5G-ENSURE

(Project Number— 671562)

A Trust Model for 5G

5G-ENSURE Workshop, ETSI Security Week
Sophia Antipolis, 16 June 2017

Mike Surridge,
University of Southampton IT Innovation Centre
ms _at_ it-innovation.soton.ac.uk

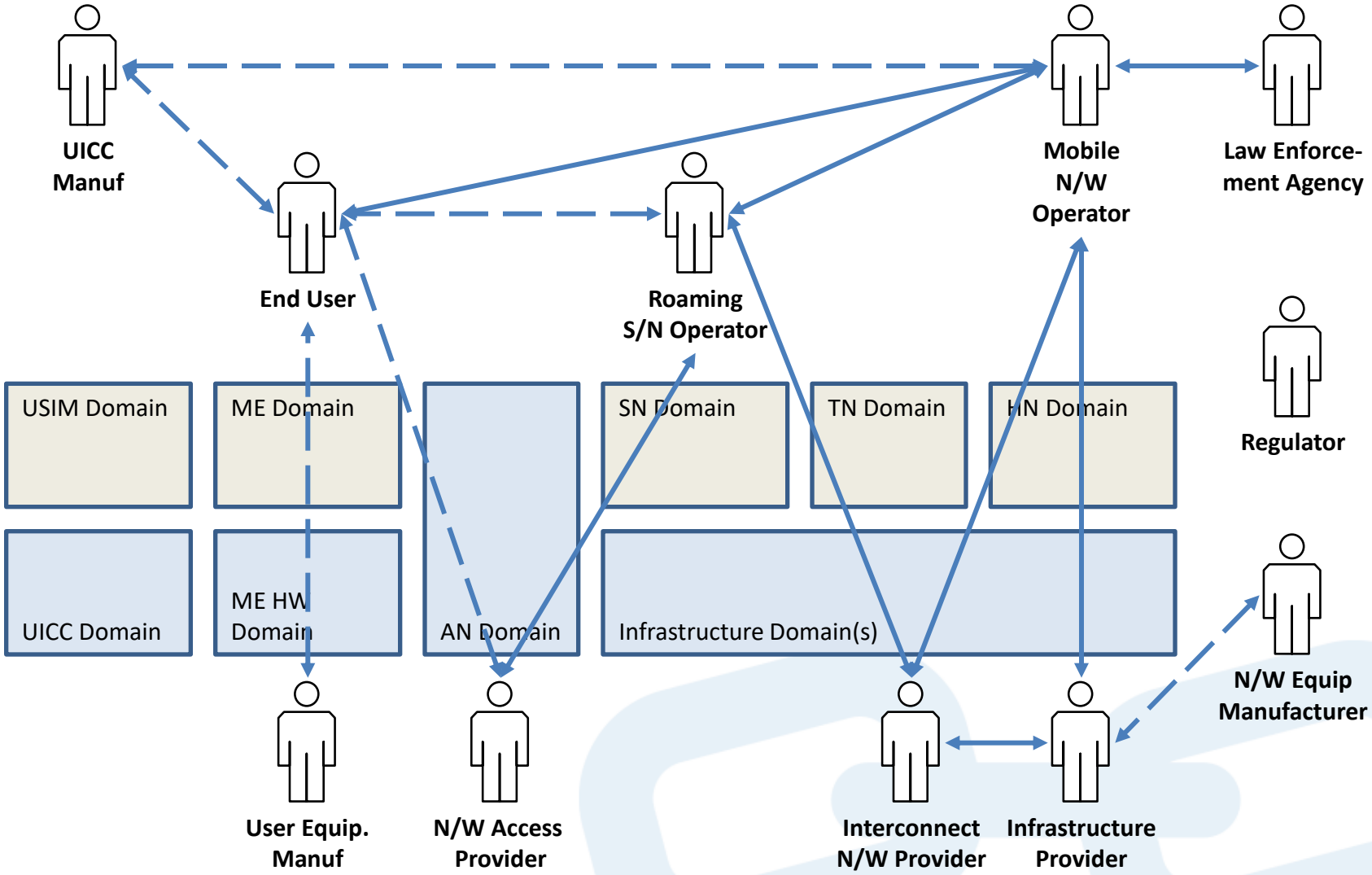
What is Trust?

