SilverLine: Data and Network Isolation for Cloud Services

Yogesh Mundada
Anirudh Ramachandran
Nick Feamster

Cloud Computing Advantages

- Reduced operational costs
- Reduced management overhead
- Easier resources scaling
- Lowers the barrier to entry for new services

Cloud revenue for 2010 was $68 billion.
Estimated revenue for 2014 is $150 billion.

Recent Cloud Data Leak Incidents

- Microsoft BPOS cloud service data breach

  (Dec 2010)
- Heroku cloud application platform vulnerability

  (Jan 2011)
- Dropbox hash-tag security flaw (May 2011)

Occurrences such as these make adoption of the cloud harder

Top Cloud Computing Threats

- Shared resources
  - Heroku

- Data loss and leakage
  - Microsoft BPOS
  - Dropbox

SilverLine Solution: Isolation

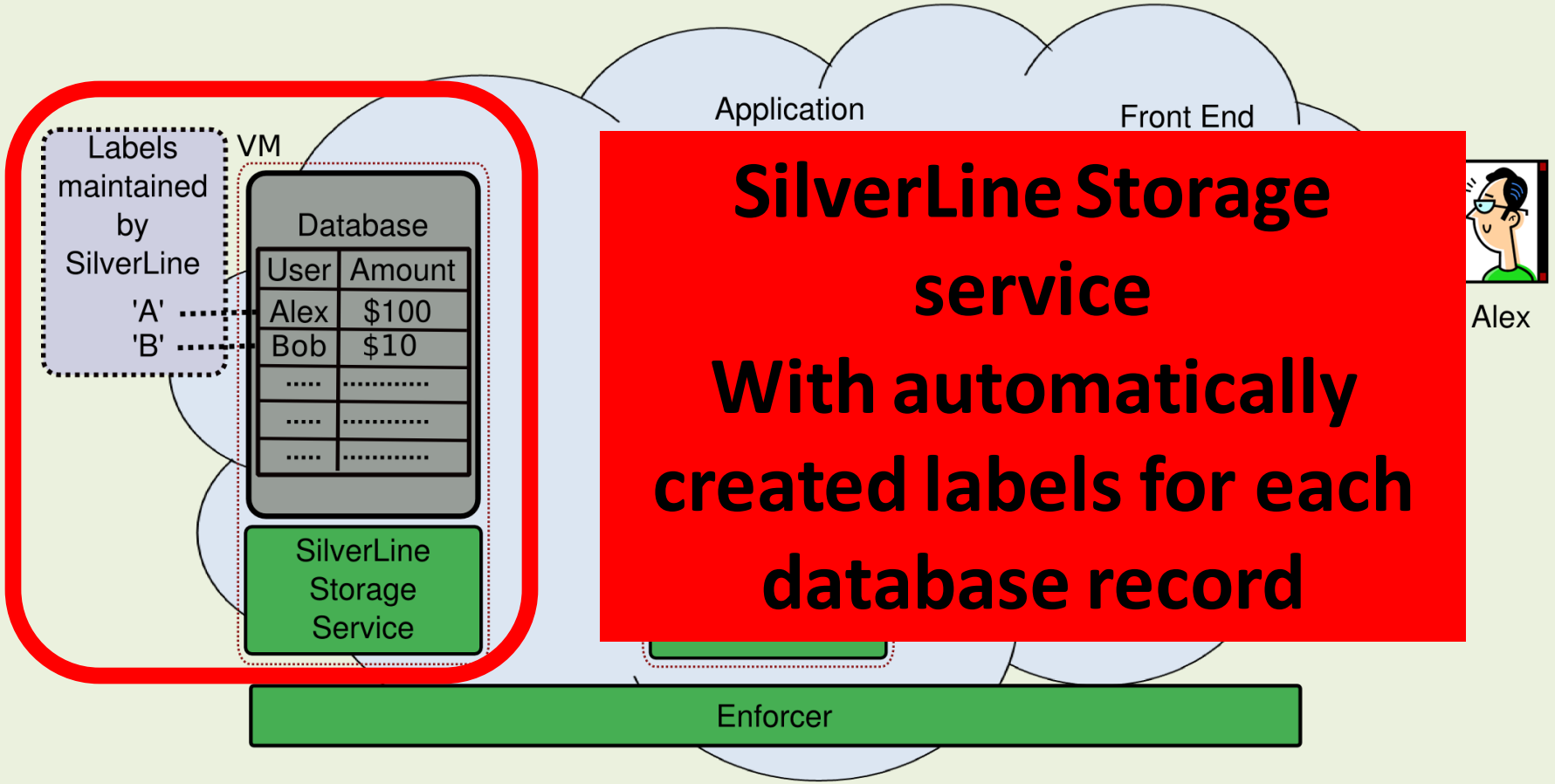
Problem	Attack	Solution
Data Loss	**Service exploit, Operating environment exploit, Misconfigurations**	**SilverLine's Information Flow Tracking and Control**
Network Side-Channels	Gain more information about the environment through namespace, RTT and hop-count study	SilverLine's obfuscation of network metrics to reduce the information entropy.

