Bern University
of Applied Sciences

Append-only Bulletin Board

Definitions and Operations

Severin Hauser

PhD Colloquium, Bregenz, October 28th, 2014

Content

- Introduction
- Basic Operations
- Properties
- Summary and Outlook

Introduction

Vocabulary

- Property - A Board has properties. e.g. append-only
- Message - Is posted to the bulletin board
- Attribute - Is added to a posted message to ensure a board property
- Post - A post represents the message and all it's attributes

Append-only

- No posted message m can be deleted
- No posted message m can be altered
- $\mathcal{P}_{\langle t \rangle} \subseteq \mathcal{P}_{\langle t+1 \rangle}$

Other Properties

- Prevent board flooding
- Give the user a receipt
- etc.

Basic Operations

Simple Operations

- Simple bulletin board
  - $\mathrm{Post}(m) \rightarrow$ post a message $m \in \mathcal{M}$, where $\mathcal{M}$ is the set of possible messages the board can accept
  - $\mathrm{Get}() : R \rightarrow$ retrieve the current state of the board as result R

Post

- Either the user or the board can add an attribute to m
  - list of user attributes α
  - list of board attributes β
- The post $p = (m, \alpha, \beta)$ is stored in $\mathcal{P}$
- For the user to gain full knowledge of the post, β must be returned.

$$\mathrm{Post}(m, \alpha) : \beta$$

Get

- Limit the result R by introducing query $Q \subseteq \mathcal{M} \times \mathcal{A} \times \mathcal{B}$
  - $R = \{(m, \alpha, \beta) \in \mathcal{P} : (m, \alpha, \beta) \in Q\} \subseteq \mathcal{P}$
- The board can add result attributes γ to R

$$\mathrm{Get}(Q) : R, \gamma$$

Properties

Properties

- Post properties
  - Adds an attribute to either α or β
- Get properties
  - Adds an attribute to γ
  - is added by the bulletin board
- Further properties
  - Adds additional operations to the board. Does not require attributes

Sectioned

- Allows to separate unrelated messages into different sections
  - e.g. the data of various elections
- User attribute $s \in \mathcal{S}$ must be provided

Grouped

- Messages are organized into groups
- Messages in the same group are usually similar
- user attribute $g \in \mathcal{G}$ must be provided
- $\mathcal{G}$ is the same for every section s.

Typed

- Depends on Grouped
- Defines for g_i the set of correct messages $\mathcal{M}_i \subseteq \mathcal{M}$
- Does not add an attribute

Certified Posting

- With this property every user receives after a successful post a receipt from the board
- Board attribute $S_p = Sign_{sk_{BB}}(m, \alpha, \beta_l)$ is added by the bulletin board where
  - sk_{BB} is the secret key of the bulletin board
  - β_l is the sublist of all board attributes before S_p

Certified Reading

- This is a get property
- With this property the bulletin board commits to every result R
- Result attribute $S_Q = Sign_{sk_{BB}}(Q, R, \gamma_I)$ is added by the bulletin board
  - γ_I is the sublist of γ added before S_Q

Notifying

- This property belongs to further properties
- It allows an entity e to register for a Query Q on the bulletin board
- If a post full fills Q, e is notified.
- This property results in the following two operations:
  - Register(e, Q) : c
    Where Q represents the query for the messages the entity is interested in and c a return code, which can be used to unregister.
  - Unregister(c) : -
    By providing his/her return code c, one can unregister and will not receive any further notification.

Summary and Outlook

Outlook

- Trust assumptions for the bulletin board
- Verifiable append-only bulletin board
- Dependencies of the properties for verifiability

Questions?

http://e-voting.bfh.ch

severin.hauser@bfh.ch