Secure Asset Transfer Protocol: Problem Definition & Assumptions

IETF114 – SAT BOF

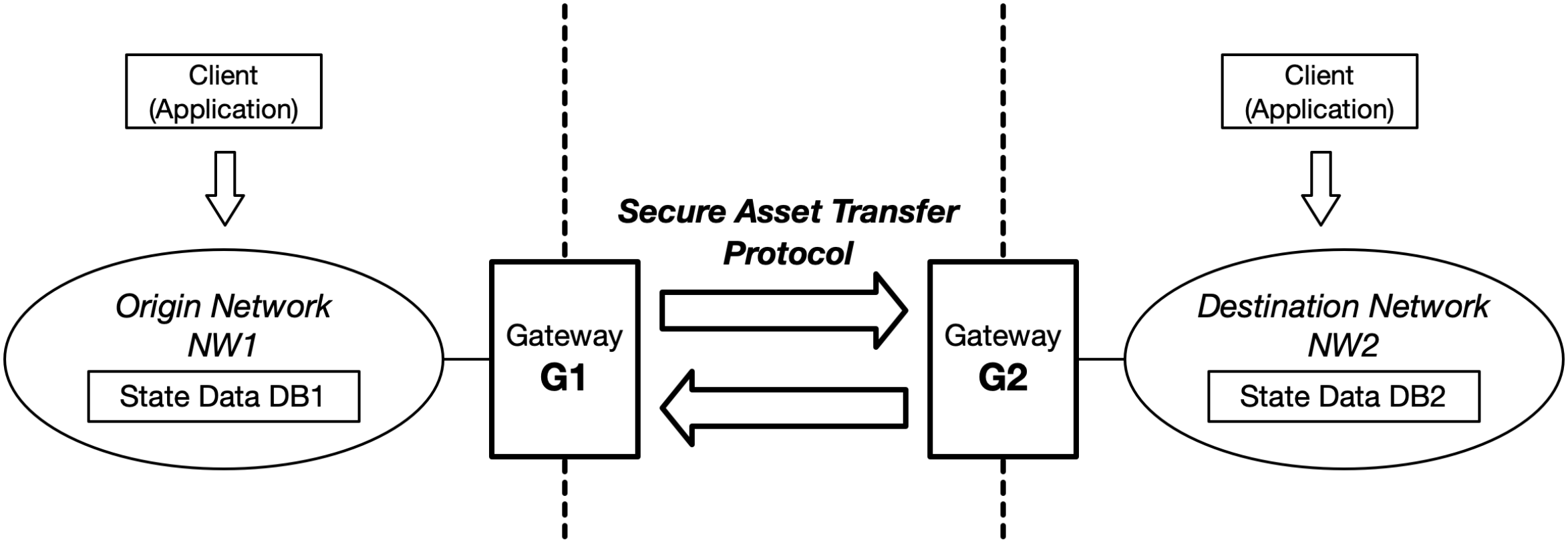
26 July, 2022

Thomas Hardjono (MIT)

Terminology

- *Network*: a group of computers (“nodes”) that share common state information (“state data”) regarding a digital asset
- *Digital asset*: unique value-bearing data-object
- *Valid (Validity)*: value represented by the data-object is legally recognized to be in one network at any one time
- *Gateway*: computer authorized to act on behalf of a network
- *Asset transfer*: move digital asset from one network to another while maintaining validity

Terminology



Problem Statement

- An interoperability protocol that permits the movement of a unique *value-bearing data-object* (“asset”) from one network to another,
- while guaranteeing that the data-object is *valid* in one network only at any one time, and that
- the transfer is *verifiable* by an independent authorized 3rd party