- Trust = firm belief in the reliability, truth, or ability of someone or something (OED)
  - in practice, trust is (one possible) response to risk
- Risks associated with a socio-technical system can be addressed by
  - refusing to use the risky system features (risk avoidance)
  - introducing security measures (risk reduction)
  - making another actor responsible (risk transfer)
  - assuming the risk will not cause harm (risk acceptance)
- Acceptance and transfer both involve trusting one or more actors or components, explicitly or implicitly

Trust in 4G Networks

- Based on three main precepts
  - actors are relatively few in number and known to each other
  - mutual trust is largely between actors with a similar set of roles and/or expectations, e.g. between MNOs
  - market segmentation means they usually don't compete in situations where cooperation is needed, e.g. across borders
- Example: MNOs will operate as home network and serving network providers in different regions
  - they take different roles in different regions
  - they have similar concerns and expectations of each other when acting in each of these roles

Main Elements of the 4G Trust Model



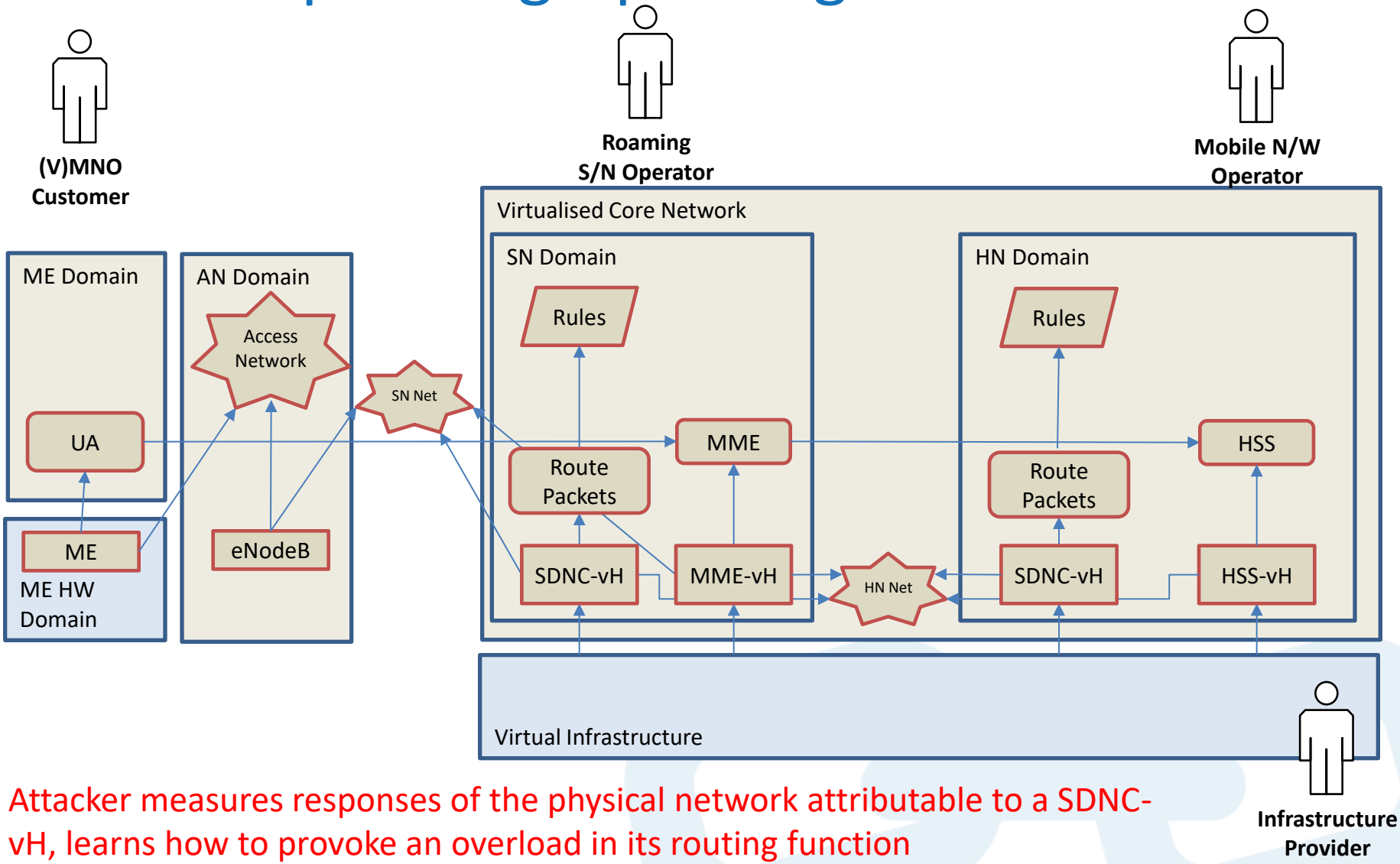
