

## Concerning "Modeling" of Computer Security

D. Elliott Bell

Trusted Information Systems, Inc.

**Abstract.** "Modeling" in the context of computer security has the same connotation as in the fields of science and engineering, that of an abstraction used for the consideration of a problem of interest. One recent criticism of the Bell-La Padula model confused this notion of "modeling" with a foundational notion of "model" or "interpretation" and, in addition, included intrinsic errors of reasoning.

### MODELS IN SCIENCE

"Models" in the computer security field have generally been constructed as an aid in analyzing "security" properties of interest. [see, for example, 1-15]. In this usage, computer security models fall into the tradition of physical science, engineering, and much of mathematics. The general paradigm is the trading of detail for clarity by the suppression of irrelevant detail in favor of simplified abstractions for analysis.

The success of abstraction as a way to treat difficult problems has been enormous. The laws of universal gravitation developed by Newton in his consideration of solar-sized celestial mechanics did not treat all the factors in a terrestrial environment and did not anticipate events larger and smaller than the ones of interest (for example, relativistic effects near large masses and nuclear interactions), but his progress in understanding the topic at hand was important and well-founded.

"Modeling" in the physical sciences has usually dealt with a set of external constraints. In the physics of Newton's time, for example, constructing abstractions of observed events such as light and the motion of planets that both correctly described the events and allowed the formulation of testing predictions was de rigueur. The three laws formulated by Kepler concerning the motions of planets were acceptable as a pure description. From Newton came the general explanatory theory, universal gravitation, from which the motion of planets could be derived. His theory agreed with current observations and provided specific predictions of great accuracy about the future motion of the sun's satellites. When the motion of Uranus was found to vary significantly from the predictions based on Newton's theory, it was possible to analyze the variation and to postulate the presence of a previously-unseen planet whose gravitational effect would cause the discrepancies observed. The strength of the Newtonian model was increased in this demonstration that the model could guide the way to expanding the set of observed celestial facts.

Newtonian celestial mechanics as a model of the external reality of planets, satellites, and the sun includes the characteristics of (1) accurate description of the phenomena of interest, (2) general

This work was partially funded by Government contract MDA904-86-G-0028.

mechanisms for the analysis of such phenomena, and (3) specific analyses, some deriving known results and others providing testable predictions (a kind of single-blind experiment of the predictive power of the model). As a representative of the concept of a "model" as an abstraction of the reality of concern, Newton's model is close to ideal.

Newton's theory also demonstrates other fates to which abstraction-models are prey. Newton's theory could not accommodate the observed motion of Mercury. It required relativistic notions of geodesics as the "paths that light travels" rather than Euclidean straight lines to resolve that anomaly. Further, Newton's theory when applied to the evolving understanding of atoms fell short. Quantum mechanics was required to deal with atomic and nuclear phenomena, not least because the important factors of behavior at that scale were not included in Newton's considerations. Thus, Newton's theory, in a historical perspective, demonstrates that a model can have omitted a detail of importance or could find its success causing practitioners to apply it beyond its range of applicability. Both these situations embody an undesirable aspect of a model, aspects one can term "incompleteness" and "inapplicability". Surely one could not fault Newton's model of the solar system for failing to take the weak nuclear force into account. One could have criticized it for failing to represent the interaction of Uranus and Neptune properly (had that been so), or for having errors found in the derivation from the law of universal gravitation to the observed facts of planetary motion (were that the case).

Another undesirable feature of a model of physical science is a failure to survive a test of a prediction that distinguishes it from a rival model. In 1935, Albert Einstein and two colleagues published a summary of their unease about the implications of the "Copenhagen Interpretation" of quantum mechanics [16]. Part of that paper described a thought-experiment that concluded that the Copenhagen Interpretation implied that two photons speeding away from each other could affect each other at enormous distance, despite the limitations of the speed of light. The paper concluded that "No reasonable definition of reality could be expected to permit this." This paper's central thesis, called the "EPR paradox", posed an important challenge to the correctness of the Copenhagen interpretation. In 1982, an experiment carried out under the leadership of Alain Aspect [17] demonstrated that the proposed experiment did indeed match the prediction of the Copenhagen interpretation, and did not confirm the negative conclusions of the EPR paradox. The Aspect experiment confirmed the "soundness" (in the sense of freedom from demonstrated flaw) of the Copenhagen interpretation and showed the EPR point of view to be "unsound." It is important to note that the intellectual difficulty was the apparent conflict between the implications of the model and "reality": the apparent "paradox" is only a conflict between reality and your feeling of what reality 'ought to be' [18].

