



The IT Innovation Centre

Colin Upstill

cu@it-innovation.soton.ac.uk

Northrop Grumman Visit

12 May 2016

About the IT Innovation Centre

- An applied research centre advancing a wide range of information technologies and their deployment in industry, commerce and the public sector
- Application-driven R&I themes
 - human-centric computing and information sciences (HCIS)
 - interdisciplinary R&I including HCI, H2M, psychology, sociology, law, ethics
 - big data, information discovery & decision support
 - semantic interoperability, semantic alignment and enrichment.
 - geo-tagging, geo-semantics and geo-parsing
 - data fusion, reasoning, context awareness
 - information security and risk management
(the subject of the rest of this presentation)
 - addressing security as a barrier to adoption of novel IT
 - focusing on the practical issues for real-world applications
 - usability and operability, trust, risk management, scalability and cost

Security and Trust

Threat Modelling and Risk Management

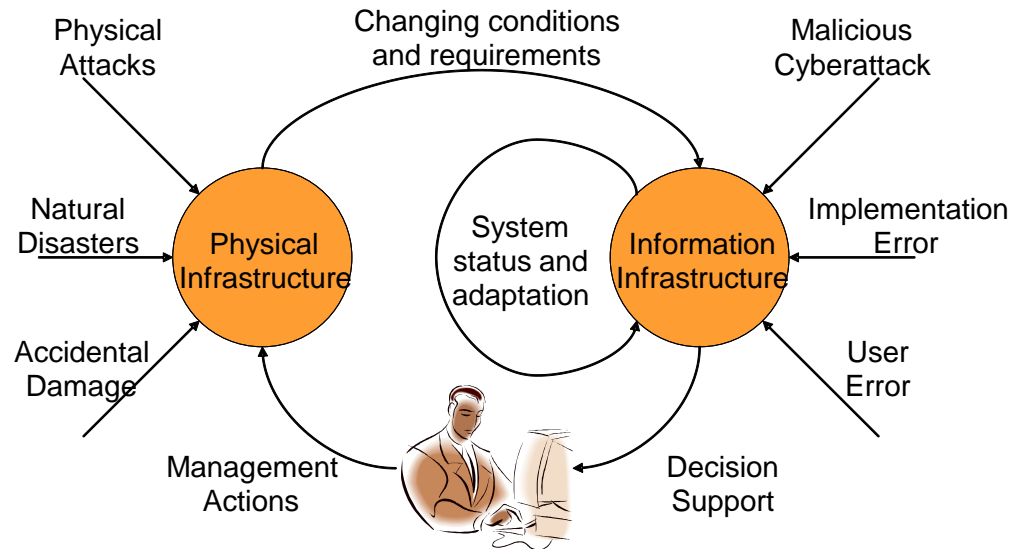
Mike SurrIDGE and Colin Upstill

Northrop Grumman Visit

12 May 2016

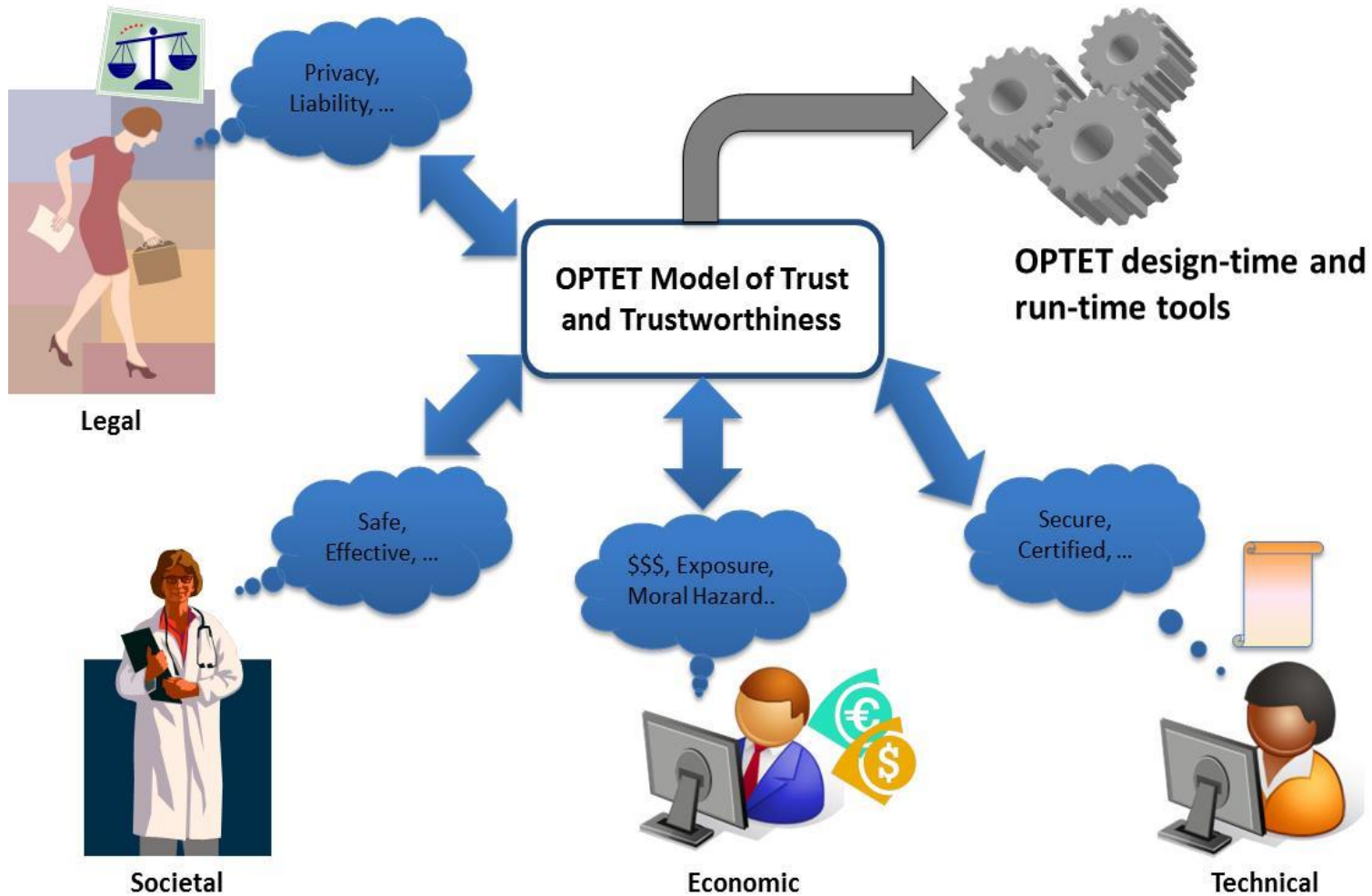
SERSCIS: Semantically Enhanced Resilient and Secure Critical Infrastructure Services