SilverLine Data Isolation

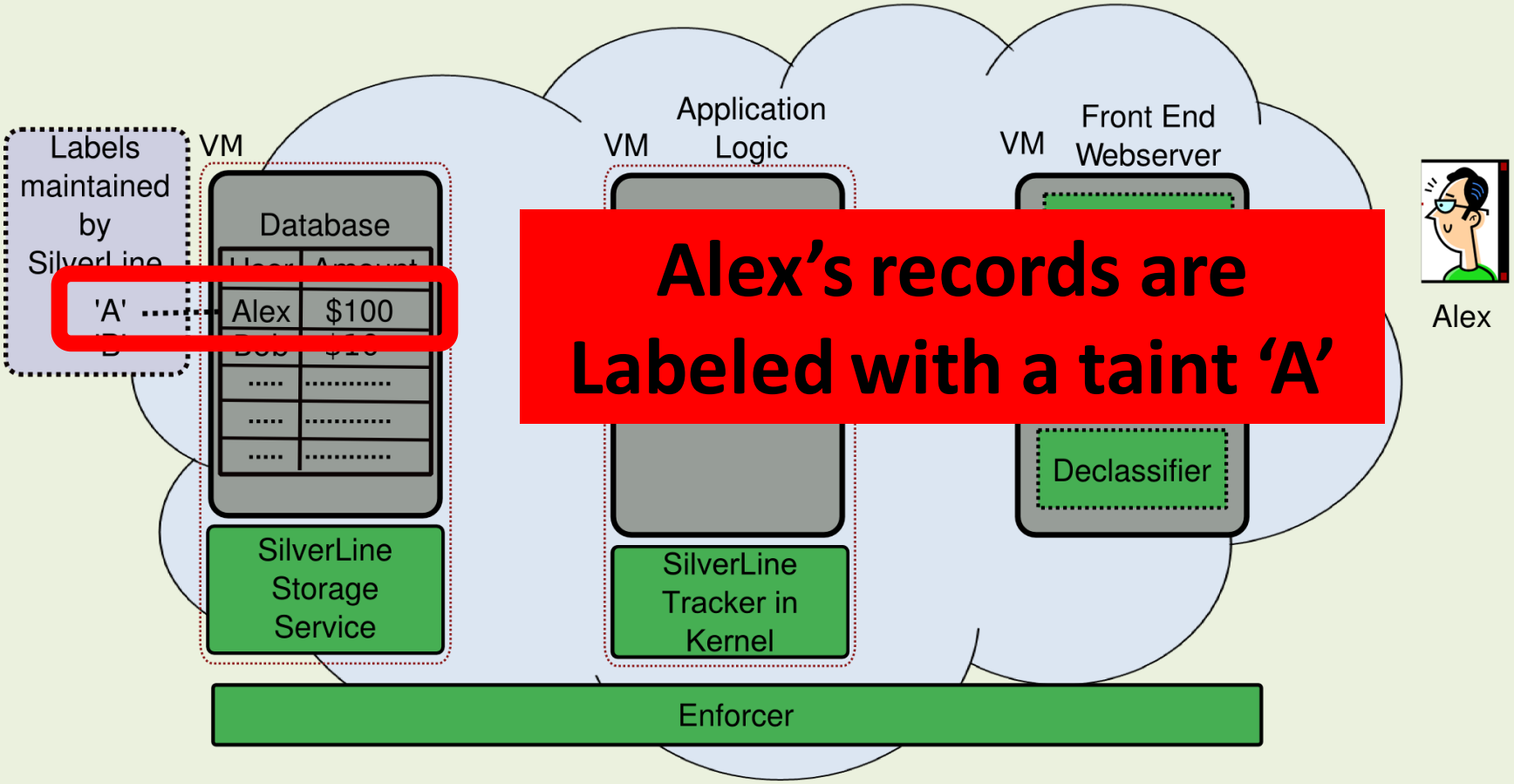
- Information Flow Tracking
  - Add taints or labels to data
  - Track the taints
  - System Call Hooks

- Components of the system
  - Tracker: Initialize and track taints, on end hosts
  - Enforcer: Stop unauthorized data flow, in the network

