Security & Privacy for Self-Adaptive Systems

Breakout group 4

Premise

- Secure systems are adaptive by nature
  - M: detect security violation, privacy leak
  - A: compute risks
  - P: ranking/prioritising/trading-off/selecting countermeasure
  - E: enacting countermeasures

Question 1

- *Can self-adaptation techniques helps us engineer secure systems in a more systematic way?*

+ adapt the protection according to assets/threats/ environment

- If attacker also adapt their behaviour this may hurt security

矛 盾

Kp ⊈ Ka, SAS ↑ S&P

Kp ⊈ Ka, SAS ↓ S&P

Question 2

- *What is the impact of self-adaptation on security and privacy?*
- Both SAS and Secure system try to best deal with unforeseen situations/deal with uncertain behaviour
- Challenge: How to ensure/maintain security when the system involve uncertain adaptive behaviour?