TF-M Generic Threat Model

David Hu

2021 Jan

Agenda

- Threat Modeling basic concepts
- TF-M Threat Modeling
- TF-M generic Threat Model

arm

Threat Modeling basic concepts

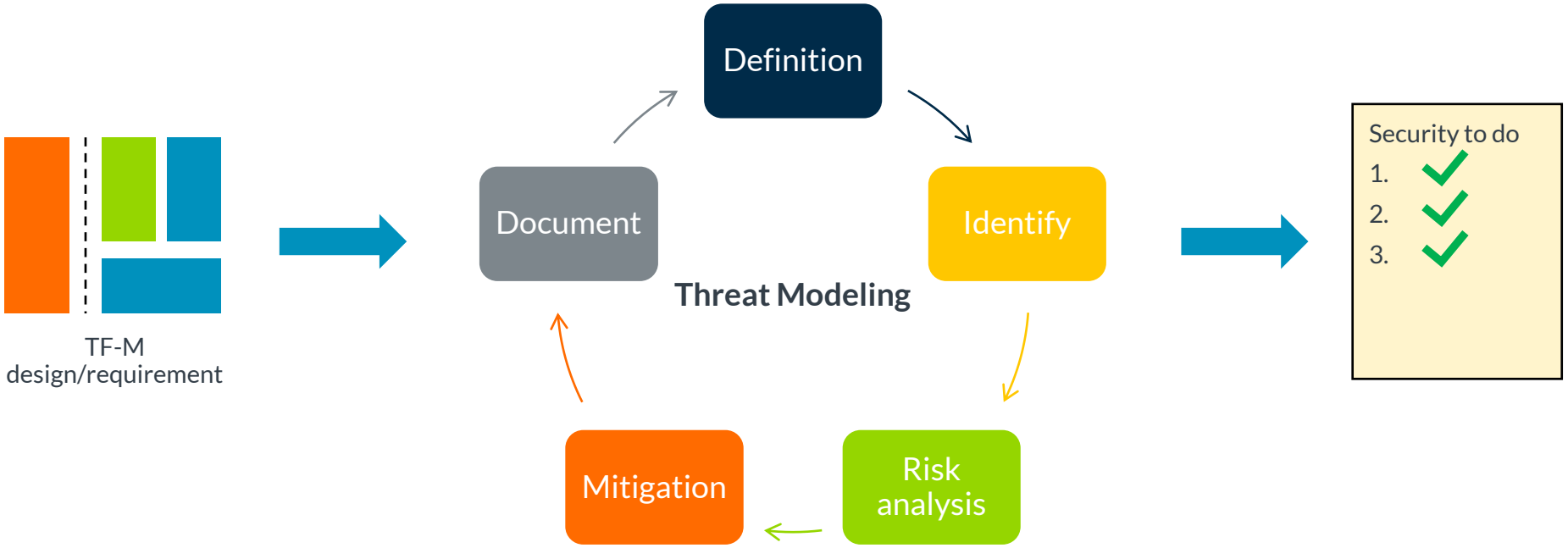
Threat Modeling

- How to make a system (more) secure?

arm

Threat Modeling

- A core element of Secure Development Lifecycle (SDL)
  - Identify and prioritize potential security weaknesses
  - Identify mitigations against identified threats



