THE TIMES THE SUNDAY TIMES
GOOD UNIVERSITY GUIDE 2020
INSTITUTE OF TECHNOLOGY OF THE YEAR

AIT Research

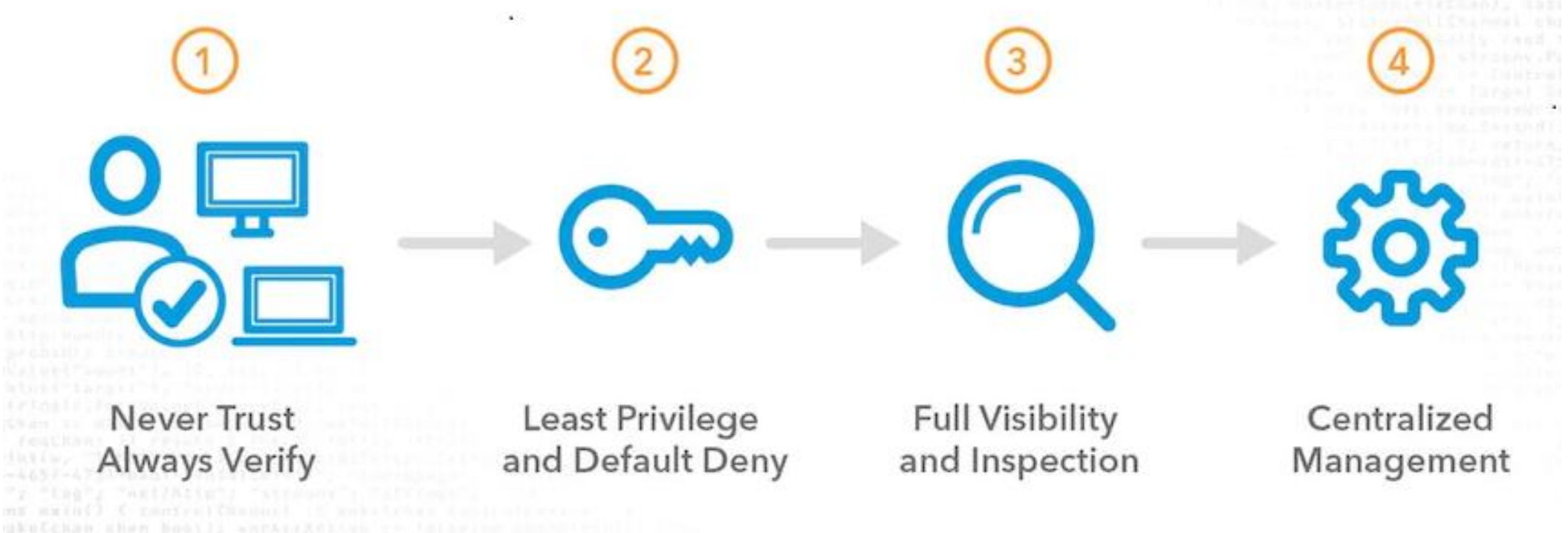
The Context Aware Security Policy Language for Zero Trust Network

Shiyu Xiao, Brian Lee, Nadia Kanwal
Software Research Institute, Athlone Institute of Technology, Athlone, Ireland

