Stepping-stone Intrusion Upstream Detection Using Round-Trip Time Distribution

Jianhua Yang, *Ph.D*

Professor
TSYS School of Computer Science
Columbus State University

Layout

- 1. Background
- 2. Techniques to detect stepping-stone
- 3. Upstream Detection
- 4. Our contribution

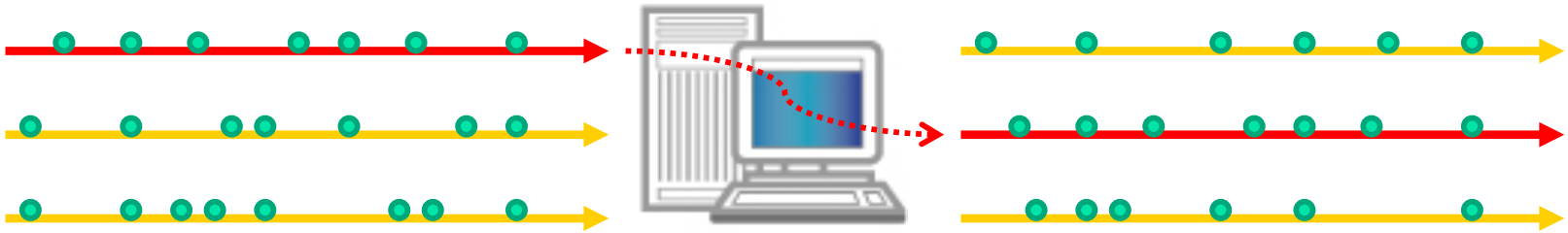
1. Background

- Intrusion
  - Stepping-stone

Stepping-stone intrusion detection techniques

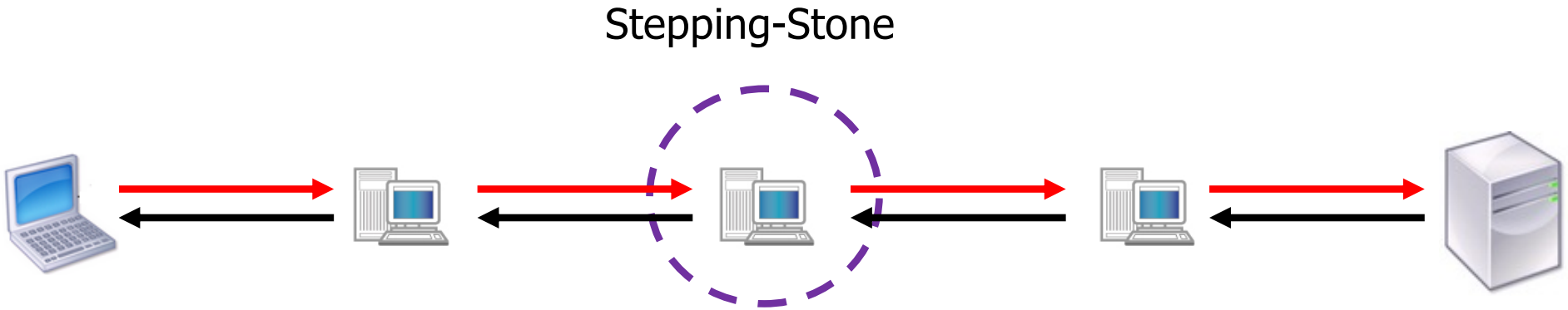
- Content thumbprint
- Time-based thumbprint
- RTT based detection
- Length estimation

Stepping-Stone Detection



Finding correlation between gaps of incoming packet stream and outgoing packet stream.