## MODELS IN COMPUTER SECURITY

These general views of "model" in science have been described in some detail in order to illuminate the context in which "modeling" of computer security was undertaken in the early 1970's. As a particular example, the Bell-La Padula model [19-23] was undertaken to provide a before-the-fact analysis tool for the consideration of the general design problem of conceiving and constructing "secure computer systems". It was held that such modeling of computer security required that a resulting "model" satisfy the following characteristics:

- descriptive capability — the ability to describe the situation of interest;
- general mechanisms — analytical tools to aid in the analysis of "secure computer systems"; and
- specific solutions - direct synthesis and analysis aid in the consideration of specific computer systems.

As illustrated above, these characteristics fall directly in line with the usual notion of a "model" in the physical sciences, as well as in engineering and many branches of mathematics.

In the case of computer security, however, there was not as clear an external reality against which to compare the model as was the case in the physical sciences. Part of the initial problem was resolving the slippery nature of the terms "security" and "secure". The direction that was taken in [19-23] was to define carefully those terms as they were to be used in the model itself. The intent was to divide review of model results into two distinguishable parts: the appropriateness of the definition of "security" and a critical review of the "soundness" (that is, "freedom from error") of the treatment of defined-security. The decision to call the specially-defined notion "security" was deliberate: the facets incorporated are important facets of the intuitive notion of "security". The intent was to treat the initially identified facets and then augment the definition with additional facets.

The facets of intuitive-security included in defined-security were identified sequentially rather than all at once. The first facet included was the notion of "confidentiality" or "compromise of information". The facet was included as the simple-security property (so-called as it is the direct analogue to published military regulations about access to classified documents).

a state satisfies the simple-security property (ss-property) provided every access of a subject to an object in a view-mode satisfies the condition that the security level of the subject dominate the security level of the object.

The second facet was the notion of informal need-to-know, the idea that a person is allowed access only to those documents required in the performance of assigned tasks. The model representation was as the discretionary-security property:

a state satisfies the discretionary-security property (ds-property) provided every access of a subject to an object in any mode satisfies the condition that it is explicitly recorded as permitted within the access matrix, the repository of permission data.

The third facet included was a derived property. It was derived from consideration of factors outside the realm of the model itself, but it comprised an internal counter to the external problem of unauthorized information flow. This facet of defined-security was called "\*" -property" (read "star-property") and addresses the prevention of information flow into objects of inappropriate security level.

a state satisfies the \*-property provided every object currently accessed in a view-mode by a particular subject has a security level that is dominated by the security level of every other object currently accessed by that subject in an alter-mode.

These three facets of intuitive-security are the totality of defined-security within the Bell-La Padula model. Those facets are not all the facets of intuitive-security of interest: that fact was noted in the Unified Exposition and Multics Interpretation volume of the model documents [22, pp. 67-73]. Nevertheless, within the context of a "model" as an abstraction within which to investigate a problem of interest, the Bell-La Padula model does capture those three facets — surely three highly desirable characteristics — and does so in a way that allows both initial, rough analysis of design plans (or accomplishments) and more incisive analysis in the process of trying to represent the design of interest in modeling terms.