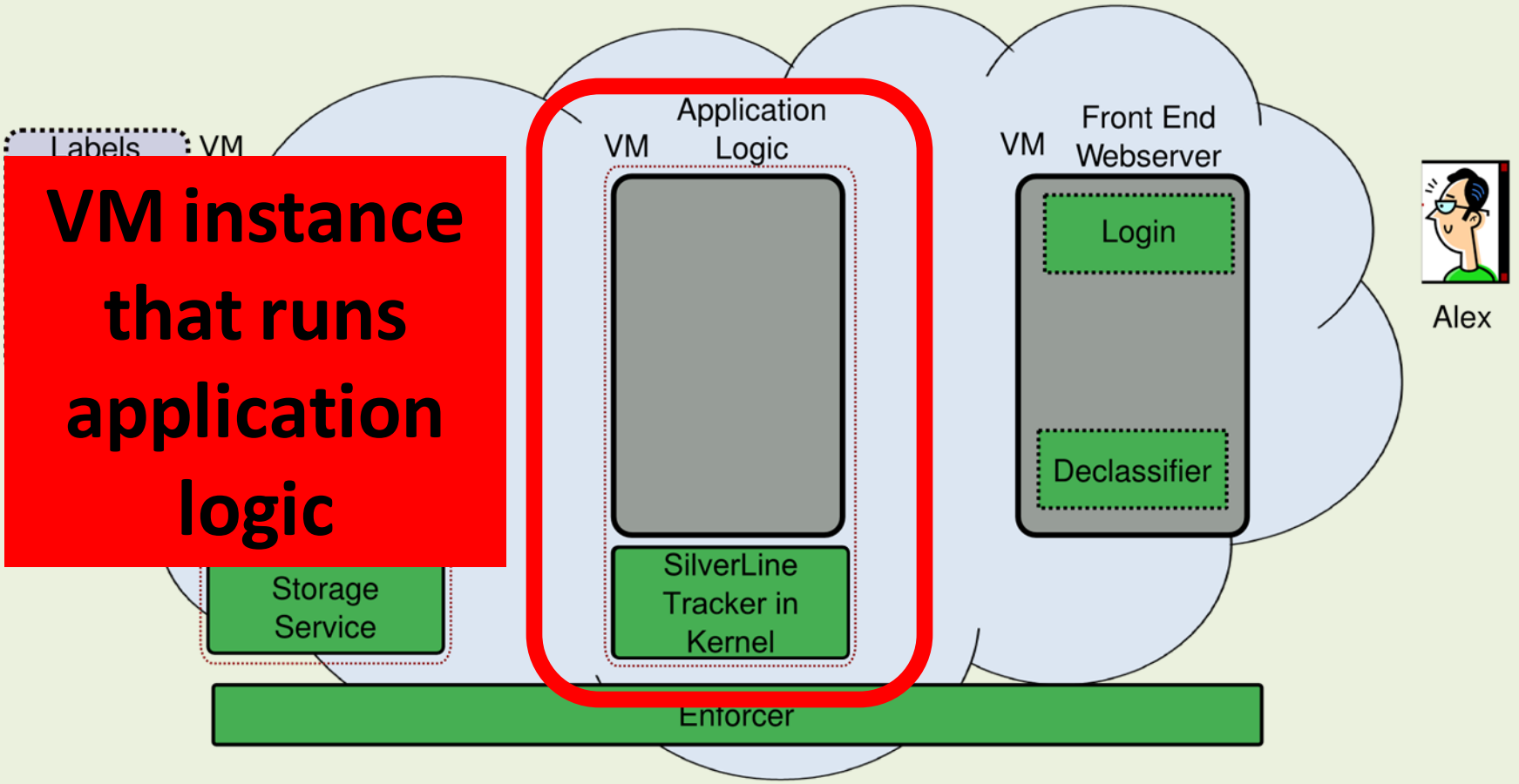
Example Setting



Example Setting

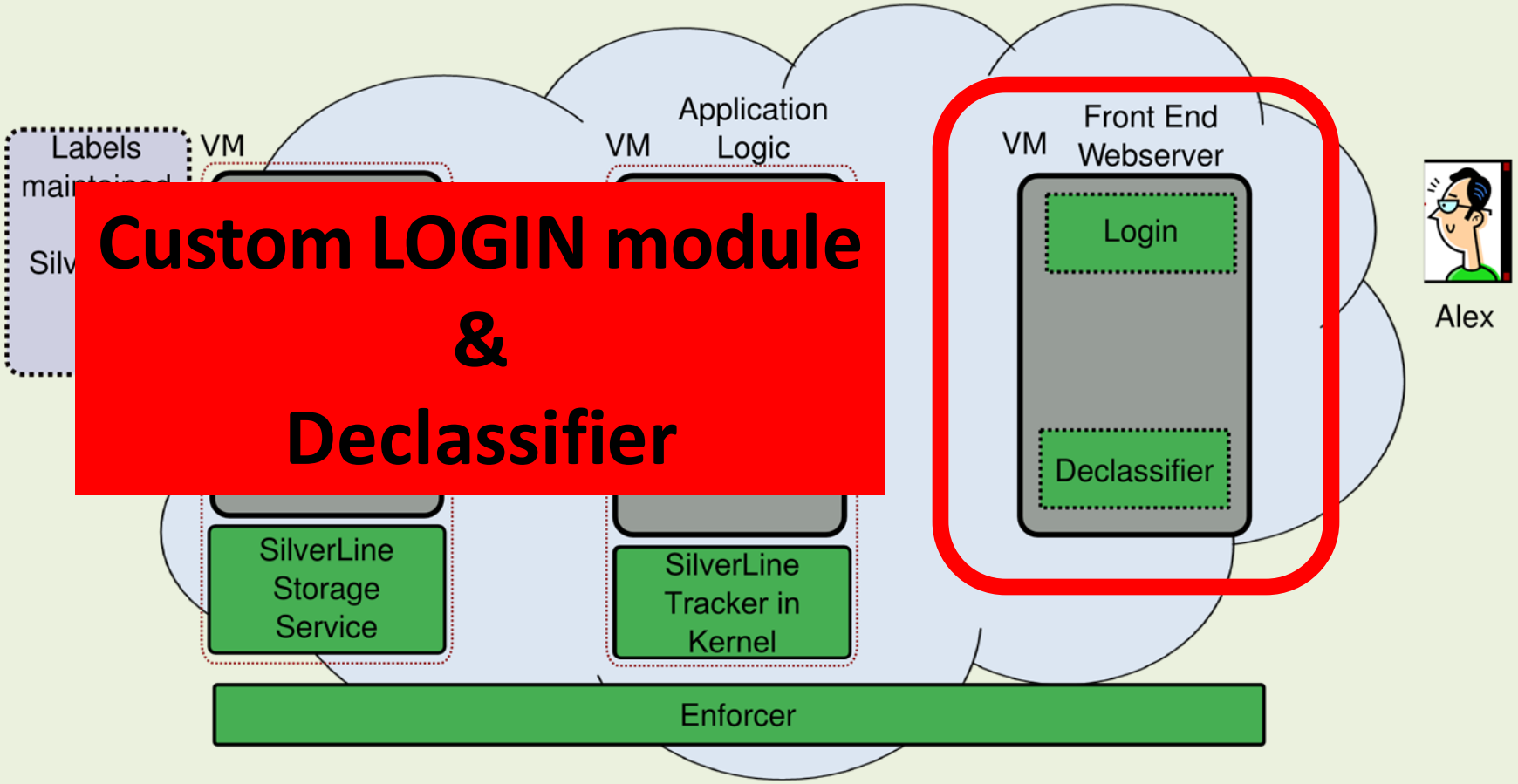


Example Setting

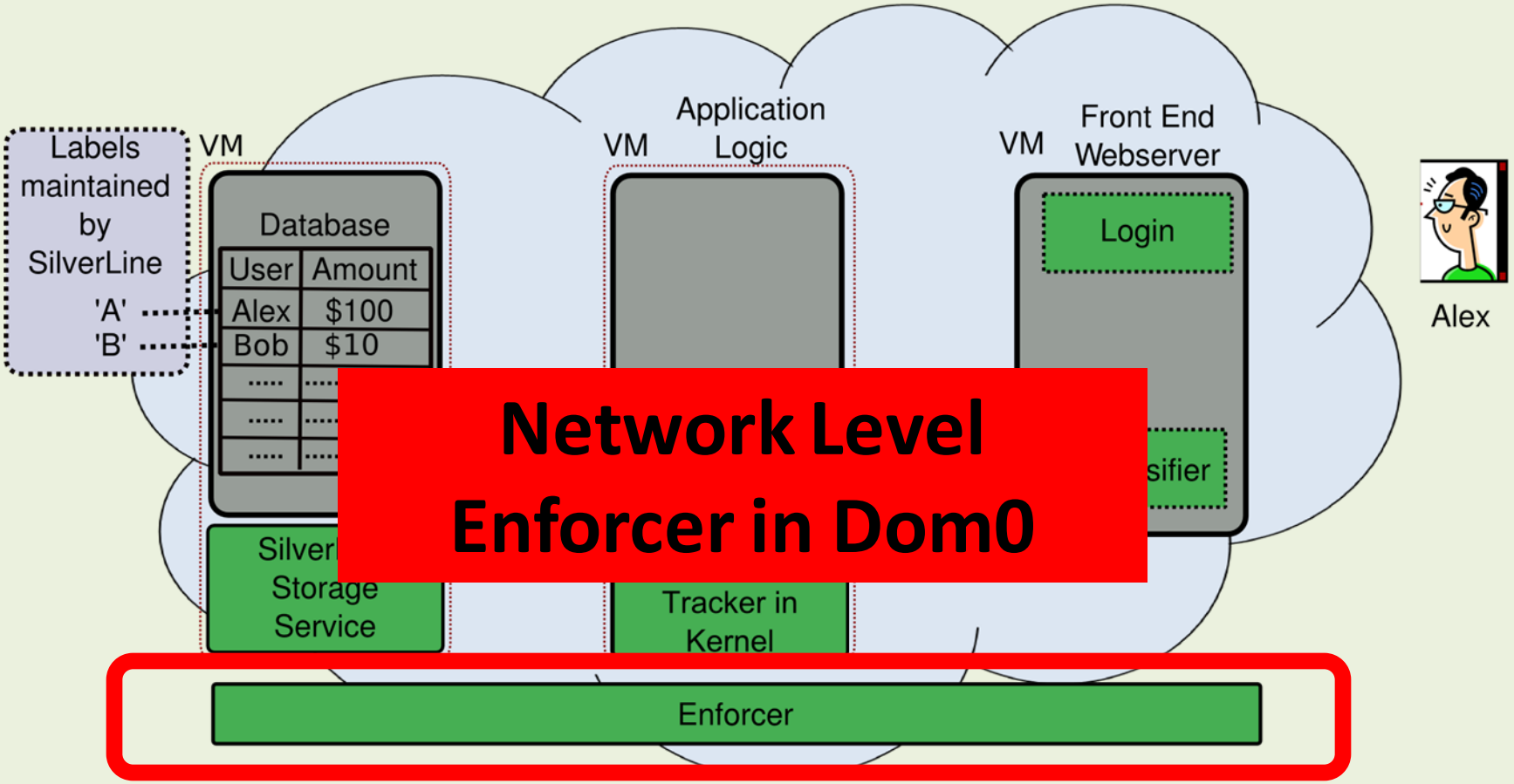