- Managing risks from ICT interdependency
 - more info sharing → high efficiency → low resilience
 - compromise cascade effects
- Need agile adaptation to changes in hostile environments



- Semantic models for run-time risk assessment
 - semantic models of threats to interdependent ICT services
 - design-time reasoning to identify potential risks
 - run-time diagnosis of system behaviour
- Validated using a simulation of Vienna airport

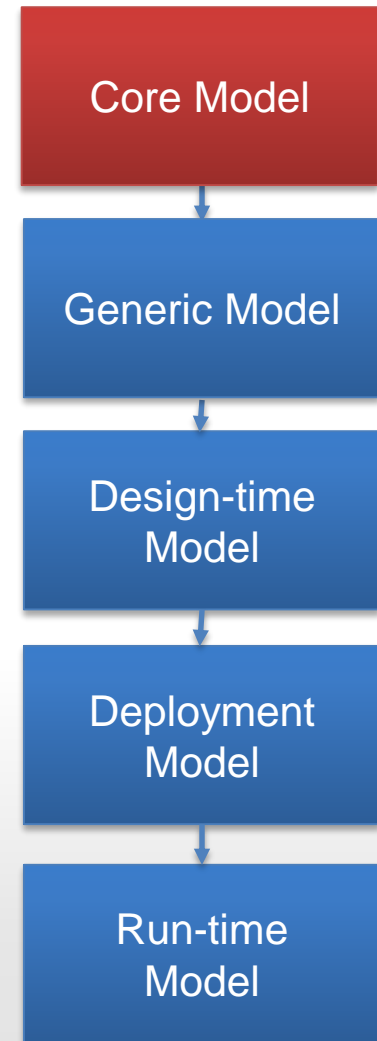
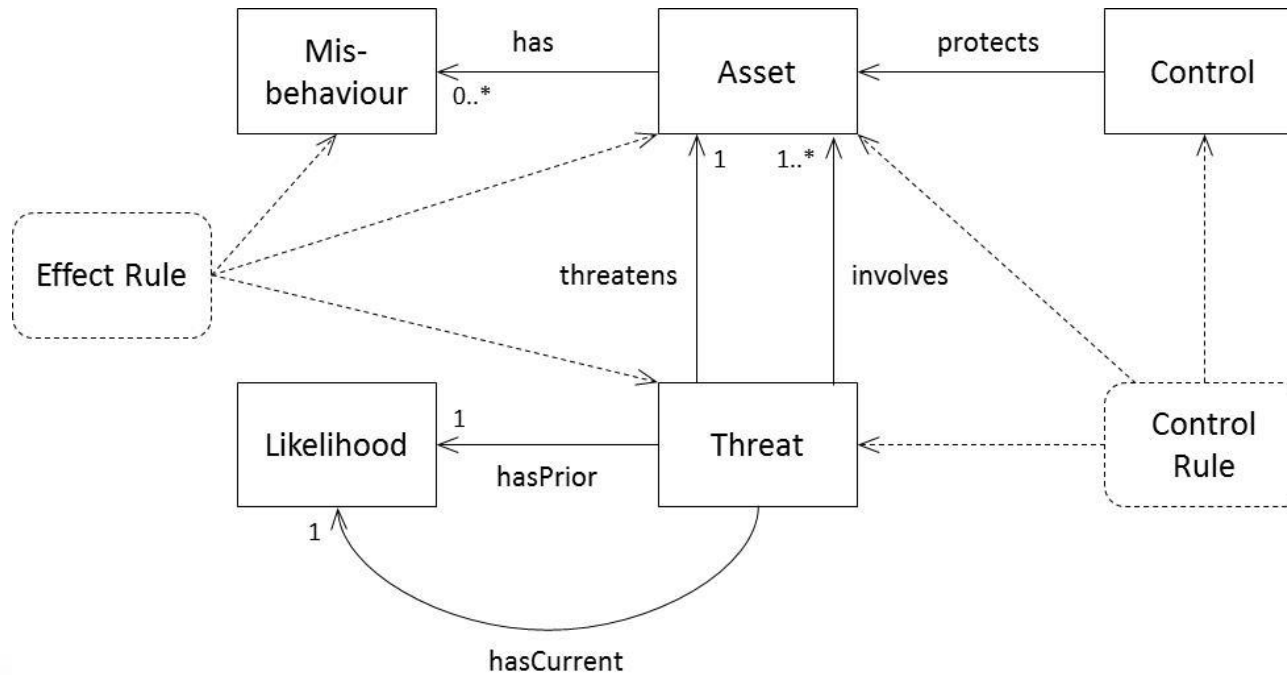
Semantic Models of Trust and Trustworthiness



