Mobile Networks, Nokia
Aalto University

Vipul Kumar (Nokia, Aalto University)
Supervisors: Lachlan Gunn (Aalto University), Sokratis Katsikas (NTNU)
Advisor: Esa Metsala (Nokia)

Security for AI/ML in RAN applications

- Threat Modelling for AI/ML features in Radio Access Network
- AI/ML based features in mobile networks leads to more vulnerable surface

The problem

- Security landscape of AI/ML based features in RAN must be evaluated
- Deviation from classical AI/ML threats and vulnerability needs to be studied

Threat Actors

- Identify threat actors from operator's viewpoint
- Assess the goals, capabilities and knowledge of each threat actor group

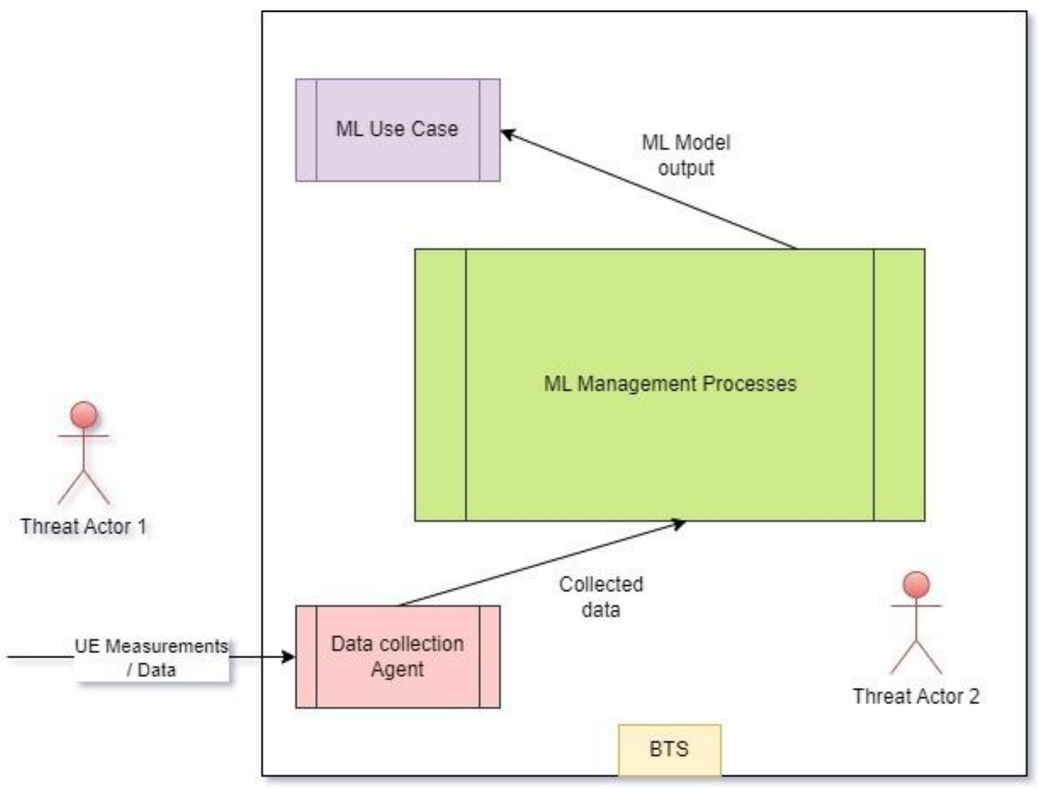

Figure 1: Threat Actors : The more dangerous **Threat actor 2** represent groups with white/grey box access and are usually involved with feature development, maintenance or operation.

Threats

- Three major categories : Evasion, Poisoning and Privacy Attacks
- Training data a major and most vulnerable asset

Threat Model

- Redefine threat modelling definitions in context of AI/ML in RAN
- Identify RAN assets, classify threat actors, and evaluate probable threats

Threat	Affected Asset	Attack Phase	STRIDE Mapping	NIST Mapping

Figure 2: A part of the threat modelling template. The identified threats are mapped to redefined STRIDE and NIST categories.

Conclusion

- RAN secure from some of the threats by design
- The AI/ML related threats can be engineered for RAN applications which is different from the classical methods
- Prevention is easier than mitigation

Aalto University

Contact: vipul.kumar@aalto.fi

NOKIA