Developing Anomaly Detection Model for Security Auditing Service

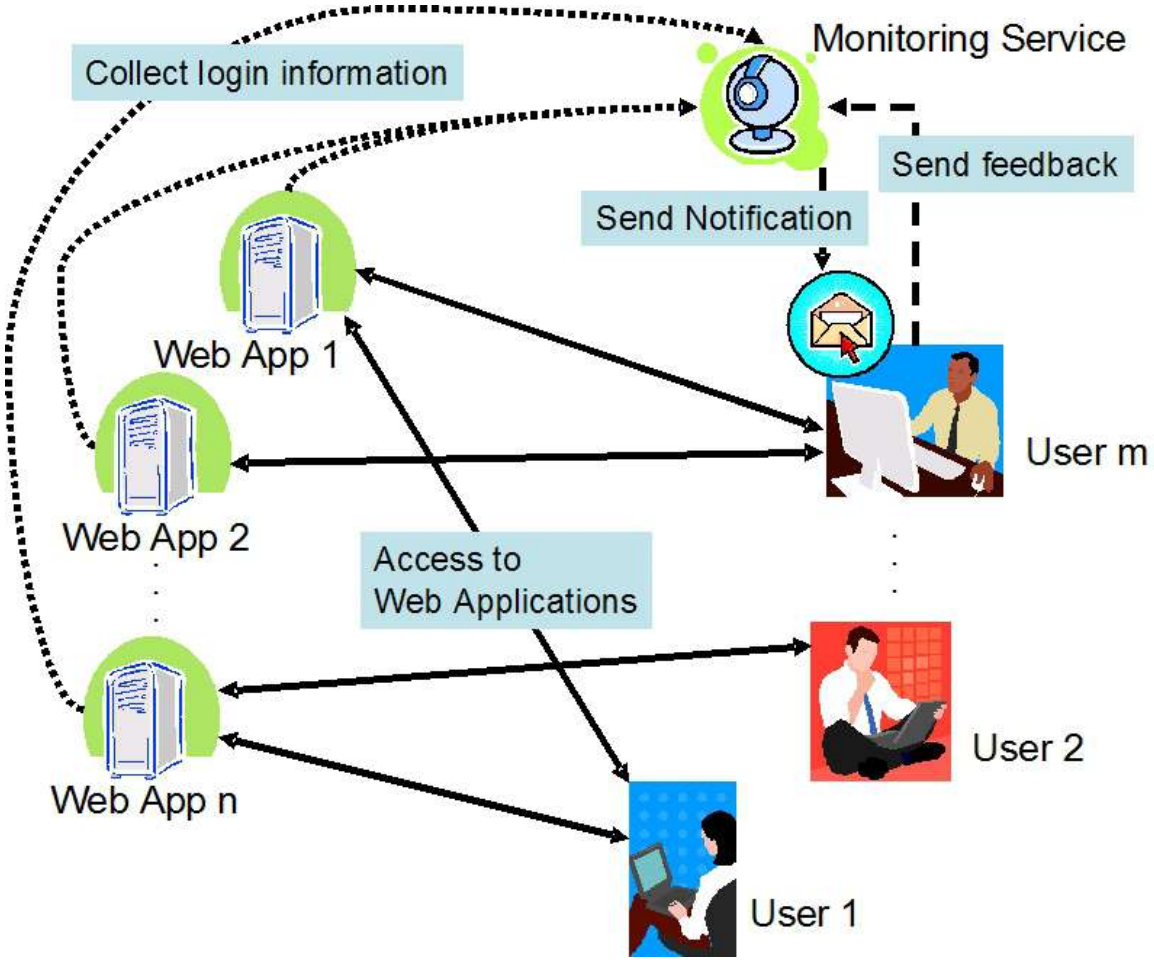
Daisuke Mashima

(with Professor Mustaque Ahamad)

