Hardware Security Risk Assessment: A Case Study

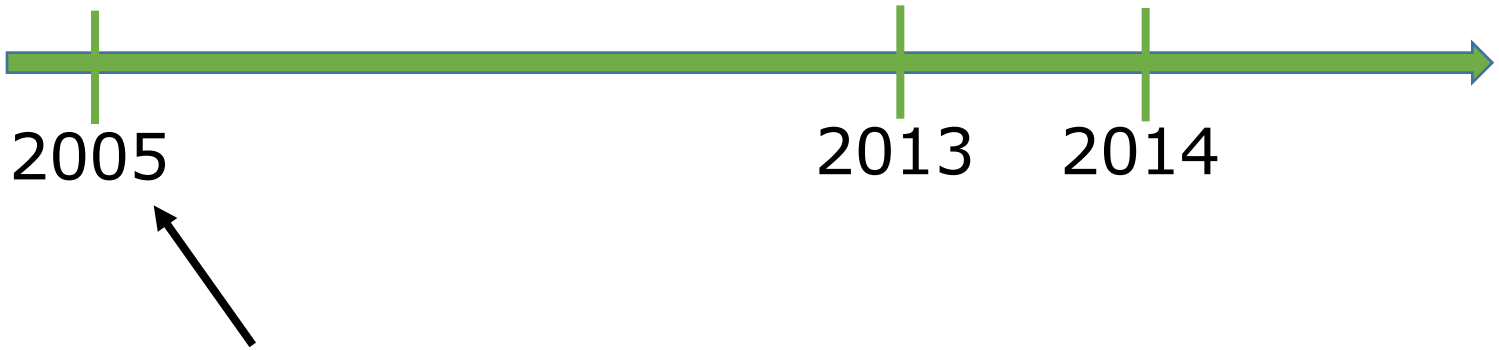
Authors: Brent Sherman, David Wheeler

May 4, 2016

2016 IEEE International Symposium on HOST

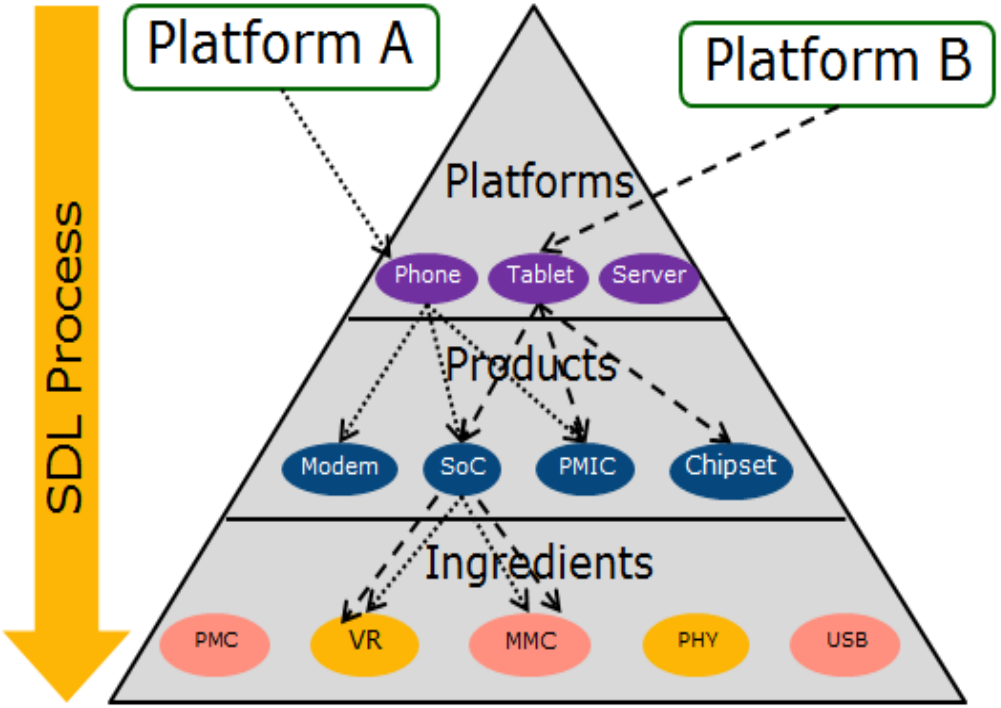
THE ROOT OF TRUST SECOE

Introduction