5G Trust Challenges

- The number of stakeholders will increase
  - virtualisation introduces new roles and allows greater distribution of and competition for each roles
- Stakeholder interests will be more diverse
  - many networks will be governed by ‘vertical’ stakeholders rather than traditional MNOs
  - network functions may be provided by specialised operators
- New risks will arise from the complexity and dynamicity of these virtualised systems and business networks
- We cannot assume actors have the same understanding of potential risks or available risk treatments

5G-ENSURE Approach to Trust

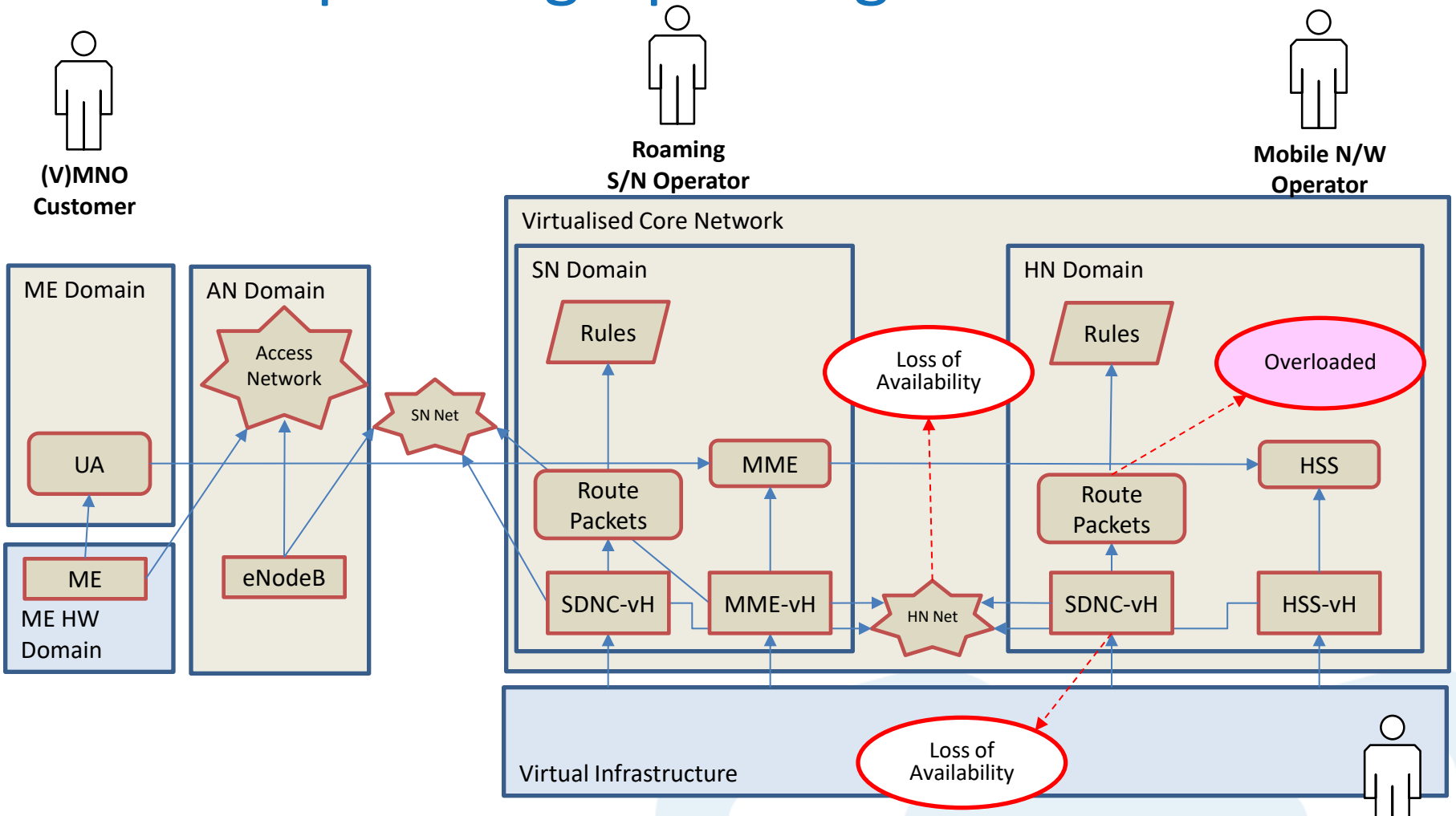
- Identify risks that are new or require new management strategies in 5G networks
  - 31 scenarios collected by the consortium
  - 43 use cases identified in these scenarios that potentially involve novel risks or novel risk management strategies
- Identify how these affect stakeholders, and how they may be mitigated by which stakeholders
- Rigorously specify trust assumptions as a fundamental part of the 5G-ENSURE security architecture
  - i.e. how stakeholder(s) are expected to share the responsibility for managing these (and other) risks

