Internet Financial EXchange (IFEX)

Security Considerations

This section is addressed to implementers and enumerates specific security related considerations in the deployment of IFEX based systems. Obviously, it is nonexhaustive; in addition to the points enumerated below standard computer security measures MUST be employed, or an insecure system is likely to result.

Transport Selection

Implementers should consider whether they need their transport to be resistant to traffic analysis.

As a transport neutral protocol, careful transport selection for IFEX deployments is critical to implementation security.

From a security standpoint, potential transports SHOULD be evaluated on at least the following criteria.

Traffic Analysis Considerations

Two primary techniques appear to be employed to frustrate traffic analysis: indirect routing, and chaffing and winnowing. (The latter by liberal definition includes the relatively well known field of steganography as a subset.)

Authentication

If the transport in use provides adequate authentication (for instance, some kind of secure physical link layer) then transaction overheads can be reduced at the IFEX message level. Such configurations MAY be attractive for certain classes of deployment, for example low latency environments such as High Frequency Trading (HFT) systems.

Non-repudiation

If the deployment environment includes adequate non-repudiation (for instance, internal systems within a single organization where adequate audit trails are known to exist and a secure physical link layer is in use), then transaction overheads MAY be reduced at the IFEX message level. Such configurations MAY be attractive for certain classes of deployment, for example low latency environments such as High Frequency Trading (HFT) systems.

Encryption

...

Protocol-Level Considerations

Intrasecond Transaction Identifier (ISTI)

To avoid disclosure of ledger transaction frequency, the Financial

Transaction Identifier (FTID) Intrasecond Transaction Identifier (IS-FTID) portion SHOULD be assigned pseudorandomly rather than sequentially.

By Attack Vector

Resource Exhaustion
Due to the requirement for parties within IFEX to consider and maintain state regarding financial transactions, it is prudent to consider the potential threat of storage and processing resource exhuastion due to deliberate malice (as in Denial of Service attacks), node misbehavior and other circumstances.

Whilst overall financial transaction state differs in that in IFEX's case it is maintained in a non node-local fashion, in broad terms IFEX adopts a view similar to that of [SMTP]. That is, at any given time one particular node MAY be considered to be primarily responsible for expected transaction state transition.

Maximum Message Sizes
IFEX purposefully excludes fixed size limits on message structures. Implementers should carefully consider their bandwidth and processing resources when determining the boundaries for acceptable messages.

Traffic Analysis
While traffic analysis threats are not unique to IFEX, implementors MUST be aware that traffic analysis MAY reveal significant amounts of sensitive financial information; implementers SHOULD select transport strategies with this information in mind.

Latency / Timing Analysis
In some cases, the outcome of a system's IFEX transaction MAY be possible to determine purely by analyzing the latency between the transaction request and response components of a suspected transaction.

Destination Analysis
Traffic analysis MAY reveal with which remote party or parties suspected IFEX transactions are being performed.

Comments

You do not have permission to add comments.