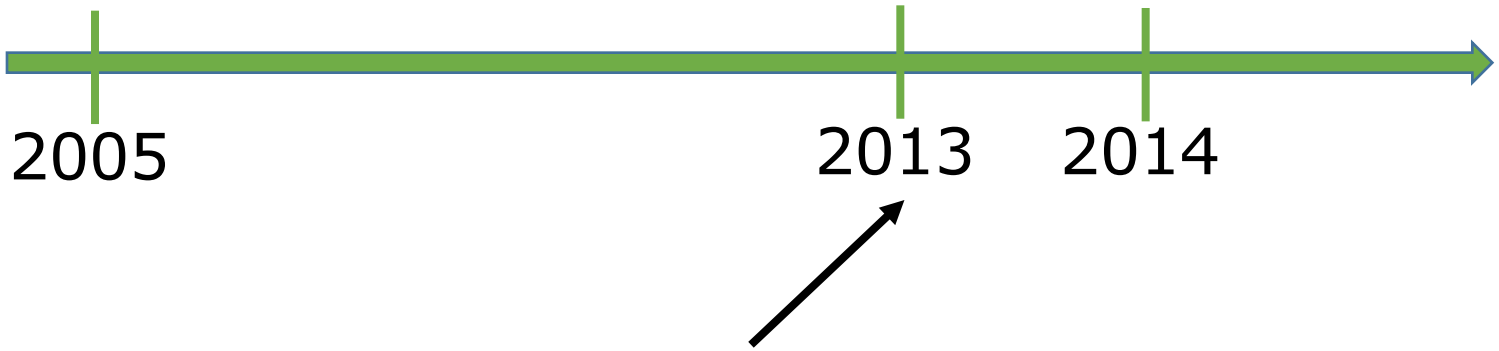


Intel incorporated a modified version of Microsoft's Security Development Lifecycle (SDL) process

- Performed at the platform-level
- Manageable product portfolio

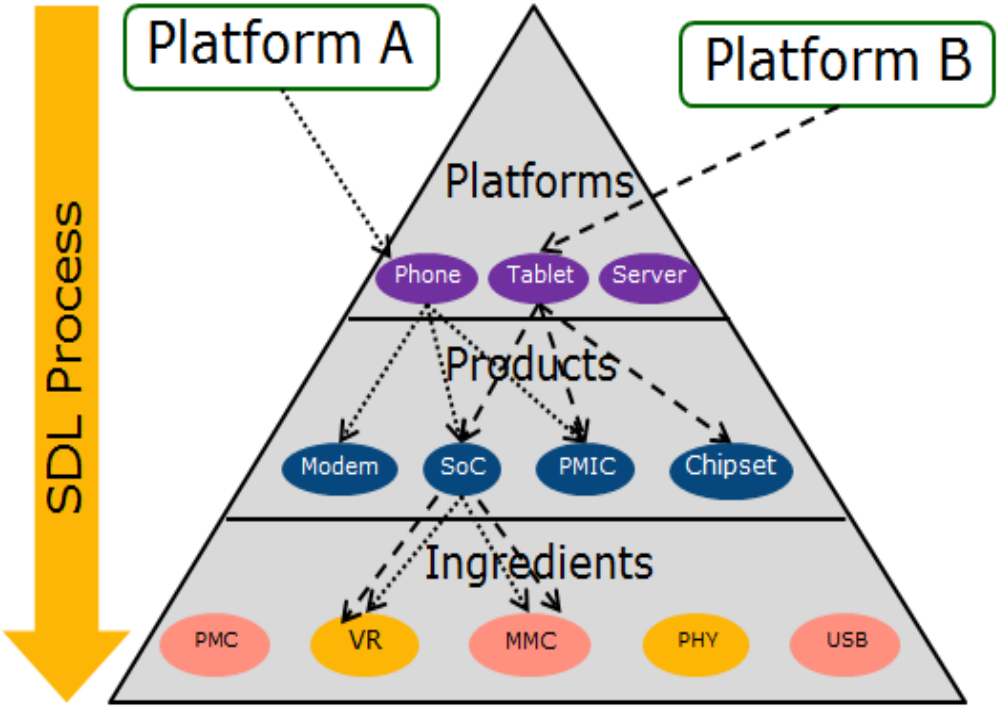


Introduction (cont)

