



# 5G-ENSURE

(Project Number— 671562)

## Trust Modelling in 5G Networks

SecSoN Workshop, ACM SIGCOMM 2018  
Budapest, 24 August 2018

Mike Surridge,  
University of Southampton IT Innovation Centre  
[ms\\_at\\_it-innovation.soton.ac.uk](mailto:ms_at_it-innovation.soton.ac.uk)



# Overview

- ▣ How we defined trust: risks and interdependency
- ▣ 5G Trust challenges: virtualisation and new actors
- ▣ Machine understandable threat modelling
- ▣ Example of 5G specific threats from 5G-ENSURE
- ▣ Trust survey results and implications
- ▣ Modelling results: threats to trust, root causes and control strategies, quantification of trust
- ▣ Stakeholder dependencies and responsibilities
- ▣ Status and future work

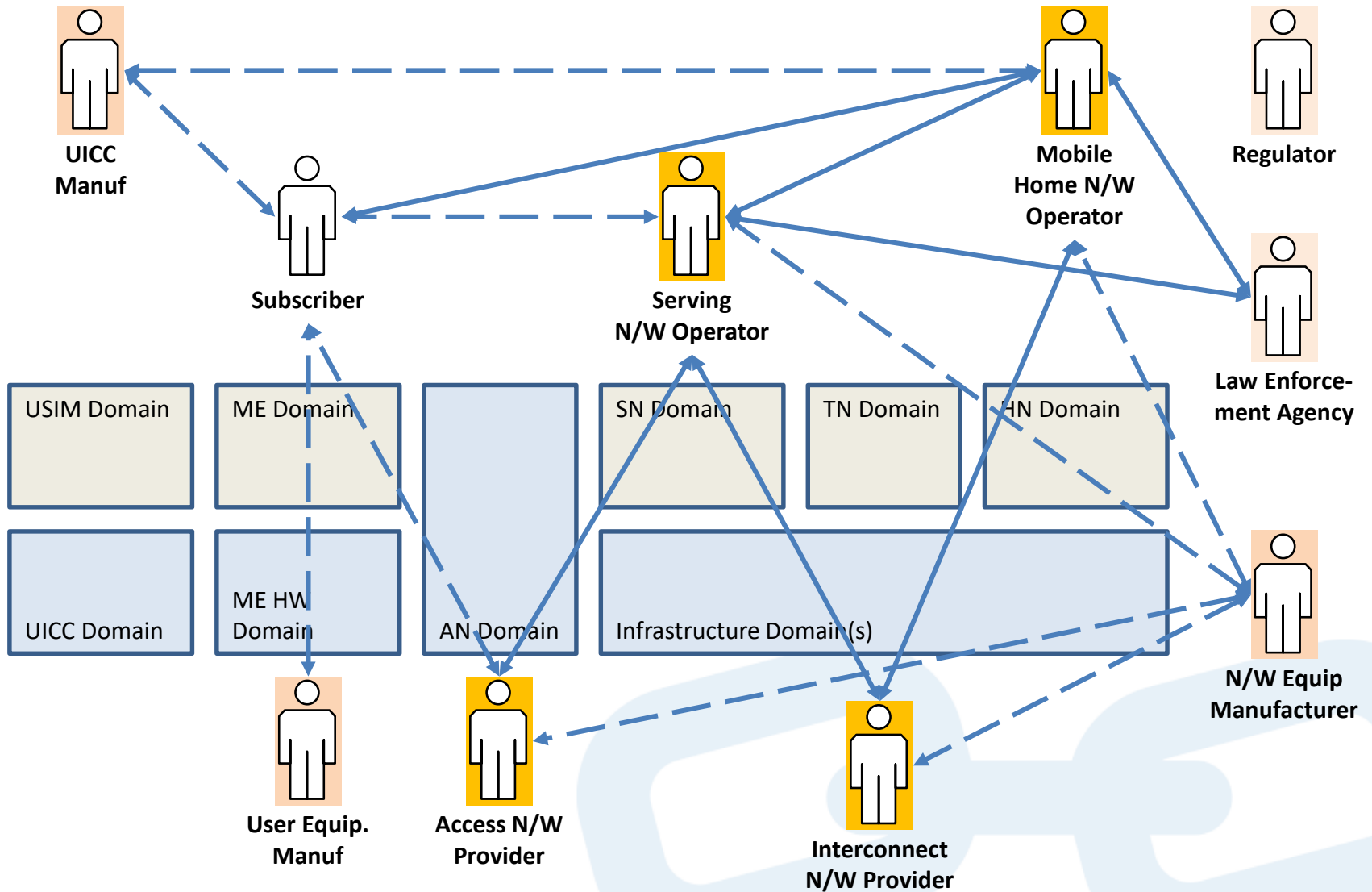


# What is Trust?

- 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)
  - assuming the risk will not cause harm (risk acceptance)
  - introducing security measures (risk reduction)
  - making another actor responsible (risk transfer)
- All except the first involve explicit or implicit trust in actors or components of the socio-technical system



