Using Bigraphs to Model System Architecture

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

Presentation Outline

- The layered security model
- Introduction to bigraphs
- Modelling critical infrastructure with bigraphs
- Further work

Existing Systematic Models

Basic Concepts and Taxonomy of Dependable and Secure Computing
- Avizienis, Laprie, Randell and Landwehr
- Longstanding work to Classify the important aspects of dependability including security

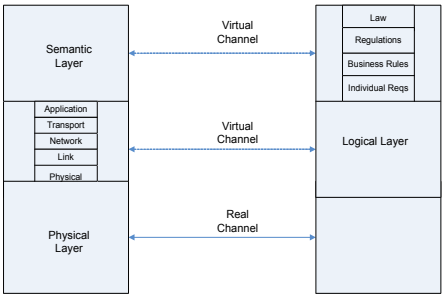
Practical Architectures for Survivable Systems and Networks
- Neumann and Parker organised systems into eight layers for security analysis
- The external environment, user, application, middleware, networking, operating system, hardware and internal environment

A Common Language for Computer Security Incidents
- Longstaff and Howard present a classification system for network security incidents
- Shows the different types of entity involved in an attack and their interrelationships

The Layered Security Model

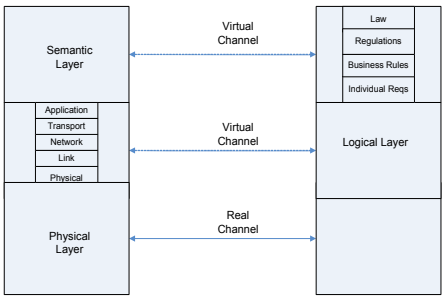
- Systems are modelled in a three-layer hierarchy
- The *semantic* or *conceptual layer* is the top layer
  - Includes people, organisations and system requirements
- The *logical layer* is the intermediate layer
  - Contains intangible entities including data and software that are stored and processed on computers
- The *physical layer* is the bottom layer
  - Represents the physical existence that all entities have in the real world
  - Includes both tangible objects and electromagnetic radiation

Three-layer model with sub-layers



- Each layer can have sub-layers for detailed analysis
- We use Tanenbaum's five-layer network model as sub-layers of our logical layer
  - The link, network and transport layers are intermediate sub-layers
  - The upper application and lower physical sub-layers interface to the social and physical layers of our model respectively

Locations and communication



- Each layer has a separate concept of location and distance between entities
- Entities at each layer have different extents, dependencies and interactions
- Entities in different locations use channels to communicate
  - Channels at higher layers are virtual, and must use a physical channel to communicate

Modelling protection requirements

- All systems have a horizontal scope at every layer
- Neumann considers four conceptual locations for compromise at every layer
- From outside, above, within and below
  - Protection from an external entity at the same layer requires horizontal controls
  - Protection from a higher layer entity requires a vertical boundary between the layers
  - Insiders should be constrained by partitioning the system with additional internal system boundaries they should not be able to breach
  - Some components that control the system must be trusted and so they should be made simple enough to assure

Conclusion - All entities, apart from unconditionally trusted entities, should be outsiders relative to one or more controls that moderate their use of the system.

Representing the 3-layer model using bigraphs

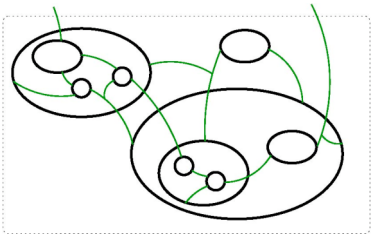
- Any system represented in our model can be transformed into a bigraph
- Use the two levels of bigraphs to represent the lower two layers of our model
  - Physical and logical layers are directly modelled
  - Locations and communication channels can be physical or logical
    - Represented by different types
  - Semantic layer is represented indirectly through lower level activities and effects
- Vulnerabilities are never removed by the application of security mechanisms, but are transformed into other vulnerabilities
  - All vulnerabilities have a physical or logical location or channel
  - The protective mechanism and the channel between the protection and the resource is vulnerable
  - Directly modelled by reaction rules in bigraphs, but not considered in most security models
    - Keys are stored in locations that must be protected with additional controls
    - Cryptographically protected resources exist in a virtual location encapsulated within special nodes that represent the protection
- Attackers have physical and logical scope and powers that can be represented by bigraphs
  - Sites represent their location
  - External names represent their potential communication
  - Rewriting rules specify their powers