VM instance that runs application logic

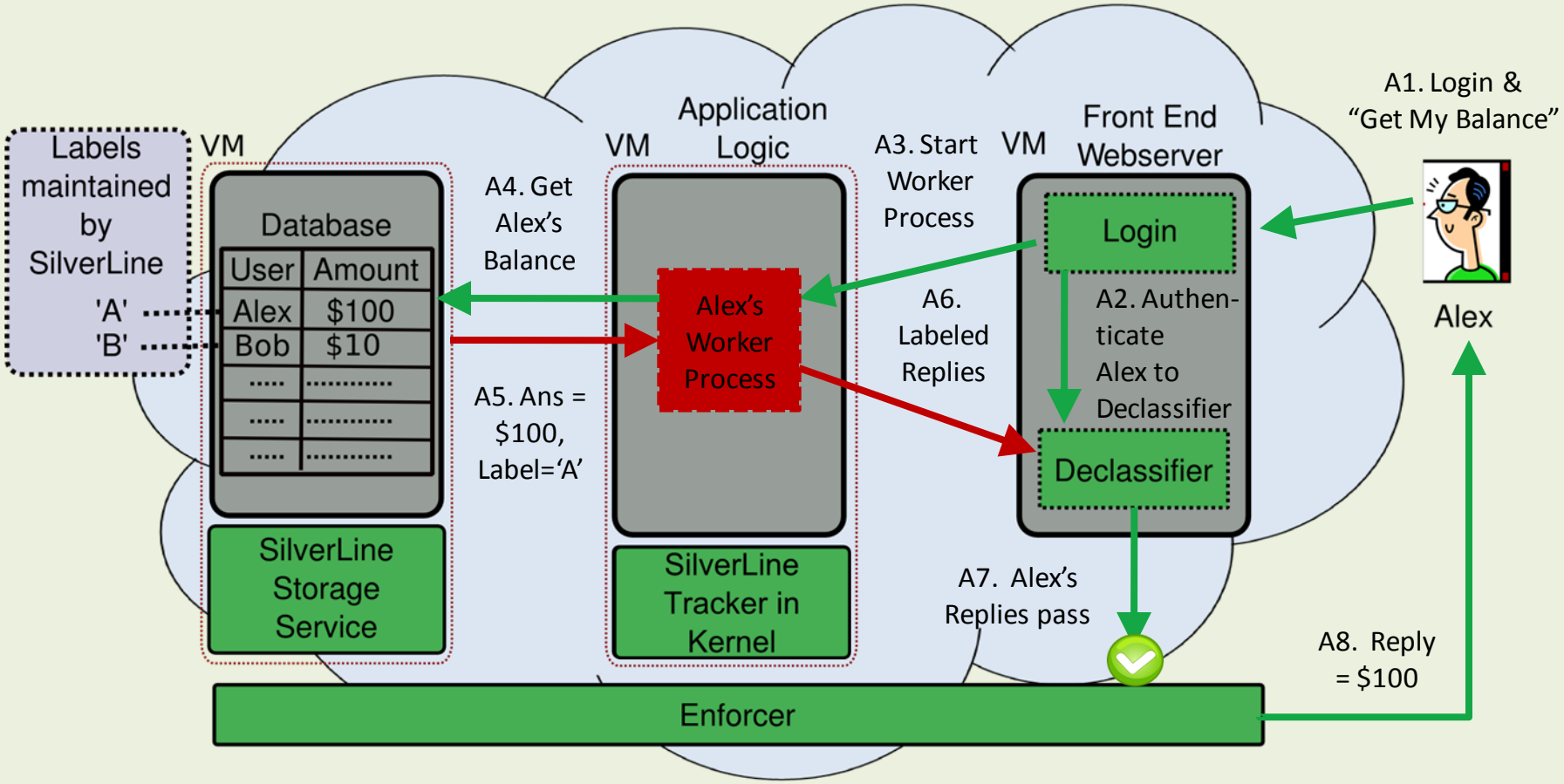
Example Setting



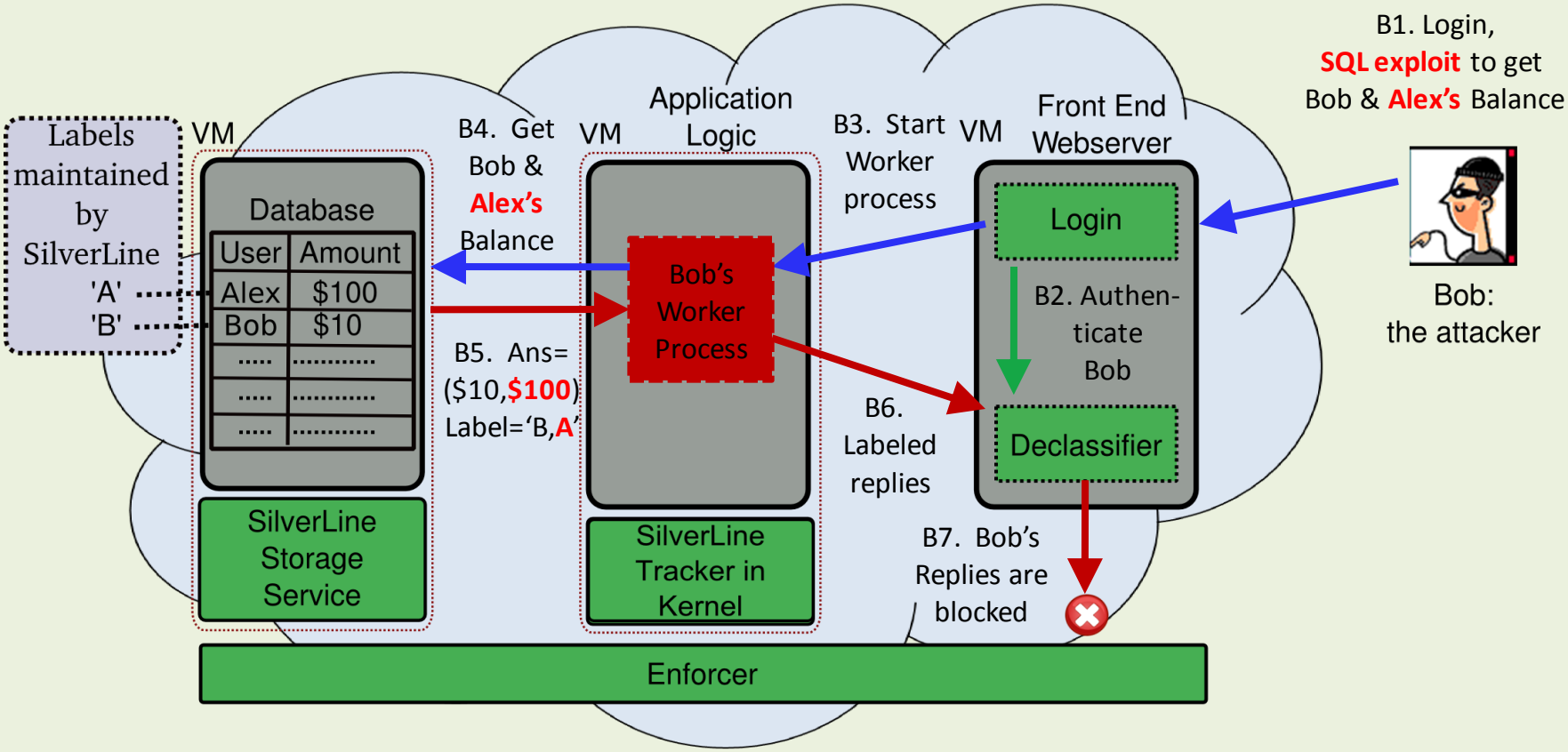
Example Setting