# Trust Dependencies in 4G Networks



# 5G Trust Challenges

- Trust in 4G networks is based on three main precepts
  - actors are relatively few in number and known to each other
  - mutual trust is largely between actors with similar roles and expectations, e.g. all n/w operators have similar roles
  - market segmentation limits competition and creates a need for cooperation, e.g. across borders
- In 5G networks, especially vertical applications we have
  - more potential n/w operators with more diverse interests
  - less common understanding of security requirements, solutions and dependencies in 'vertical' applications
  - new dependencies and risks due to extensive virtualisation



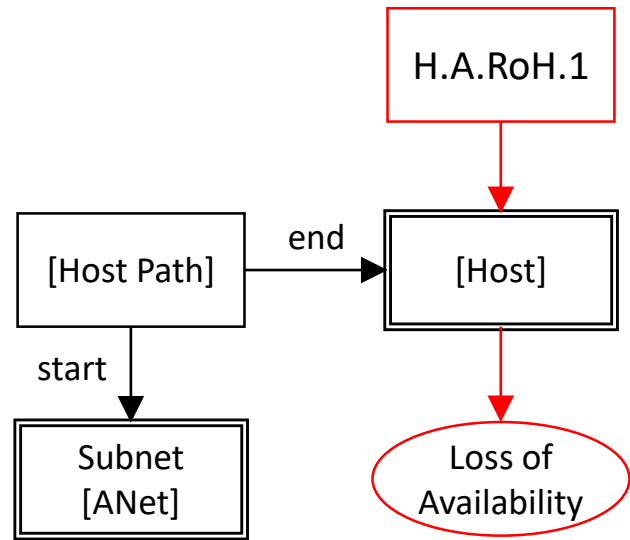
# 5G-ENSURE Approach to Trust

- 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
- Analyse how these and other common threats would be addressed using the 5G-ENSURE security architecture
  - analysed using a semantic modelling approach and machine reasoning to ensure nothing is overlooked
  - handled by the Trust Builder tool developed in the project
- Determine trust dependencies between stakeholders



