"Operating System Protection Through Program Evolution"

Dr. Frederick B. Cohen

"…one of the major reasons attacks succeed is because of the static nature of defense, and the dynamic nature of attack."

Outline

- Attacks and Defense
  - a brief look at the types of attack evolution can help prevent
- Program Evolution
  - what is it?
  - why do we want it?
  - a problem to consider.
- Program Encoding
  - an overview of an evolution technique.

Attack & Defense

- The Ultimate Attack
  - Physical access to system
  - Knowledge of system
    - Exploitation of known weaknesses
- The Ultimate Defense
  - Increase complexity of attack to make cost of attack to high
    - "…security through obscurity..."

What is Program Evolution?

- Automated creation of equivalent programs
  - "..consider two programs equivalent if, given identical input sequences, they produce identical output sequences."
  - An evolved program may run faster/slower, or take more/less space than the original.
  - An evolved program may or may not increase the complexity of attack.
- Techniques for Evolution
  - Instruction/Sequence Equivalence, Instruction Reordering
  - Variable Substitution, Adding/Removing of Jumps/Calls
  - Garbage Insertion, Program Encoding, Simulation….

Purpose of Evolution

- Diversity
  - an attacker who defeats one evolution of a program may not be able to apply the same attack to another evolution of the same program.
- Obscurity
  - evolution obscures the underlying program, making analysis potentially more difficult.

What Does This Program Do?

```
int x = 0, y = 5, z = 0;
for(int p = 0; p < 10; p++) {
  z = foo(p, y);
  y = y + 1
  x = z;
  print x;
}
```

```
int foo(int x, int y) {
  float t = x/2, u = (y*2)/4;
  if(u > t)
    t = 4 * t + 2 * y;
  else
    t = 2 * t + 1;
  return t;
}
```

```
int x = 0;
for(int i = 0; i < 10; i++) {
  x = i + 1;
  print x;
}
```

it prints the sequence 1,2,3 .. 10.

Program Encoding

- Choose symbols to replace program symbols, interpret new symbols at runtime to generate original program.
  - encryption and compression are forms of encoding.
  - can have significant performance impact.

What does this say ? “svool 406-495”

Answer : “hello 715.725”

· a simple encoding - the i^{th} letter of the alphabet is mapped to the $(27 - i)^{th}$ letter, a similar scheme for digits...

Conclusion

- This article gives a lot of information on evolution techniques and ways of overcoming the inherent difficulties of evolutionary defenses.
- I would recommend it to anyone interested in methods of obscuring program code / executables.