## USING THE MODEL

The way in which this model is put to use is important in trying to understand both criticisms and defenses. As a tool for the construction of trusted systems, use of the model must entail two distinct activities. The first is **faithful representation**: one must use the descriptive capability of the model to describe the system accurately. Without an accurate description, the second activity, **analysis**

of the model's representation of the problem, will be neither relevant nor instructive. In the case of a model that uses the notion of states and transitions, the activity of faithful representation requires both that all relevant transitions be identified and that every identified transition be described correctly. Analysis of a model's representation of a situation is limited by the results of the faithful representation activity: correct analysis of an incomplete or flawed model of the situation will not be valuable. Thus the use of a model requires thoughtful comparison of the details of the situation to the definitions and limitations of the model to be employed. An error at any step using the model will lead to faulty implications.

It is important to note that the intrinsic modeling results apply exclusively to the analysis portion of model use. The critical step between the situation of interest and the descriptive capability and general mechanisms of the model is that of faithful representation. It is further important to realize that the implications of the model to a situation are limited to those issues included within the purview of the model.

## THE CRITICISM

The criticism of the Bell-La Padula contained in [24] rests on a hypothetical "system" termed "System Z." The essence of System Z is a single state transition that downgrades every object in the system to lattice-low and grants permission to access every object in every mode to every subject in the system. Since the point of System Z is the transition rather than any proposal of a system for implementation, the transition of [24] will be referred to here as the Basic Z Rule, or *BZR*. To facilitate a precise description of *BZR*, a brief review of modeling terms and concepts is required.

The model of [19-23] expresses events and situations of interest in terms of "subjects" (active entities denoted collectively as *S*) and "objects" (passive entities denoted collectively as *O*). The concept of a subject "accessing" an object is addressed using abstract access modes  $A = \{r, e, w, a, c\}$ . The access modes notations were chosen for mnemonic value — *r* for *read*, *e* for *execute*, *w* for *(read)/write*, *a* for *append*, and *c* for *control*. Nevertheless, the access modes are strictly speaking uninterpreted and not identical to instances of similarly-named access modes in particular com-

puter systems. The only implications of the abstract access modes are that an  $r$  access mode implies the ability to view the contents of the accessed object, but not the ability to alter its contents. Similarly,  $e$  implies the ability neither to view nor to alter the object's contents;  $w$  implies both view and alter capability;  $a$  implies the ability to alter but not to view; and  $c$  represents the ability to "control" access to the object and does not imply the ability to view or alter the contents of the object in question. A subject's accessing an object in an access mode  $x$  is represented as a triple  $(S, O, x)$ . The complete set of current access is the set  $b$ .

Access permission is reflected in an access matrix  $M$ .  $M$  is indexed by  $S$  and  $O$ ; the entries are a subset of the set of abstract access modes and reflect the modes of access  $M$  allows to subject  $S$  with respect to object  $O$ .

Elements of both  $S$  and  $O$  have security levels, defined by a function  $level: S \cup O \rightarrow L$ , where  $L$  is a set of security levels, partially ordered by a relation  $dom$ . Every subject also has associated with it two other levels, the "alter-minimum" ( $a-min$ ) and the "view-maximum" ( $v-max$ ), with the limitations that  $level(S) dom v-max(S) dom a-min(S)$ . Two security levels  $L_1$  and  $L_2$  are  $dom$ -related (denoted by  $dom-rel$ ) provided that either  $(L_1 dom L_2)$  or  $(L_2 dom L_1)$ . The functions ( $level, v-max, a-min$ ) are referred to collectively as  $f$ .

A state consists of a triple  $(b, M, f)$ ; the set of all states is denoted by  $V$ . A state is defined to be "secure" provided it satisfies the simple-security-property, the discretionary-security-property, and the \*-property:

- a state satisfies the simple-security-property (ss-property) provided every current access by a subject  $S$  to an object  $O$  in a mode that implies viewing of the object's contents (specifically,  $r$  or  $w$  mode) satisfies the condition that  $level(S) dom level(O)$ ;
- a state satisfies the discretionary-security-property provided that every current access by a subject  $S$  to an object  $O$  in access mode  $x$  implies that  $x \in M_{s, o}$ ;

and

- a state satisfies the \*-property provided every current access by a subject  $S$  to an object  $O$  satisfies the conditions that
  - \*-property provided every current access by a subject  $S$  to an object  $O$  satisfies the conditions that
    - (v) if the mode of access implies viewing of the object's contents (specifically,  $r$  or  $w$  mode), then  $[v-max(S) dom level(O)]$  and  $[a-min(S) dom-rel level(O)]$ ,
  - and
  - (a) if the mode of access implies altering the object's contents (specifically,  $a$  or  $w$  mode), then  $[level(O) dom a-min(S)]$  and  $[v-max(S) dom-rel level(O)]$ ;