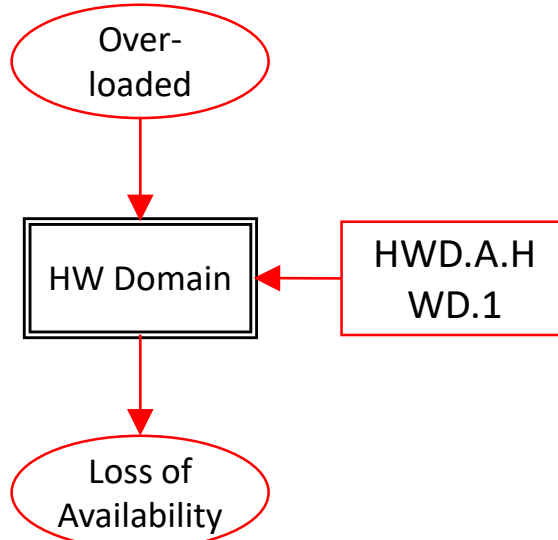
# Example Threats

## Primary Threat



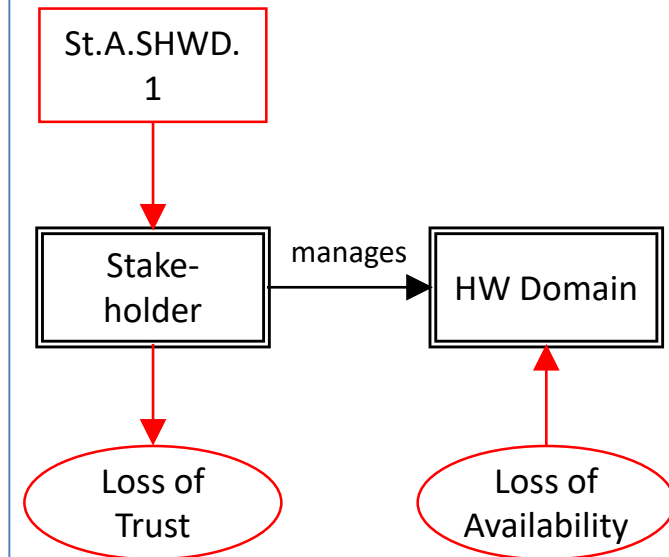
Remote Anonymous Exploit Compromises Device Availability