Introduction

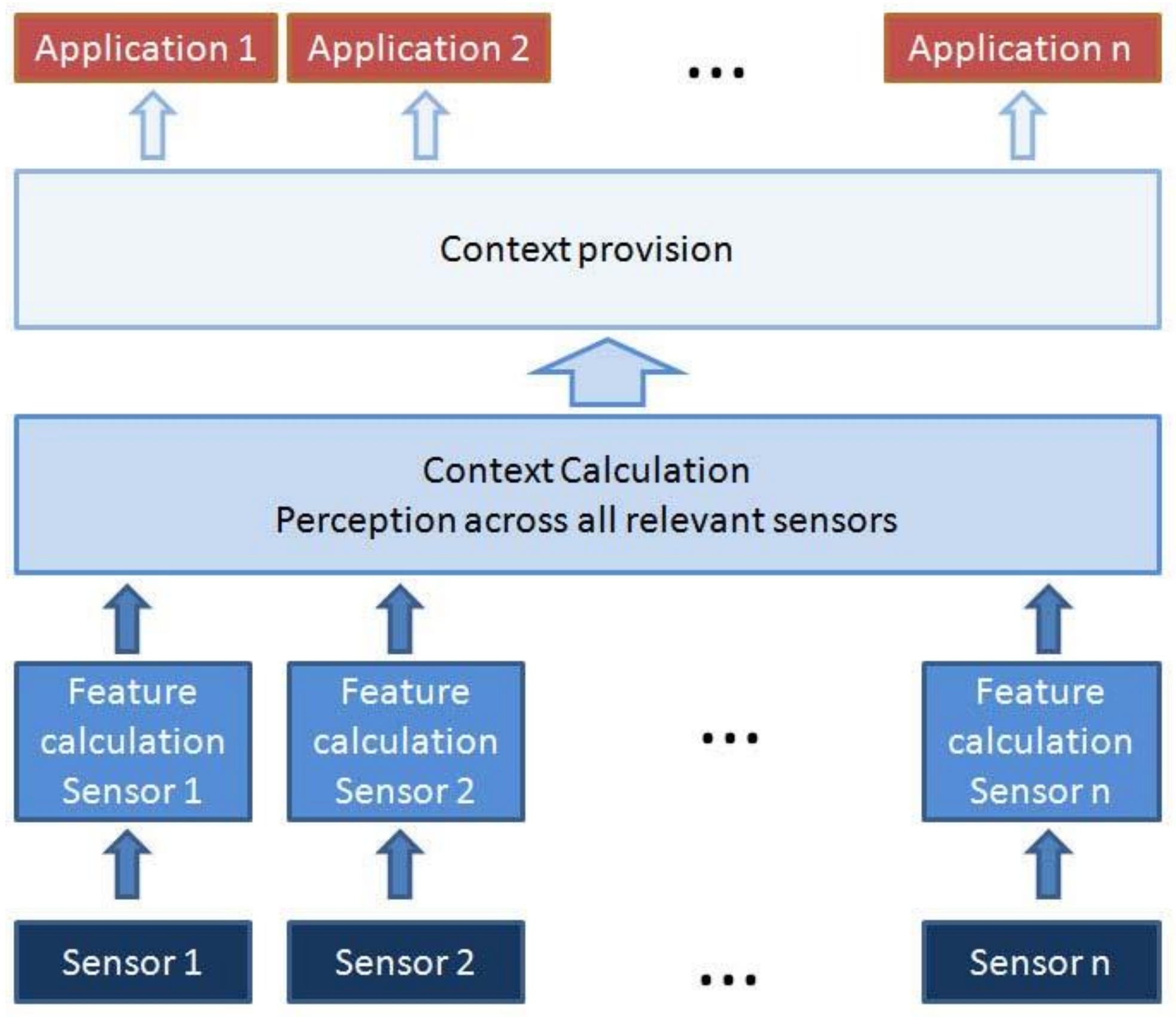
With the development of the pervasive computing, the number of devices accessing to network is increasing. Though this condition brings us a more convenient and intelligent lifestyle, accompanying with it is the higher possibility of information breach no matter it is intentional or inadvertent. Moreover, as traditional constructs of on-site employees and on-premises solutions fade, the traditional perimeter security model no longer fit into modern networks and usage pattern. To mitigate this issue, a more effective model, Zero Trust Networking (ZTN) was proposed. Through the guiding principle of "never trust, always verify", the network is assumed as a hostile place needing to deal with threads from both outside and inside. The massive context attributes and complicated security requirements result in the difficulty of manually implementing every access control rule. There is an immediate need of a policy language specification that enables automatically generating access control rules, using context information. Extensive research works have been proposed, focusing on policy language. Nevertheless, few of them are optimised for ZTN scenarios. The project aims to enable context-aware features in an access control system (implemented with a dedicated policy language) for ZTN.

Zero Trust Network


1
2
3
4
Never Trust Always Verify
Least Privilege and Default Deny
Full Visibility and Inspection
Centralized Management

Zero Trust is a hostile network security model assuming both external and internal network existing threats. With dynamic evaluation of the trustworthiness and segmented network access, the framework only allow the authenticated requests to access the its target resources.