Secure System Designer

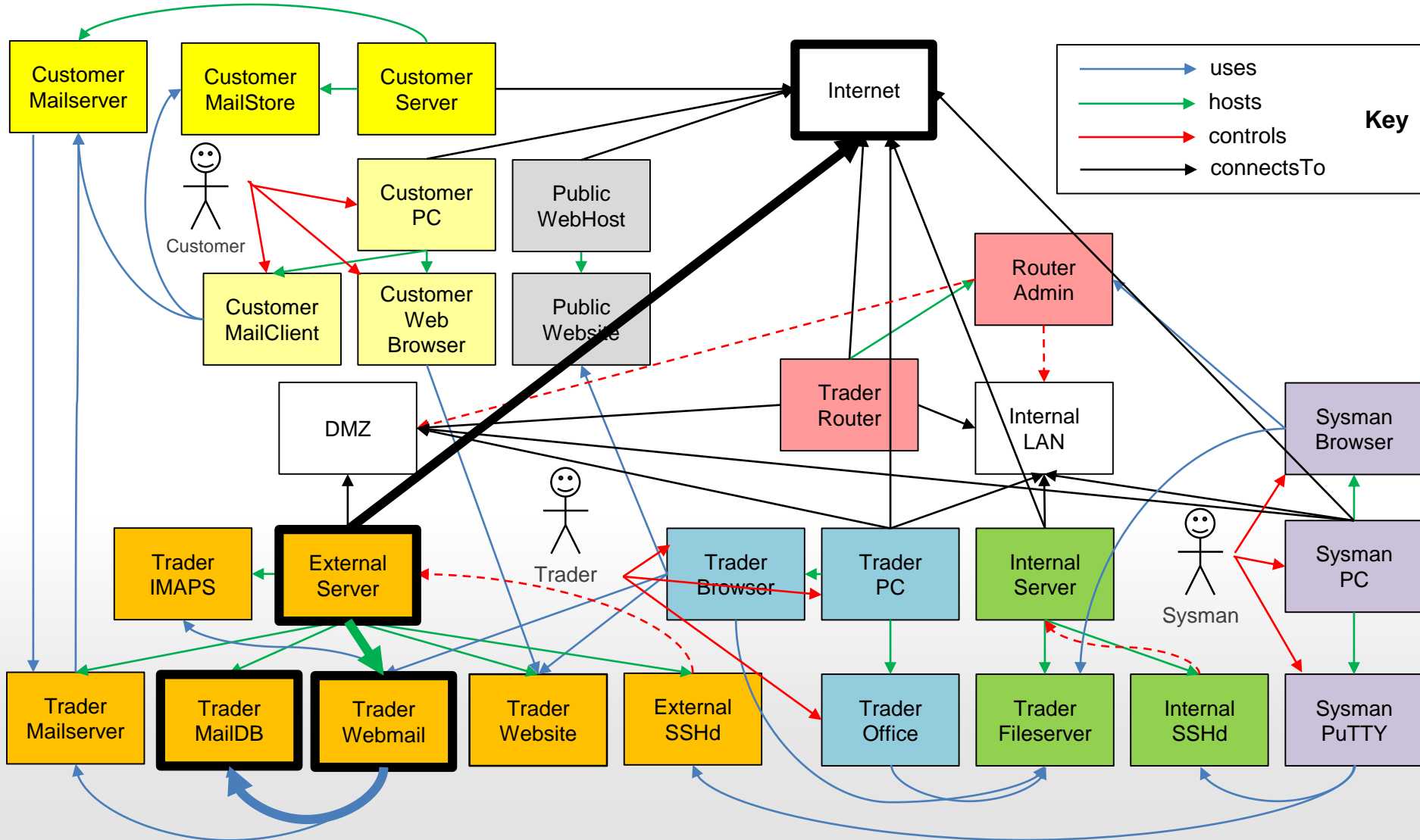
- Based on work done in SERSCIS and OPTET, and now being developed in several projects
- GUI for systems modelling
- Fully automated threat identification
- Objective, reproducible results
- Threats based:
 - RFC 4949 action/consequence combinations
 - CVE analysis
- Controls targeting UK Cyber Essentials scheme
- Reporting capabilities
- RDF system model encoding for knowledge reuse