## Secondary Threat



Overload on the HW Domain causes a loss of Availability

## Threat to Trust



This causes the HW domain operator to lose trust in the network

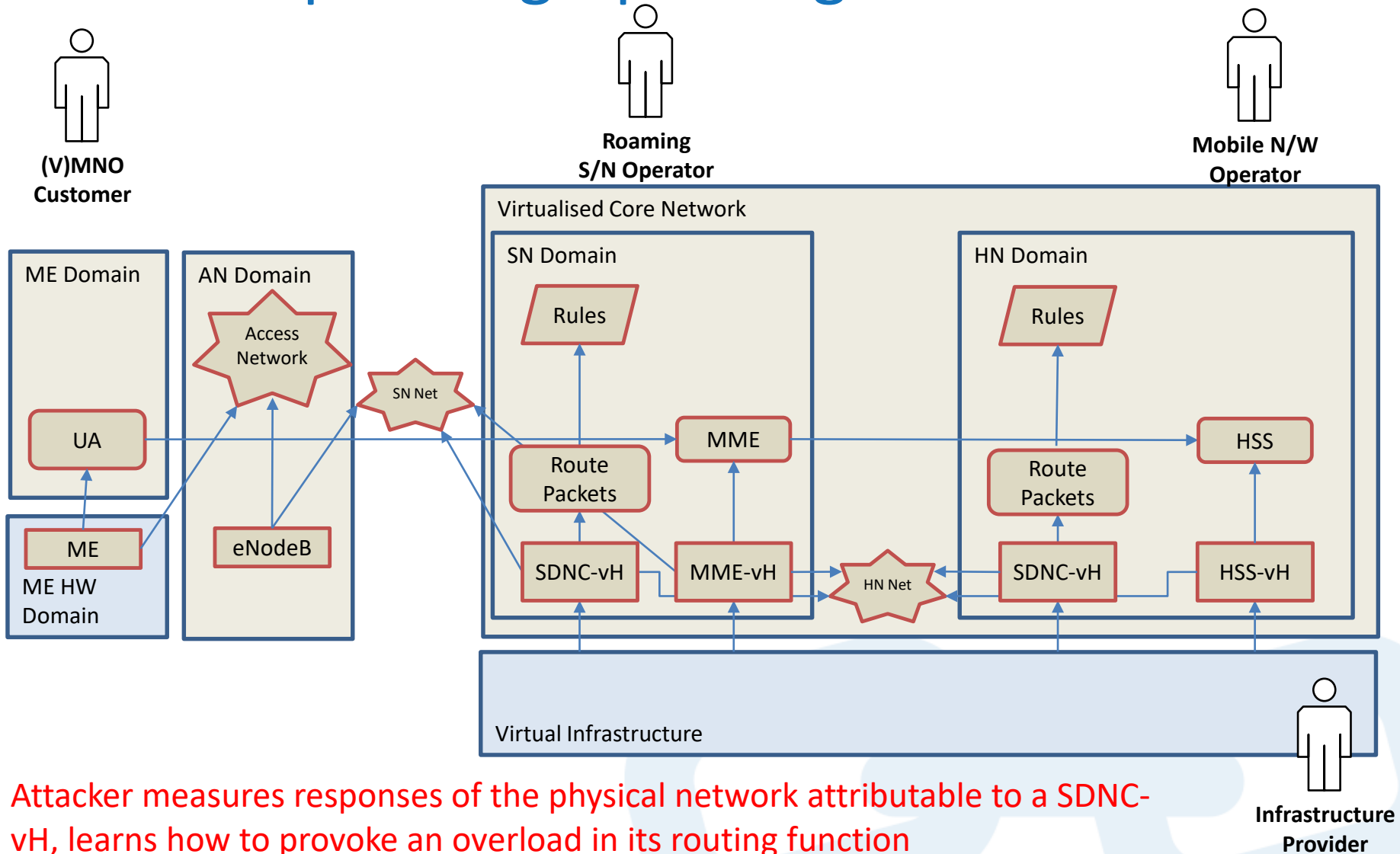


# Threat Coverage

- Primary threat models covered
  - internal bugs (including dishonest stakeholders)
  - unauthorised local and remote access
  - remote exploits against devices and services
  - remote injection via services on back end databases
  - impersonation (spoofing) and interception (snooping) attacks
- Secondary threats covered the propagation of overload, unavailability, loss of integrity, loss of control,...
- Added specialised threats against 5G Networks from the scenarios developed by 5G-ENSURE partners