A system is a subset of  $X \times Y \times Z$ , where  $X$  is a sequence of "requests" (inputs) from the set  $R$ ,  $Y$  is a sequence of "decisions" (outputs) from the set  $D$ , and  $Z$  is a sequence of states from the set  $V$ . More specifically, if  $W$  is a relation on  $R \times D \times V \times V$ , then  $\sum(R, D, W, z_0)$  is the system defined by

$(x, y, z)$  is in  $\sum(R, D, W, z_0)$  if and only if  $(x_t, y_t, z_t, z_{t-1})$  is in  $W$  for each  $t$  in  $T$  (the totally ordered time set), where  $z_0$  is an initial state of the

system, usually of the form  $(\emptyset, M, f)$ .

$\sum(R, D, W, z_0)$  is ss-secure (ds-secure, \*-property-secure) if  $z_t$  is ss-secure (ds-secure, \*-property-secure) for every  $t \in T$  and every  $(x, y, z)$  in  $\sum(R, D, W, z_0)$ .  $\sum(R, D, W, z_0)$  is defined to be "secure" if it is ss-secure, ds-secure, and \*-property-secure.

The relation  $W$  is usually defined by a set of rules  $\{\rho\}$   $\rho: R \times V \rightarrow D \times V$ . A rule associates with each request-state pair (input) a decision-state (output). A rule  $\rho$  is secure-state-preserving if and only if  $v^*$  is a secure whenever  $\rho(R, v) = (D, v^*)$  and  $v$  is a secure state. Ss-property-preserving, \*-property-preserving, and ds-property-preserving rules are defined analogously.

The principal results of [22] (together comprising the Basic Security Theorem) are that given an initial state that is secure (satisfies the ss-property, the \*-property, and the ds-property) and a set  $\omega$  of rules, each one of which is secure-state-preserving, the resulting system  $\sum(R, D, W(\omega), z_0)$  is itself secure.

A description of the basic Z rule within this rule structure is straightforward. Let  $M_{BZR}$  represent the access matrix each cell of which consists of the complete set of access modes  $A$ . Let  $LOW: S \rightarrow \{lattice-low\}$ . For a security level function  $level$ , let  $level_{BZR}$  denote the security level derived from  $level$  by setting  $level_{BZR}(object) = L-low$  and  $level_{BZR}|_S = level|_S$ ; that is,  $level_{BZR}$  has the same value for every subject in  $S$  and assigns the lowest value in the set of security levels  $L$  to every object in  $O$ . Following the notation of [23], the unspecified boolean function  $bzr(subject, v)$  below represents limitations on the applicability of BZR outside the purview of security concerns.

The basic rule of system Z can thus be represented as follows:

**Request:**  $R = (regrade, S)$

**Semantics:** Subject  $S$  requests that all objects be regraded to  $L-low$  and that  $M$  be set to allow all subjects to access all objects in all modes

$$BZR(S, v) = \begin{cases} (yes, (b, M_{BZR}, (level_{BZR}, LOW, v-max))) & \text{if } bzr(S, v) \\ (no, v) & \text{otherwise} \end{cases}$$

The claimed implications of BZR, as stated in [24], are as follows:

The fact that system Z gives all subjects access to all objects shows that it is the Bell-La Padula model that is inadequate. [24, p.128]

This claim is serious if valid. A critique of that premise, however, requires the consideration of another meaning for the word "model".