Modelling Threats and Assessing Risks



- Core model: underpins the basic modelling approach and tooling
 - created by semantics experts
- Risks are related to threats, likelihood and consequent asset or system misbehaviour

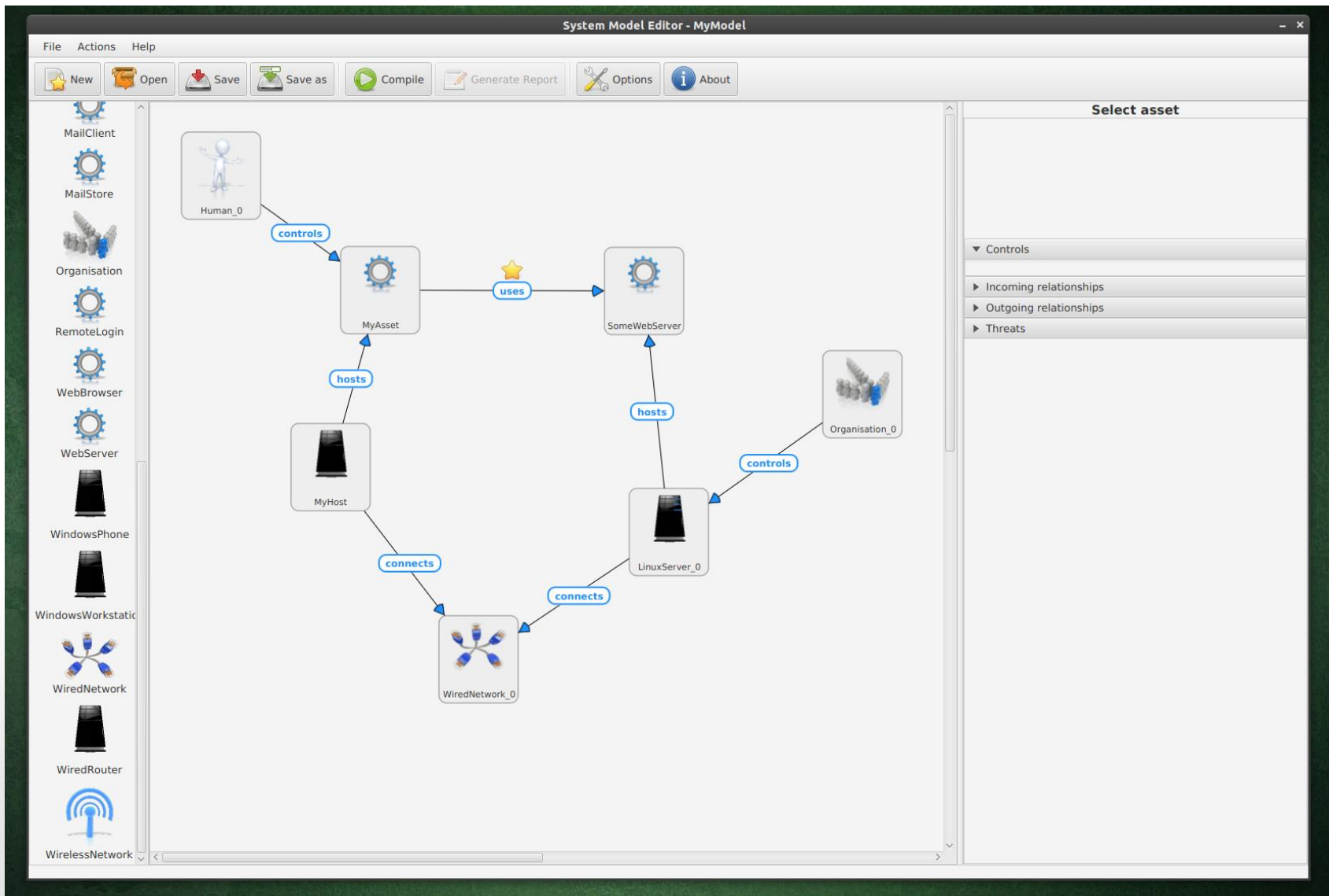
Example: SME Network Analysis



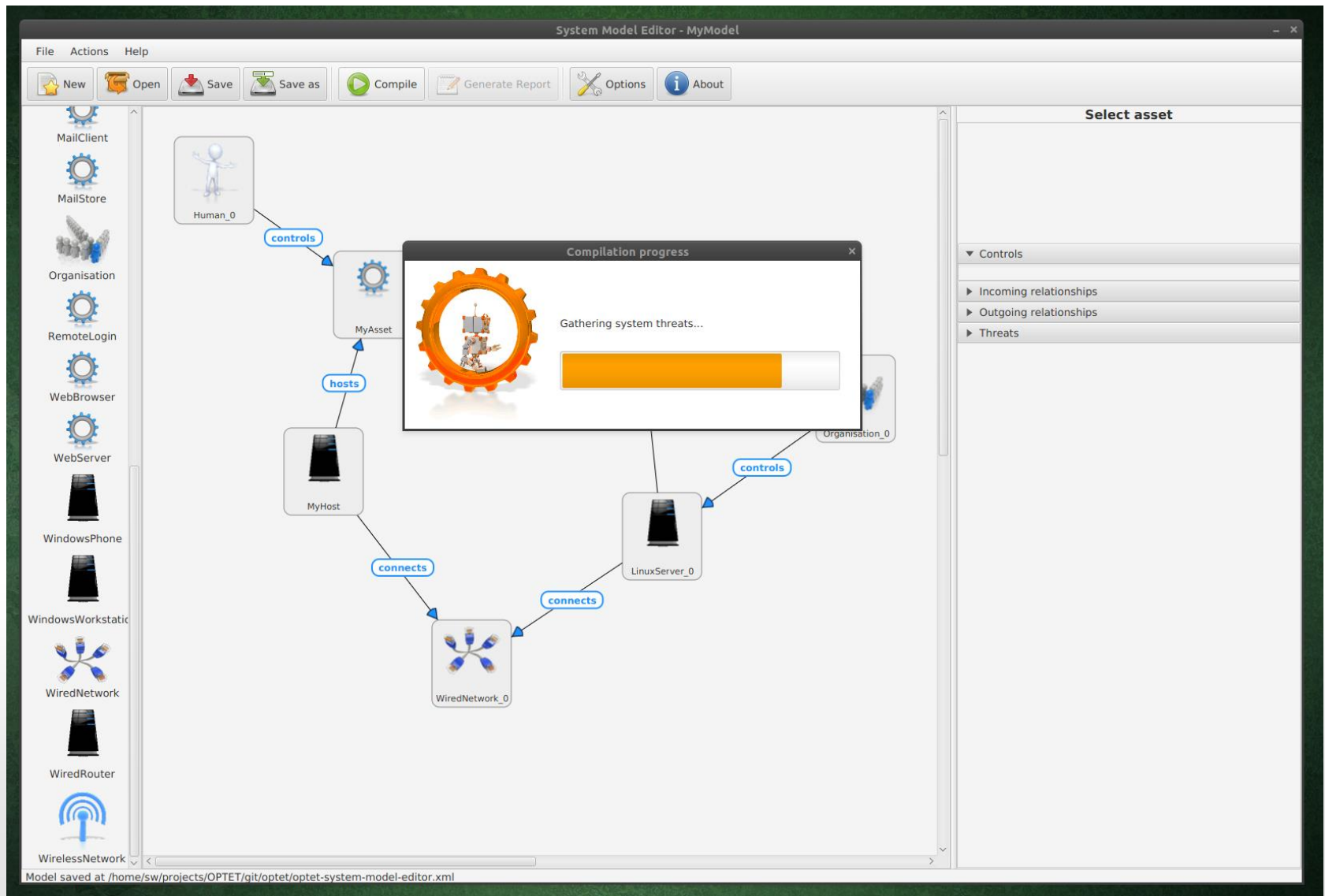
Threat Modelling

Stefanie Wiegand

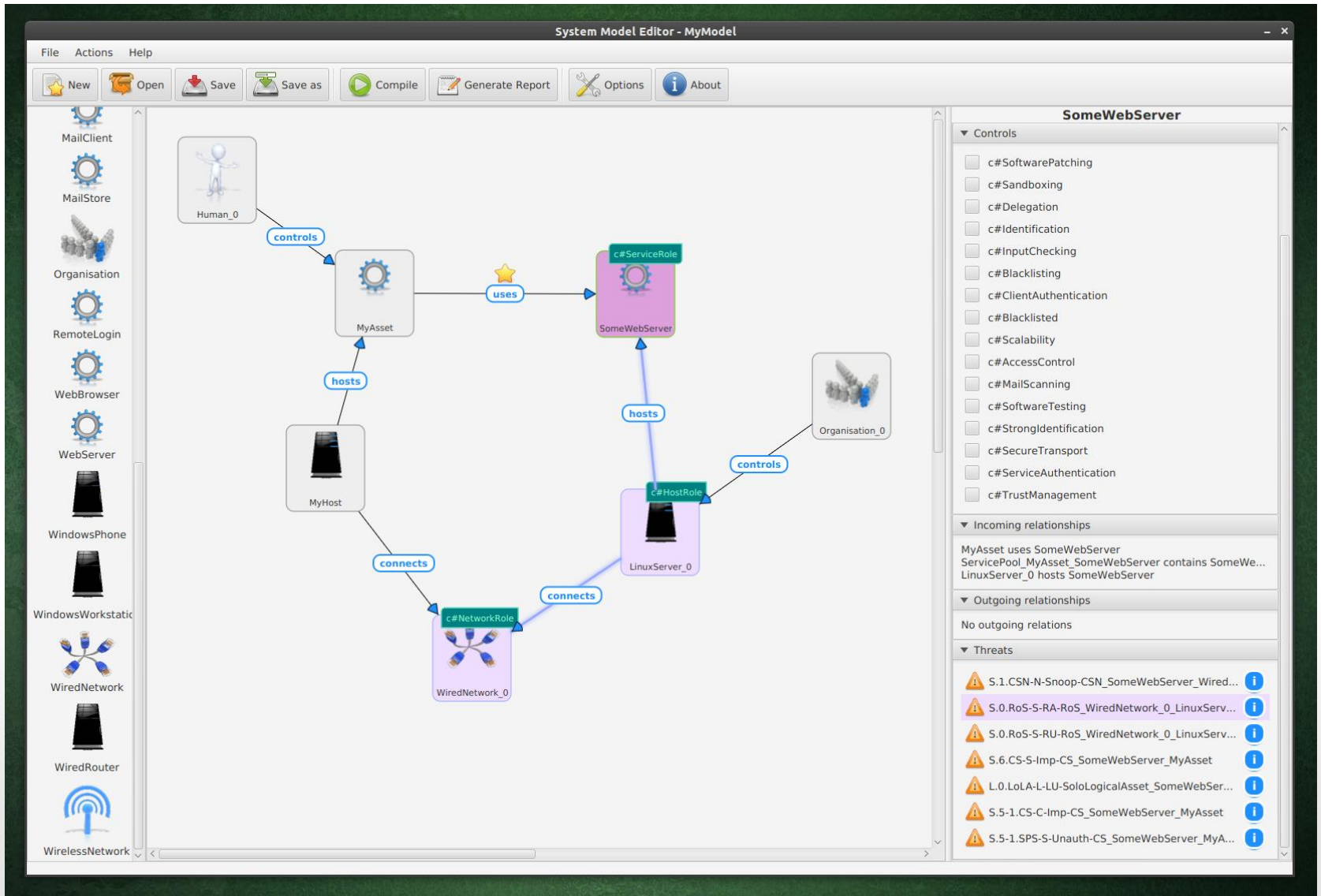
Building the Model



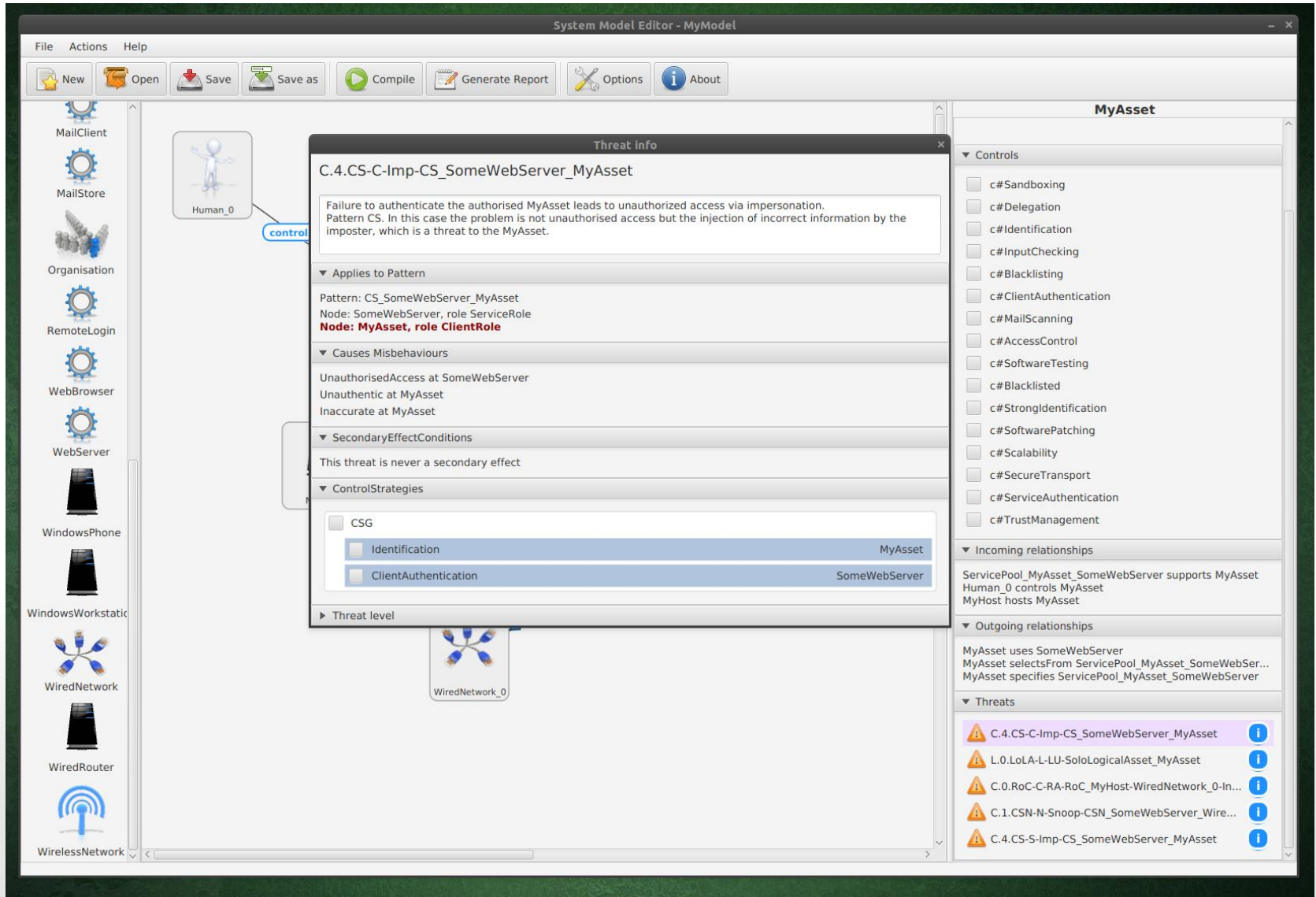
Compiling the Model



Analysing the Model



Analysing the Model



