### **Attack Design**

The side channel vulnerability enables an adversarial user to discover the time of their hidden auditing event. Since the attack involves intricate manipulations to a complex data-structure, it is much easier to convey via a slide show. As such, please see the accompanying slide-deck: proofs/Collab\_Attack.pdf. The slide-deck describes the vulnerable data structure and the attack, including pseudocode and a worst case analysis.

**Proof Script**

The proof script sends UDP packets to the server in order to conduct the attack as described in the slide deck. In order to differentiate between insertions that induce a split and those that do not, the proof script makes use of a hard-coded response time threshold. The attacker determines his threshold by analyzing the program offline; i.e., the determination of time threshold does not count against attacker’s operation budget. Based on data in Figure 1 of the design document, the proof script takes 1,000,000 ns as its time threshold.

**Secret Value**

Collab is packed with canned event data, including a hidden auditing event for user ‘picard’. His hidden auditing event has ID 622448. To ensure the secret is worst case, the hidden auditing event was placed into the largest interval between canned event IDs. Within that interval, an event ID was selected which would take the maximum number of binary search steps.

**Operation Budget**

We define an attacker operation as the sending of a UDP request to the Collab server. The Collab server listens for requests on UDP port 7688, and each request can be sent to the Collab server in a single UDP packet. We therefore specify the attacker's operation budget in terms of UDP packets sent to the Collab server on port 7688.

The attacker's goal is to determine the event identifier (an integer) of the hidden auditing event scheduled for user 'picard'. In particular, the attacker is to develop an attack which can discover the secret 100% of time by sending no more than 140 UDP packets to the Collab server on port 7688.