Motivation and Scope

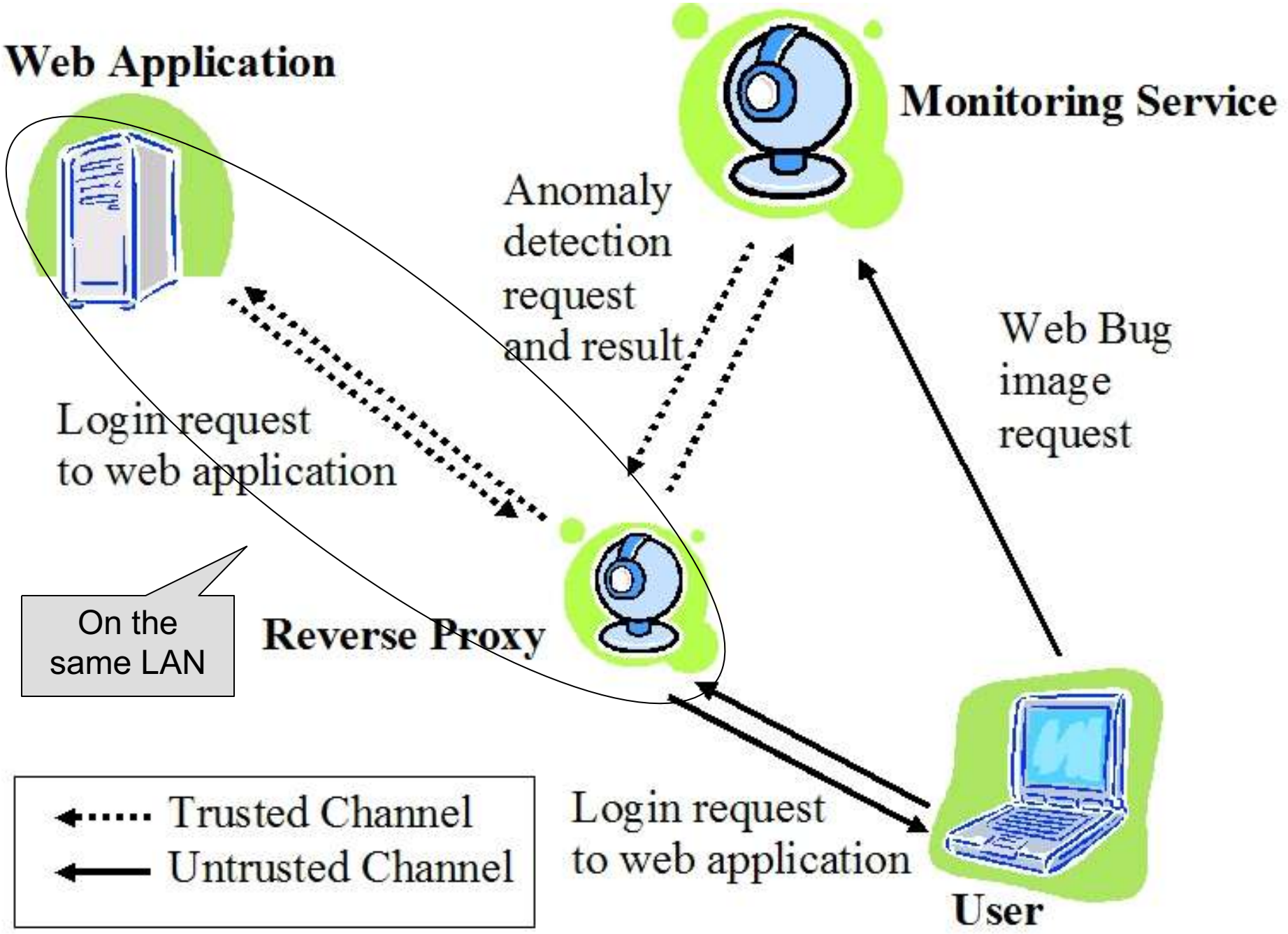
- Online identity theft is going to be more serious
  - Emergence of novel Internet devices
  - Diversity of Internet users
- Prevention of identity theft is never perfect.
  - Social engineering etc.
- We have to do detection in addition to prevention.
- The system must be transparent not only to users but also to existing applications
- We focus on detecting suspicious login to web applications.