The screenshot shows the 'System Model Editor - MyModel' interface. A 'Threat info' dialog box is open, displaying details for the threat 'C.4.CS-C-Imp-CS_SomeWebServer_MyAsset'. The dialog includes a description, applicable patterns, misbehaviours, secondary effect conditions, and control strategies. The right-hand panel, titled 'MyAsset', lists various controls (e.g., c#Sandboxing, c#Delegation) and shows incoming and outgoing relationships. A list of threats is also visible at the bottom of the right panel.

Threat info

C.4.CS-C-Imp-CS_SomeWebServer_MyAsset

Failure to authenticate the authorised MyAsset leads to unauthorized access via impersonation. Pattern CS. In this case the problem is not unauthorised access but the injection of incorrect information by the imposter, which is a threat to the MyAsset.

▼ Applies to Pattern

Pattern: CS_SomeWebServer_MyAsset
Node: SomeWebServer, role ServiceRole
Node: MyAsset, role ClientRole

▼ Causes Misbehaviours

UnauthorisedAccess at SomeWebServer
Unauthentic at MyAsset
Inaccurate at MyAsset

▼ SecondaryEffectConditions

This threat is never a secondary effect

▼ ControlStrategies

- CSG
 - Identification MyAsset
 - ClientAuthentication SomeWebServer

► Threat level

MyAsset

▼ Controls

- c#Sandboxing
- c#Delegation
- c#Identification
- c#InputChecking
- c#Blacklisting
- c#ClientAuthentication
- c#MailScanning
- c#AccessControl
- c#SoftwareTesting
- c#Blacklisted
- c#StrongIdentification
- c#SoftwarePatching
- c#Scalability
- c#SecureTransport
- c#ServiceAuthentication
- c#TrustManagement

▼ Incoming relationships

ServicePool_MyAsset_SomeWebServer supports MyAsset
Human_0 controls MyAsset
MyHost hosts MyAsset