Stepping-Stone Detection



Contribution –Result 1

Attack1		CCT30			AWS1			AWS2			AWS3	
Test 1	0	90.18	9.82	0	91.96	8.04	0	92.86	7.14	0	96.4	3.6
Test 2	0	79.83	20.17	0	80.67	19.3	0	88.24	11.8	0	92.44	7.56
Test 3	9.4	76.07	14.53	11.1	75.21	13.7	12	77.78	10.3	0	91.45	8.55
Test 4	0.5	84.65	14.85	0	86.14	13.9	0	88.61	11.4	0	94.06	5.94
Test 5	0	87.83	12.17	0	85.22	14.8	0	87.93	12.2	0	95.65	4.35
Test 6	0	84.17	15.83	0	84.17	15.8	0	85.61	14.4	0	93.53	6.47
Test 7	6.62	82.12	11.26	7.95	80.13	11.9	9.93	79.47	10.6	0	90.07	9.93
Test 8	0	91.67	8.33	0	93.52	6.48	0	95.37	4.63	0	96.3	3.7
Test 9	0	85.71	14.29	0	88.39	11.6	0	91.96	8.04	0	93.75	6.25
Test 10	0	92.86	7.14	0	93.75	6.25	0	93.75	6.25	0	97.32	2.68
Average	1.65	85.51	12.84	1.91	85.92	12.18	2.19	88.16	9.66	0.00	94.10	5.9

Contribution – Result 2

Average	1.65	85.51	12.84	1.91	85.92	12.18	2.19	88.16	9.66	0.00	94.10	5.9
Attack 2		CCT30			AWS1			AWS2			AWS3	
Test 1	0	89.83	10.17	0	90.76	9.24	0	90.76	9.24	0	92.44	7.56
Test 2	12.3	86.89	0.82	12.2	86.99	0.81	0	95.12	4.88	0.81	97.56	1.63
Test 3	0	92.41	7.59	0	93.75	6.25	0	93.75	6.25	0	93.75	6.25
Test 4	0	89.61	10.39	0	89.74	10.3	0	89.74	10.3	0	91.03	8.97
Test 5	0	84.42	15.58	0	85.9	14.1	0	87.18	12.8	0	92.31	7.69
Test 6	0	86.84	13.16	0	90.91	9.09	0	90.91	9.09	0	93.42	6.58
Test 7	0	84.62	15.38	0	87.34	12.7	0	87.34	12.7	0	92.41	7.59
Test 8	0	80.26	19.74	0	85.71	14.3	0	84.42	15.6	0	87.01	13
Test 9	0	91.14	8.86	0	93.75	6.25	0	92.41	7.59	0	96.25	3.75
Test 10	0	92.77	7.23	0	92.86	7.14	0	92.86	7.14	0	96.43	3.57
Average	1.23	87.88	10.89	1.22	89.77	9.01	0.00	90.45	9.55	0.08	93.26	6.66

Contribution – Result 3

Attack 3		CCT30			AWS1			AWS2			AWS3	
Test 1	0.78	87.5	11.72	1.53	87.02	11.5	0.77	86.15	13.1	0	93.08	6.92
Test 2	0	88.79	11.21	0	88.79	11.2	0	89.72	10.3	0	92.52	7.48
Test 3	0	87.59	12.41	0	87.59	12.4	0	86.13	13.9	0	91.24	8.76
Test 4	0	88.82	11.18	0	89.41	10.6	0	89.41	10.6	0	92.94	7.06
Test 5	0	91.8	8.2	0	91.8	8.2	0	92.62	7.38	0	94.26	5.74
Test 6	0	93.48	6.52	0	93.48	6.52	0	93.48	6.52	0	95.65	4.35
Test 7	0	89.17	10.83	0	90.83	9.17	0	93.33	6.67	0	95	5
Test 8	0	91.67	8.33	0	92.5	7.5	0	90.83	9.17	0	92.5	7.5
Test 9	0	89.93	10.17	0	88.14	11.9	0	91.53	8.47	0	94.07	5.93
Test 10	0	86.61	13.39	0	86.61	13.4	0	87.5	12.5	0	91.96	8.04
Average	0.08	89.54	10.40	0.15	89.62	10.23	0.08	90.07	9.85	0.00	93.32	6.68

Summary/Question

Questions?