#### ANOTHER CONCEPT OF "MODELING"

The term "model" has a different sort of meaning in the context of the foundations of mathematics. When logicians and foundational mathematicians have a set of axioms and wish to establish its consistency (its inability to imply contradictory statements), they construct a "model" satisfying the axioms. The idea is that by demonstrating an example of the class represented by the axioms, one can show conditional consistency: the example is consistent provided the basis of the example is consistent. This is an example of the conser-

vation of complexity. One can show the consistency of Riemannian geometry (no parallels) by giving a model based on a sphere, with great circles playing the role of "lines". This, however, presumes the consistency of Euclidean geometry. One can show the consistency of Euclidean geometry by using the Cartesian identification: ordered pairs of numbers for points, equations for lines and curves, and so on. This argument presumes the consistency of arithmetic. Unfortunately this regression leads to fundamental difficulties represented by Gödel's theorem. The search for consistency, like the search for absolutes in foundational work, founders on the inherently intractable nature of reality.

The use of the term "model" in [24] is neither model-as-abstraction nor that used in consistency discussions. There the identification is made between "defining the concept of security" and "constructing formal security policy models" (p. 123). The following discussion states that "a security model should be formulated [two separate ways] and then both formulations should be proven equivalent" (p. 124). As an motivating analogy, the several "explications" of predicate calculus are offered, with the concepts of "completeness theorem" and "soundness theorem". A completeness theorem in the sense of [24] shows that every derivable formula is valid (in the sense of being a "logical truth" or "tautology") [25, p. 55]. A soundness theorem in the sense of [24] shows that every valid formula (that is, a tautology) is derivable.

It is interesting to note that these uses of the term "model" are in contrast to the usual usage in science and mathematics. "Model" usually connotes an abstraction, whereas the consistency usage connotes a more concrete example and the separate-explications usage views a "model" as being less a tool than a topic of foundational research. The difficulty these varying connotations pose is the possibility of confusion about which sort of model is at issue and what standards are appropriate for judging that model.

### THE CLASH OF PERSPECTIVES

Judging a model-as-abstraction proceeds as described in MODELS IN SCIENCE above. One checks for its fidelity to relevant facts about reality. One checks that the topic addressed is the topic of interest. One checks for errors in the analysis.

Judging a model in the realm of foundational studies can be very difficult. The demonstration of consistency involves building an example (a "model" or "interpretation") that satisfies the set of axioms of interest. The consideration of redundant and complementary explications of a concept proceeds by establishing that the two (or more) explications mutually imply each other.

The goals and methods are clearly substantially different. There is also the potential for confusion based on the "overloading" of the word "model." However, that overloading does not justify the application of cross-field standards to a "model". A model such as the Bell-La Padula model that was constructed as an abstraction to allow analysis free of irrelevant detail never claimed to be a justification of "axioms" in a foundational sense, nor did it claim to capture all the facets of intuitive-security. Continuation of the consideration of *BZR* must, therefore, be bipartite, treating separately its implications in the context of model-as-abstraction and in the context of foundations.

### *BZR* IN THE MODEL-AS-ABSTRACTION CONTEXT

There are two points to consider. The first is the confusion between defined-security and intuitive-security. The second is the fact that *BZR* is not necessarily "insecure" from an intuitive point of view.

First of all, a system including *BZR* meets the definition of security in the Bell-La Padula model. The careful book-keeping in *BZR* assures that every following access will meet the requirements of *ds*-property. With the point of view that a model is supposed to aid the construction of trusted systems, this observation devolves to the question of whether the transition *BZR* is desired. If it is desired, it can be represented. If it is not desired, it can be avoided. The fact that the naive intuition of some views *BZR* as "insecure" is no reflection on the defined-security notion of the Bell-La Padula model. It explicitly forswore inclusion of any intuitive-security property except the *ss*-property, the *ds*-property, and the *\**-property. If one's intuition leads to a desire to avoid *BZR*, one can add to the definition of system security in the Bell-La Padula model to preclude such transitions.