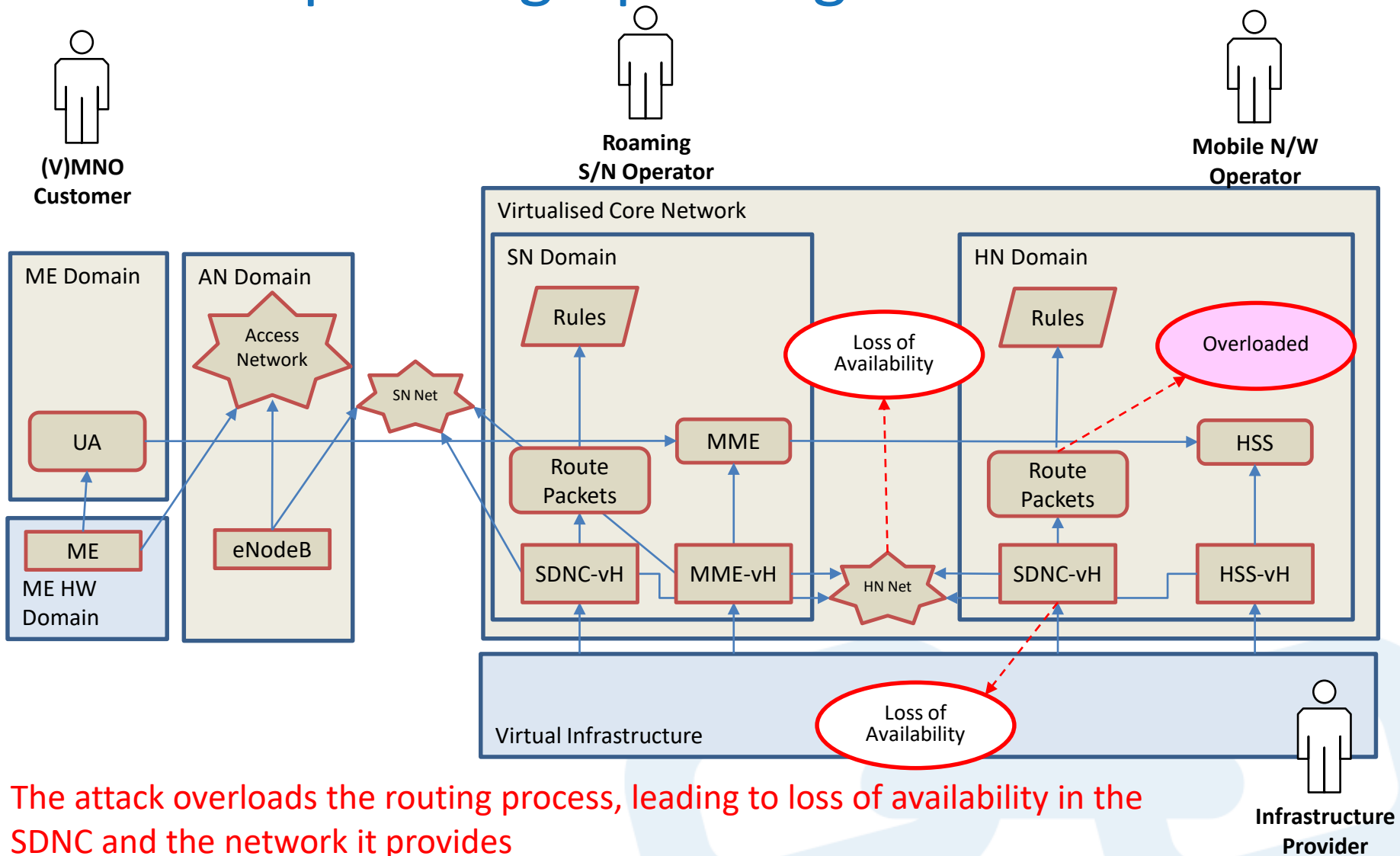
# Example: Fingerprinting DoS on SDNC



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

Secure System Modeller - 5G-Demo

Home View Models test

100% Total threats: 246 Treated: 0 (0%)

Asset Palette

- ArchAsset
- HostedAsset
- NetworkAsset
- Space
- Stakeholder

**Threat Editor**

H.O.HP.1\_HP\_SDNC-HN-H\_SDNC-HN

Description: Propagation of Overload: An overloaded SDNC-HN may overload its SDNC-HN-H

Applies To Pattern

Cause

Effects

Secondary Effects

- Loss of availability at HSS
- Loss of availability at HSS-H
- Loss of availability at LogicalSegment-HSS-H
- Loss of availability at LogicalSegment-HSS-H
- TransitNetwork.HomeNetwork
- Loss of availability at LogicalSegment-SDNC-SN-H
- ServingNetwork.TransitNetwork
- Loss of availability at LogicalSegment-SDNC-SN-H
- ServingNetwork.TransitNetwork

Close Editor

SDNC-HN

SDNC-HN-H

SDNC-HN-H

Type: Host

Description: a (possibly virtualised) device that can store and/or process data

Cardinality: -1 to -1 Save

Incoming relations (3)

Outgoing relations (5)

Control sets (0/5)

