Effective Acquaintance Management for Collaborative Intrusion Detection Networks

Carol Fung, Jie Zhang, and Raouf Boutaba

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

• Background
• Intrusion Detection and Collaboration
• Acquaintance Management
• Evaluation
• Conclusion
Network Intrusions

• Worms, Viruses, Malware
  – Storm worm (2007)
  – Conflicker (2008)

• Botnet

• Attack motivation
  – ID theft, Credit card, Privacy spying, Online account, Spamming, DoS, etc.
Intrusion Detection Systems

- Network-based
- Host-based
Host-based IDS (HIDS)

- Monitor computer activities, files, and compare against malicious patterns
  - Traditional HIDS such as OSSEC, Tripwire
  - Antivirus systems
- A single HIDS can be vulnerable to new attacks
  - Collaboration improves detection accuracy
Collaborative Intrusion Detection

- **Information sharing** (DShield, NetShield)
- **Expertise sharing** (Cloud-AV)
Who to collaborate with?

- Existing solutions
  - Fixed number
  - Fixed thresh-bar

- Our Contribution
  - An automatic acquaintance management
  - Cost efficient acquaintance selection
Our Approach

**Step 1:** Know your candidates

**Step 2:** Cost function modeling

**Step 3:** Consensus reaching
Know the Candidates

- Learn the quality of a candidate
  - False positive rate and True positive rate
  - Using test messages to gain experience
  - Bayesian learning

\[ F \sim \frac{1}{B(\alpha, \beta)} x^{\alpha-1} (1 - x)^{\beta-1} \]

- Cumulative evidences on false diagnosis
- Cumulative evidences on true diagnosis
- Distribution of False Positive rate
- Beta function
Cost Function Selection

- Cost on maintenance of collaborators
  - Increases with the number of collaborators
- Cost on false decisions
  - Cost of false positive and false negative decisions

\[
C_{\text{total}} = M(A) + R(A) \\
= C_m |A| + \\
\sum_{y \in \{0,1\}^{|A|}} \min\{C_{fn} \pi_1 \prod_{i} T_i^{y_i} (1-T_i)^{1-y_i}, C_{fp} \pi_0 \prod_{i} F_i^{y_i} (1-F_i)^{1-y_i}\}
\]

- Maintenance cost
- Cost on raising alarm
- Cost on no alarm
Acquaintance Selection Algorithm

**Algorithm 1**: Select the optimal acquaintance list with minimal cost

- Brute Force for a short candidate list and greedy for a long candidate list

**Algorithm 2**: Acquaintance management to find mutual agreement among nodes

- Probation period

- Collaboration connection is established only if both peers select each other
Evaluation - Cost Efficiency

![Cost Efficiency Graph](image)

- Overall Cost vs. Number of Collaborators
- Different lines represent different FN values: FN=0.1, FN=0.2, FN=0.3, FN=0.4, optimal
- The graph shows the cost efficiency across varying numbers of collaborators for different FN values.

Acquaintance Management for CIDN
Evaluation - Convergence

![Graph showing the FN Rate of Acquaintances vs. FN Rate]
Evaluation - Stability

![Graph showing collaboration period vs FN rate of acquaintances for different FN values (0.1, 0.3, 0.5).]
Evaluation – Incentive Compatibility

![Graph showing the relationship between FN Rate of Nodes and Cost, with a notable increase from day 200 onwards.](image-url)
Conclusion

• Proposed an automatic acquaintance selection algorithm for collaborative intrusion detection networks
• Find optimal acquaintance list which leads to the minimum cost
• The acquaintance management algorithm holds the properties of efficiency, stability, and incentive-compatibility
Thank You
Bayesian Learning

\[ \alpha: \text{Cumulative evidences on false diagnosis} \]
\[ \beta: \text{Cumulative evidences on true diagnosis} \]

\[ \alpha = 2\beta \pm 10 \]