arm

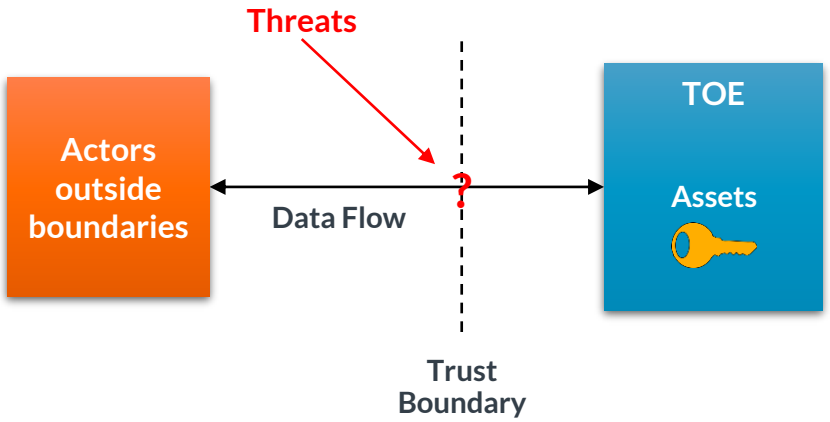
arm

TF-M Threat Modeling

Methodology

TF-M specific process

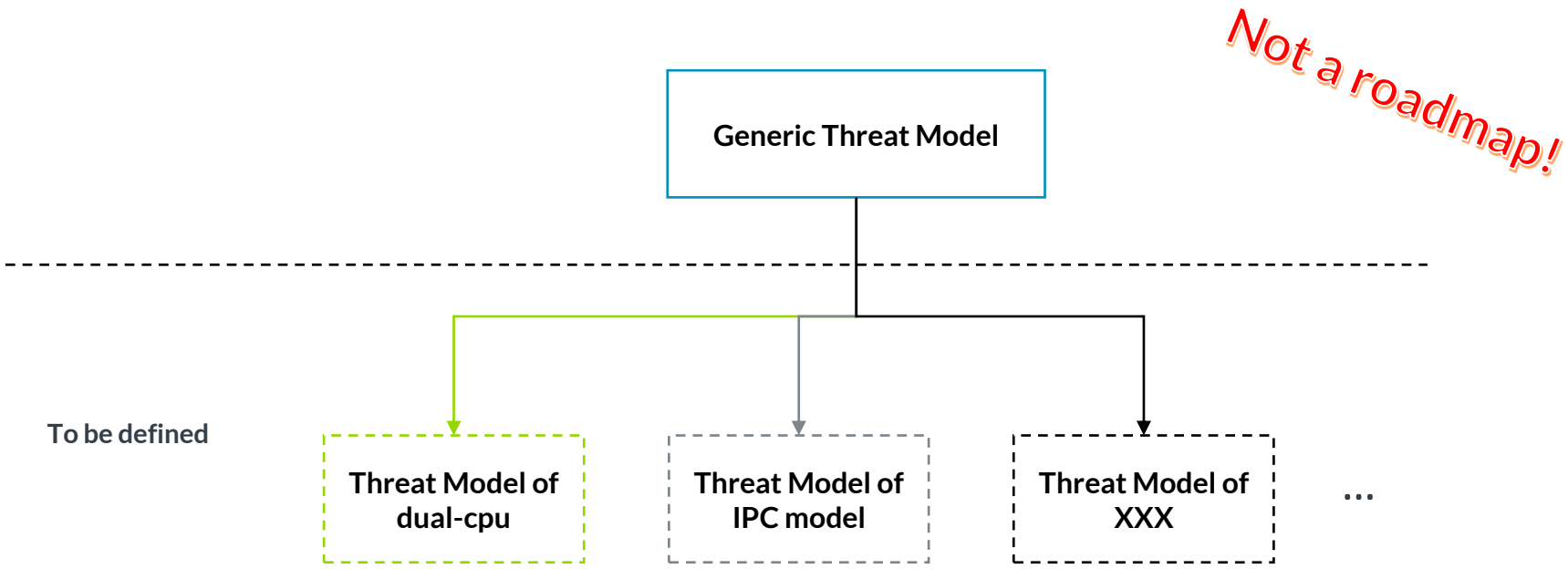
- Identifying Target of Evaluation (TOE)
  - The entity on which Threat Modeling is performed
    - Varies in different usage scenarios
    - Identify Trust Boundary
- Asset identification
  - Resource of value protected by TOE
    - Varies in different TOEs/usage scenarios
- Data Flow Diagram (DFD)
  - Data accesses across Trust Boundaries
- Threats identification
  - Based on data flows
- Threats Prioritization
  - Depends on severity, difficulties, etc.
  - A standard qualitative scheme is preferred
- Mitigations
  - Whether system has mitigated against threats found



arm

Structure

- To cover various TF-M usage scenarios, configurations and modules
  - A generic threat model
    - An overall analysis of TF-M implementation and identify general threats and mitigation.
    - Link
  - Specific threat models
    - Focus on specific usage scenarios, configurations and modules