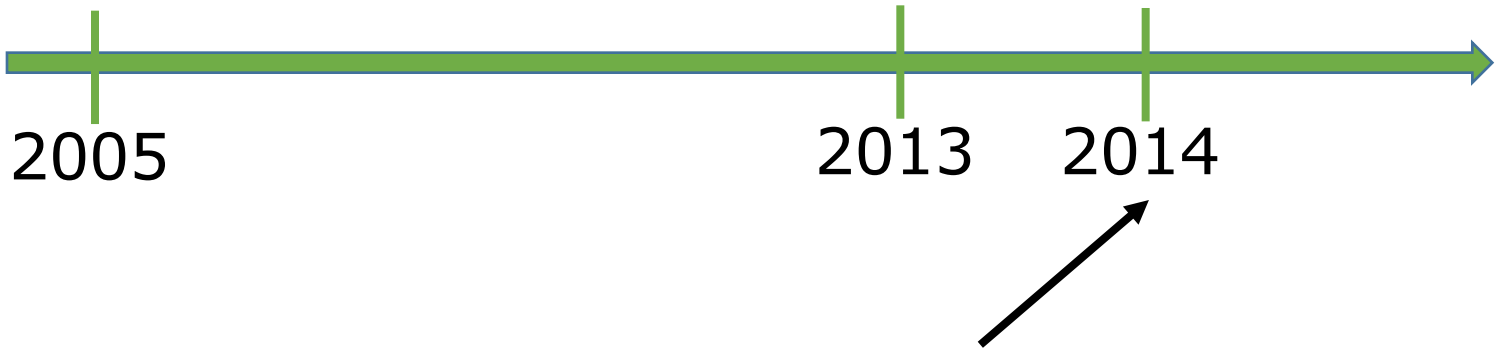


Product portfolio had increased by ~5x

- Multiple derivatives
- Product teams weren't efficient
- No SDL re-use

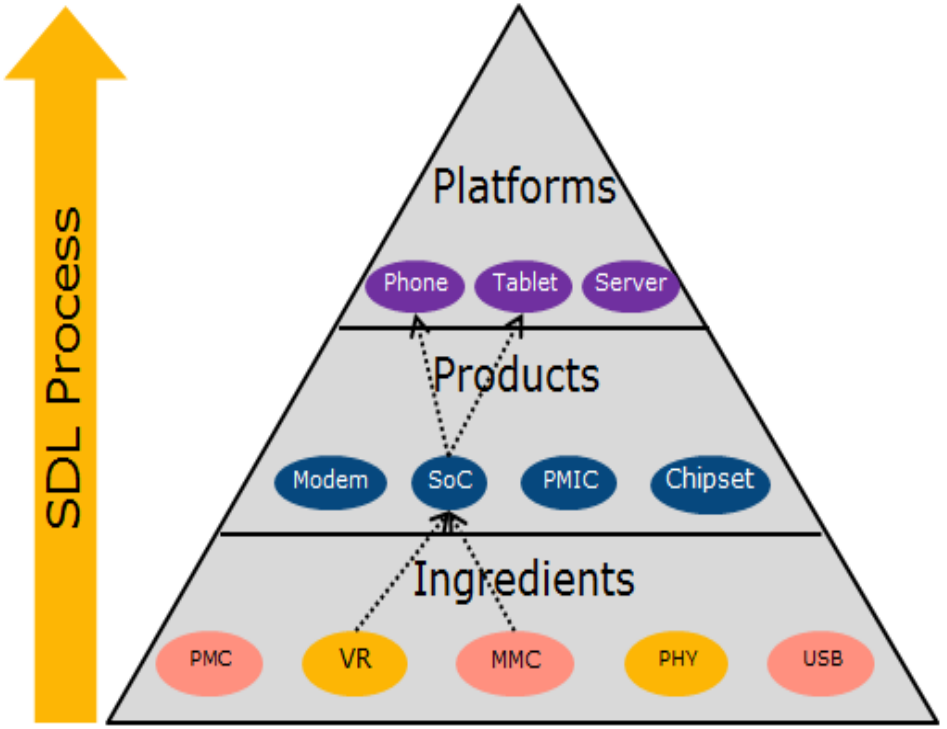


Introduction (cont)