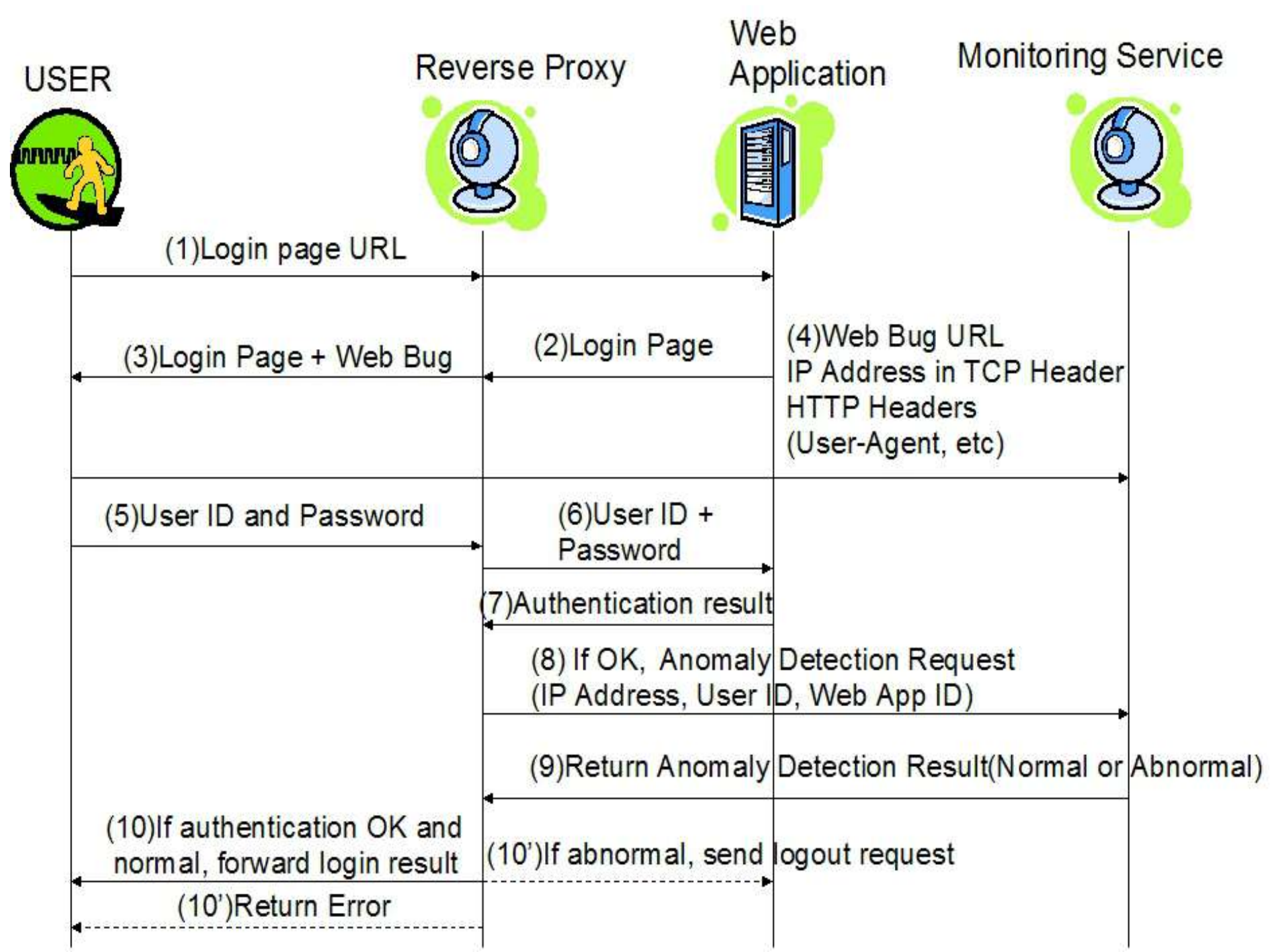
Abstract Image

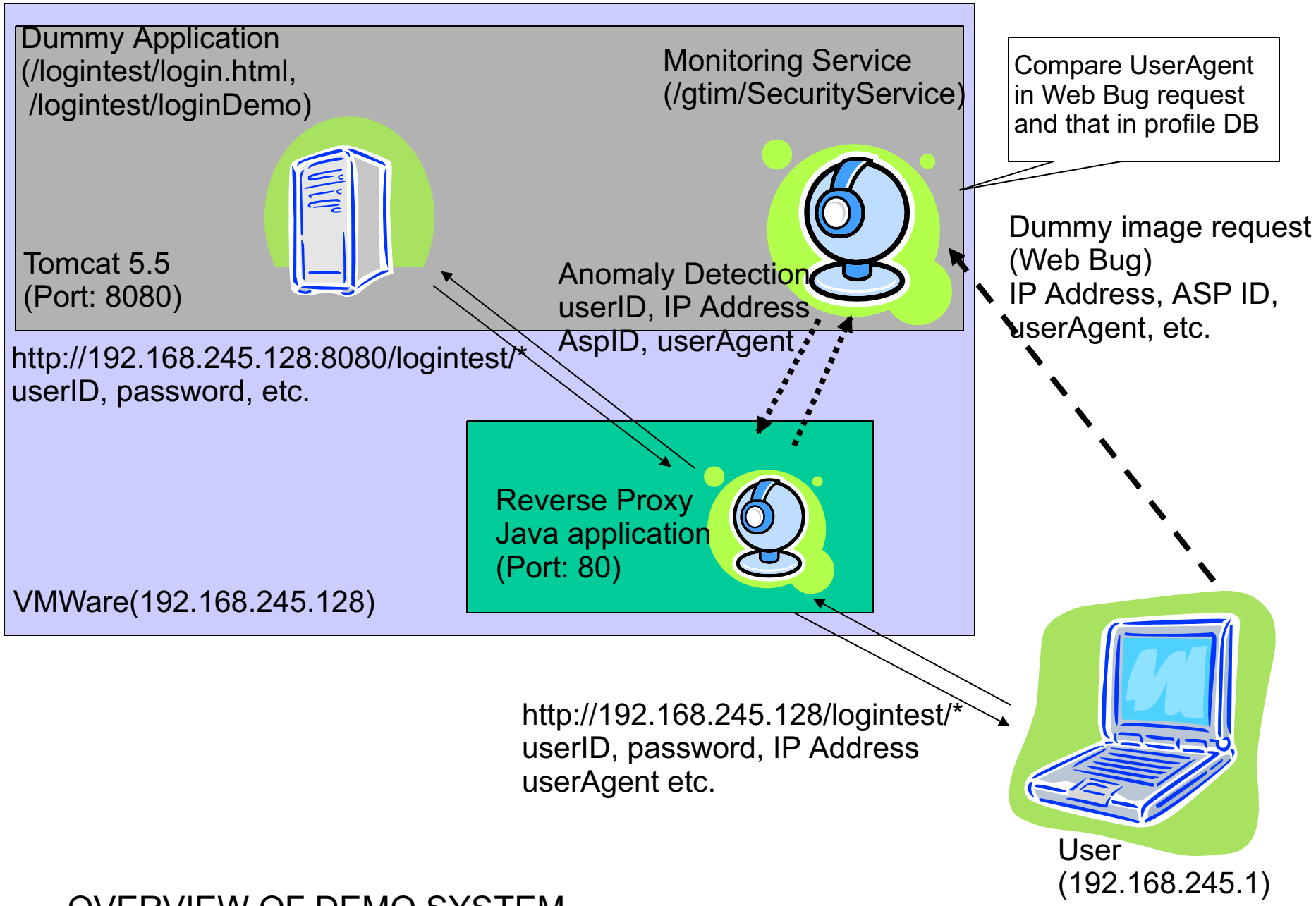


Identity-usage Monitoring System

- System Architecture
  - Centralized Monitoring Service
    - Conduct anomaly detection
  - Decentralized Reverse Proxy
    - Send login information to Monitoring Service
  - Web Bug
    - Make user send information automatically


Web Application
Monitoring Service
Anomaly detection request and result
Web Bug image request
Login request to web application
On the same LAN
Reverse Proxy
Trusted Channel
Untrusted Channel
Login request to web application
User


USER
Reverse Proxy
Web Application
Monitoring Service
(1)Login page URL
(3)Login Page + Web Bug
(2)Login Page
(4)Web Bug URL
IP Address in TCP Header
HTTP Headers
(User-Agent, etc)
(5)User ID and Password
(6)User ID + Password
(7)Authentication result
(8) If OK, Anomaly Detection Request
(IP Address, User ID, Web App ID)
(9)Return Anomaly Detection Result(Normal or Abnormal)
(10)If authentication OK and normal, forward login result
(10')If abnormal, send logout request
(10')Return Error