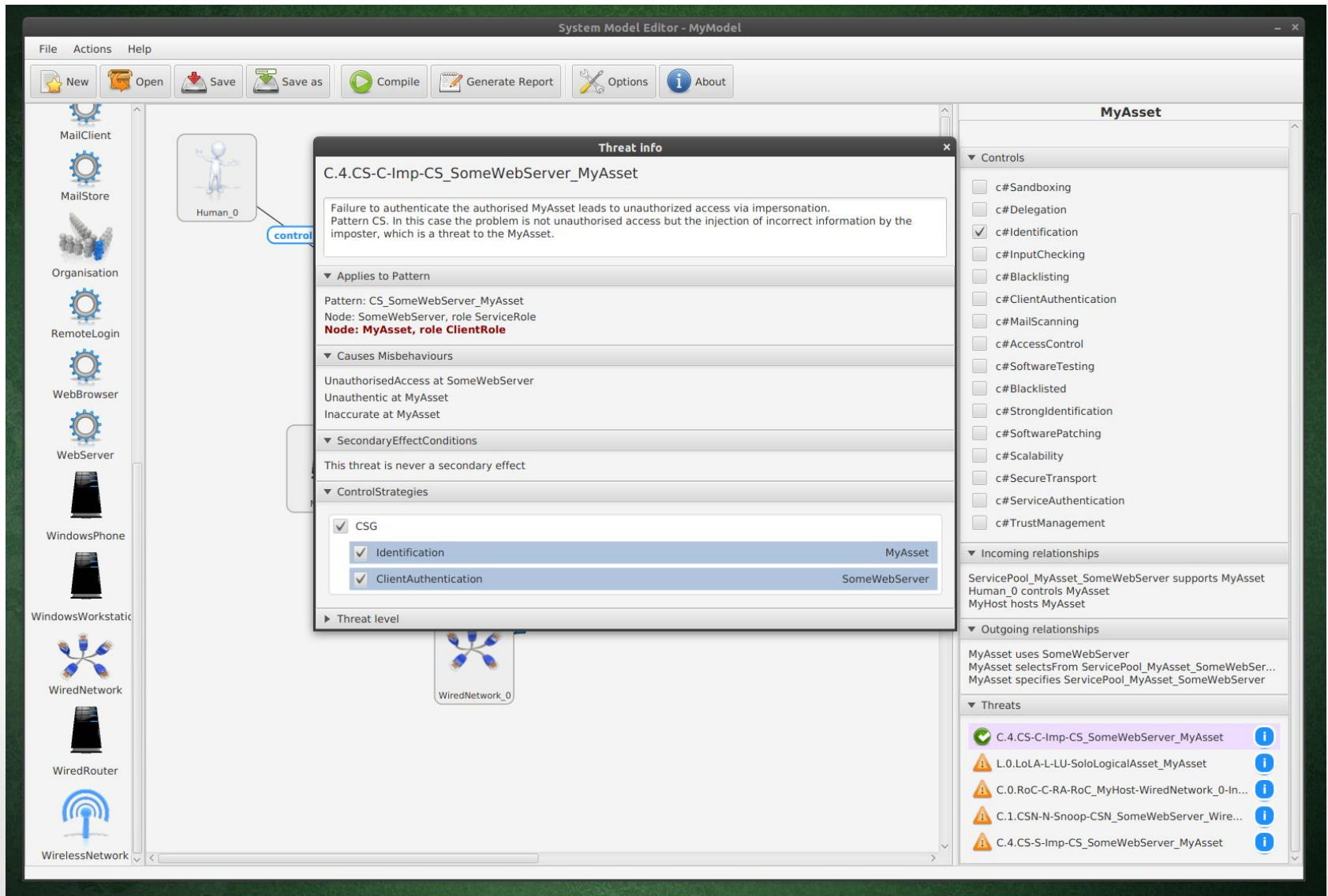
▼ Outgoing relationships

MyAsset uses SomeWebServer
MyAsset selectsFrom ServicePool_MyAsset_SomeWebSer...
MyAsset specifies ServicePool_MyAsset_SomeWebServer

▼ Threats

- C.4.CS-C-Imp-CS_SomeWebServer_MyAsset
- L.0.LoLA-L-LU-SoloLogicalAsset_MyAsset
- C.0.RoC-C-RA-RoC_MyHost-WiredNetwork_0-In...
- C.1.CSN-N-Snoop-CSN_SomeWebServer_Wire...
- C.4.CS-S-Imp-CS_SomeWebServer_MyAsset

Analysing the Model



The screenshot displays the 'System Model Editor - MyModel' interface. A 'Threat info' dialog box is open, showing details for the threat 'C.4.CS-C-Imp-CS_SomeWebServer_MyAsset'. The dialog includes a description, applicable patterns, misbehaviours, secondary effect conditions, and control strategies.

Threat info dialog content:

- Title:** C.4.CS-C-Imp-CS_SomeWebServer_MyAsset
- Description:** Failure to authenticate the authorised MyAsset leads to unauthorized access via impersonation. Pattern CS. In this case the problem is not unauthorised access but the injection of incorrect information by the imposter, which is a threat to the MyAsset.
- Applies to Pattern:**
 - Pattern: CS_SomeWebServer_MyAsset
 - Node: SomeWebServer, role ServiceRole
 - Node: MyAsset, role ClientRole**
- Causes Misbehaviours:**
 - UnauthorisedAccess at SomeWebServer
 - Unauthentic at MyAsset
 - Inaccurate at MyAsset
- SecondaryEffectConditions:**
 - This threat is never a secondary effect
- ControlStrategies:**
 - CSG
 - Identification (MyAsset)
 - ClientAuthentication (SomeWebServer)
- Threat level:** (collapsed)

The main interface shows a 'MyAsset' control list on the right and a 'Threats' list at the bottom right. The 'Threats' list includes:

- C.4.CS-C-Imp-CS_SomeWebServer_MyAsset (Info icon)
- L.0.LoLA-L-LU-SoloLogicalAsset_MyAsset (Warning icon)
- C.0.RoC-C-RA-RoC_MyHost-WiredNetwork_0-In... (Warning icon)
- C.1.CSN-N-Snoop-CSN_SomeWebServer_Wire... (Warning icon)
- C.4.CS-S-Imp-CS_SomeWebServer_MyAsset (Warning icon)



www.it-innovation.soton.ac.uk