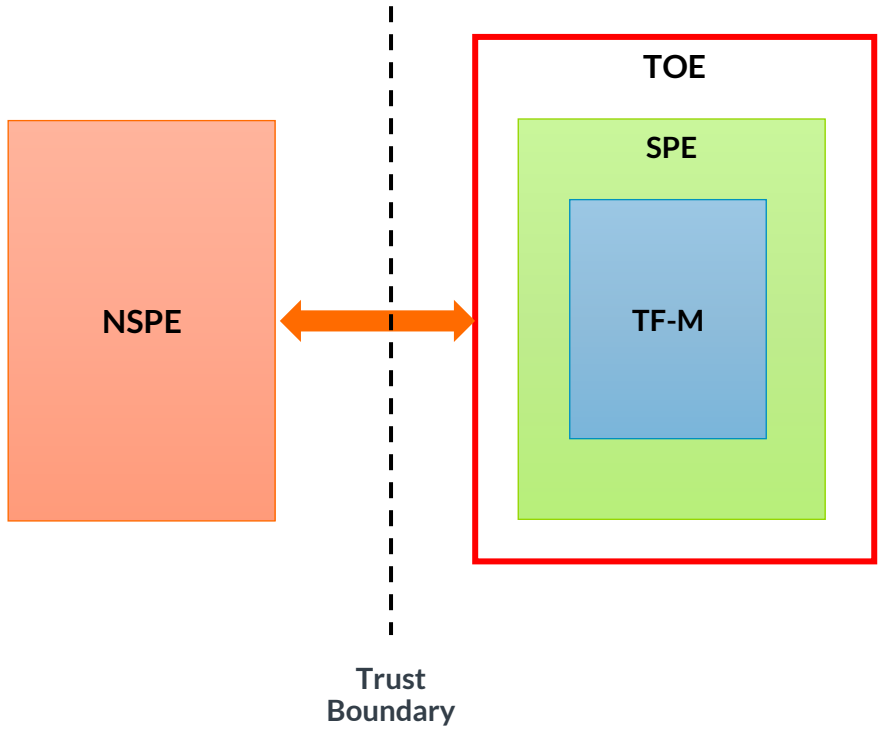
arm

arm

TF-M generic Threat Model

Identifying TOE

- TOE
  - Secure Processing Environment (SPE)
    - TF-M
    - Interactions with other components running in SPE
  - How to protect SPE from NSPE?
- Trust boundary
  - Isolation between NSPE and SPE



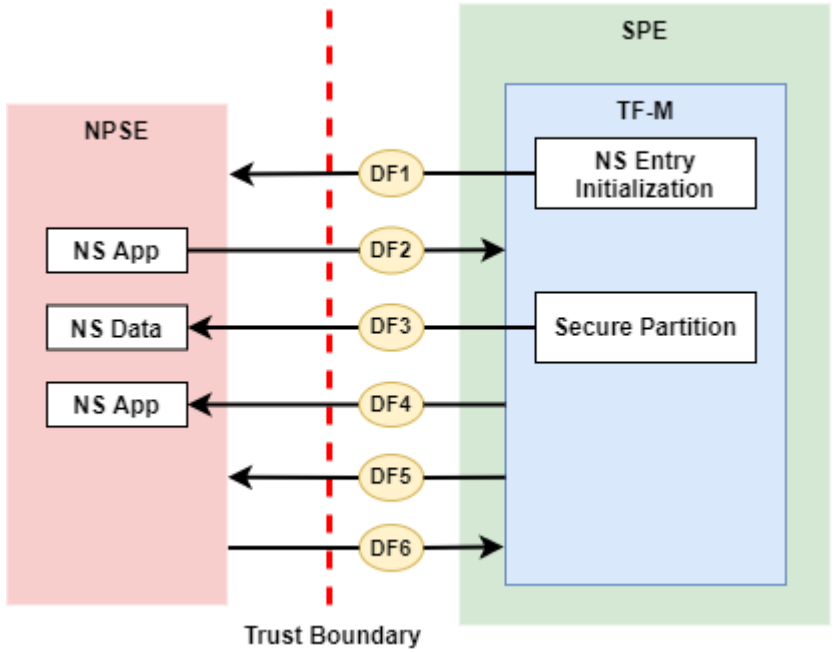
arm

Asset identification

- Hardware Root of Trust (RoT) data, e.g.
  - Hardware Unique Key (HUK)
  - Root authentication key
  - Other embedded root keys
- Software RoT data, e.g.
  - Secure Partition Manager (SPM) code and data
  - RoT service code and data
  - NSPE data stored in SPE
  - Data generated in SPE as requested by NSPE
- Availability of entire RoT service
- Secure logs, including event logs

