A PERSPECTIVE ON INTEGRITY MECHANISMS

Ravi Sandhu

Department of Information Systems and Systems Engineering
George Mason University, Fairfax, VA 22030-4444

Agreement on the meaning of integrity remains elusive. In spite of considerable effort, the NIST workshop of January 1989 was unable to make much progress on this issue. Rather than attempt to resolve this debate here, let us simply accept the common viewpoint that integrity is concerned with information modification rather than information disclosure or information availability.

Fortunately there is a general consensus that integrity is an important problem, in both the military and commercial sectors. It is also generally accepted that information integrity requires something beyond traditional discretionary controls. There is however little consensus on precisely what non-discretionary controls are needed. Two extreme viewpoints are summarized by the following quotes.

> "... some separate mechanisms are required for enforcement of these policies, disjoint from those of the Orange Book." *Clark and Wilson*

> "Fortunately, techniques to protect against information modification are almost always the same as (or a subset of) techniques to protect against information disclosure." *Gasser*

In our opinion the Clark-Wilson attitude is the correct one, i.e., integrity requires non-discretionary access-control mechanisms other than label-based mandatory controls.

There are many researchers who share Gasser's point of view, although they are usually willing to extend label-based mandatory controls to execute and append operations in addition to reads and writes. Our principal objections to this line of thought are outlined below.

1. Examples of label-based integrity controls inevitably require trusted subjects. Indeed almost all subjects need to be trusted to some extent. We believe this proliferation of trusted subjects is a basic property of integrity. The problem with label-based controls is that trust can be bounded only in terms of read, write, append and execute operations. On the other hand the Clark-Wilson concepts offer a fundamentally different view of trust based on higher level operations and sequences of operations.

2. With label-based controls the audit trail is writable (appendable) by everybody and therefore of low integrity. This is disturbing since the whole point of an audit trail is to have high integrity. Label-based controls also do not enforce the obligation to write to the audit trail, they merely specify that it may be written.

3. The combination of independent integrity labels and confidentiality labels does not provide any additional power than obtained by each in isolation, i.e., precisely the same controls can be enforced using integrity labels alone or confidentiality labels alone. So the label-based view of integrity is essentially equivalent to lattice-based confidentiality.

Finally let us consider the following argument in support of label-based controls: all we know how to implement are label-based access controls so we had better figure out how to implement integrity on that basis. This argument ignores the substantial literature on non-label based non-discretionary access controls. It is moreover timid in being bottom-up rather than top-down. Mechanisms should be derived to support policies not vice versa.

We hope the opportunity of this panel discussion will help build a consensus that:

1. Much remains to be done in the way of basic applied research and it is premature to expect a single model or framework to solve all integrity problems.

2. Existing theory and principles can be used to implement far superior integrity controls than provided by existing systems.

These positions are often regarded as mutually exclusive. In many technical fields they coexist quite comfortably. One might add that similar statements can be made for information security (i.e., secrecy, integrity, availability) in general.

Ravi Sandhu is an Associate Professor of Information Systems and Systems Engineering at the George Mason University. Prior to that he was an Assistant Professor of Computer and Information Science at the Ohio State University. He holds the B.Tech. and M.Tech. degrees in Electrical Engineering respectively from IIT Bombay and Delhi, and the M.S. and Ph.D. degrees in Computer Science from Rutgers University. He has published numerous technical papers on information systems security. Among his current research activities he is directing a project on Models, Mechanisms and Methods for Integrity Policies.

TH0287-3/90/0000/0279$01.00 © 1990 IEEE