Account Lockouts: Characterizing and Preventing Account Denial-of-Service Attacks

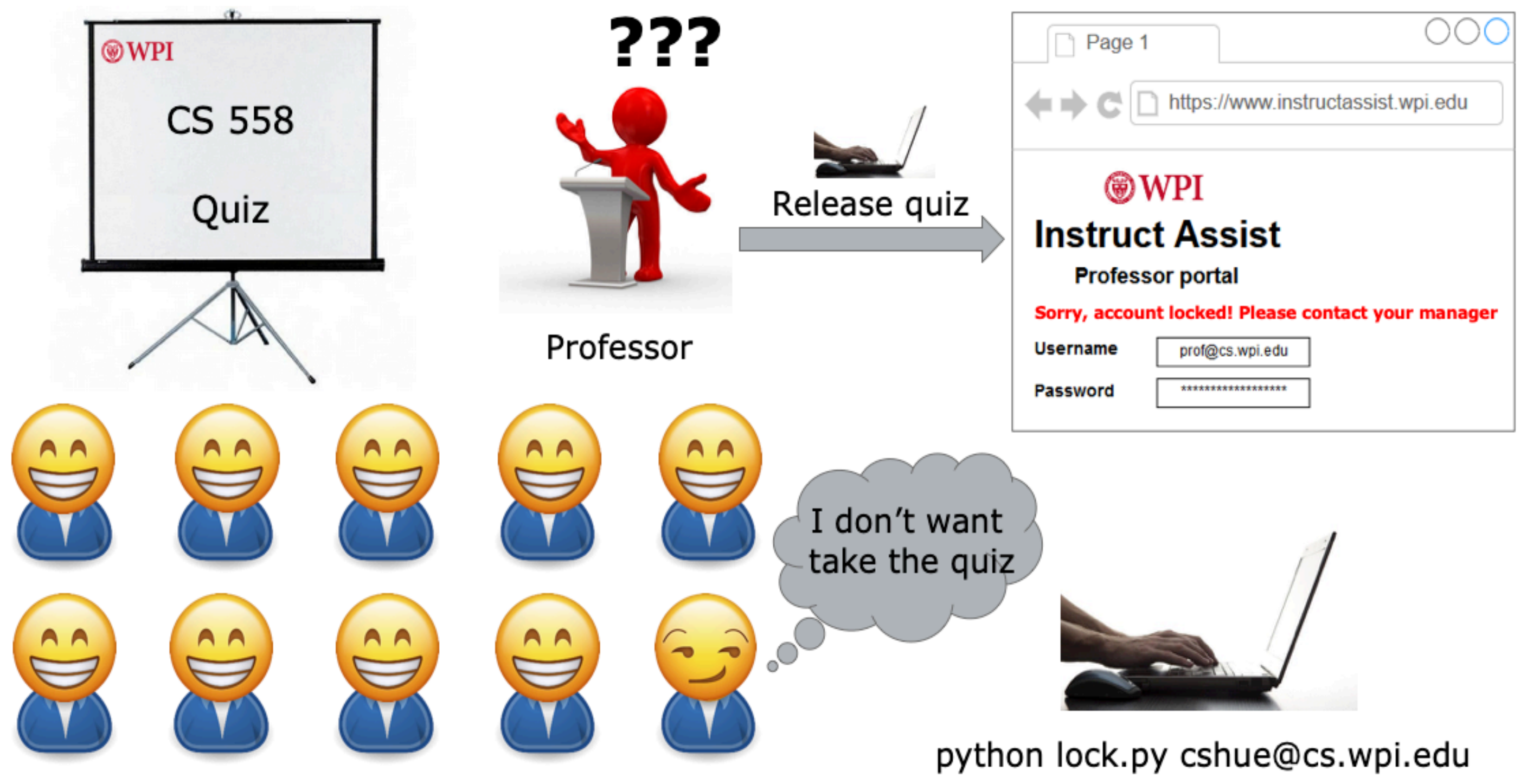
Yu Liu, Matthew R. Squires, Curtis R. Taylor, Robert J. Walls, Craig A. Shue

Introduction

- Enterprises lock accounts after a given number of failed login attempts, which combats password guessing.
- However, attackers can easily find a target username (e.g. from the email addresses) and launch an account lockout attack by logging in with a series of incorrect passwords.
- Account lockout thresholds and durations vary by security standard, but each make lockouts easy to trigger.

