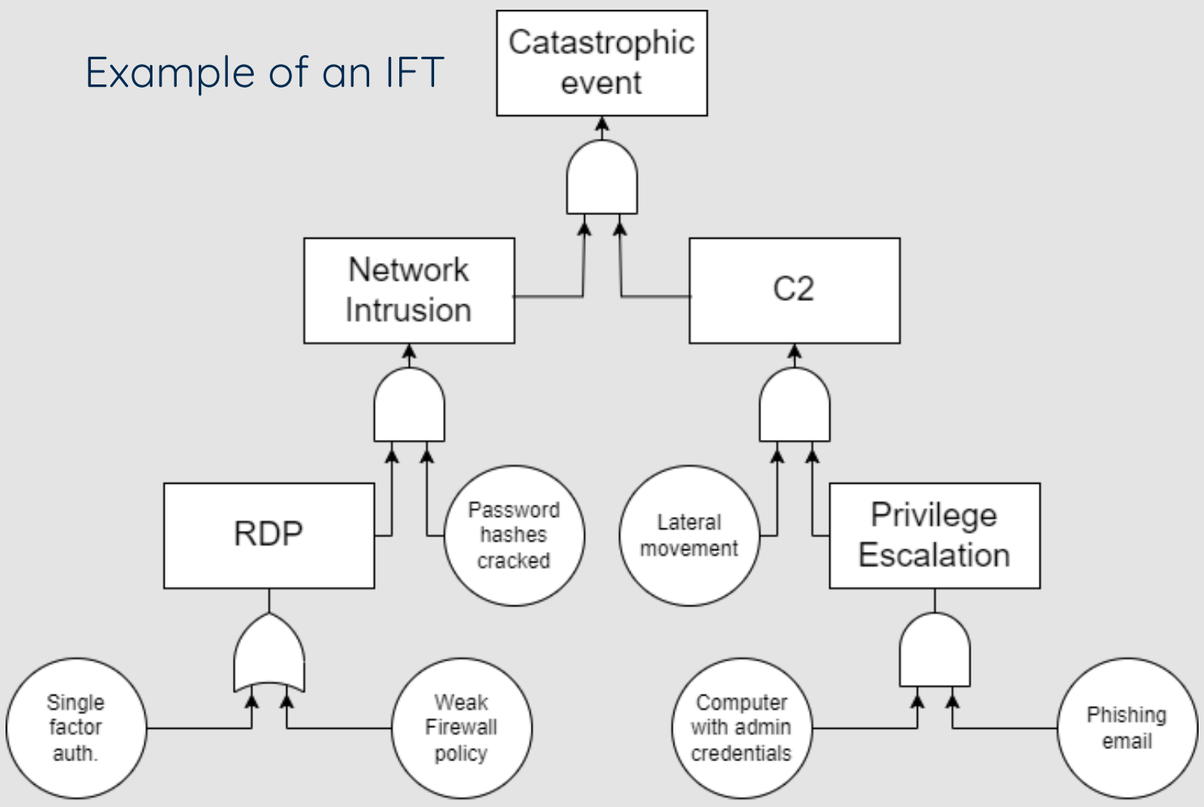
DYNAMIC RISK ASSESSMENT FOR CRITICAL NATIONAL INFRASTRUCTURES

MOTIVATION

Attacks against Industrial Control Systems (ICS) are becoming increasingly more frequent. ICS are critical to the safety of Critical National Infrastructures (CNI), however they combine legacy systems with modern Internet of Things (IoT) devices which expose them to greater cyber risks. CNI cannot simply shut down in case of a cyber attack as this might be disruptive.