Bigraph Purpose

- Bigraphs are graphs with two constituent graphs representing locality and connectivity separately
- They are an attempt at a unifying theory for program semantics
  - Have been shown to capture the semantics of the π-calculus, Petri nets and mobile ambients faithfully
- Important aid to understanding systems with both physical and logical aspects
  - Ubiquitous systems
- Understanding systems at multiple layers is essential for security

This introduction to bigraphs is based on “Axioms for bigraphical structure” by Robin Milner

Bigraph description

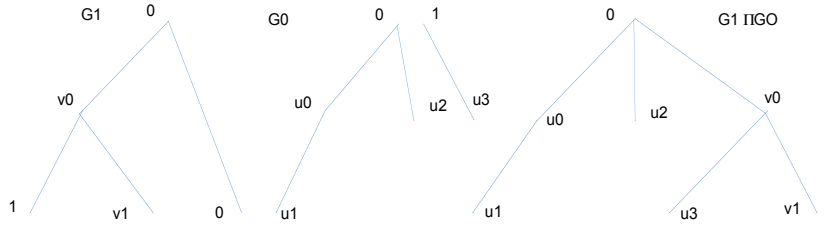


- The ovals are nodes of the bigraph, which are the common component of the underlying place and link graphs.
- Place graph edges are shown implicitly
  - The nodes are nested inside each other to represent placing one entity inside another
- Link graph edges are show explicitly
  - Each node has ports which may be linked to other nodes which models communication
- The linking and the placing of nodes is independent, shown by the way links cross node boundaries in the diagram
- Each external link (shown emerging from the top in the diagram) can be joined to some link of a host bigraph to model external communication

Place Graph

- A *place graph* G = (V, ctrl, prnt): m→n has:
  - An *inner width* m and an *outer width* n, both positive integers
  - ctrl: V→ κ represents the kind of nodes
  - A *parent map* prnt: m∪V →V∪n
- Represents n locations with a forest of n trees
- Represents m sites where other bigraphs can be placed
- The prnt map is the usual parent function for trees
  - Represents containment
- Places can be real or virtual locations
  - Keys, files and programs inhabit virtual locations

Composing Place Graphs

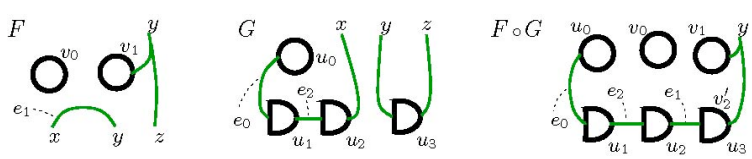


- Each root of the place graph G_0 is planted in a site of G_1
  - Identification points disappear in the composition
- If $G_i = (V_i, ctrl_i, prnt_i)$: $m_i \rightarrow m_{i+1}$ (i = 0, 1) be place graphs,
- $G_1 \circ G_0 = (V, ctrl, prnt)$ has prnt = $(Id_{V0} \cup prnt_1) \circ (prnt_0 \cup Id_{V1})$.
  - prnt(p) = $prnt_0(p)$ if $p \in m_0 \cup V_0$ and $prnt_0(p) \in V_0$
  - prnt(p) = $prnt_1(m)$ if $p \in V_0$ and $prnt_0(p) = m \in m_1$
    - new parent node in inhabitant graph
  - prnt(p) = $prnt_1(p)$ if $p \in V_1$

Link Graphs

- A link graph G = (V, E, ctrl, link): X→Y
  - Finite sets X of inner names, Y of outer names
  - Function link: X∪P → E∪Y called the link map.
    - The inner names X and ports P are the *points* of G, and the edges E and outer names Y its *links*.
    - The link map connects the attachment points to a communication channel
    - The interior link graph has a communication pattern that is enabled by the exterior link graph through the binding between interfaces
- We draw a link graph's inner names below it, and its outer names above
- Outer names can represent local or global communication
  - An outer name is an *open* link, an edge is a *closed* link
- The link graph can represent point-to-point or group communication
  - The link map is a hypergraph, so 'edges' can connect several points