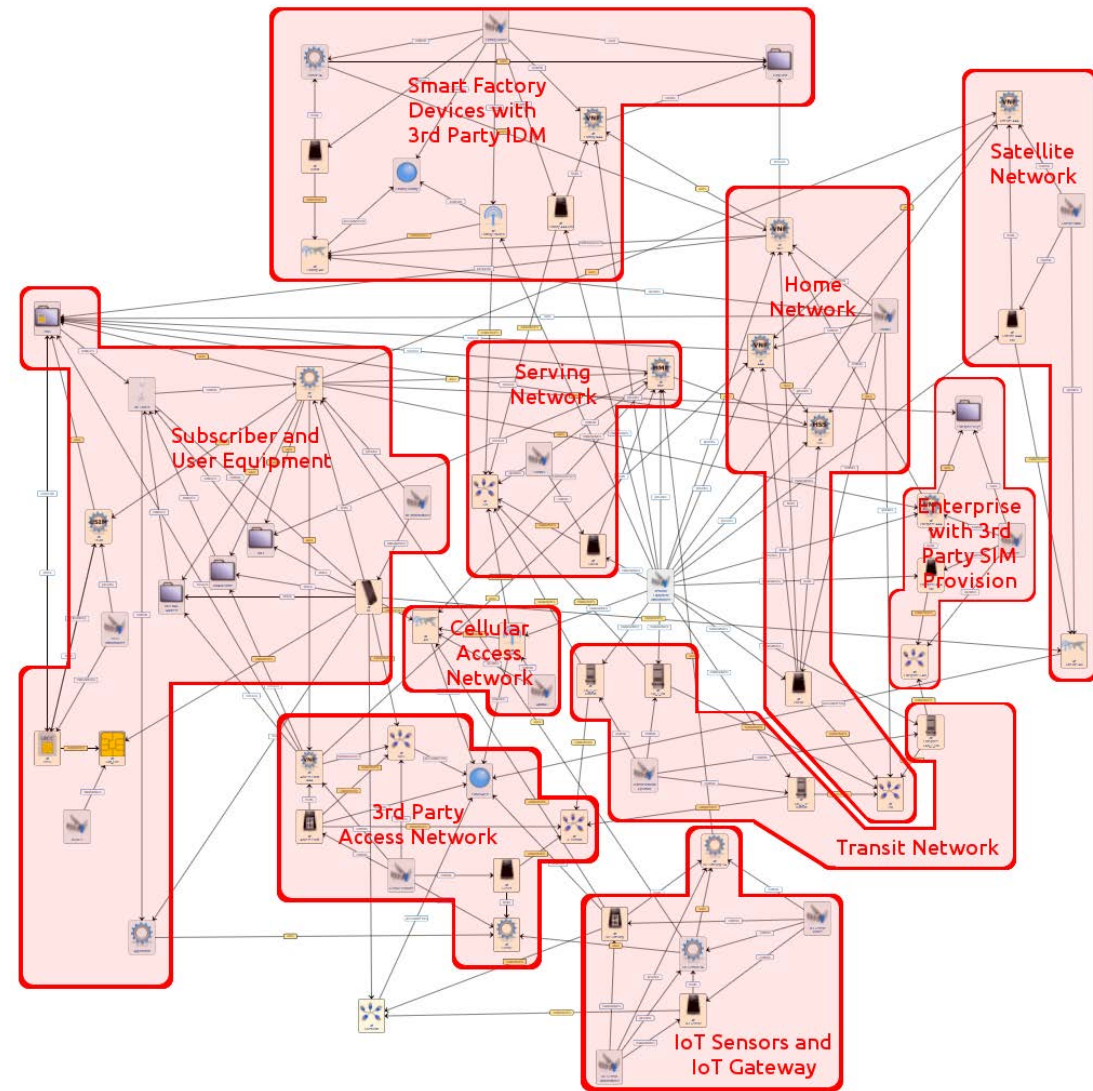
Threats (0/11)

- H.A.H.1\_SoloHost\_SDNC-HN-H Edit
- H.A.H.2\_SoloHost\_SDNC-HN-H Edit
- H.A.H.HWD.1\_HHWD\_VIP Infra Domain\_SDNC-HN-H Edit
- H.A.RoH.1\_RoH\_SDNC-HN-H\_HomeNetwork\_HomeNetwork Edit
- H.A.RoH.1\_RoH\_SDNC-HN-H\_HomeNetwork\_ServingNetwork Edit
- H.A.RoH.1\_RoH\_SDNC-HN-H\_HomeNetwork\_TransitNetwork Edit
- H.I.RoH.1\_RoH\_SDNC-HN-H\_HomeNetwork\_HomeNetwork Edit
- H.I.RoH.1\_RoH\_SDNC-HN-H\_HomeNetwork\_ServingNetwork Edit
- H.I.RoH.1\_RoH\_SDNC-HN-H\_HomeNetwork\_TransitNetwork Edit
- H.O.HP.1\_HP\_SDNC-HN-H\_SDNC-HN Edit
- H.U.H.1\_SoloHost\_SDNC-HN-H Edit

Misbehaviours (4)