Example: Fingerprinting DoS on SDNC



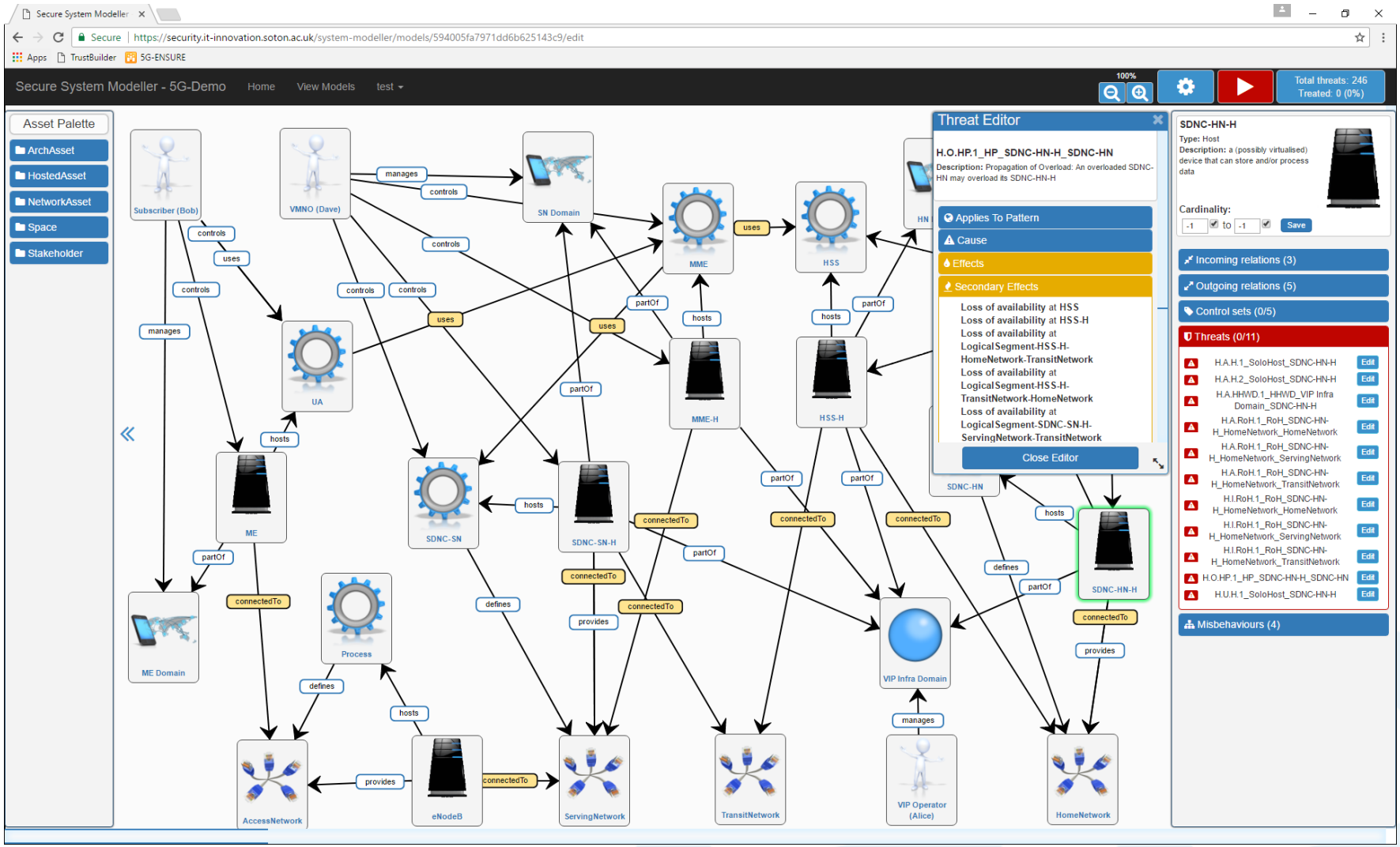
Attacker measures responses of the physical network attributable to a SDNC-vH, learns how to provoke an overload in its routing function