Context Aware Security

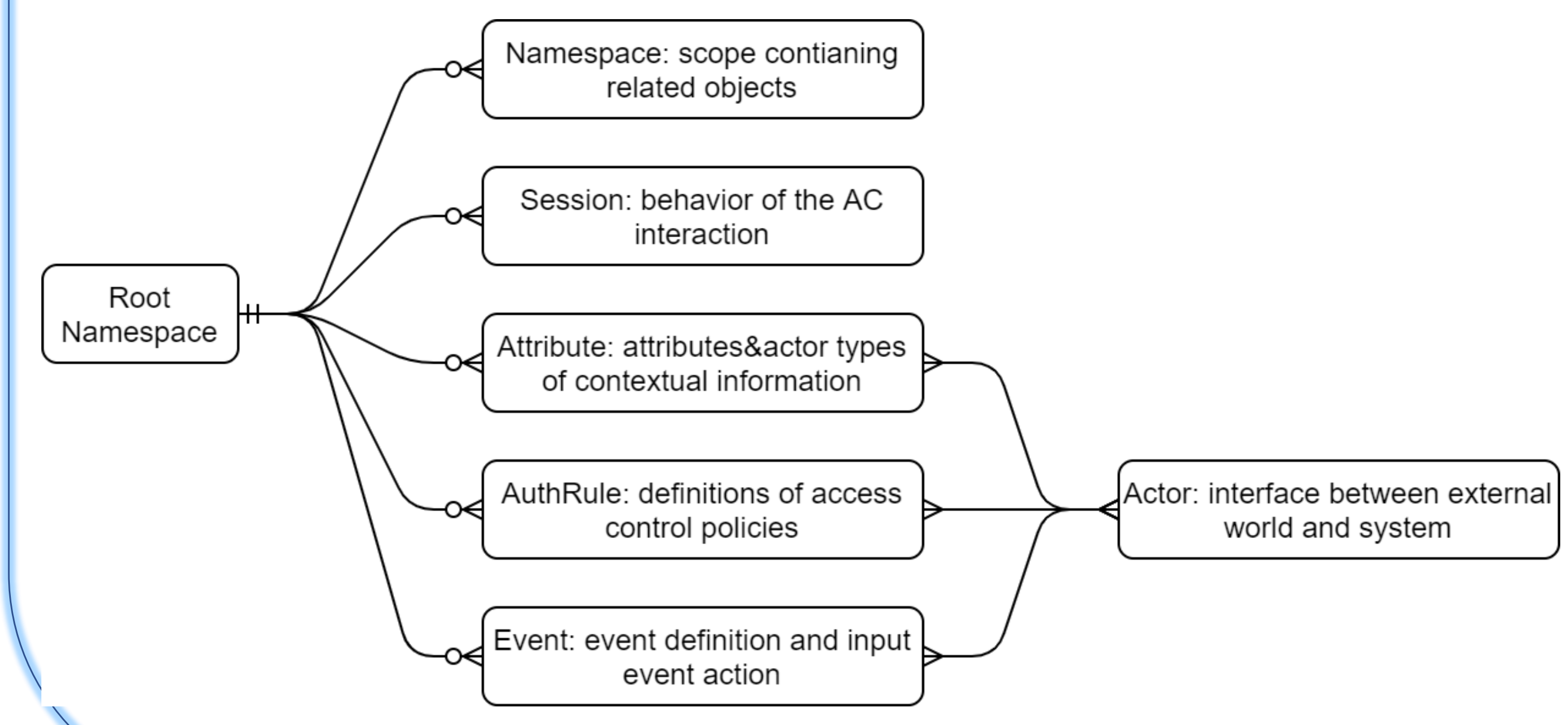

Application 1
Application 2
…
Application n
Context provision
Context Calculation
Perception across all relevant sensors
Feature calculation Sensor 1
Feature calculation Sensor 2
…
Feature calculation Sensor n
Sensor 1
Sensor 2
…
Sensor n

As it is indicated by the picture, the sensors are continuously sensing and periodically logging the detected context information data. When requests come in, the feature calculation sensors are trigged to collect and model the needed context data. Then in the context calculation phase the system percepts across all relevant sensors to do arithmetic operations on the context information to provide conditions for decision making. And the result is delivered to the users telling the requester if he is permitted or denied to access the system.

PAROLE Policy Language Specification

The PAROLE policy language is used to enable policy specification and enforcement for risk-based access control. It also includes the key Risk-Adaptive Access Control and Usage Control extensions of decision continuity and attribute mutability.

The policy language contains 6 main structures as indicated by the picture.


Root Namespace
Namespace: scope contianing related objects
Session: behavior of the AC interaction
Attribute: attributes&actor types of contextual information
AuthRule: definitions of access control policies
Event: event definition and input event action
Actor: interface between external world and system

Workflow:

When a requester wants to access the resource, the session is activated. According to the event type, the actors start to collect the related contextual attributes data. Then the data is transferred to AuthRule block to make the decision on this request. Iff the current request is allowed, then the next event is popped into event-queue. Otherwise, the request is denied.

Future Work

- To ensure the context type we will include in the system;
- Implement parser and interpreter for a subset of the PAROLE language；
- To verify its operation for ZTN access control；
- Emulation of operation of policy language in a synthetic environment；
- To compare with the existing context-aware policy language.

THE TIMES THE SUNDAY TIMES
GOOD UNIVERSITY GUIDE 2020
INSTITUTE OF TECHNOLOGY OF THE YEAR

AIT Research