Telecommunication Requirements draft-zhuang-sacm-telereq-00

Xiaojun Zhuang <zhuangxiaojun@chinamobile.com>,
Minpeng Qi <qiminpeng@chinamobile.com> (presenter)
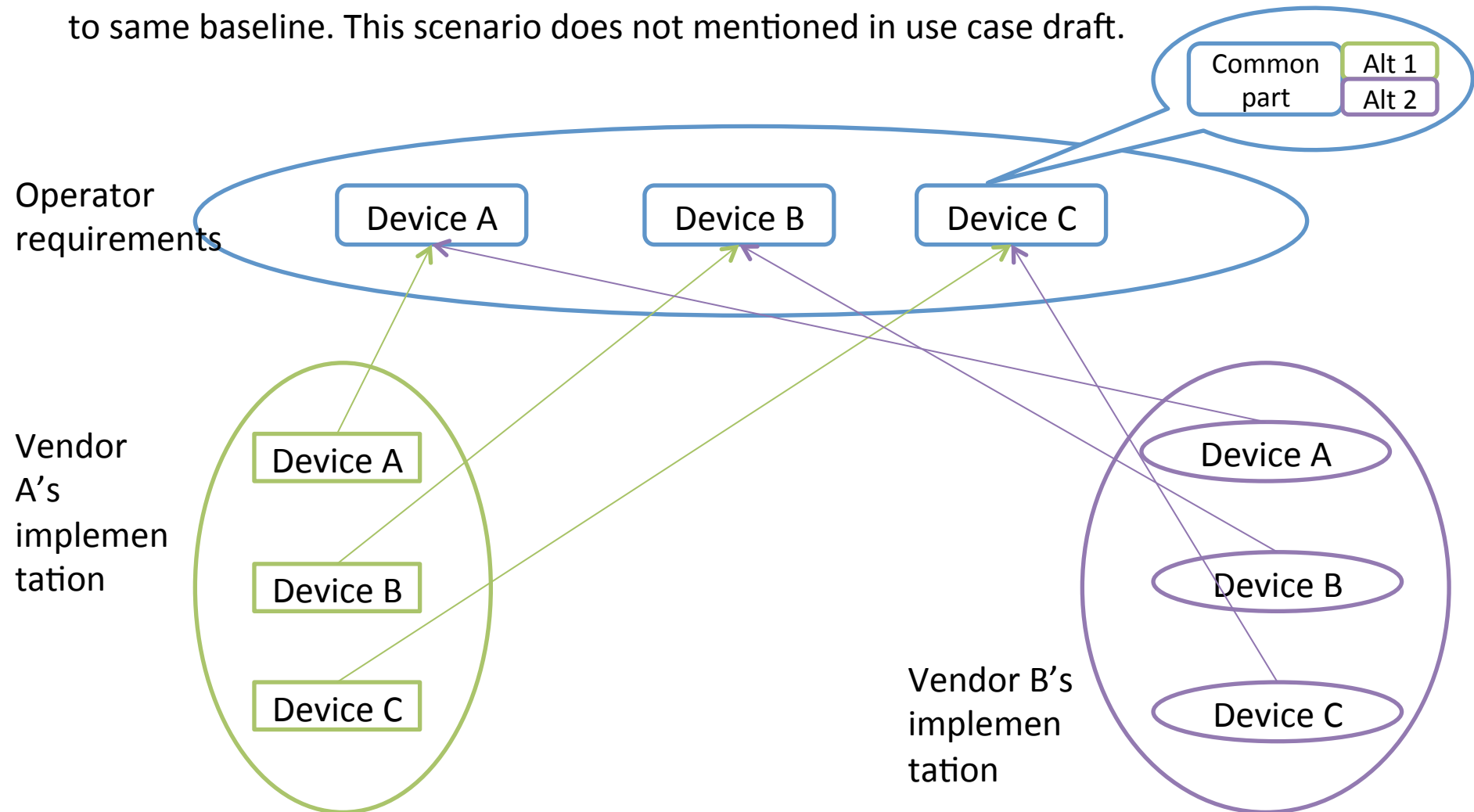Judy Zhu <zhuhongru@chinamobile.com>

Outline

- Problem statement

- New use cases for telecommunication equipment

Problem statement

- Current statement：
  - The use cases of SACM are only for enterprise in the endpoint, but the vast majority of them can be applied in the scene of telecommunications network.
- Problem statement：
  - There are following problems for the safety assessment of telecommunications network equipment:
    - Telecommunication network equipments need more complex baseline setting.
    - Lack of process after that equipment security policy does not meet the security posture , and it needs remediation and triggering the new assessment.
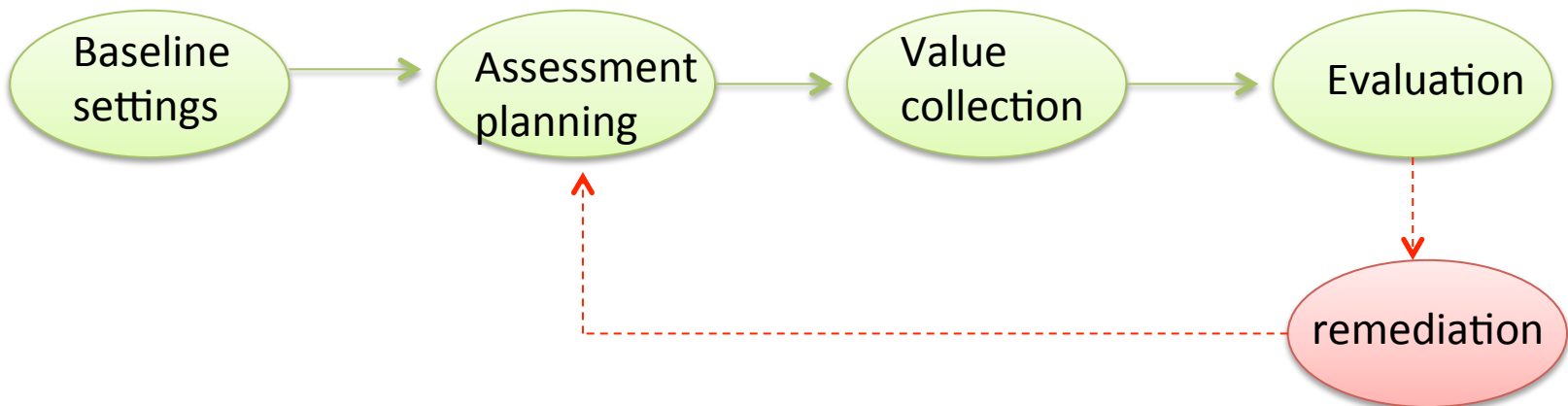
Security baseline

Issue: For the same requirements, different vendors have different implementations, which cause different detailed security attributes. However, same requirement leads to same baseline. This scenario does not mentioned in use case draft.

Common part | Alt 1
Alt 2

Operator requirements

Device A   Device B   Device C

Vendor A's implementation

Device A

Device B

Device C

Vendor B's implementation

Device A

Device B

Device C

Remediation

- In use case draft, it covers
  - Baseline settings
  - Assessment planning
  - Value collection
  - Evaluation
- However, it lacks
  - Remediation
    - If evaluation shows there are mistakes on specific attributes, the details of when and how to recover to normal state.

New use cases for telecommunication equipment

- Use case 1： security policy baseline setting
  - This use case describes the process of setting security policy baseline of the telecommunication equipment.
- Use case 2: Security posture remediation
  - This use case describes the process of remedying security posture when the posture evaluation result of has not complied with the operators security policy.

Thank you!