The prohibition needed is, in fact, the principle of tranquility included in [19]. Tranquility as stated there is the system characteristic that object security levels do not change after the initial state  $z_0$ . That version of "tranquility" will be termed "strong tranquility" in this paper; the term "weak tranquility" will be used to refer to the system characteristic of not changing object security levels unless explicitly requested by a subject authorized to initiate such a change of security levels. In fact, the relation *W* in the several evolving instantiations of the Bell-La Padula model exhibit strong tranquility with the exceptions of the change-object-security-level rules, and those rules exhibit weak tranquility. Thus, *BZR* only highlights an additional facet of intuitive-security that is a candidate for incorporation into an extension of defined-security. The desirability of including this additional facet within defined-security rests on an intuitive feeling the *BZR* violates the spirit of intuitive-security.

There are, nevertheless, perfectly acceptable reasons to want to include *BZR* within the repertoire of system rules. To introduce the place of *BZR* in the construction of trusted systems, let us consider a scenario of a modeler working in tandem with a design team in developing a new trusted system. The modeler is reviewing the last set of design documentation and is engaged in the faithful representation activity. He goes through the creation of a faithful representation of the new material, and at the end of the exercise, discovers that *BZR* is on his list of rules to represent the system. He views that as odd: not many rules regrade every object in the system. He therefore goes to his designer opposite. He points out the presence of *BZR* in the interpretation of the system, and asks, "Is that what you meant?" There are two cases.

Case (1) She responds: Absolutely not. You're sure that's there? They check. It is there. The design is changed so that it is not there.

Case (2) She responds: Absolutely. This is a system designed for forward observers. They pack it in on their backs, and part of the functional specification is that it have a

function to destroy all sensitive information in the event of imminent capture or overrun. So we overwrite every file, then regrade the cleansed objects to UNCLASSIFIED. Of course, the overwrites aren't visible at the modeling level (it's just writes, after all, rather than initial- or terminal- object accesses that are reflected at the model level). The only part visible at the TCB interface is the regrade of everything to UNCLASSIFIED.

In case (2), the invocation of *BZR* at every state transition would occasion some discussion, leading most likely to restrictions on the invocation of *BZR*, both in the system design and in the modeling representation of the system. Note that the imposition of invocation limitations is nothing more within the modeling context than the refinement of the additional-policy boolean *bzr*.

This scenario is not contrived. There are numerous systems accredited for system high use that have just such functionality. Furthermore, the example of *BZR* shows, as did the difficulties with the original MITRE secure UNIX prototype [26], that overly simple rules (the original \*-property in that case) need to be refined to accommodate reality better. Trusted subjects resulted from the prototype's difficulties. The inadvisability of absolutely prohibiting *BZR* and care in circumscribing the use of *BZR* seem to be the clear implications here.

This consideration of *BZR* in the context of model-abstraction has shown that its undesirability does not rest on intrinsic considerations but on intuitive-security notions, notions that are not universal. This reliance on intuition persists into the consideration of *BZR* in the context of foundations:

#### BZR IN THE CONTEXT OF FOUNDATIONS

The introduction of *BZR* in [24] purported to demonstrate the "inadequacy" of the Bell-La Padula model. What was in fact done was to demonstrate that the two proposed explications - using secure states and using secure transitions - were not two aspects of the same thing. The conclusion that it is the Bell-La Padula model that suffers from inadequacy is unjustified.

Consider the following definitions on the set of integers:

Definition A:  $d$  is a GCD of  $a$  and  $b$   $\equiv$

$$[(c | a \ \& \ c | b) \Rightarrow c | d]$$

Definition B:  $d$  is a GCD of  $a$  and  $b$   $\equiv$

$$[d | a \ \& \ d | b] \ \& \ [(c | a \ \& \ c | b) \Rightarrow c | d]$$

Definition H:  $d$  is a GCD of  $a$  and  $b$   $\equiv$

$$[d > 0] \ \& \ [d | a \ \& \ d | b] \ \& \ [(c | a \ \& \ c | b) \Rightarrow c | d]$$

According to definition A, 0 is a GCD of 4 and 6, as are 2 and -2. According to definition B, both +2 and -2 are GCD's of 4 and 6, 0 is not. According to definition H, only +2 is a GCD of 4 and 6. Can one conclude, therefore, that any of the definitions are "unsound" or "inadequate"? Three different definitions of GCD have been presented, no two of them equivalent; no conclusions about soundness or inadequacy are justified. Insistence that definition A, in diverging from normal mathematical definitions of GCD, is somehow flawed is another example of the error of identifying a definition with one's (personal) intuition. When intuitions differ — as do the definitions above from [27] and [28] —

the folly of over-reliance on intuition becomes evident.