Standard	Lockout Thresholds	Lockout Periods
NIST	100	30 seconds – 60 minutes
SANS	5	30 minutes
PCI	6	30 minutes

Example Attack Scenario



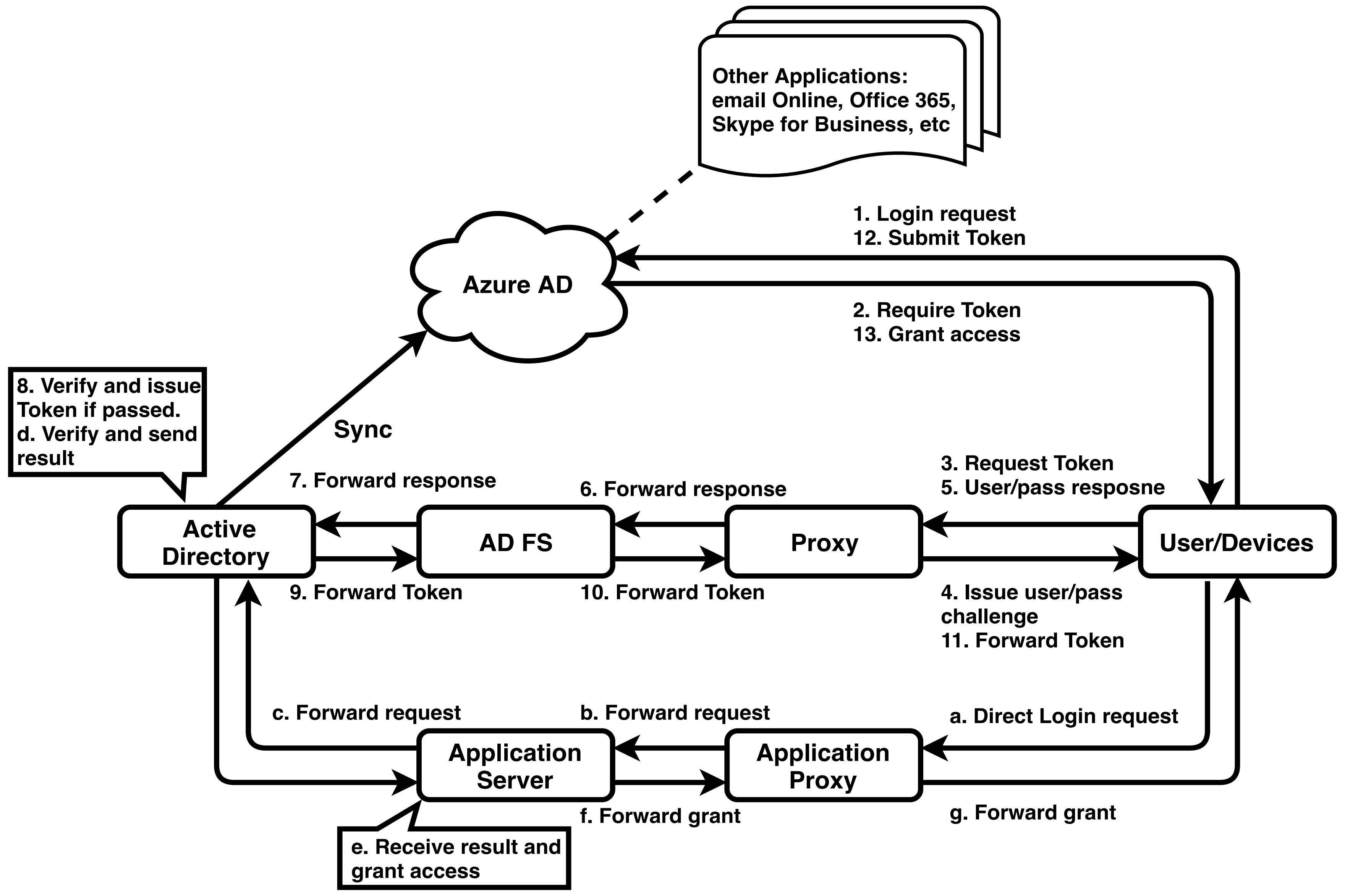
```
python lock.py cshue@cs.wpi.edu
```

Research Questions

- Is this attack a threat to real-world enterprises?
- If so, how many organizations are affected?
- Without modifying the legacy systems and devices, how can we stop password guessing while granting access to legitimate users?

