powers
- Using some logical specification language such as B or Z is a very common method of developing robust software
  - Progressively refined into executable code whilst maintaining correctness at each stage
- In our more formal work, we specify system security using the Event Calculus and search for undesirable behaviour by model checking in LTL

Ian Bayley and Hong Zhu, Formalising Design Patterns in Predicate Logic, The 5th IEEE International Conference on SOFTWARE ENGINEERING AND FORMAL METHODS, 2007, pp25-36.

Ian Bayley and Hong Zhu, Specifying Behavioural Features of Design Patterns in First Order Logic, Proc. of COMPSAC 2008, pp 203-210.

Plan

- Formalise attack patterns from the Common Attack Pattern Enumeration and Classification (CAPEC) overseen by MITRE
  - As are many other security taxonomies such as Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE)
- Precise meanings potentially allows the creation of accurate recognition software that can be deployed in network devices, hosts and applications
  - Their current informality means that their utility is limited to manual use
  - Automation possibly helps to ease the creation of correct defensive measures
- May enable provable security against certain attacks, assuming the defensive controls are operational
  - Rather than from some abstract and generic definition of security
- Implemented fields in the attack pattern are annotated for their level, location, purpose and behaviour
  - Aid translation into programs at the various network nodes at different locations and levels with their particular recognition and response abilities
  - Intend to use description logic in OWL that is the foundation of our security ontology (not discussed here)

CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC), May 2011, MITRE, at http://capec.mitre.org.

Deduction and abduction

- **Deduction:** From a conditional statement $P \rightarrow Q$, and a fact P
- Conclude Q from the hypothesis and the statement
- $P \rightarrow Q$ (general rule), P (Known information) $\Rightarrow$ Q (Valid conclusion)
- **Abduction:** The reverse process of arriving at an explanatory hypothesis for some observation
  - Crucial step in the scientific method
- $P \rightarrow Q$ (general rule), Q (Known information) $\Rightarrow$ P (Possible cause)
- Asserting P is a fact is a logical fallacy called affirming the consequent or post hoc ergo propter hoc
  - May be many possible explanations for Q
  - Reason why scientific theories can never be proven, only falsified

Abduction in forensic investigation

- Determine the attack pattern that describes all the known ways that a particular incident can occur
- Transform into a security or forensic pattern containing the evidence that may be accessible to the defence
  - Direct observation may be impossible and we may have to rely on indirect information
- Search for these patterns on collected data with abduction
  - Form various hypotheses for the cause of detected anomalies
  - Search for these in the log files and set flags to collect related incident data in future
- Act on the most likely cause to improve the system to stop such incidents in future
- Possibly select the best location to deploy defences based on the hypothesised cause
  - Do the least damage to legitimate traffic whilst stopping the attack

Security and forensic patterns

- Network nodes and host endpoints do not have complete visibility of incidents or the powers to respond
- Logical specification for the security and forensic patterns is divided into components for each level
- Then implemented on each node according to their level, location, observational and response abilities
  - Supported by our framework by its separate conception of location, observation and power at each logical level
- Use the upper application, transport and network layers for Internet attacks
  - Transport and network layer are sublevels of our operating system level with wider horizontal scope
  - Merge the service layer into the others for simplicity
- Representation in OWL and description logic

Logging

- Many current logging options are inflexible and limited by collecting incomplete information in special formats
  - Making them difficult to merge, or
  - Using the lowest common denominator of translation into syslog format thereby losing unique data
- Need to collect, merge and analyse enough contextual information to make correct decisions about system use
  - Performing forensic analysis after the event, as reactive response in real time is too difficult
- Requirements include:
  - Determining legitimate use as well as denying illegitimate use
  - Discovering the impact of successful incidents
    - Sony PlayStation credit card breach
  - Discovering how and where failed attacks are stopped
  - Discovering and holding perpetrators accountable

Splunk

- We use Splunk for logging and merging observed data from various sources
  - ‘Google for machine data’
- Splunk can potentially collect and merge the data needed to detect attack vectors
  - May require data from multiple network locations
  - May require the full information available from both the network and host applications
- Need little apps to help convert different data sources into Splunk logs
- Consolidated logs allows discovery and analysis of the passage of attack packets
- Collect data continuously
  - Avoids losing the initial data if we set alerts on anomalies instead
  - Collect all relevant data and then discard every few minutes if there are no discovered anomalies

Experimental setup

- Use existing tools to develop and launch automated attacks on our experimental network
  - Such as the Metasploit framework
- Checked by generating large amount of legitimate network traffic along with the attack packets
  - Can use a packet generator to generate a large amount of background traffic
- Check if the network meets its specification of allowing legitimate use whilst stopping undesirable incidents
  - Run the experiment again after defences are deployed to ensure that the attacks cannot occur
  - Use newly generated attack packets consistent with the attack patterns
  - Also discover how much legitimate traffic is being discarded

Network design

- Our formalisation of attack patterns leads to the idea of secure-by-construction systems or proactive defence
  - May be possible to prove that certain attacks must fail
  - Or how they may succeed, which shows where we need to deploy additional defences
- From the formal model of system architecture, distribution of defensive controls, location and type of critical assets and potential threat actors and abilities
  - Proof will generally depend on internal controls being correct and unreachable by the adversary, otherwise all bets are off
- Can all be tested to show theory matches practice
  - Once the defences have been deployed, we run experiments to ensure that the attacks cannot occur
  - Discover successful attacks and iterate defensive controls until they are all stopped

Network black box

- Network and application data can be saved for incident investigation
  - Can create a visual representation for the path and timeline to display incident progression including its hypothesised cause
- Our incident framework helps systematic analysis and response
- Need forensically sound collection of log data
- Use separate devices or networks for log storage
  - Log to a remote server or tamperproof device inaccessible by the perpetrator
- Collect forensic data for incidents that are difficult to stop
  - Insider threat from privileged employees such as system administrators
- May be able to determine accountability to hold the perpetrator responsible after the incident
  - Determine the relevant information required beforehand from the forensic patterns
- Determining impact is crucial to aid recovery
  - In the Sony PlayStation credit card breach, they did not know how many credit cards details were compromised

Conclusions and further work

- Demonstrated a three layer architectural security model
  - Social, logical and physical layers with sublevels
  - A holistic model for forensic analysis
- Formalising attack patterns in predicate logic
  - Discover the analogous security and forensic patterns by intersecting attack patterns with the defensive capabilities
- Used abduction for discovering incident causes
  - Detailed incident analysis searching for relevant prior events
- Lab experiments in forensic analysis
  - Execute attacks and analyse effects on network
  - Collecting, merging and analysing incident data with Splunk
- A network black box with Splunk
  - Aids enforcement of accountability, impact determination and effective recovery

References

C Blackwell, A Security Ontology for Incident Analysis, *6th Cyber Security and Information Intelligence Research Workshop*, ACM Press, 2010.

C Blackwell, A Framework for Investigative Questioning in Incident Analysis and Response, *7th Annual IFIP WG 11.9 International Conference on Digital Forensics*, 2011.

C Blackwell, A Forensic Framework for Incident Analysis Applied to the Insider Threat (submitted)

C Blackwell, A Network Black Box with Splunk for Forensic Analysis, 5th International Conference on Cybercrime Forensics Education & Training, 2011.

C Blackwell, Formally Modelling Attack Patterns for Forensic Analysis, 5th International Conference on Cybercrime Forensics Education & Training, 2011.