CERIAS

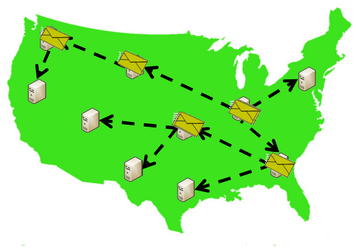
The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

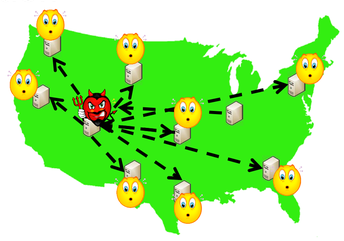
Gatling: Automatic Attack Discovery in Large-Scale Distributed Systems

Hyojeong Lee, Jeff Seibert, Charles Killian and Cristina Nita-Rotaru

Department of Computer Science and CERIAS, Purdue University



- To gain confidence that an implementation is bug-free: use automated test techniques
  - Model checker
  - Symbolic execution



- To gain confidence that the system will work under attack?
  - -Think about possible attacks
  - -Manually implement to verify the attack

We need an automated technique to find attacks

Problem

We want to find automatically:

- **Performance attacks** conducted through messages by insiders
- In large-scale distributed systems
- Using real implementations
- Minimal input from developer

Challenges

- **Malicious Implementation**
  - -Lying message is protocol dependent
  - -Random bit-flipping is not effective
- **Space Space Explosion**
  - -Too many possible actions and combinations
- **Fuzzy Metric**
  - -Unlucky run vs. successful attack?

Event-based simulator: steady performance

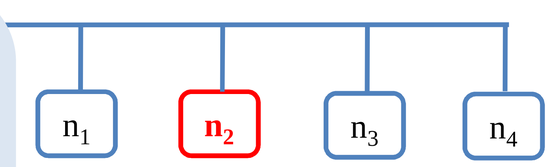
Fault injector: injects malicious actions to mimic malicious implementation

Modelchecker: model checker style exploration + greedy algorithm to build up attack

Simulator

Event Queue

Time	Dest	Message
1504	n_3	B9 43 …
1515	n_1	95 A2 …
1527	n_3	A8 1D …
1534	n_4	4E 74 …
1540	n_2	52 F6 …



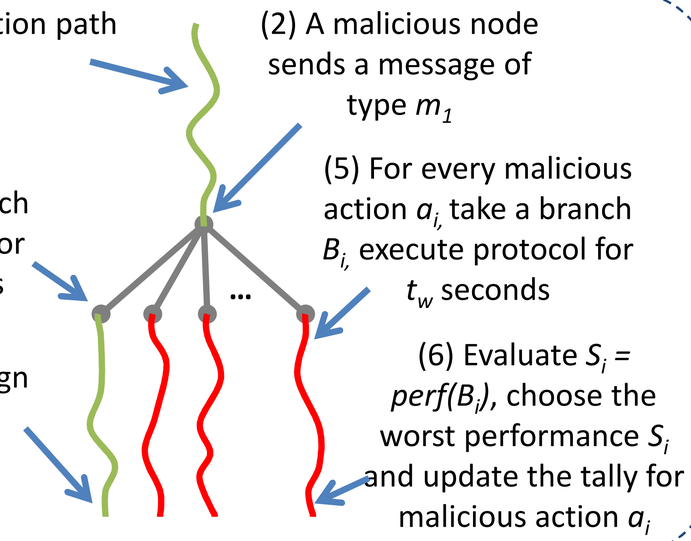
Message Delivery Action
- Drop
- Dup
- Delay
- Divert

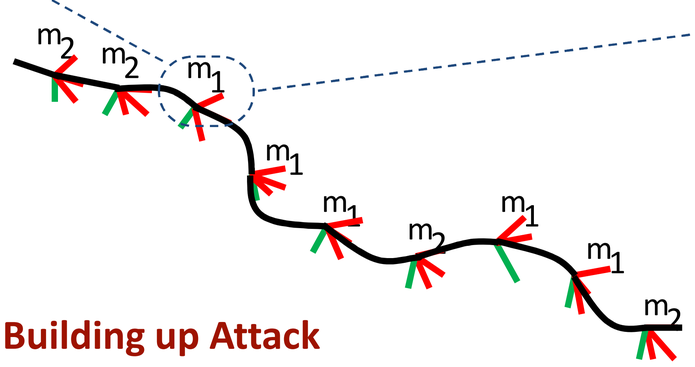
Message Lying Action
- Zero
- Min and max
- Spanning
- Scaling
- Random

Malicious actions (faults)

- Message delivery actions are applied to a particular message
- Message lying actions are applied to a particular field inside the message

Greedy Action Selection Procedure





Performance Tally

	Benign	Drop	Delay	Lie
m_1	1	1	3	0
m_2	0	0	0	3

Building up Attack

Greedy selection is tallied and Gatling builds up an attack by combining results

(Example threshold: 3)

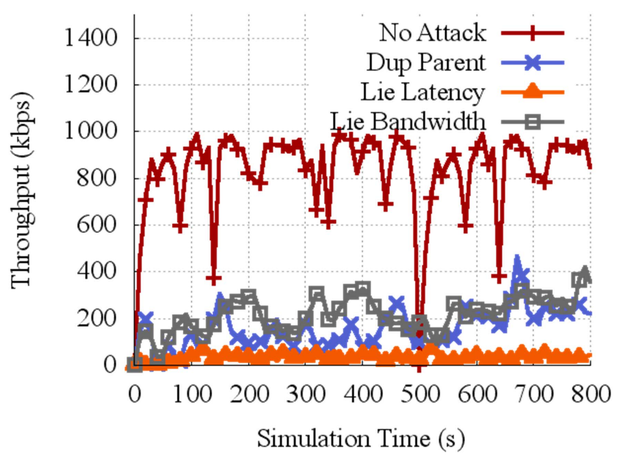
Gatling output:
<m_1, Delay; m_2, Lie>

Summary of Result

Target Systems	Attack Types
BulletPrime Vivaldi Chord DHT ESM Scribe	17 lying 12 drop 6 delay 5 duplicate 1 divert

	Number of Attacks
Previously Reported	20
Newly Found	21
Total	41

Each attack took a few minutes to a few hours to discover



Attacks found in ESM

-No Attack: baseline

-Dup Parent: Malicious node duplicates and diverts parent accept message and drops data later

-Lie Latency/Lie Bandwidth: Malicious node lies about its performance and drops data later

CERIAS

Discovery Park e-Enterprise Center