Case Study: Microsoft Active Directory

- Used by 95% percent of Fortune 1000 companies
- Supports a variety of applications like Office 365, Skype for Business, and Workday
- Provides Single-Sign-On (SSO) to applications



Threat Measurement

Production Environment Study:

- An organization with over 5,000 employees gave us permission to test the attack on their system.
- From an attacker's perspective, we identify the attack surfaces.
- We target those attack surfaces and successfully locked the test account, which was confirmed by their IT staff.

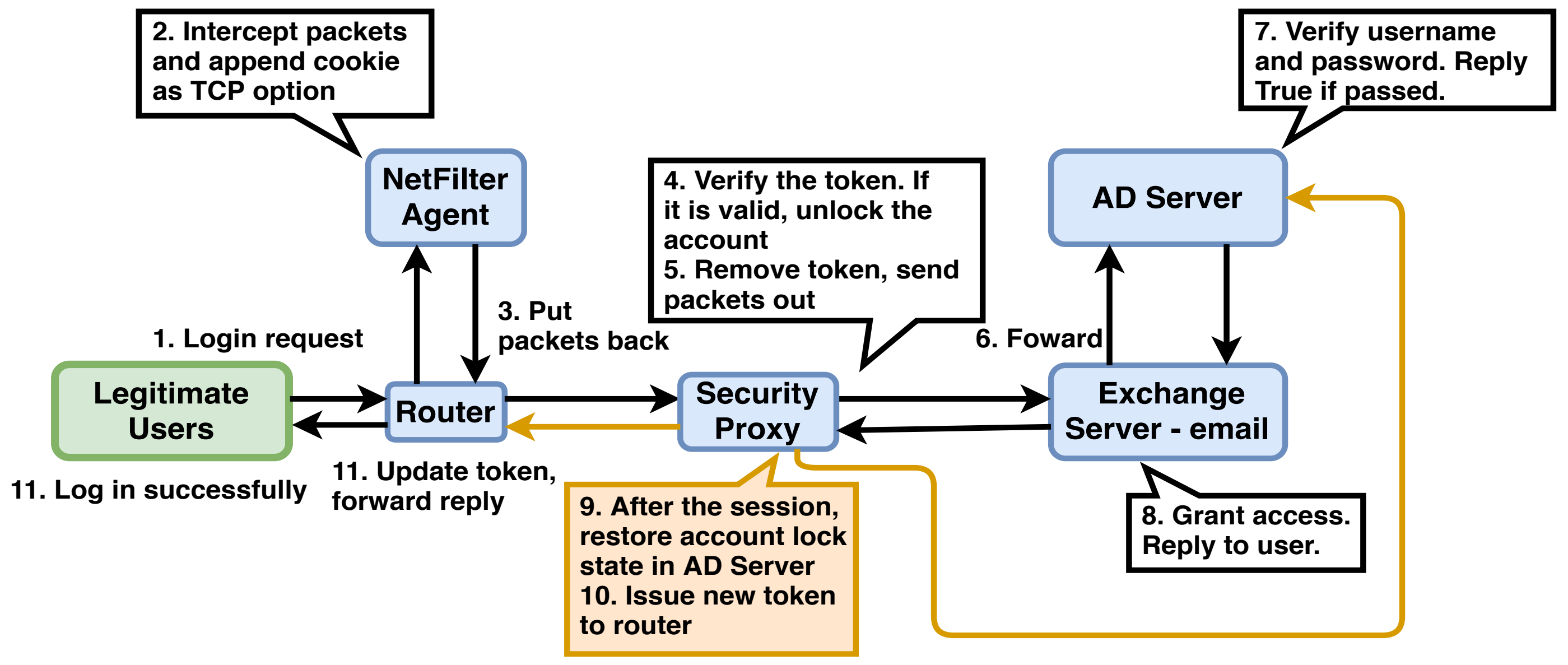
Large Scale Measurements:

- Focus on Fortune 1000 companies and 1066 top higher education organizations
- Identify attack surface exposed by Active Directory and related applications
- Result: 58% of Fortune 1000 and 77% of the education organizations are affected

Token-based Countermeasures

Residential router token insertion

- Home router inserts tokens into TCP options
- Security proxy verifies token. If valid, it unlocks the account, removes the token and sends request.