# Network Models



- In the 5G-ENSURE project we used two models
  - one capturing diversity of stakeholder roles (see left)
  - one capturing virtualisation using a MANO architecture
- For the paper we had to present only one model
  - used a simplified version of the first model
  - focused on the traditional 4G network roles
  - intended for comparison between 4G and 5G cases



# Measuring Trust

- ▢ Guided by a trust survey conducted by VTT (one of our 5G-ENSURE partners)
  - ▢ covered basic attitudes to technology, specific applications and potential threats
  - ▢ collected 53 responses, most from 'tech savvy' Scandinavians
- ▢ Main conclusions from the survey
  - ▢ risk management is a shared responsibility
  - ▢ almost any type of threat affects trust in the network
- ▢ We therefore weighted all threats equally
  - ▢ our measure of trust or dependency is the number of root cause threats prevented from causing a loss of trust



# Trust (Dependency) Finding Algorithm

For each stakeholder  $S$  (a potential trustor)

Find threats to trust  $\{T(S)\}$ : **handled by automated analysis in Trust Builder**

For each threat to trust

Find root cause threats  $\{R(T(S))\}$ : **automated analysis in Trust Builder**

For each root cause threat

Find control strategies that block the threat (or its secondary effects)

If the control strategy is used in the 5G-ENSURE security architecture

For each control

Find the asset where control is applied

Find the stakeholder(s) (trustees)  $\{Q\}$  who must implement it

For each trustee  $Q$  add +1 to the dependency of  $S$  on  $Q$





# Analysis: Causes of Loss of Trust

Trustor	Type of Threat					
	Remote Exploit on a Service	Remote Exploit on a Device	Network DoS Attack	Impersonation Attack	Snooping Attack	Internal Errors
Access N/W Operator		15				2
Home N/W Operator	323	132	96	48		13
Serving N/W Operator	150	70	50	25		8
Subscriber	523	311	140	122	6	44



# Analysis: Trust Dependencies

Trustor	Trustee						
	Access N/W Op	Home N/W Op	Serving N/W Op	Subscriber	ME Manuf	N/W Equip Manuf	UICC Manuf
Access N/W Operator	17					17	
Home N/W Operator	30	608	80	18		324	78
Serving N/W Operator	15	164	152	20		191	
Subscriber	59	804	283	159	56	471	177
Dependencies	104	968	363	38	56	1003	255

