Toward Automatically Generating Double-Free Vulnerability Signatures Using Petri Nets

Ryan Iwahashi[1], Daniela A.S. de Oliveira[1], S. Felix Wu[1], Jedidiah R. Crandall[2], Young-Jun Heo[3], Jin-Tae Oh[3], and Jong-Soo Jang[3]

[1] University of California, Davis
[2] University of New Mexico
3 ETRI

Vulnerability Signatures Vs. Exploit Signatures

- Vulnerabilities – programming errors
- Exploits – attack specific vulnerabilities
- Finite number of Vulnerabilities
- Characterize the vulnerability
- Host based IDS and Network based IDS

ASN.1 Windows Double Free Vulnerability

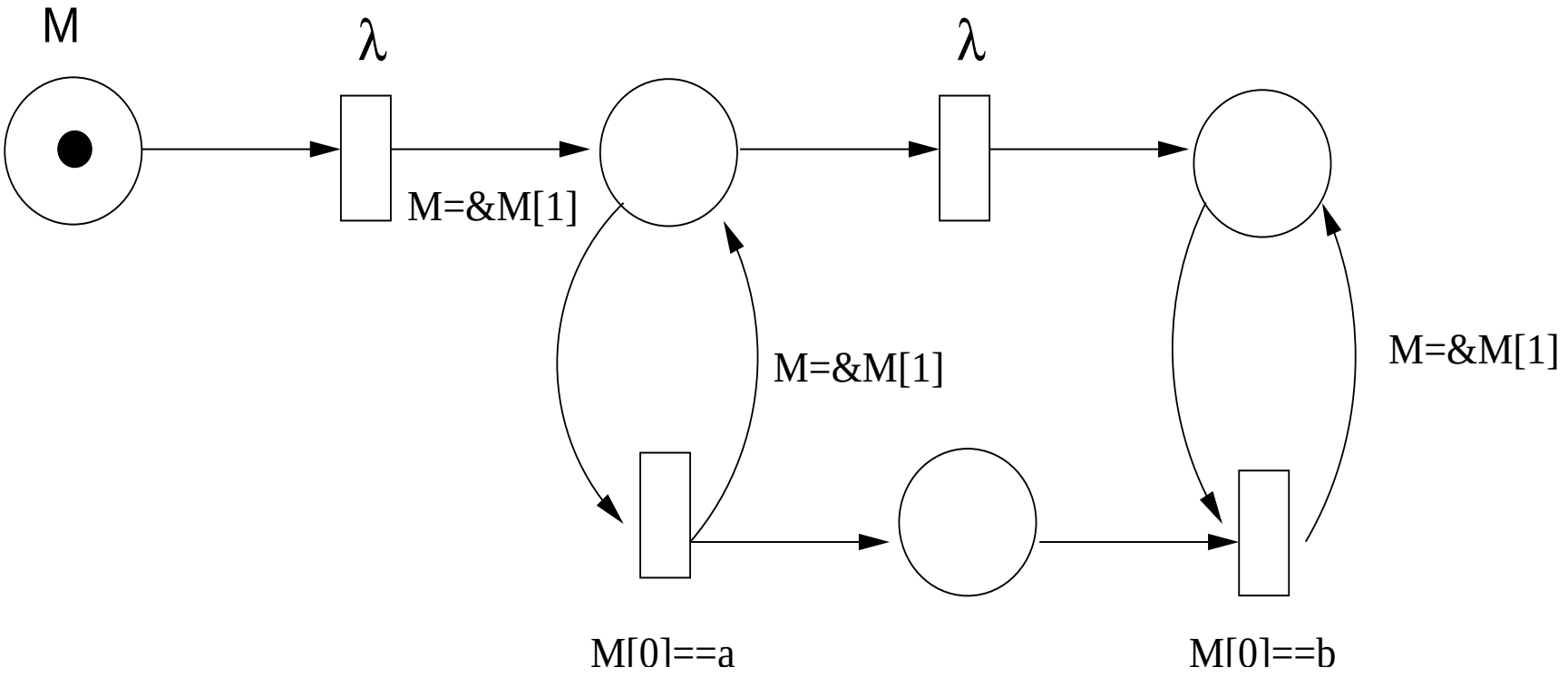
- Very Interesting Vulnerability
  - Double Free vulnerability
  - Control Flow Sensitive
  - Data Flow Sensitive
  - Easily made polymorphic or metamorphic
- Attacker can gain administrative control using register springs