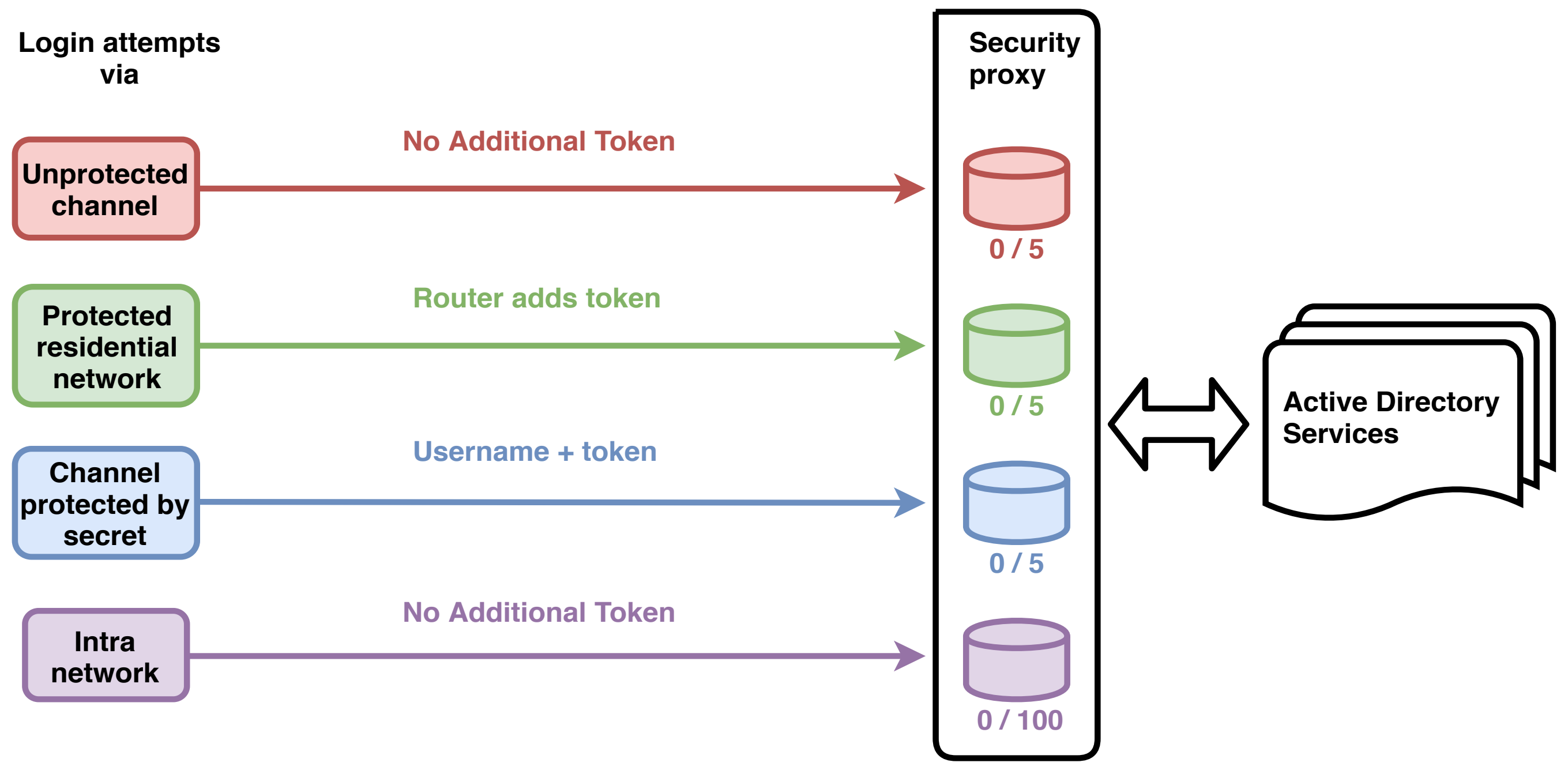

2. Intercept packets and append cookie as TCP option
7. Verify username and password. Reply True if passed.
NetFilter Agent
4. Verify the token. If it is valid, unlock the account
5. Remove token, send packets out
AD Server
1. Login request
3. Put packets back
6. Foward
Legitimate Users
Router
Security Proxy
Exchange Server - email
11. Log in successfully
11. Update token, forward reply
9. After the session, restore account lock state in AD Server
10. Issue new token to router
8. Grant access. Reply to user.

Shared secret information:

- Username + delimiter + code
- Code only known by client and server, e.g. employee ID number

Authentication Pool

- Incorporate various authentication methods, such as IP geolocation
- Separate lockout counter for each channel



Evaluation

- Prove that users with valid token can always access to their accounts
- Our methods add up to 180 milliseconds delay to the first packet, which is not likely to be perceived by users.