Significantly less trust in the Access N/W

Significantly more trust in the Home N/W

Reduced dependency on the Serving N/W



# Analysis: Expectations of Trustors

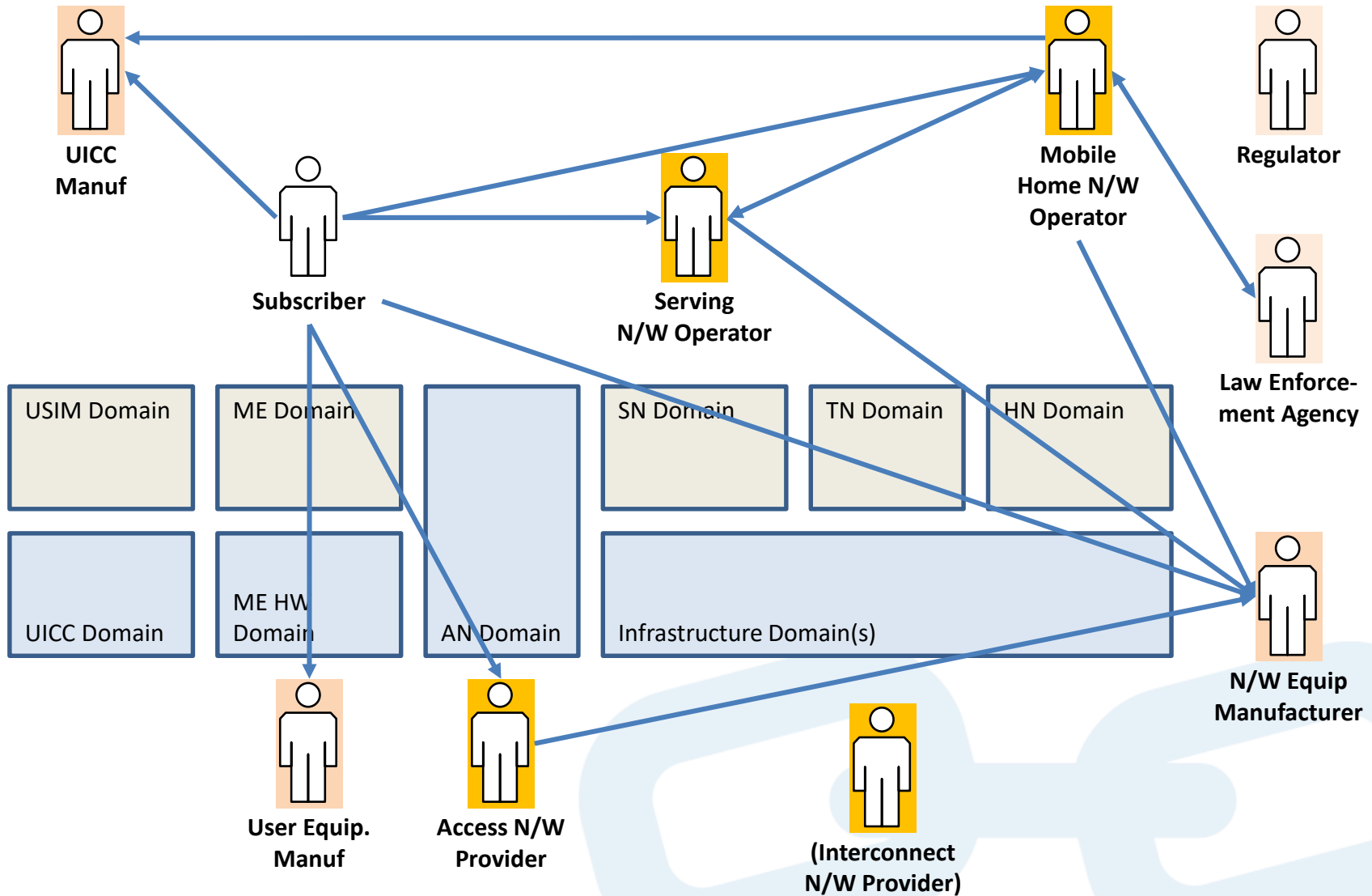
Trustee	Type of Security Measures							
	Patch Mgmt	Security Monitoring	Traffic Mgmt	ID/Cert	Client AuthN	Service AuthN	Access Controls	Encryption
Access N/W Operator	31	30	60					
Home N/W Operator	930	154	106	65	125	5	188	3
Serving N/W Operator	290	72	60	55	35			3
Subscriber	56	30		75		30		6
ME Manuf	56							
N/W Equip Manuf	1003							
UICC Manuf	248	7						

Monitoring and management is crucial to ensure access to Home N/W services

Home N/W Operator now controls access



# Major Trust Dependencies in a 5G Network



## Current Status and Future Work

- ▣ 5G-ENSURE is now finished – full report available online
- ▣ Presented results to GSMA and promoted use risks (and threats) to describe and measure trust
  - ▣ e.g. in vertical application pilots and roll outs
- ▣ The trust modelling tool is available to 5G-PPP partners
  - ▣ we can't provide full support for free now the project is over, but we can provide some assistance
  - ▣ contact me if you are interested in trying it
- ▣ The tool is now being adapted to support ISO 27005 risk analysis for data protection in the cloud
  - ▣ see for example H2020 Project 731678 RestASSURED



# Acknowledgement

- ▣ This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 671562
- ▣ See <http://www.5gensure.eu/> for more details





# 5G-ENSURE

(Project Number— 671562)

## Trust Modelling in 5G Networks

SecSoN Workshop, ACM SIGCOMM 2018  
Budapest, 24 August 2018

Mike Surridge,  
University of Southampton IT Innovation Centre  
[ms\\_at\\_it-innovation.soton.ac.uk](mailto:ms_at_it-innovation.soton.ac.uk)