In the same way, the lack of equivalence between the secure-transition definition of "security" and Bell-La Padula's defined-security demonstrates no more than that the definitions are different. To conclude that "it is the Bell-La Padula model that is inadequate" is to fall into the trap of using one's own intuition as a guide for discriminating between alternative candidates for a definition of something like intuitive-security. "But the history of thought has not dealt kindly with the doctrine of clear and distinct ideas, or with the doctrine of intuitive knowledge implicit in the suggestion." [25, p. 23]

It would have been fair comment to state that the definition in the Bell-La Padula did not include facets of intuitive-security that were personally desired. That contention, however, would have to face the need for emergency overrun functionality described above.

The presentation of [24] includes with the principal fault (intuiting the concept of security and deriving overly-strong conclusions therefrom) several smaller difficulties.

- Following the introduction of *BZR* and the principal (inaccurate) claim that the Bell-La Padula model is inadequate, [24] then asserts that "it should be clear that any explication of security based solely on the notion of a secure state must fail for a similar reason." (p. 128) While it may be that no secure-state explication can be shown to be equivalent to the secure-transition explication of [24], the paper's argument in no sense justifies the conclusion: a single example does not justify a claim of universality.
- The notion that the Basic Security Theorem is a justification of the model is repeated once more (pp. 123 & 126). The importance of the Basic Security Theorem is in demonstrating that a desirable property is inductive. Inductivity is not a justification, just a pleasant characteristic of properties. There exist all four combinations of (inductive or non-inductive) & (desirable or non-desirable) properties.
- An accurate comment on the definition of "secure appearance" in the footnote on p. 126 concludes with the implicitly strong statement that "without this restriction, the BST [Basic Security Theorem] . . . is false." As noted by reference, the falsity is of the nature of a secure system that begins in a not-necessarily secure state, jumps to a secure state, and remains secure. The recast theorems (A1, A2, and A3) and corollary A1 should have been of the following form to avoid this difficulty: For an  $\alpha$ -secure state  $x_0$ ,  $\sum (R, D, W, x_0)$  is  $\alpha$ -secure iff  $W$  satisfies [set of conditions]. The error was real but not devastating. The overstatement masked rather than illuminated.

#### CONCLUSION

The Bell-La Padula model was created in the tradition of a model as abstraction. It carefully circumscribed the area of discourse it intended to treat. In that context, the criticism of [24] showed no flaws in the model. The claims to the contrary were based on the notion of a model as a definition

of intuitive-security and an overloading of the terms "model" and "security". The presentation of [24] itself was flawed, unearned results being claimed and unjustified logical steps being taken.

#### Acknowledgements

The forcing function in the preparation of this paper was the November SIGSAC session arranged by C. Weissman. The final form of this paper was substantially affected by my participation in that forum. In addition, the interaction with my colleagues was invaluable in the preparation of this paper. Especially notable were S. Walker, T. Lee, M. Schaefer, J. Landauer, N. Kelem, N. Bowman-Bell, D. Cooper, and J. Rushby.