Normal User's Interaction



An Attacker's Interaction

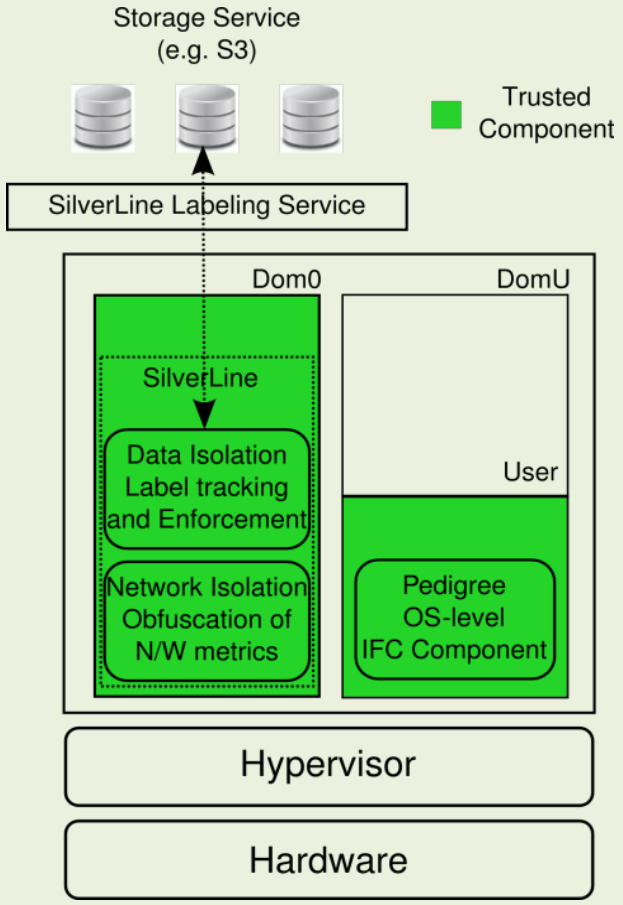


SilverLine Configuration

- Labeling Service
  - Specify Taint Creation Policy

when query := "INSERT" **and** table := "USERS": *Generate a new label; add it to the DB record*

- Custom **Login** module
  - Provided by each tenant
  - Authorizes legitimate users

