T1555.501 Hardware Security Module Key Signing

Description: Adversaries may gain unauthorized access to a Hardware Security Module (HSM) to sign keys and/or other derived key material that can be used to achieve additional goals.

An HSM is a hardware component that handles keying material (storage, computation). They can take the form of a plug-in card or an external device that attaches directly to a server. An HSM contains secure crypto-processor chips. MNOs use HSM

appliances as a Root of Trust to secure their PKI infrastructure, which is used to sign certificates for gNBs and NFs.

Although an HSM protects key material from compromise and from export if configured properly, an adversary may obtain privileges allowing them to utilize a legitimate HSM functions, e.g., through PKCS #11 function calls, Cryptoki library, etc., such that an adversary may obtain signatures and derivative key material seen as legitimate by other MNO NFs.

Labelling:

* Sub-techniques: N/A
* Applicable Tactics: credential-access

Metadata:

* Architecture Segment: App layer
* Platforms: HSM
* Access type required: Service Account
* Data Sources: Application Logs, Access Logs
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Credential compromise | An adversary would compromise a function or service that has privileges to perform operations using the HSM and use other techniques to obtain the credentials. The adversary may perform operations from the compromised environment or exfiltrate the credentials to another system to perform the operations and conduct further activities. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1018 | Restrict users of HSM to minimal privileges from only permitted NFs |
| M1026 | Ensure administrative accounts for HSM are carefully managed to minimize potential admin credential compromise. This may include use of privileged access workstations, privileged account management solutions, separation of duties approaches, etc. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Obtain service account credentials | Adversary acquires credentials with legitimate privileges to conduct operations using the HSM. Adversary has a position to initiate transactions with the HSM. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| HSM | A physical computing device that safeguards and manages digital key material, performs operations such as encryption and decryption, signature generation. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0028 | Analyze access logs for appropriate use by admins |
| DS0015 | Analyze the application logs for access from appropriate NFs and appropriate/typical use |
| DS0029 | Monitor for activity from unexpected sources |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Adversary is able to perform crypto operations fraudulenty. | Adversary would have the ability to perform signing and cryptographic operations that would permit the adversary to masquerade as a legitimate authorized user and perform operations against NFs. |

References:

|  |  |
| --- | --- |
| Name | URL |
| Baseline Security Controls –NO-009, FS.31 version 2.0,GSMA, February 2020 | https://www.gsma.com/security/wp-content/uploads/2020/02/FS.31-v2.0.pdf |
| A New Trust Model For The 5G Era, Thales, October 2020 | https://cpl.thalesgroup.com/sites/default/files/content/research\_reports\_white\_papers/field\_document/2020-10/New-Trust-Model-For-5G-Era-WP.pdf |