Example of an IFT



METHODOLOGY

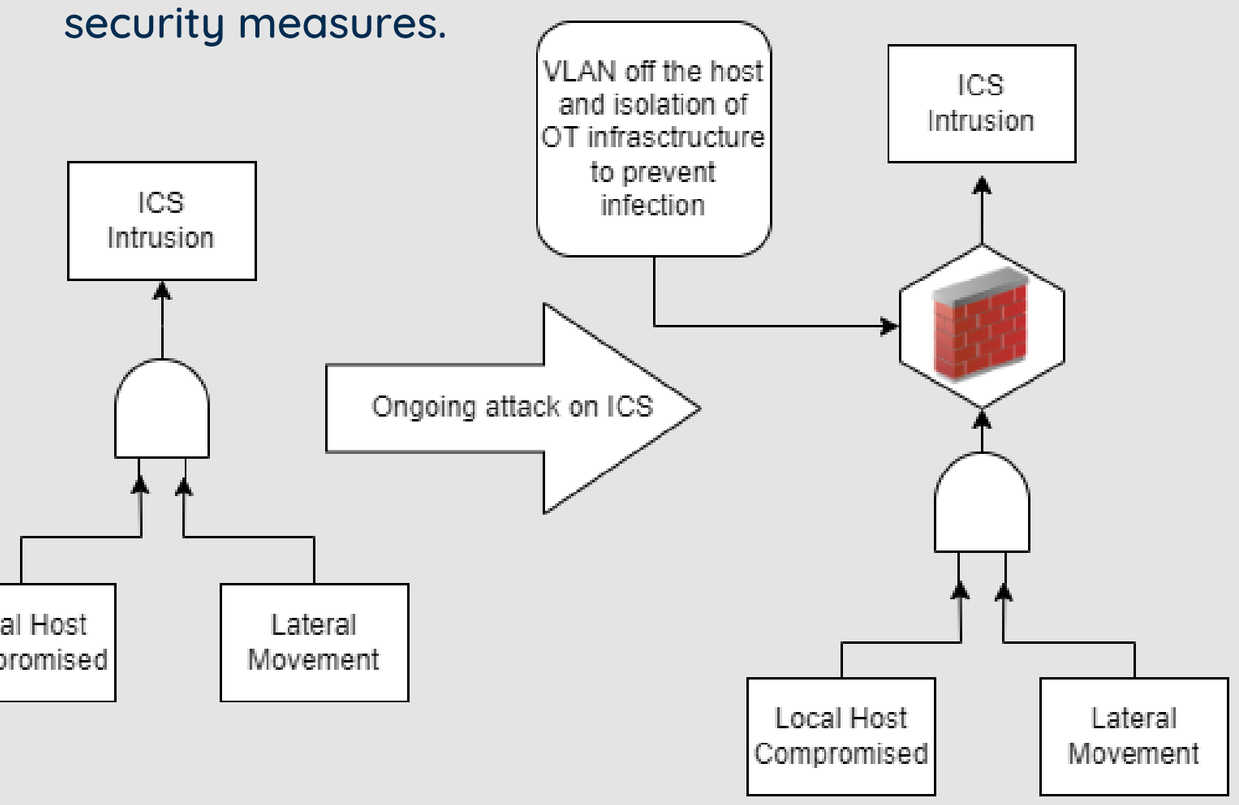
- Literature review & study of past events
- Development of IFTs from realistic scenarios developed in collaboration with QinetiQ
- Development of near real-time generalised network representation for CNI
- Informing a model for dynamic IFTs by combining the above which inform inhibit gates
- Deployment and improvement of the model on the testbeds in the lab

PROBLEM

Traditional risk assessments are static and they are nowhere near real-time representation. During on-going cyber attack it is deemed necessary to understand its implications and attacker's motives to isolate compromised parts and maintain the CNI in a semi-operating state while eliminating the threat.

Incident Fault Trees (IFTs) are frequently used in risk assessments as they provide a retrospective modelled representation of safety incidents. However modelling severe cyber threats against ICS leads to the creation of multiple and complicated IFTs which even a safety professional would find challenging to analyse and deduce where they should focus on during an ongoing attack.

There is a need for a near-real-time model which would apply an IFT body of knowledge on incoming data from an ongoing safety incident. This model would identify the branches of specific IFT(s) to focus on and derive the appropriate security measures.



Kostas Anastasakis

Supervisors:

Professor Awais Rashid
awais.rashid@bristol.ac.uk

Dr Sridhar Adepu
sridhar.adepu@bristol.ac.uk

In Partnership with:

QINETIQ

UKRI

Bristol Cyber Security Group