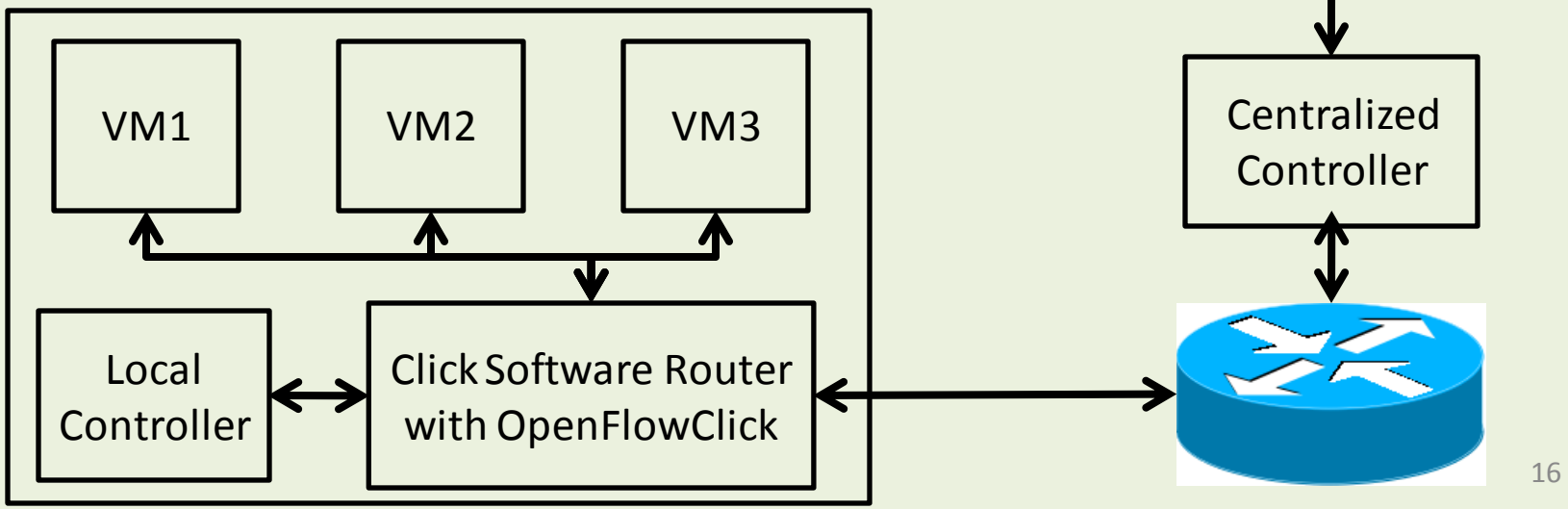


SilverLine Solution: Isolation

Problem	Attack	Solution
Data Loss	Service exploit, Operating environment exploit, Misconfigurations	SilverLine's Information Flow Tracking and Control
Network Side-Channels	**Gain more information about the environment through namespace, RTT and hop-count study**	**SilverLine's obfuscation of network metrics to reduce the information entropy.**

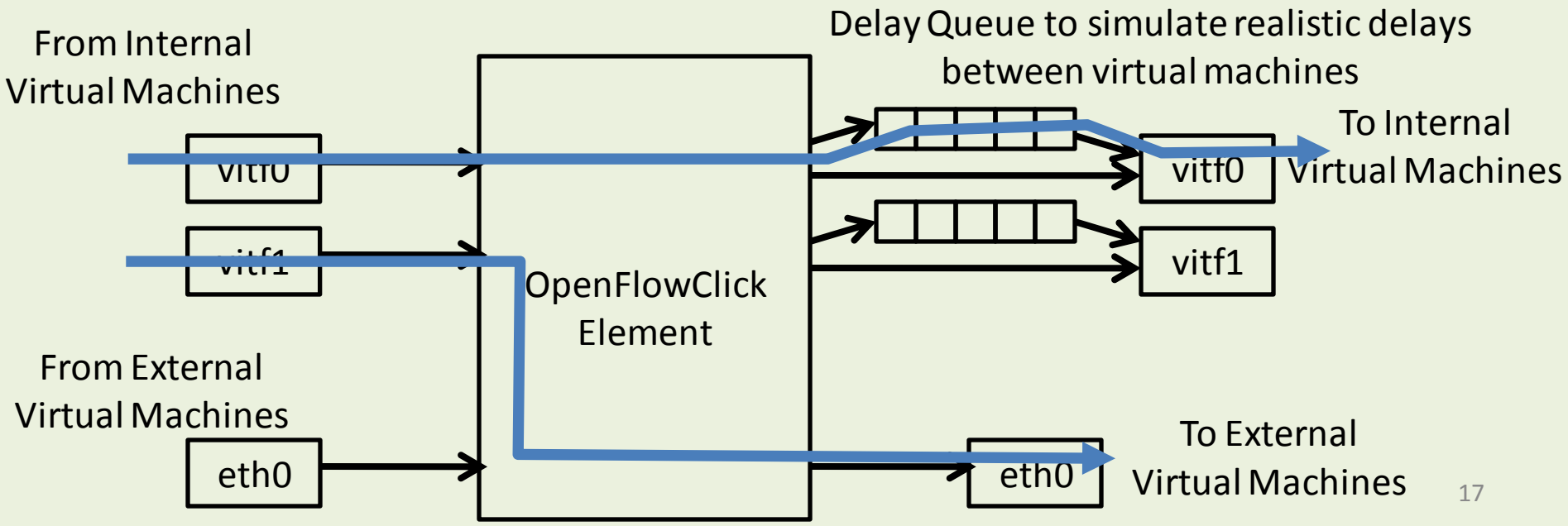
SilverLine Network Isolation

- IP address obfuscation
  - Actual Internal IP to Pseudo IP
  - OpenFlow protocol
- Entirely in the software
- Minimal changes



