Robust and Scalable Trust Management Model for Collaborative Intrusion Detection

Carol Fung, Jie Zhang, Issam Aib, and Raouf Boutaba

David R. Cheriton School of Computer Science,
University of Waterloo
Outline

• Introduction
• Related Work
• Framework
• Trust Model
• Results
• Conclusion
Cyber Threats and Intrusion Detection Systems (IDS)

• Cyber Threats
  – Viruses, Worms, Malware, and Denial of Service attacks

• Intrusion Detection Systems
  – Firewalls, Antivirus Software, Signature-based Intrusion Detection Systems, and Anomaly-based Intrusion Detection Systems
Intrusion Detection Networks
Distributed collaboration

• Who?
  – Host-based IDSes across administrative boundaries

• How?
  – Exchange alerts and request diagnosis

• Problem?
  – Trust management

IP=11.22.33.44 time=3:05am…

High risk
Related Work

• Duma et al. [DEXA 2006]
  – Use simple average of past experience for trust values
  – Aggregate feedback from all acquaintances
  – Suffer from various attacks

• Fung et al. [DSOM 2008]
  – Use forgetting factor to discount old experience
  – Aggregate feedback from trusted peers
  – Scalability problem
Paper Contribution

• Dirichlet-based trust management model
  – Uses Bayesian approach
  – Improved detection accuracy
  – Better robustness and scalability
Network Architecture

- Acquaintance (List)
- Test Message
- Real Request
- Feedback

Test Message/Real Request

Feedback
Trust Evaluation Framework

Step 1: Feedback Satisfaction Mapping

Step 2: Trust Evaluation

Step 3: Feedback Aggregation
Feedback Satisfaction Mapping

Satisfaction Level

r - Expected Answer

Received Answer

0 1 2 3 4 5

1 2 3 4 5

0 1 2 3 4 5

r
Trust Model

1. $s_1, s_2, \ldots, s_k$ are the $k$ possible satisfactions levels
2. $S$ is the satisfaction probability vector $(p(s_1), p(s_2), \ldots, p(s_k))$

$$f(p(s_1), \ldots, p(s_k) \mid \xi) = \text{Dir}(p \mid \gamma) = \frac{\Gamma\left(\sum_{i=1}^{k} \gamma_i\right)}{\prod_{i=1}^{k} \Gamma(\gamma_i)} \prod_{i=1}^{k} p_i^{\gamma_i - 1}$$

Dirichlet model gives the density function of $S$

$\gamma = \text{accumulated experiences in each satisfaction level (forgetting factor)}$
Trust Evaluation

Trust value is the expectation of the trust variable

\[ T = E[Y] = \frac{1}{\gamma_0} \sum_{i=1}^{k} w_i \gamma_i \]

\[ \sigma^2[Y] = \frac{1}{\gamma_0^2 + \gamma_0^3} \sum_{i=1}^{k} w_i \gamma_i \left( w_i (\gamma_0 - \gamma_i) - 2 \sum_{j=i+1}^{k} w_j \gamma_j \right) \]

Confidence of trust estimation can be approximated as:

\[ C = 1 - 4\sigma[Y] \]
Observations about Trust

- More recent experiences have higher influence on trust values than old ones.

- Good experiences lead to higher trust.

- Frequent experiences lead to higher confidence levels of trust estimation.
Feedback Aggregation

• Now we have trust values to all acquaintances

• We use weighted average to aggregate their feedbacks
  – Only aggregate feedback from trusted acquaintances
  – Use trust value as weight
Scalability of the System

- We use an adaptive approach to reduce test message rate
  - Reduce test messages rate to highly trusted nodes and highly untrusted nodes
Simulation Setup

- Discrete event simulation
- $n$ random IDSes with various expertise levels in a grid zone
- IDS model for expertise level and detection ability
- Honest and dishonest nodes
Simulation Results (1)

Fig 1. Trust values and expertise levels

- High expertise
- Medium expertise
- Low expertise
Fig 3. Trust value of malicious node under betrayal attack
Simulation Results (3)

Fig 4. Test message rate under different models

Test Messages/day

Days

DSOM (previous)/all
Dirchlet-based/low expertise
Dirchlet-based/med expertise
Dirchlet-based/high expertise
Dirchlet-based/betrayal

DSOM
Dirichlet
Conclusion

- Proposed a trust-based IDS collaboration system
- Used the Dirichlet model to evaluate the trust values of each IDS
  - Model the confidence level of trust estimation
  - Proposed an adaptive test messages rate to reduce the communication overhead
- Improved performance, scalability, and robustness
Thank You!
Simulation Result(3)

Fig 5. Detection rate under inconsistency models
Fig 2. Confidence level and test message rate
Dirichlet Distribution

Dirichlet-based Trust Management Model
Dirichlet Distribution (con.)

A discrete random variable $X$ has $k$ possible outcomes. We denote the probability of each outcome to be $\{p_1, p_2, \ldots, p_k\}$.

We observed outcome $i$ has appeared $\gamma_i - 1$ times. Then the probability of each outcome satisfies Dirichlet probability function:

$$f(p_1, \ldots, p_k \mid \gamma_1, \ldots, \gamma_k) = \frac{1}{B(\gamma)} \prod_{i=1}^{k} p_i^{\alpha_i-1}; \quad B(\gamma) = \frac{\prod_{i=1}^{k} \Gamma(\gamma_i)}{\Gamma(\sum_{i=1}^{k} \gamma_i)}$$

Example: Toss a dice 10 times, observations on each side of the dice is $\{2,0,1,4,1,2\}$.

Then the probability density function is,

$$f(p_1, \ldots, p_6 \mid \{3,1,2,5,2,3\}) = \frac{\Gamma(3)\Gamma(1)\Gamma(2)\Gamma(5)\Gamma(2)\Gamma(3)}{\Gamma(16)} p_1^2 p_2^0 p_3^1 p_4^5 p_5^1 p_6^2$$
Robustness of the System

- Sybil attack
- Newcomer attack
- Betrayal attack
- Collusion attack
- Inconsistency attack