Petri Net Intrusion Detection System

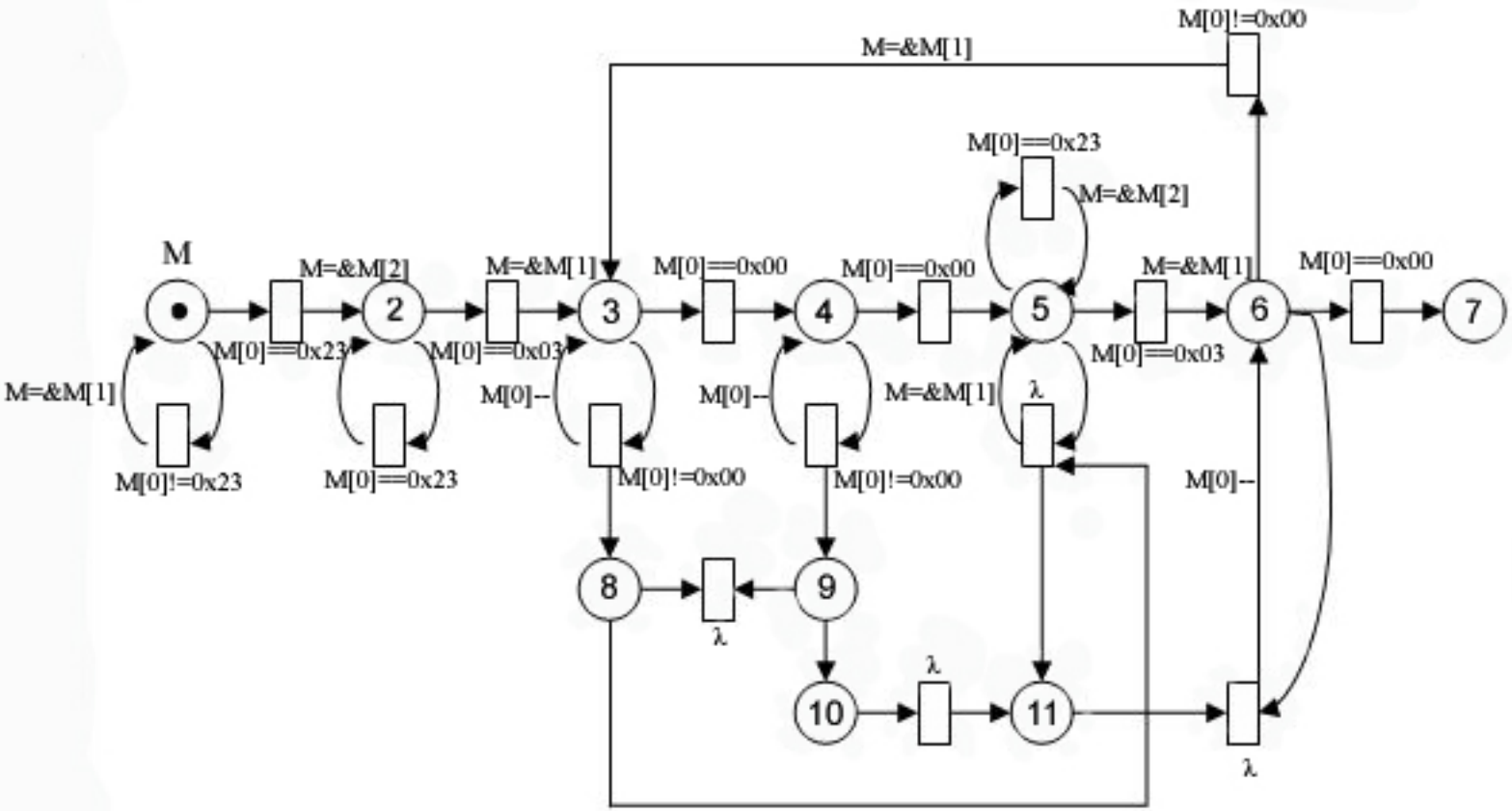
- Graphical and mathematical modeling tool
- 5-tuple description:
- PN = P, T, F, W, M_0
  - P = Places
  - T = Transistions
  - F = arcs (flow relation)
  - W = weights of arcs
  - M_0 = Initial Marking

Petri Net Intrusion Detection System (cont.)

- Quick Example ca^nb^n:



Petri Net Intrusion Detection System (cont.)



Comparisons to other types of Intrusion Detection Systems

Signature Class	Attacks	False Negatives	Valid Traces	Seconds
ASN.1 Daemon	887965	0	112035	305
Regular Expressions	1000000	0	0	17
Symbolic Constraints	71691	928309	0	144
Turing Machines	887965	0	112035	72
Petri Nets	1000000	0	0	71

Signature Class	False Positives	Seconds
Retular Expressions	167432	934
Symbolic Constraints	7	967
Turing Machines	0	1083
Petri Nets	3	9147

Thanks!