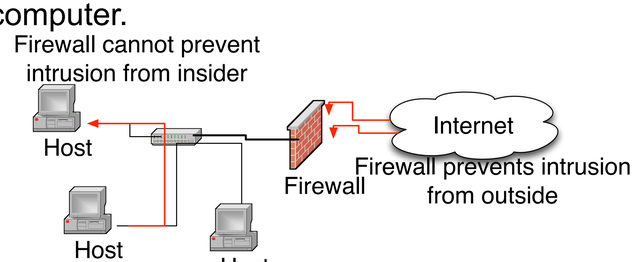
An Architecture of Crowdsourced Intrusion Detection System

Daniel Song, Kyung Hwa Kim, Henning Schulzrinne
Dept. of CS, Columbia University in the City of New York

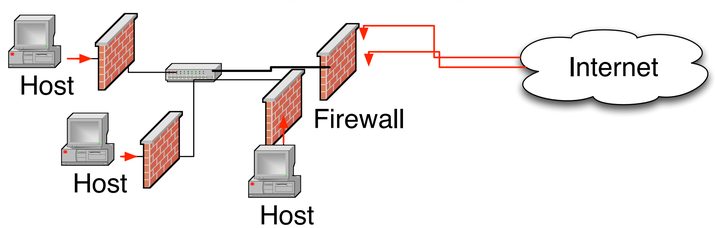
Motivation

- Firewalls focus on intrusion from outside.
- What about the malicious attempt from the inside?
- It is difficult to detect whether an outgoing traffic is a malicious traffic, so we suggest a system that
  1. asks the user about the traffic.
  2. collects the data and learns from it.
- Collaborative method can strengthen the IDS but different people have different knowledge on computer.

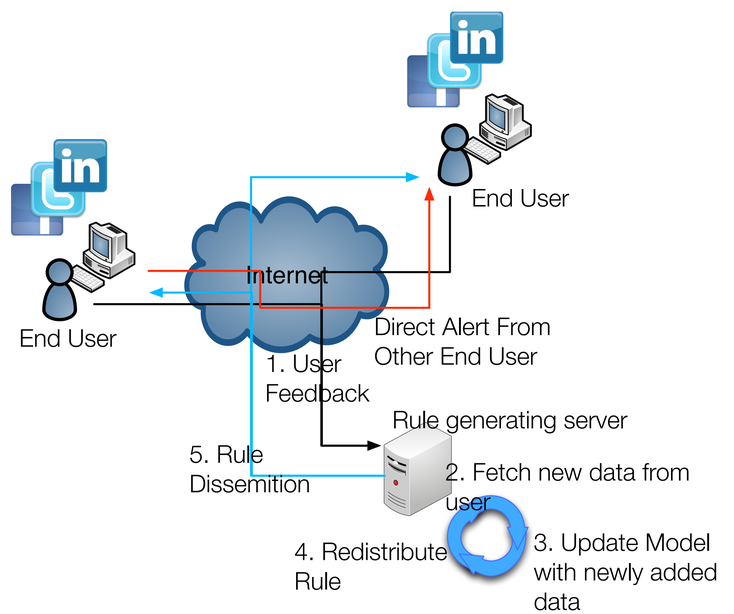


Goal

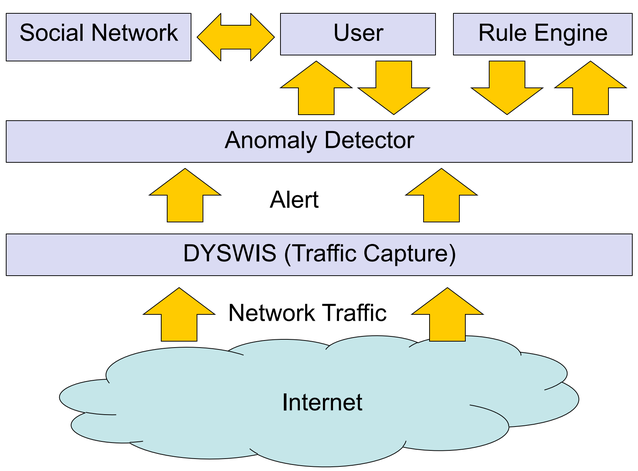
- Detect suspicious outbound traffic of a host to find out whether the host is compromised.
- Use users' feedbacks as a training set of a supervised anomaly detection.
- Differentiate the user using Social Network services like linked-in.
- Different user will have different trust factor based on Social Network profile. (e.g network experts will have higher initial *tf*)



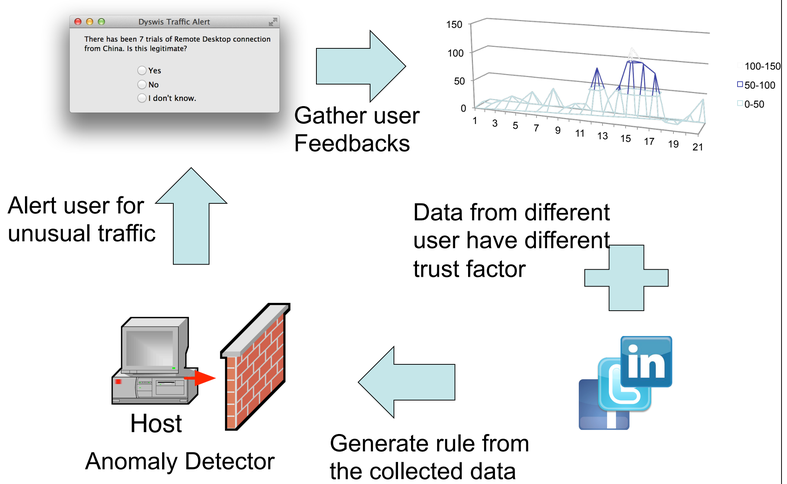
Collaborative Intrusion Detection



Rule Engine



Supervised Machine Learning



Trust Factor

- Trust factor (*tf*) is first determined by social network profile.
- *tf* will change overtime based on the quality of the data. (e.g if the user continuously create noise data, lower the *tf*)
- Data from the network admin has higher *tf.*

Future Work

- Experiment using simple linux program like nmap.
- Experiment using real malware.
- Deploy tools and gather real data.