2020

Towards an Experimental Testbed to Study Cyber Worm Behaviors in Large Scale Networks

Harish Kunta
Georgia State University

Bhavya Induri
Georgia State University

Anu G. Bourgeois
Georgia State University

David Maimon
Georgia State University

Ashwin Ashok
Georgia State University

Towards an Experimental Testbed to Study Cyber Worm Behaviors in Large Scale Networks

HARISH KUNTA, BHAVYA INDURI, ANU G. BOURGEOIS, DAVID MAIMON, AND ASHWIN ASHOK

ACM WINTECH 2020

EVIDENCE-BASED CYBERSECURITY RESEARCH GROUP – EBCS.GSU.EDU

Preliminary goals

- Want a real world experiment to capture true evidence of worm behavior
- Set up experiments in an actual network as opposed to a simulation or testbed environment
- Would capture actual dynamic factors from varying network load
- Identify propagation paths
- Determine parent-child (infector-victim) relationship
- Determine order of infections

Preliminary Work

Node	IP Address	Building #
PI-1	10.51.198.127	26
PI-2	10.51.197.217	26
PI-3	10.50.168.124	37
PI-4	10.55.101.245	27
PI-5	10.50.168.178	37
PI-6	10.49.198.221	25
PI-7	10.49.199.64	25
PI-8	10.55.101.96	27
PI-9	10.48.73.162	6
PI-10	10.50.168.97	37

Scanning Cases

Sequence - Sequence

- Sequentially iterate thru subnets
- Sequentially iterate thru hosts
- Double nested

Sequence - Random

- Sequentially iterate thru subnets
- Randomly select hosts
- Double nested

Pseudorandom - Sequence

- Sequentially iterate thru a.b portion
- Randomly select c portion of subnet
- Sequentially iterate thru hosts
- Triple nested

Pseudorandom - Random

- Sequentially iterate thru a.b portion
- Randomly select c portion of subnet
- Randomly select hosts
- Triple nested

Preliminary results

Node	2	3	4	5	6	7	8	9	10
1	(0,0)	(0,0)	(0,0)	(0,0)	(100,0)	(0,0)	(100,0)	(100,100)	(100,0)
2	(0,0)	(0,0)	(0,0)	(0,0)	(0,100)	(0,0)	(0,0)	(0,0)	(0,0)
3	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,100)	(0,0)	(0,0)	(0,0)
4	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,100)
5	(0,0)	(0,100)	(0,0)	(0,24)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
6	(0,0)	(0,0)	(0.7,0)	(100,76)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
7	(100,100)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
8	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,100)	(0,0)	(0,0)
9	(0,0)	(100,0)	(99.3,100)	(0,0)	(0,0)	(100,0)	(0,0)	(0,0)	(0,0)
10	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)

Sequence – Sequence case

Node	2	3	4	5	6	7	8	9	10
1	(0.7,0)	(34.5,0)	(47.9,0)	(37.3,0)	(100,0)	(0,0)	(51.4,0)	(100,100)	(28.2,0)
2	(0,0)	(0,0)	(0,0)	(0,0)	(0,100)	(0,0)	(0,0)	(0,0)	(0,0)
3	(0,0)	(0,0)	(0.7,0)	(0,0)	(0,0)	(0,100)	(0,0)	(0,0)	(0,0)
4	(0,0)	(0,34.5)	(0,0)	(0,37.3)	(0,0)	(0,0)	(0,0)	(0,0)	(0,28.2)
5	(0,0)	(0,47.2)	(0,0)	(0,40.1)	(0,0)	(0,0)	(0,0)	(0,0)	(0,50.7)
6	(0,0)	(33.8,18.3)	(33.8,0)	(30.3,22.5)	(0,0)	(0,0)	(30.3,0)	(0,0)	(35.9,21.1)
7	(99.3,100)	(0,0)	(0,0)	(0.7,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
8	(0,0)	(0,0)	(0,47.9)	(0,0)	(0,0)	(0,0)	(0,52.1)	(0,0)	(0,0)
9	(0,0)	(31.7,0)	(17.6,52.1)	(31.7)	(0,0)	(100,0)	(18.3,47.9)	(0,0)	(35.9,0)
10	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)

Sequence – Random case

Pseudorandom – Random case

Node	2	3	4	5	6	7	8	9	10
1	(1.6,0)	(35.3,0)	(51.1,0)	(32.6,0)	(53.3,0)	(46.7,0)	(46.7,0)	(100,100)	(32.1,0)
2	(0,0)	(0,0)	(0,0)	(0,0)	(0,52.7)	(0,47.3)	(0,0)	(0,0)	(0,0)
3	(0,0)	(0,0)	(0,0)	(0,0)	(0,47.3)	(0,52.7)	(0,0)	(0,0)	(0,0)
4	(0,0)	(0,35.9)	(0,0)	(0,32.6)	(0,0)	(0,0)	(0,0)	(0,0)	(0,33.7)
5	(0,0)	(0,42.9)	(0,0)	(0,45.1)	(0,0)	(0,0)	(0,0)	(0,0)	(0,45.1)
6	(44,0)	(19,21.2)	(19.6,0)	(21.7,22.3)	(0,0)	(0,0)	(15.2,0)	(0,0)	(15.2,21.2)
7	(54.4,100)	(12,0)	(1.6,0)	(16.3,0)	(0,0)	(0,0)	(4.9,0)	(0,0)	(17.4,0)
8	(0,0)	(0,0)	(0,53.3)	(0,0)	(0,0)	(0,0)	(0,48.4)	(0,0)	(0,0)
9	(0,0)	(33.7,0)	(27.7,46.7)	(29.4,0)	(46.7,0)	(53.3,0)	(33.2,51.6)	(0,0)	(35.3,0)
10	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)

Automated Delivery – Robots & Drones

Future goals

- Set up policies for mitigation of impact or interruption of attack
- Move to a wireless setting for unknown robots/drones coming in as attacker or target
- Maintain privacy and security of data held
- Protect against possible cyberphysical attack of taking over robots