Towards malware-resistant networking environment

Dennis Gamayunov
Computer Systems Lab
CS Department
Moscow State University
Malware propagation issues

Main focus: malware, which exploits memory corruption attacks remotely

1) Best observed on a large scale

2) Moore law vs. Gilder law

Besides:
- Content filtering is better done as close to the source as possible
- HIDS/AV administration issues, heavy resource usage

Ideas for better mitigation:
- Detect and filter at network level
- Try to minimize exploitation impact at host level

Dennis Gamayunov, Lomonosov Moscow State University, gamajun@cs.msu.su
Network level: wire-speed shellcode filtering

Task of **optimal shellcode detection** can be divided into three subtasks:

- **Subtask 1 – Shellcode classification**
  - Build a set of classes of shellcode «building blocks» and corresponding feature space

- **Subtask 2 – Library of simple classifiers**
  - Build a set of algorithms, capable of detecting specific classes of shellcode «building blocks» (i.e. NOP, GetPC, decryptors, etc)

- **Subtask 3 – Optimal hybrid classifier**
  - Solve an optimization problem of generating data flow graph of elementary classifiers, which covers all classes, and is optimal in terms of FP rates and computational complexity.

**Research deliverable:**
shellcode detection library
Host level: fine-grained privilege control

Task of application privilege control can be divided into three subtasks:

- **Subtask 1 - Program slicing**
  - Split CFG into the set of non-overlapping blocks: the number of privileges per block is less than overall number of privileges in the initial SELinux profile

- **Subtask 2 – Generating normal behavior model**
  - Build normal program behavior model as DFA where symbols are syscalls and checkpoints passing

- **Subtask 3 - Run-time behavior monitoring**
  - Get the parameters of syscalls and checkpoints in run-time, pass them to the normal behavior model and effectively utilize the model output

---

Dennis Gamayunov, Lomonosov Moscow State University, gamajun@cs.msu.su
Summary: two complementary research directions

- **Fast polymorphic shellcode detection in network flow**
  - Aim — detect massive phenomena like worm propagation as close to the source as possible
    - Build hybrid shellcode classifier, optimal in throughput and FP rates
    - Generate signatures with very short lifetime to use in existing filtering devices

- **Fine-grained application privilege control at host level**
  - Aim – minimize the negative effect of successful exploitation of unknown vulnerabilities in software
    - Build «privilege flow graph» for application in terms of SELinux
    - Monitor execution trace and enforce «hard» least privilege principle

Dennis Gamayunov, Lomonosov Moscow State University, gamajun@cs.msu.su