#### REFERENCES

- [1] Clark Weissman, "Security Controls in the ADEPT-50 Time-Sharing System," AFIPS Conf. Proc. 35, FJCC 1969, 119-133.
- [2] B.W. Lampson, "Dynamic protection structures," AFIPS Conf. Proc. 35, FJCC 1969, 27-38.
- [3] K.G. Walter *et al.*, "Primitive Models for Computer Security," ESD-TR-74-117, Electronic Systems Division, Hanscom AFB, MA, January 1974.
- [4] R.M. Graham, "Protection in an information processing utility," *Comm ACM*, 15 May 1968, 365-369.
- [5] Lance J. Hoffman, "The Formulary Model for Access Control and Privacy in Computer Systems," Stanford University, SLAC-117, UC-32, May 1970.
- [6] G. Scott Graham and Peter J. Denning, "Protection - Principles and Practice," *AFIPS Conf. Proc.* 40, SJCC 1972, 417-429.
- [7] D. Bonyun, "A New Model of Computer Security with Integrity and Aggregation Considerations," I.P. Sharpe Assoc., Ottawa, March, 1978.
- [8] Dorothy E. Denning, "A Lattice Model of Secure Information Flow," *Comm. ACM*, 19, 5 (May 1976), 417-429.
- [9] M.A. Harrison, W.L. Ruzzo, J.D. Ullman, "Protection in Operating Systems," *Comm. ACM*, 19, 8 (Aug 1976), 461-471.
- [10] "Scomp Interpretation of the Bell-La Padula Model," Honeywell Information Systems, 25 October 1984.
- [11] John McLean, "A Formal Statement of the MMS Security Model," *Proc.*, 1984 Symposium on Security and Privacy, Oakland, CA, 29 April - 2 May 1984, 188-194.
- [12] G.J. Popek, "Access Control Models," ESD-TR-73-106, ESD, Hanscom Field, MA, February 1973.
- [13] G.J. Popek and D.A. Farber, "A Model for Verification of Data Security in Operating Systems," *Comm. ACM*, 21, 9 (Sep 1978), 737-749.
- [14] D.D. Schnackenberg, "Development of a Multilevel Secure Local Area Network," *Proc.*, 8th National Computer Security Conference, Gaithersburg, MD, 30 September - 3 October, 1985, 97-104.
- [15] B.J. Walker, R.A. Kemmerer, G.J. Popek, "Specification and Verification of the UCLA Unix Security Kernel," *Comm. ACM*, 23, 2 (Feb 1980), 118-131.
- [16] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review* 47, (1935), 777-780.
- [17] Alain Aspect in *Physical Review Letters* 49, p. 1804.
- [18] Richard Feynman, Rober Leighton, and Matthew Sands. *The Feynman Lectures on Physics, Volume III*, Addison-Wesley: Reading, MA, 1981.
- [19] D. Elliott Bell and Leonard J. La Padula, "Secure Computer Systems: Mathematical Foundations," MTR-2547 Vol. I, The MITRE Corporation, Bedford, MA, 1 March 1973. (ESD-TR-73-278-I)
- [20] Leonard J. La Padula and D. Elliott Bell, "Secure Computer Systems: A Mathematical Model," MTR-2547 Vol. II, The MITRE Corporation, Bedford, MA, 31 May 1973. (ESD-TR-73-278-II)
- [21] D. Elliott Bell, "Secure Computer Systems: A Refinement of the Mathematical Model," MTR-2547 Vol. III, The MITRE Corporation, Bedford, MA, December 1973. (ESD-TR-73-278-III)
- [22] D. Elliott Bell and Leonard J. La Padula, "Secure Computer Systems: Unified Exposition and Multics Interpretation," MTR-2997, The MITRE Corporation, Bedford, MA, July 1975. (ESD-TR-75-306)
- [23] D. Elliott Bell, "Secure Computer Systems: A Network Interpretation," *Proc. 2nd Aerospace Conference*, McLean, VA, 2-4 December 1986, 32-39.
- [24] John McLean, "Reasoning About Security Models," *Proc.*, 1987 Symposium on Security and Privacy, Oakland, CA, 27-29 April 1987, 123-131.
- [25] Ernest Nagel and James R. Newman, *Gödel's Proof*, New York University Press: New York, 1958.
- [26] W. L. Schiller, "Design of a Security Kernel for the PDP-11/45," MTR-2709, The MITRE Corporation, Bedford, MA, 30 June 1973.
- [27] Garrett Birkhoff and Saunders MacLane, *A Survey of Modern Algebra*, The MacMillan Company: Toronto, 1965.
- [28] I.N. Herstein, *Topics in Algebra*, Blaisdell Publishing Company: New York, 1965.