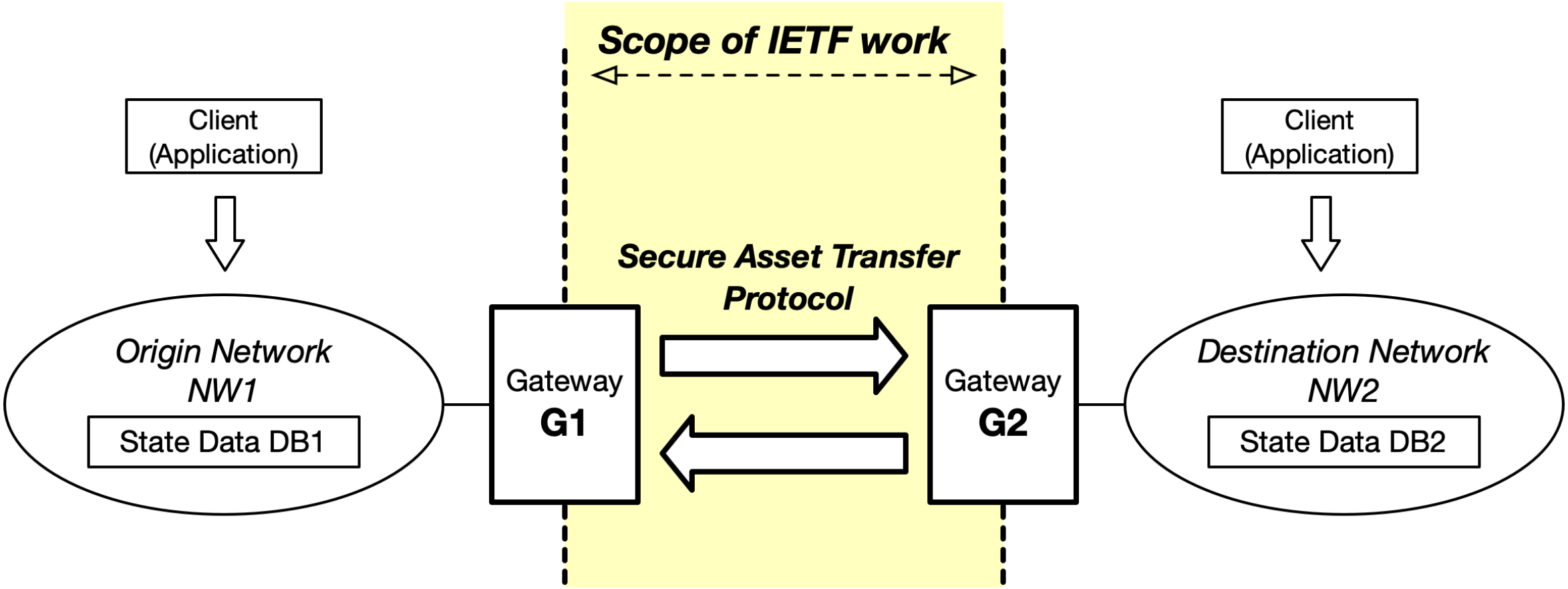
Assumptions

- Both networks share common semantics about the data-object and the notion of validity
- One or both networks are opaque
- “Gateways” implementing the transfer protocol are trusted
- Information subsets (views) of a data-object maybe shared with authorized external parties

Proposed Approach: Gateway Model

- Interoperability “lessons learned” from the Internet Architecture
- One (or more) gateway in front of each network
- Peer gateways implement a *Secure Asset Transfer* (SAT) protocol
- Each gateway handles (hides) the interior characteristics of its network

Proposed Scope of Work



SAT Protocol Modes

- *Asset Transfer*: Unidirectional transfer of asset
- *Data Sharing*: sharing of information (views) regarding data-object with external authorized entity (nb. asset not transferred)
- *Asset Exchange* (swap): Simultaneous & coordinated swaps of two assets in two networks

Proposed Scope of Work

- API-endpoint definitions
- Resource identifiers
- Message payload definitions & message format
- Message flows:
  - 3 phase commit – ACID properties
  - Security and liveness properties

Main technical drafts

- Gateway architecture draft
- Secure Asset Transfer Protocol draft

Other drafts

- Use Cases (TBD)

Thank You & Questions

Contact: hardjono@mit.edu