Colored Petri nets as the enabling technology in Intrusion Detection Systems

Andrey M. Dolgikh
MS in Computer Engineering
Degree and Specialization Sought:
Doctor of Philosophy in Electrical & Computer Engineering
Conventional antivirus

Program → Match → Signature database

Perfect match – virus detected
Virus body detected

Signature

B R A K E E I T T

B R A K E E I T
Part of program

Signature
Utilization of binary signatures
(source: Kaspersky Lab)

- Current IDS depend on ever-growing databases of binary signatures
Utilization of Malicious functionalities
(source: Trend Micro Inc.)
Understanding behavior

• Sentence:
  – Send the password to the Internet

• Words:
  – Password, Internet, The, Send, To

• Letters:
  – PasswordInternetTheSendTo
Behavior

User mode

Functionality level

Open/read ➔ Open/write ➔ Cmd /c dir

API calls

API1 ➔ API2 ➔ API3

API6 ➔ API7

System Calls

System Service Executive

Operations

File Objects

Handle 1

Handle 2

Memory Sections

Handle 1

Handle 5

Kernel mode

In natural language

MS Excel:
Do something useful

Virus:
Send password to Internet

something do useful

password send internet

something password useful do send internet

somesswordsendint

usefuthingpaldoernet
How to model functionalities? - Via CPN.
How CPN works? – it assembles appropriate system calls into functionality

Call\(_{11}(134,\ldots)\)

56 = Call\(_{5}(23,\ldots)\)

90 = Call\(_{22}('cmd.exe',\ldots)\)

Call\(_{11}(h_{11}^1 = 56,\ldots)\)

Call\(_{8}(23,12,\ldots)\)

Call\(_{8}(23,90,\ldots)\)

Functionality:

\(h_2 = \text{Call}_5(h_1,\ldots)\)

\(\text{Call}_{11}(h_2)\)

\(h_3 = \text{Call}_{22}('cmd.exe',\ldots)\)

\(\text{Call}_8(h_1,h_3,\ldots)\)
Questions ???