Network application attack recovery

Meng Yu, Peng Liu, Wanyu Zang
Cyber Security Lab & Networking Research Center
Penn State University
http://ist.psu.edu/s2
How to defend?

- **Protection** (access control, authentication, etc.)
- **Detection** (intrusion detection systems)
- **Response** (push back against DDoS attacks)
- **Recovery** (restore the system to its original integrity level)
Why do we need recovery?

- No perfect defense.
- Attackers can always compromise your system.
- We need to recover the system under successful attacks.
- Improve the survivability.
How does damage spread?

Attacks: \( x := 2 \)

Infected: \( y := x + 1 \)

Through data dependences: generates wrong \( y \)

Through the control dependence: invoke wrong task

Infected: if \( (x < 10) \) then \( y = 5 \)
How to trace the damage?

- Inspect dependence relations to trace damage spreading.

Check if a transaction is dependent on (affected by) known malicious transactions to determine if it is corrupted.
How to remove the effects of damage?

- UNDO affected transactions.

UNDO backward
How to repair the damage?

- REDO affected transactions.
More efficient than checkpoints

- Checkpoints
  All work after the checkpoint will be lost after roll back.

- Our work
  Only damaged tasks need repairs.
  Innocent tasks will be kept untouched.
Comparison with Intrusion Detection Systems

A: Damage caused directly by attackers

B: Damage caused by executing legitimate tasks which are dependent on damaged tasks.

Intrusion Detection Systems: can find A; cannot find B. Our system: based on A can find B
Impact of the system load

![Graph showing the impact of system load on processing normal workflow tasks]

- System load: 30%
- System load: 50%
- System load: 20%

The graph illustrates the performance of processing normal workflow tasks under different system loads. As the system load increases, the performance of processing tasks decreases, indicating a negative impact on system efficiency.
Impact of the attacking density

![Graph showing the impact of different attacking densities on increasing latency of normal tasks over time.]

- Attacking density: 10%
- Attacking density: 20%
- Attacking density: 30%
Impact of the IDS delay

Average IDS delay: 5 seconds
Average IDS delay: 15 seconds
Average IDS delay: 30 seconds
Task numbers

- Accumulative number of recovery tasks to repair damage
- Accumulative number of malicious tasks identified by the IDS
- Accumulative number of malicious tasks identified by the recovery system
Interesting?

- We proposed three different recovery strategies (conservative, optimistic, and aggressive).
- We proposed two mathematical models for performance evaluation (Continuous Time Markov Chain and queuing network).
- We built a prototype system and obtained exciting experimental results.
- Published in ICDCS’04, And more!
More work in the future

• Collaborative recovery in a distributed system.
• Effective and efficient recovery information exchanging.
• Configurable and adaptive recovery strategies.