Adopted a bottom-up approach to maximize SDL re-use to increase efficiency

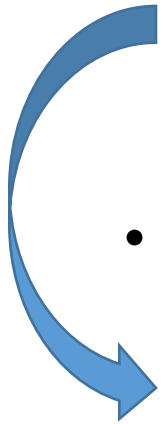
- Apply SDL at the ingredient level (IP)
- Product teams tasked with only integration SDL



However, we created a big bottleneck…

Introduction (cont)

- SDL (Step 1): Initial risk assessment
  - Defines SDL scope (i.e. which activities apply based on risk level)
  - Typically performed by 3 individuals:
    - **Security expert** - mandatory
    - Lead architect - mandatory
    - SDL lead/manager
  - Manual process: ~30mins



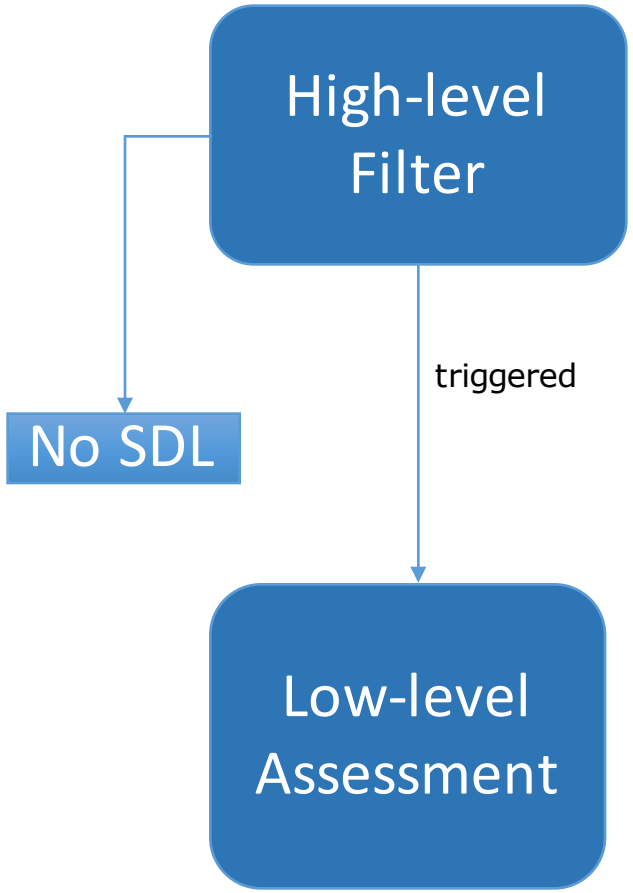
Bottleneck: Security experts are a shared resource and couldn't support this task for 100s of IPs

Security Risk Assessment (SRA) Tool

- Description: A questionnaire of known security concerns to quickly assess an IP's risk level

- Objectives:
  - Design so a non-security person can complete
  - Quickly filter out IPs having acceptable risk (i.e. no SDL required)
  - Assign SDL activities based on the determined risk level

SRA Tool Flow



The purpose is to quickly identify IPs that do not require SDL:

1. Already been through the SDL process (early adopters)
2. Is 100% "reuse" (i.e. no modifications)
3. Had no security incidences in the past 2yrs

Deep-dive into 8 categories of known security concerns (next slide)

Low-Level Assessment

Areas/Topics:

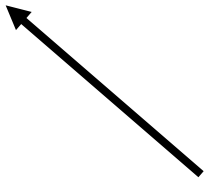
1. Interface connections: access protections, non-standard signals, etc.
2. Debug Features: authorization, bypassing protections, etc.
3. Firmware: authentication, patching, anti-rollback protections, etc.
4. Cryptography: NIST compliance, use-cases, etc.
5. Memory access: protected ranges, aliasing, decoding, etc.
6. Power/state flows: shadowed registers, PDoS, saved-state, etc.
7. Privilege level: privilege escalation, virtualization, etc.
8. Third-party: security assurance evidence

Low-Level Assessment

- Total 37 questions. All mandatory.
- Each question is binary (yes/no) and weighted based on severity
  - If triggered, the weight is added to the overall risk level
- A Risk Assessment Score (%) is calculated once all questions are answered
  - This % is used as a single metric to determine SDL activities

