Outline for March 12, 2003

Reading: text, §22.1–22.5, 22.7, §18

Discussion Problem

Here's a little quiz to inspire you when you study for the final.

1. How long did the Hundred Years War last?
2. In which country are Panama hats made?
3. Where does catgut come from?
4. What is a camel's hair brush made of?
5. What kind of creatures were the Canary Isles named after?
6. What was King George VI's first name?
7. What color is a purple finch?

There! Wasn't that easy?

Outline for the Day

1. Malicious logic
   a. Quickly review Trojan horses, viruses, bacteria; include animal and Thompson's compiler trick
   b. Logic Bombs, Worms (Schoch and Hupp)
2. Ideal: program to detect malicious logic
   a. Can be shown: not possible to be precise in most general case
   b. Can detect all such programs if willing to accept false positives
   c. Can constrain case enough to locate specific malicious logic
   d. Can use: writing, structural detection (patterns in code), common code analyzers, coding style analyzers, instruction analysis (duplicating OS), dynamic analysis (run it in controlled environment and watch)
3. Best approach: data, instruction typing
   a. On creation, it's type "data"
   b. Trusted certifier must move it to type "executable"
   c. Duff's idea: executable bit is "certified as executable" and must be set by trusted user
4. Practise: Trust
   a. Untrusted software: what is it, example (USENET)
   b. Check source, programs (what to look for); C examples
   c. Limit who has access to what; least privilege
   d. Your environment (how do you know what you're executing); UNIX examples
5. Practise: detecting writing
   a. Integrity check files a la binaudit, tripwire; go through signature block
   b. LOCUS approach: encipher program, decipher as you execute.
   c. Co-processors: checksum each sequence of instructions, compute checksum as you go; on difference, complain
   d. Sandboxes: confine protection domain of process
6. Assurance
   a. Trust and assurance
   b. Requirements
   c. Policy, design, implementation, operational assurance
   d. Quick review of life cycle

And Their Answers

1. 116 years (from 1337 to 1453).
2. Ecuador.
3. From sheep and horses.
4. Squirrel fur.
5. A large breed of dogs. The Latin name was *Insularia Canaria* - “Island of Dogs.”
6. Albert. When he came to the throne in 1936 he respected the wish of Queen Victoria that no future king should be called Albert.
7. The distinctively colored parts are crimson.

Courtesy of Peter Langston via the YUCKS digest.