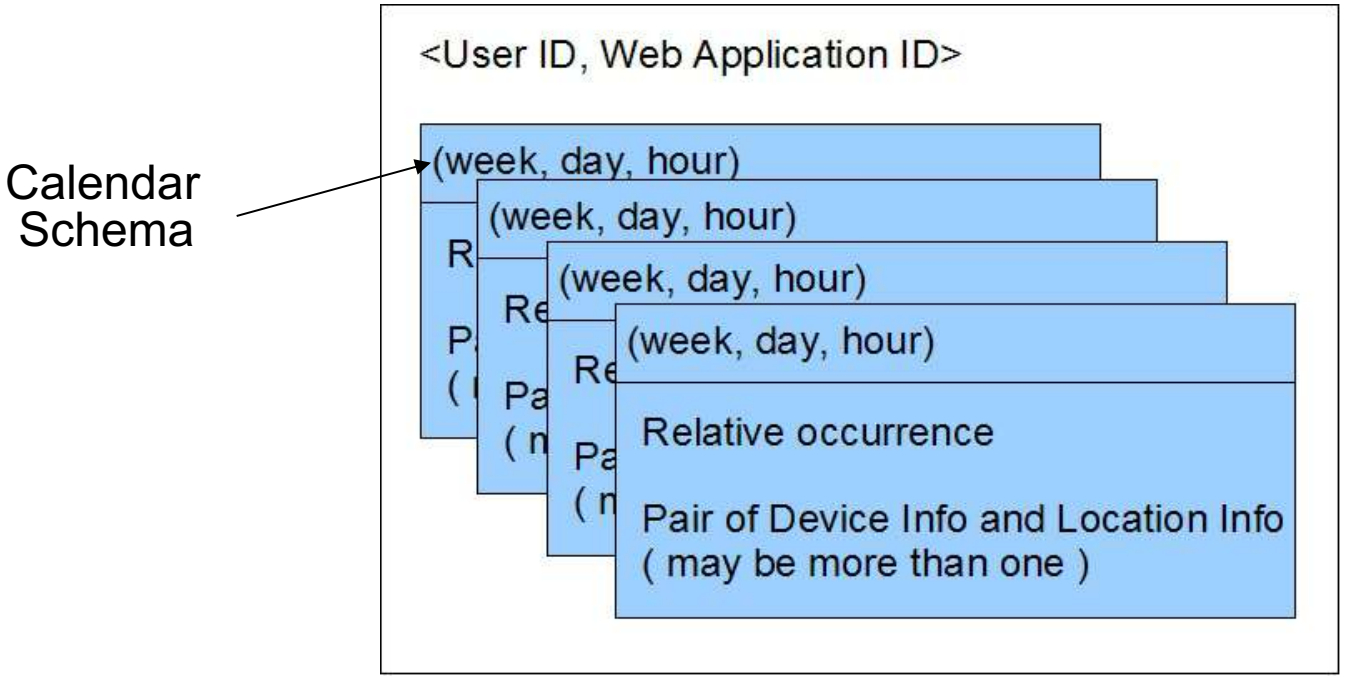
OVERVIEW OF DEMO SYSTEM

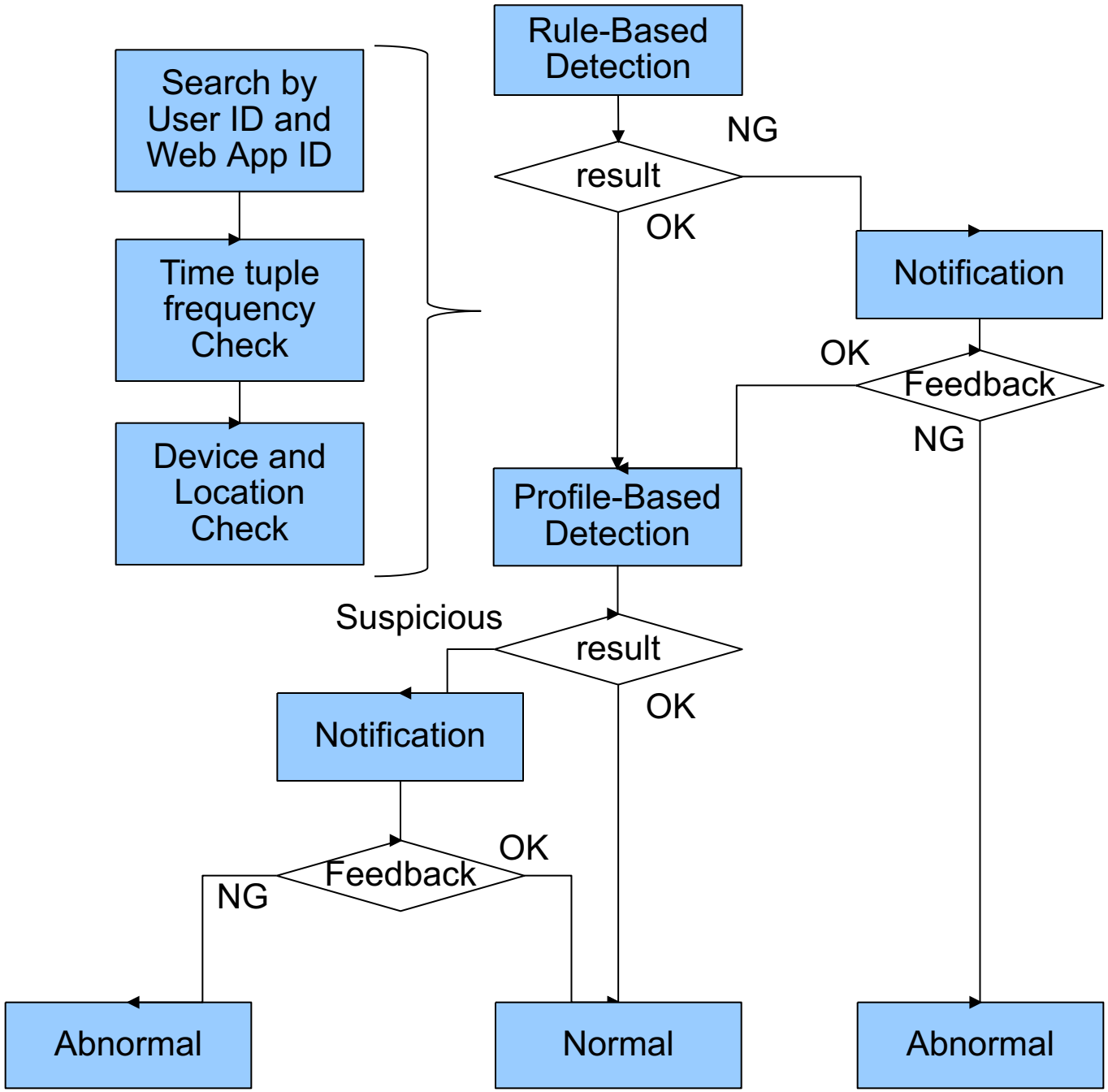
Detail of Anomaly Detection Process

- Periodic Detection
  - Main purpose is creating blacklist
- Frequency of the source IP address
  - Total number of access
- Per-request Detection
- Based on blacklist and user's individual profile
- Define user's individual profile for time category
  - Ex. Weekdays and weekends
  - Calendar Schema
- Utilize Delay-based IP Geolocation technique
  - Higher availability and precision
  - Can detect IP Spoofing "to a certain extent."

Individual Profile

- Defined under each pair of user ID and Web App ID
- By categorizing wisely, the number of tuples can be reduced.




Rule-Based Detection
Search by User ID and Web App ID
Time tuple frequency Check
Device and Location Check
result
NG
OK
Notification
OK
Feedback
NG
Profile-Based Detection
Suspicious
result
OK
Notification
Feedback
OK
NG
Abnormal
Normal
Abnormal

Interaction between Monitoring Service and Users

- Must be independent of the Internet
- Automated phone call to users' cell phones is a strong candidate.
  - Most people have cell phones.
  - As long as phone companies are trustworthy, the channel is regarded as secure.

Future work

- Future work includes
  - Improve anomaly detection model
    - User Profiling
    - Intrusion Detection
  - Evaluation
    - System Architecture
    - Security
    - Performance
    - Precision of detection

Thank you very much for your attention.