Composing link graphs

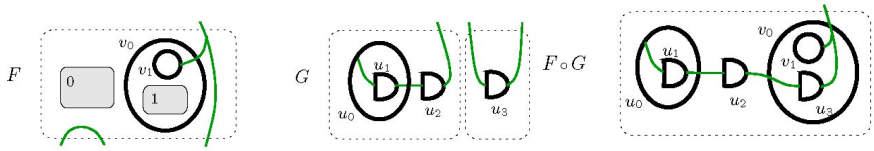


- The outer names of the interior link graph link to an exterior link graph via its corresponding inner names
- Let $G_i = (V_i, E_i, ctrl_i, link_i): X_i \rightarrow X_{i+1}$ (i = 0, 1) be two link graphs, then $G_1 \cup G_0 = (V, E, ctrl, link)$ has
- $link = (Id_{E0} \cup link_1) \circ (link_0 \cup Id_{P1})$
  - $link(p) = link_0(p)$ if $p \in X_0 \cup P_0$ and $link_0(p) \in E_0$
  - $link_1(x)$ if $p \in X_0 \cup P_0$ and $link_0(p) = x \in X$
  - outer name of G_0 links to edge, which makes it local to composed graph or to outer name of G_1, which potentially makes it global
  - $link_1(p)$ if $p \in P_1$

Bigraph Definition

- Define the composition of bigraphs in terms of the underlying operations on their constituent graphs
- An *interface* I = ⟨m, X⟩ consists of
  - A positive integer m called a *width*, representing places
  - a finite set X ⊂ ξ called a *name set*
- A *bigraph* takes the form G = (V, E, ctrl, G^P, G^L): I→J
  - The interfaces I = ⟨m, X⟩ and J = ⟨n, Y⟩ are its *inner* and *outer faces*
- The map from I to J is determined by the underlying place and link graphs
  - G^P = (V, ctrl, prnt): m→n a *place graph*
  - G^L = (V, E, ctrl, link): X→Y a *link graph*

Composing Bigraphs



- The component place and link graphs are our previous examples
- The composition of the two bigraphs are formed from the combinations of the place graphs and link graphs, which have orthogonal operations
- The sites in F indicate where the roots of an inhabitant bigraph G can be placed
- Then the outer names of G are linked to the corresponding inner names of F
- Note that G can be inserted two ways into F
- The two sites of G could represent a communication pattern that is implemented when inserted into F
  - Some of the nodes in G could be keys to protect communication over F, which could represent an insecure medium such as the Internet

Reaction Rules

- Different controls can participate in different *reaction* or *rewriting rules*
- Each rule consists of a precondition, which may be transformed into a post-condition wherever it occurs
  - Both of these conditions are bigraphs
- Atomic nodes do not have internal nodes
- Complex nodes can be active or passive
  - The control is *active* if reactions can occur inside them
  - It is *passive* if no internal reaction is allowed
    - The only method of reaction possible is when the passive nodes are destroyed

Critical Infrastructure

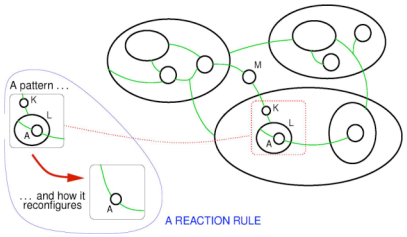
- Very complex systems that are very difficult to analyse manually
  - Large numbers of physical and computational entities and communication paths, and people with various powers
  - Large horizontal physical and logical scope
    - Allows pervasive access
  - Subject to both physical and logical attacks on resources, control systems and communication links
  - Intractable problem to avoid attacks
    - Large and unmitigated number of vulnerabilities
  - Goals of model in critical infrastructure protection
    - Finds vulnerabilities
      - Unexpected dependencies difficult to discover manually
    - Suggest remediation measures
      - Remove critical vulnerabilities
    - Continue in face of an attack
      - Avoid catastrophic failure modes
    - Helps in design of system
      - Avoid critical failure
      - Partition systems to limit damage of successful attack