SilverLine Network Isolation

- Normalize network metrics
  - Realistic RTTs between instances
  - Minimal threshold on hop counts
  - Modified openflow module for per packet decision



SilverLine

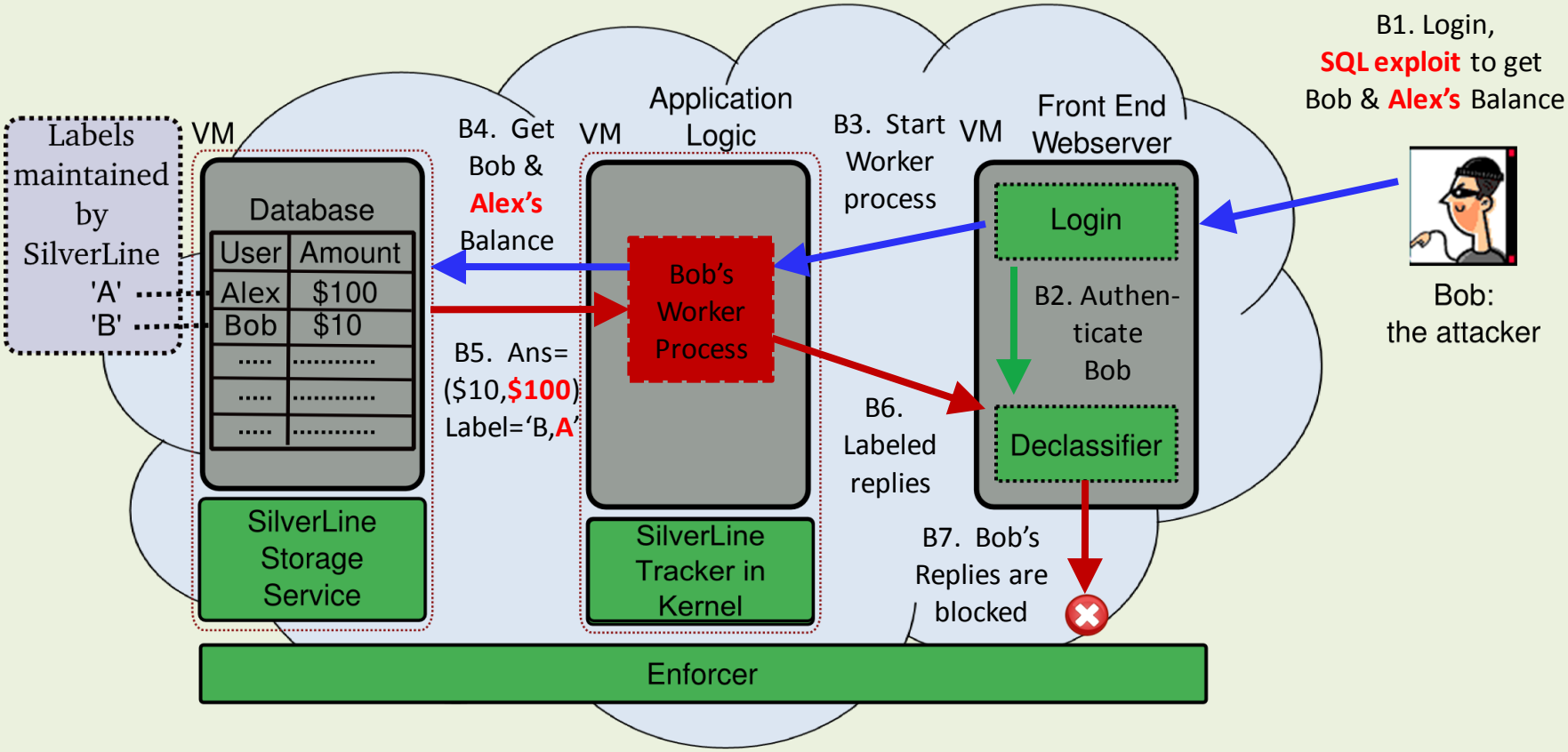
Summary

- Data Isolation: Information Flow Tracking
- Network Isolation: Reducing the entropy of the network side-channels

Future Work

- Measure the taint leakage
- Fine grained tainting in a VMM

Questions


Labels maintained by SilverLine
'A'
'B'
VM
Database
User
Amount
Alex
$100
Bob
$10
SilverLine Storage Service
B4. Get Bob & Alex's Balance
B5. Ans= ($10,$100) Label='B,A'
VM
Application Logic
Bob's Worker Process
SilverLine Tracker in Kernel
B3. Start Worker process
VM
Front End Webserver
Login
B2. Authen-ticate Bob
Declassifier
B6. Labeled replies
B7. Bob's Replies are blocked
Enforcer
B1. Login, SQL exploit to get Bob & Alex's Balance
Bob: the attacker