CSE543/Fall 2006 - Homework Questions - PRIMA

Due: Thursday, October 19, 2006 — Professor Trent Jaeger

Please read the instructions and questions carefully. You will be graded for clarity and correctness.
Short Answer - some will be one or two words – no more than 3 sentences

1. (*3pts*) What are two differences between rule C5 in the Clark-Wilson integrity model and the interpretation of these requirements in the CW-Lite integrity model?

   answer: (a) no assurance of trusted code (b) filter only at specific interfaces

2. (*3pts*) What is the impact of loading unknown code into an untrusted subject in IMA versus PRIMA?

   answer: IMA fails, PRIMA is OK.

Long Answer - no more than 2 paragraphs

3. (*7pts*) List a set of conditions/assumptions under which it would be possible to measure CW-Lite integrity using PRIMA with only boot time measurements (i.e., no need to measure individual applications as they are loaded).

   answer: Only the code loaded with a particular subject type is measured at runtime. If we knew all the possible mappings between code and subjects, then we could predict integrity at boot time. This requires that: (1) we can identify all code files and the subjects they run under; (2) these files cannot be modified; and (3) no new code files can be created. Consider a MAC policy that could express this – a pretty limited system, but it would work.

4. (*7pts*) Why is the traditional approach to remote attestation (e.g., Linux IMA) insufficient for protecting the integrity of dynamic data? What does PRIMA do to estimate the integrity of dynamic data? (don't just list a property – explain why it works)

   answer: Linux IMA uses hash values to represent code/data integrity, but these cannot be predicted for dynamic data. PRIMA estimates data integrity based on the integrity of subjects that modify the data input to a target application subject. Data modified by only trusted subjects is high integrity, and data modified by low integrity subjects must be handled by filtering interfaces of the target application subject that discard or upgrade that data immediately.

Constructions - take your time and answer clearly and completely.

5. (*10pts*) Consider a system with the following configuration for PRIMA measurement.

   Trusted subjects are: A, B, C
   Code is X, Y, Z
   Library is L

   (a) (5pts) List the PRIMA measurements that would be made under the following conditions. Include all the initial measurements that PRIMA makes before any applications are run.

   (i) Load code: Z as subject C
   (ii) Load code: X as subject A
   (iii) Load lib: L as subject A
   (iv) Load code: Y as subject B
   (v) Load lib: L as subject B
   (vi) Load code: X as subject R
   (vii) Load lib: L as subject R

(viii) Load code: Z as subject C
(ix) Load code: Y as subject C
(x) Subject B switches to filtering subject B'
(xi) Load lib: L as subject C

(b) (1pt) Would a remote party accept this system meets CW-Lite integrity if X is untrusted?

(c) (2pts) Suppose that new code W is introduced to the system. Under what conditions could W be loaded as subject A while still enabling correct verification of CW-Lite integrity?

(d) (2pts) If there is an information flow from A to B, must this be through a filtering interface if B inputs any low integrity data? Why or why not?

answer: (a) (1) measure MAC policy (2) measure trusted subjects (3) (i) measure code Z (4) (i) measure Z as C (5) (ii) measure code X (6) (ii) measure X as A (7) (iii) measure code L (8) (iii) measure L as A (9) (iv) measure code Y (10) (iv) measure Y as B (11) (ix) measure Y as C

(b) No.

(c) Must be trusted to run under subject A.

(d) No. Data from A need not come through a filtering interface unless the low integrity data also comes through that interface.