Data Flow Diagram

- Data flows across trust boundary
  - Data flows inside TOE are out of scope



Data flow	Description
DF1	TF-M initializes NS entry and activates NSPE.
DF2	NSPE requests TF-M RoT services.
DF3	Secure Partitions fetch input data from NS and write back output data to NS.
DF4	TF-M returns RoT service results to NSPE after NS request to RoT service is completed.
DF5	Non-secure interrupts preempt SPE execution in single Armv8-M core scenarios.
DF6	Secure interrupts preempt NSPE execution in single Armv8-M core scenarios.

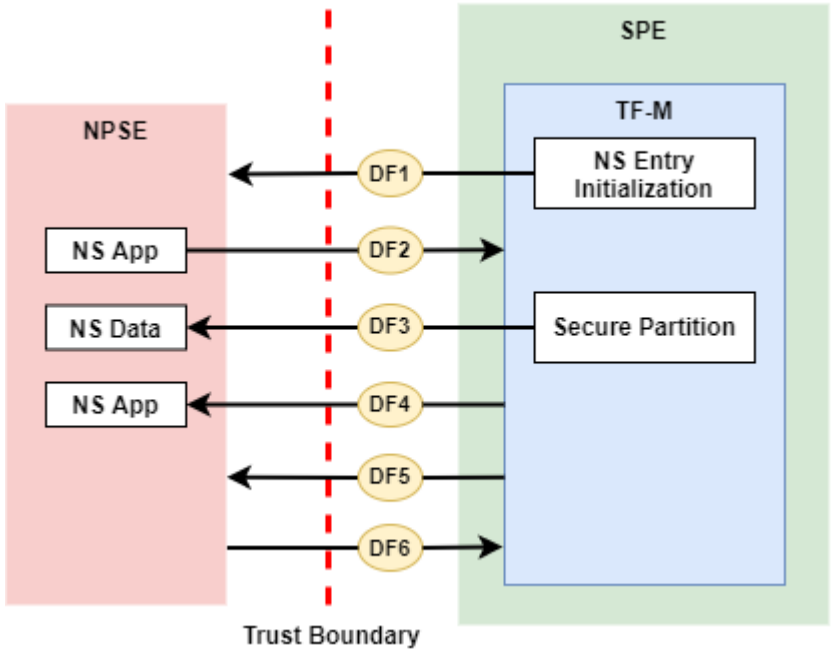
Threat identification

- STRIDE threat model
  - Categorizing threats according to risk types

	Threats	Desired property	Example
S	Spoofing	Authentication	Using another user's username and password
T	Tampering	Integrity	Unauthorized changes made to data.
R	Repudiation	Non-repudiation	Repudiation of illegal access
I	Information disclosure	Confidentiality	Reading a file not granted access to
D	Denial of Service	Availability	Consuming all system resources by making a large amount of system call
E	Elevation of Privilege	Authorization	An unprivileged process gains privileged access

Threat identification

- STRIDE-per-Interaction
  - Go through threat types on each data flow



	S	T	R	I	D	E
DF1		X		X	X	
DF2	X	X	X	X	X	
DF3		X		X		
DF4				X		
DF5				X	X	
DF6				X		

arm

Threat prioritization

- Common Vulnerability Scoring System Version 3.1 (CVSS v3.1)
  - Base metric group
    - "represents the intrinsic qualities of a vulnerability that are constant over time and across user environments"
  - CVSS Calculator

arm

Document threats

- Threat template in generic threat model document

Index	TFM-GENERIC-REQUEST-SERVICE-I-1
Description	A malicious NS application may request to read data belonging to SPE.
Justification	A malicious NS application may request SPE RoT services to copy SPE data to NS memory. The SPE data belongs to components in SPE and must not be disclosed to NSPE, such as root keys.
Category	Information disclosure
Mitigation	TF-M executes memory access check to all the RoT service requests. If a request doesn't have enough permission to access the target memory region, TF-M will refuse this request and assert a security error.
CVSS Score	7.1 (High)
CVSS Vector String	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

A detailed explanation of the threat and how it may impact TF-M

STRIDE category

How does TF-M mitigate this threat?

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה