LURK TLS/DTLS Use Cases

draft-mglt-lurk-tls-use-cases-01.txt

D. Migault, K. Ma, R. Salz, S. Mishra, O. Gonzales de Dios

01/06/2016- Interim Meeting- (Virtual)

Containers and VMs

Description:

- Application servers run within virtual environment
- TLS is used for the authentication

Problem: Absence of control of the private key

- Private keys are stored on instances are running all over the data center
- Private keys are stores on persistent images of VMs/containers
- Isolation may not sufficiently prevent access to the private keys

LURK:

- Isolates the private key and provide remote access to it
- Provides inter-operability for different applications, OS

Content Provider

Description:

- Edge Servers exposed on the Internet are at high risk - OS to application
- Protecting infrastructure with implementation diversity increases potential vulnerabilities
- Edge Servers may share the private key

Problem:

- Diversity of implementations increases the risk of a leakage of the private key
- Leakage occurring at one Edge Server affects the whole service

LURK:

- Prevents private key leaking by a corrupted Edge Server
- Limit the usability/access of the private key in case a Edge Server is corrupted
- Prevent direct access to the private key - even by providing a Key Server

Content Owner / Content Provider

Description:

- Content Owner (URL) distributes the content through a CDN

Problem:

- The Content Owner wants to remain authenticated while not providing the private key to the CDN.
- Private key may present more value than the content itself:
    - Content accessed by devices configured with the public credential need to be replaced/reconfigured in case of private key leakage
    - Content with ephemeral value presents acceptable content leakage risks
    - Content may be encrypted with DRM

LURK:

- Prevents the private key to be communicated to different third parties
- Enables inter-operability between Content Owner and multiple CDNs providers

CDNI

Content Distribution Network Interconnection Description:

- The company with which the Content Owner has contracted may further delegate delivery to another CDN with which the Content Owner has no official business relationship
- The delegating CDN may not even host the Key Server, in which case, it may proxy the communications to the upstream CDN or the Content Owner.

Problem:

- Similar as Content Owner / Content Provider
- Potential additional latency has to be considered

LURK:

- Similar as Content Owner / Content Provider

LURK Requirements

Multiple implementations of Edge Server, located in different administrative domains must be able to interact with multiple implementations of Key Servers also located in multiple administrative domains. In addition, the scope of LURK is closely related to TLS standardized at the IETF.

- R1: LURK MUST be standardized at the IETF

LURK is limited to the Edge Server and the Key Server, so it is expected to be transparent to the TLS Client. In addition, in order to be deployed in the short term, any modification on the TLS Client should be avoided.

- R2: LURK MUST NOT impact the TLS Client.

LURK is associated to TLS related operations performed by the Key Server on behalf of the Edge Server. On the other hand, interactions between the Edge Server and the Key Server also consists enable control-plan like operations such as reachability, capabilities discovery.

- R3: LURK MUST provide control plane-like facilities such as reachability, keep-alive, and capability discovery.

Key Server Requirements

The Key Server holds the Private Key, and interacts with the Edge Servers.

- R4: The Key Server MUST be able to provide the necessary authentication credential so the TLS Client and the Edge Server set an authenticate TLS Connection with the Private Key.
- R5: The Key Server MUST NOT leak any information associated to the Private Key. In particular the Key Server MUST NOT provide a generic singing/encryption oracle.
- R6: The Key Server SHOULD NOT perform any operation outside the authentication of a TLS Connection.
- R7: The Key Server MUST provide confidential information to the Edge Server over an authenticated and encrypted channel.

Edge Server Requirements

- R8: The Edge Server SHOULD be provisioned with the public authentication credentials, and so public certificate provisioning is outside of LURK.

Thank you for your attention