Risk Assessment Score (R_s)

Range (%)	Category	SDL Scope (Example)
$0 \leq R_s \leq 10$	Low	Minimal: Architecture Review
$11 \leq R_s \leq 40$	Medium	Moderate: Architecture and Design Review
$41 \leq R_s \leq 100$	High	Full SDL

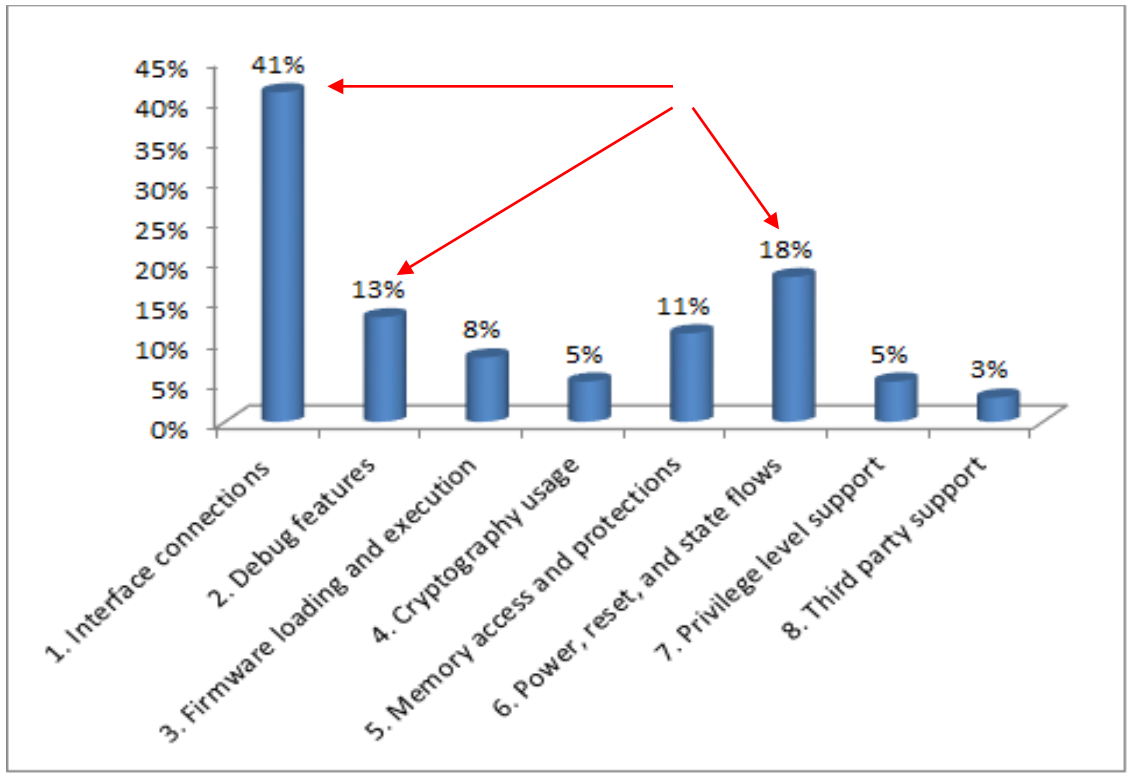


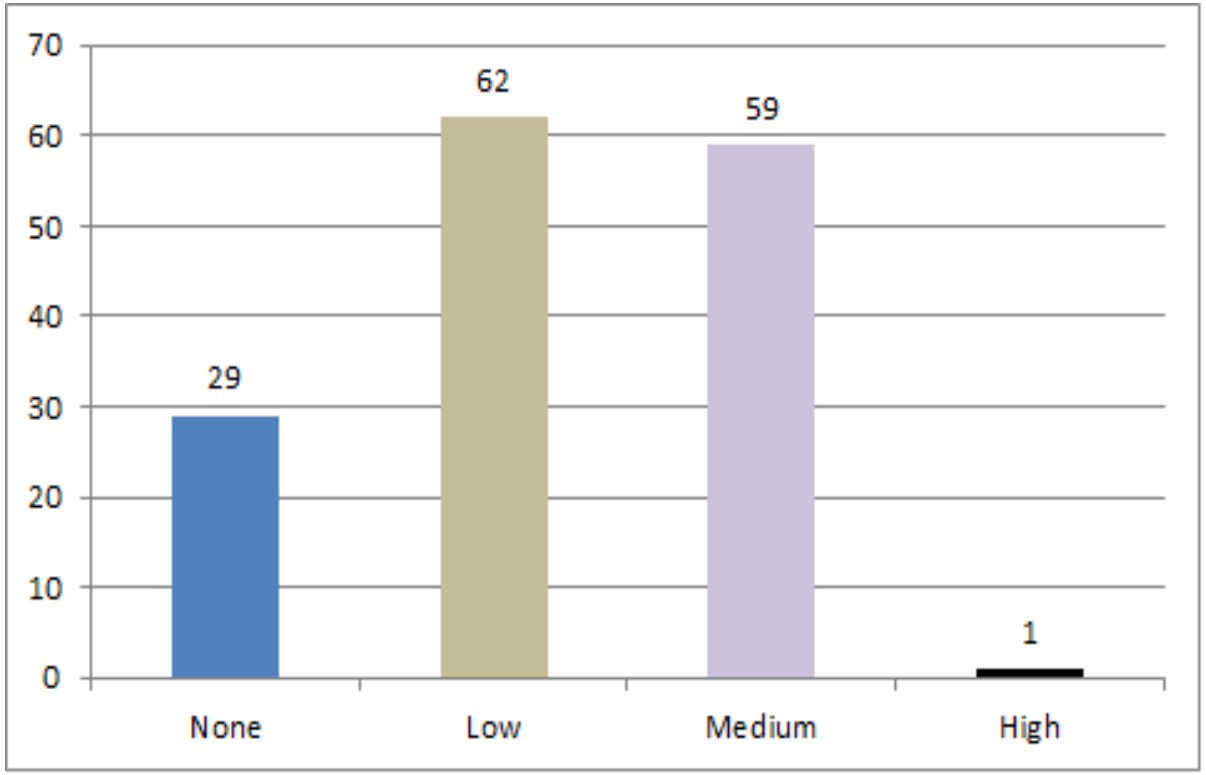
Greatest range to favor full SDL in hopes to minimize escapes

Case Study

- Over a calendar year, 151 IPs were evaluated using the SRA tool
- Each SRA result was reviewed by a security expert for false positives and negatives
  - Used to determine the accuracy of the tool
- Tool Accuracy = 83%
  - 25 errors

Raw Results


45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
41%
13%
8%
5%
11%
18%
5%
3%
1. Interface connections
2. Debug features
3. Firmware loading and execution
4. Cryptography usage
5. Memory access and protections
6. Power, reset, and state flows
7. Privilege level support
8. Third party support


70
60
50
40
30
20
10
0
29
62
59
1
None
Low
Medium
High

The Good…

- Established a consistent corporate-wide method for conducting security risk assessments for IPs
  - Produced evidence for re-use
- Discovered multiple IPs having the same issues
- Labor savings for 151 IPs = 83%

Method	Time	Participates	Total Hours
Manual	30mins	• Security Expert • Architect • SDL Lead	226.5
SRA Tool	15mins	• Architect	37.75

The Bad…

- Averaging weights diluted security concerns
  - Each question addresses a known security concern
  - As more questions get added, the impact a single concern has to the overall assessment gets minimized

- Using a single metric (Low, Med, High) to determine SDL activities gives a false sense of security assurance
  - Each security concern must be evaluated individually

Summary

- SRA tool proved to be effective for:
  - Identifying known security concerns
  - Providing consistent security assessments across multiple organizations
  - Accelerating the security assessment process in SDL

- Improvements:
  - Removed the tallied weights as a measure to determine risk
  - Removed combinational questions (“and”)
  - Every triggered question should have either a:
    1. Follow-on question or
    2. Specific action(s) associated with it
  - Avoid any ambiguity, bias, and slang/informal phrases or words
    - Interpretation of questions varies by GEO
    - English may not be the user’s first language (cultural differences)

Thank You

Definition

- Security Development Lifecycle (SDL)
  - SDL is a set of activities and milestones which can drive high-quality security outcomes in product and services development at Intel.
  - SDL is Intel's approach to make security and privacy an integral part of our product definition, design, development and validation.
  - SDL integrates with the Intel corporate product lifecycle process in order to ensure that Intel products meet Intel Security and Privacy requirements