Example: Fingerprinting DoS on SDNC



The attack overloads the routing process, leading to loss of availability in the SDNC and the network it provides

Trust Builder: Analysing Risks



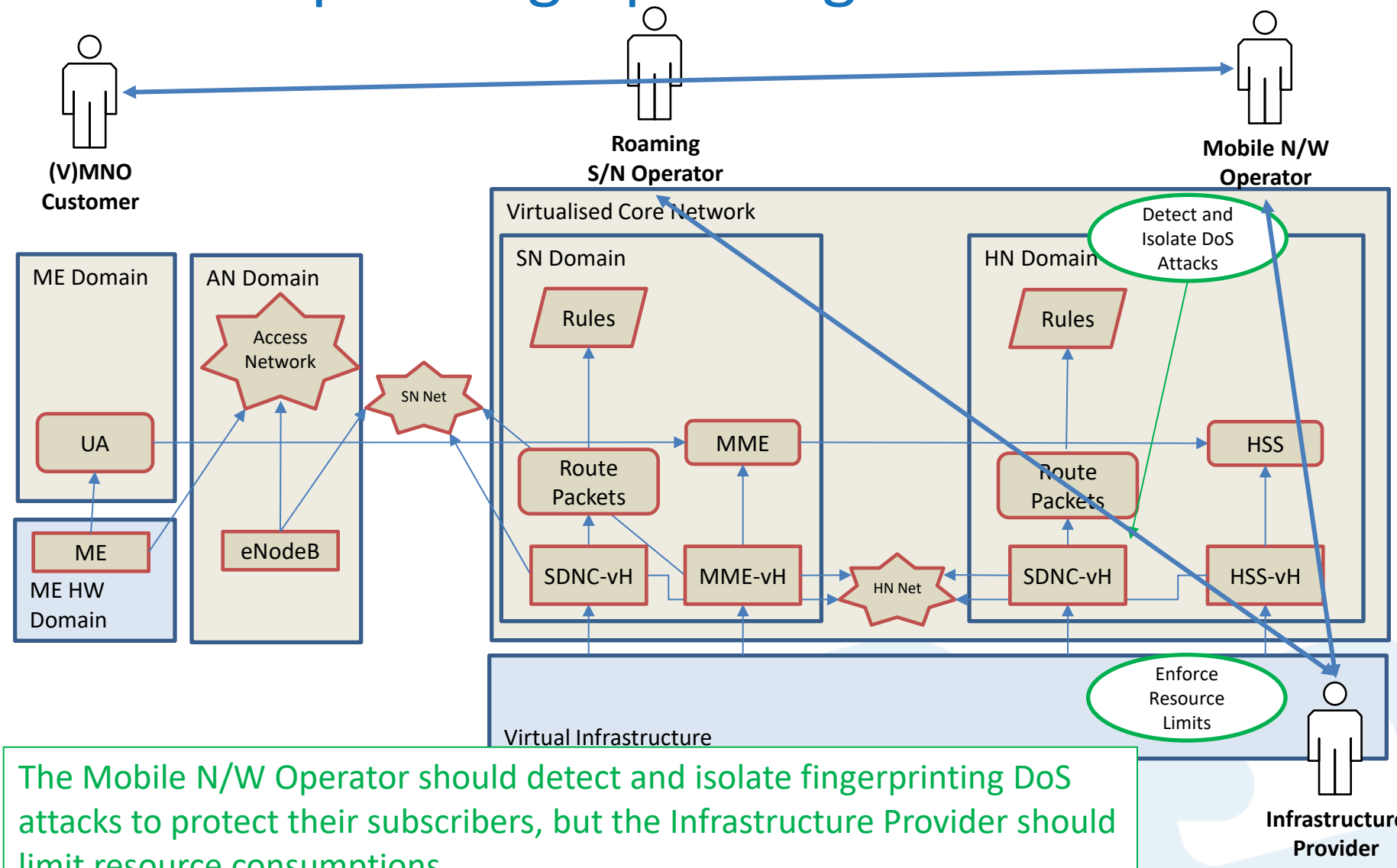
Example: Fingerprinting DoS on SDNC

- The attack on the home network SDNC produces two main secondary effect cascades
  - loss of availability of home network HSS affecting access to serving networks for subscribers
  - overload spreading to the virtual infrastructure and affecting other virtualised network slices
- Who is responsible for managing these risks, e.g.
  - should the Roaming N/W Operator provide an authentication proxy for subscribers whose home network HSS is down?
  - should the Mobile N/W Operator guarantee to limit their load on the virtualised infrastructure?

Trust Decision Catalogue (Extract)

Trustor	Trustee	Trust Assumptions
(V)MNO Customer	Mobile N/W Operator	The customer expects the MNO to provide them with an agreed upon service, which does not exceed the SLA. If the MNO fails to provide secure and reliable service, the MNO may transfer trust to another stakeholder such as Network Access Provider, SNO, or HNO depending on the cause of the issue.
(V)MNO Customer	Virtualised Mobile N/W Operator	As above, except that the VMNO may transfer responsibilities to the Virtualised Infrastructure Provider.
Infrastructure Provider	Mobile Network Operator	The infrastructure provider trusts the MNO will adhere to the SLA, which will prevent them from causing disruptions to the infrastructure and its clients. If the VMNO are using more than they are allocated, they may transfer trust to the client which might be causing the issues. The analysis shows such events from T_UC5.3_1.
…	…	…

Example: Fingerprinting DoS on SDNC



The Mobile N/W Operator should detect and isolate fingerprinting DoS attacks to protect their subscribers, but the Infrastructure Provider should limit resource consumptions

Current Status and Future Work

- Currently analysed trust assumptions in about 70% of our scenarios and potential threats
  - so far 34 trust decisions have been identified involving dependencies between stakeholders (or their components)
- Next step is to decide how (some of) these decisions should be resolved when managing risks using the 5G-ENSURE security architecture and security enablers
- The 5G-ENSURE security architecture (due Oct'17) will include trust assumptions
- Ultimate objective: include such trust specifications in future security standards

5G-ENSURE

(Project Number— 671562)

A Trust Model for 5G

5G-ENSURE Workshop, ETSI Security Week
Sophia Antipolis, 16 June 2017

Mike Surridge,
University of Southampton IT Innovation Centre
ms _at_ it-innovation.soton.ac.uk