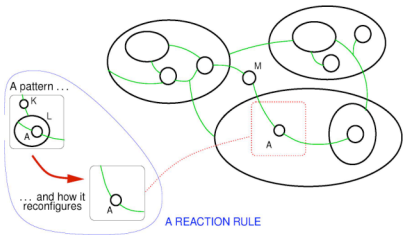
Critical Infrastructure (2)

- The bigraph representation of our three-layer model can faithfully represent critical infrastructure. It can:
  - Check objectives are satisfied
    - Can give assurance of protection of critical assets or indicate critical vulnerabilities
  - Model architectural protection using defence-in-depth
  - Model dependencies between components
  - Discover linkage between layers
    - Can discover attacks that operate and have effects at several layers
  - Handle remote effects and dependencies
    - Including transitive attacks that operate in several stages
  - Represent attackers in various locations with various powers
    - Including insider attacks
  - Model different types of network and the interaction between them
  - Model different scenarios by changes to attacker and defender

Critical infrastructure example

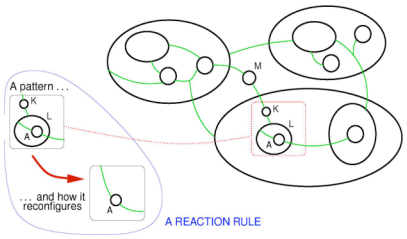
- Nodes of different types
  - Outermost ellipses are buildings
  - Circles are computers or machines
  - Intermediate size ellipses may represent rooms
- Representing requirements
  - The lower large ellipse represents a building containing a room with a telecommunication exchange or controller for an electricity substation S that can be accessed and controlled through the administrator's workstation
  - One defence goal is that there should be no path from the outside to S by either physical or logical means from unauthorised people or malware
- Cryptographic channels
  - The administrator's computer can be accessed remotely if the correct key is used for authentication, which is indicated by the graph reaction rule as shown

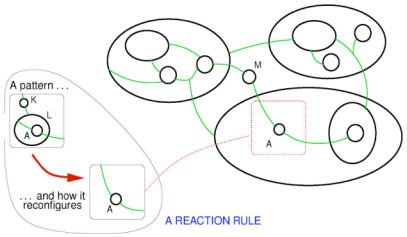




Critical Infrastructure example (2)

- A user can access the administrator's workstation remotely when he authenticates by proving he has access to the key K represented in the reaction rule
- The defence initially set up the authentication mechanism
  - Represented by the reverse of the reaction rule with the arrow in the opposite direction
- S can be accessed in multiple ways from outside
  - Logically through transitive access via the administrator's workstation A
  - Physically by entering the building and then the room
  - Via a multi-layer hybrid attack where both logical and physical accesses are combined
  - The link to the room containing S could be used to send a command having a physical effect such as cutting the power supply to S
- All these controls can be represented using bigraphs and model checking could determine if the attacker can breach any of the controls to interfere with S





Conclusion

- We demonstrated an informal three-layer model for modelling security architecture
- We formalised the model using bigraphs
- We used bigraphs to analyse a simple critical infrastructure example
- We suggested how the model unifies the treatment of insiders and outsiders
- We have used the model to represent cryptographic primitives (NSPW 2007 submission)
- We are investigating Kerberos, a complex network security protocol, that considers both physical and logical vulnerabilities

Model References

Avizienis, A, Laprie JC, Randell B and Landwehr C, “Basic Concepts and Taxonomy of Dependable and Secure Computing”, *IEEE Transactions on Dependable and Secure Computing*, vol 1, no 1 (2004).

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

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

Bigraph References

Blackwell C, “Using bigraphs to represent cryptographic primitives”, submitted to ACM New Security Paradigms Workshop (2007).

Milner R (2005), “Axioms for bigraphical structure” (revised version of Cambridge Computer Laboratory Technical Report 581) at www.cl.cam.ac.uk/users/rm135.

Milner R (2005), “Bigraphs, a Tutorial”, at www.cl.cam.ac.uk/users/rm135.