SECRETS, LIES, AND IT SECURITY

Guy King
Computer Sciences Corporation
7459 Candlewood Road
Hanover, MD 21076
gking1@csc.com
410/684-6316

"Ask me no questions, and I'll tell you no fibs."
--Oliver Goldsmith.

Abstract: Today many IT security professionals apparently believe that their discipline has three goals: confidentiality, integrity, and availability. After touching upon some doubts that this is so, this paper explores a different approach to the problem of IT security goals. Guided by the desire to anchor IT security in the most familiar features of ordinary human life, the approach is two-pronged. The first starts from our ordinary uses of the common term "security"; continues by analyzing them; and, based upon this analysis, proposes a basic definition of "IT security." The second prong looks at the everyday practices regarding information in human life, specifically, at keeping secrets and at lying. The result of this approach is less a rejection of the "C-I-A" view than a paradigm shift. IT security no longer appears an arcane subject of interest to none but its elite practitioners, but as the natural extension of our ancient practices of keeping secrets and lying, of interest and use, therefore, to all humans. Moreover, because IT threatens to destroy the accustomed boundaries which make secrets and lies possible and useful, IT security is seen to be essential to the preservation of these crucial tools of human life.

Keywords: secrets, lies, IT security, foundations, confidentiality, integrity, availability.

1: Introduction

Many Information Technology (IT) security professionals apparently believe that the question of the goals of IT security is settled; on every hand one hears repeated the names of the holy trinity, "Confidentiality, Integrity, and Availability." To put this another way, many IT security professionals apparently believe that the proper subject matter of their discipline is confidentiality, integrity, and availability.

Strangely, one does not hear a justification of this ("C-I-A") view. This is disturbing, given that the view concerns the foundations of IT security, and since the view is by no means self-evidently true.

But this paper does not dwell long on this, the prevailing view of the goals of IT security. After expressing some doubts about it in Section 2, the paper explores a different approach to the problem of IT security goals. The approach is guided by the desire to anchor IT security in the most familiar features of ordinary human life, and has two branches. Section 3 presents the first. Beginning with our ordinary uses of the common term "security," the section continues by analyzing them and, based upon this analysis, proposing a basic definition of "IT security." Section 4 presents the second branch. It looks at the

everyday practices regarding information in human life, specifically, at concealing, revealing, and probing secrets and at lying and detecting lies. This section reviews the important roles secrets and lies play in human life, and identifies the negative conditions against which we wish to protect information. The result of this approach is less a rejection of the C-I-A view than a paradigm shift. IT security no longer appears an arcane subject of interest to none except its elite practitioners, but as the natural extension of our ancient practices of keeping secrets and lying, of interest and use, therefore, to all humans. Section 5 concludes the paper with the point that because IT threatens to destroy the accustomed boundaries which make secrets and lies possible and useful, IT security is essential to the preservation of these crucial tools of human life. A postscript relates the C-I-A view and ISO 7498-2 [6] to secrets and lies.

2: Doubts concerning the C-I-A View

As just stated, the claim that IT security has three goals, confidentiality, integrity, and availability, is heard all around;[1] but one hears no justification of the claim. One has no rational basis for believing it, therefore. Moreover, there is counter evidence which indicates the claim is false. Two arguments are mentioned here.

First, are all three of these truly IT security goals? Some plausibly argue that availability, in its usual sense, is not a suitable goal for IT security.[2]

Second, is it really true that IT security has no other goals? ISO standard 7498-2, for example, identifies five security services, data confidentiality and data integrity (but not availability) plus authentication, access control, and non-repudiation. And others have argued there are additional goals.[3]

In the absence of a justification, and despite counter arguments, we can, of course, attempt to construct a justification for the claim. We might, for example, base our attempt upon the observation that information disclosure and alteration (which pertain respectively to confidentiality and integrity) apparently relate to the two most fundamental modes of information access in automated systems, namely, *read* and *write*.

If our attempt is to accommodate availability also, we can first restrict the meaning of "availability" to "protection against denial of service." Here the notion is of defending

---

[1] See, e.g., [5], par. 0.2; and [8], Section 1.3.

[2] For decades, IT professionals have used the term "availability" in the broad sense of "the probability that the system will be functioning correctly at any given time" (quoted from [9], p. 21). When IT security professionals appropriated this term and gave it a new, different, narrower meaning, "protection against denial of service," they thereby invited confusion. And they got it: numerous IT security professionals apparently now believe it is their job to achieve availability in the *broad* sense.

See also [3] for some interesting comments regarding the noncomputability of availability.

[3] See, e.g., [7].

Table 1. The Relation of C-I-A Terms to Protection Against Negative Conditions.

	READING	*WRITING*	*WITHHOLDING OF AUTHORIZED READING / WRITING*
PROTECTION OF DATA AGAINST UNAUTHORIZED...	Confidentiality	Integrity	"Availability" [= Protection Against Denial of Service]

against someone unauthorizedly denying users the accesses to information for which they are authorized. Thus, withholding takes as its "object" the authorized reading or writing of others. Relative to authorized reading and writing, withholding is at a metalevel.

Table 1 displays these relations. It displays the three goals as logically related to one another and to the fundamental access modes in automated systems. However, it would require additional support to constitute a full justification of the claim that confidentiality, integrity, and availability are the three goals of IT security. But we will leave that to others. Here we simply conclude that there is ample reason to doubt the truth of the claim. We therefore abandon it and turn down a different avenue.

3: Ordinary and Refined Meanings of "Security"; "IT Security" Defined

Like many other disciplines, key technical terms of IT security are borrowed from ordinary language, and then, gradually, given more finely drawn, more precise meanings (we'll cal these "refinements"). Such refinements, which result from analysis of uses of the terms and which are often informed by the unique character of the discipline's subject matter, form the bulk of the discipline's "terms of art."

Accordingly, in an attempt to approach anew the question of the goals of IT security, this section reviews the common uses of the term "security" (and its verb and adjective forms); analyzes these ordinary uses to make the term more precise; and then uses this analysis to define "IT security."

3.1: "Security" in Ordinary Language

In [10] one finds the following definitions and examples:

security: *1a:* freedom from danger: SAFETY
c: freedom from want or deprivation <job ~>
4a: something that secures: PROTECTION

secure: *2a:* free from danger
b: free from risk of loss

safety: *1:* the condition of being safe from undergoing or causing hurt, injury, or loss

protect: *1:* to cover or shield from danger esp. by watchful attention: make secure <policemen ~ing our cities> <a room ~ed by locked

doors>…
b: to stand at the entrance of as if on guard or as a barrier
4a: to watch over so as to prevent escape, disclosure, or indiscretion

One other datum is from the Preamble of the Constitution:

> "We the people of the United States, in order to...secure the blessings of liberty to ourselves and our posterity, do ordain and establish this Constitution...."

In ordinary language, then, "secure from," "safe from," "free from," and "protected from" are closely related in meaning.

In the first two definitions of "security," security appears as a condition or state;[4] in the third (4a), it is the means to bring that state about or to maintain it.

3.2: "Security" Refined

Analysis of ordinary uses of the word "secure" suggests the following:

- There is something (for example, jobs, cities, rooms, blessings of liberty) which is secure (or to be secured);
- That which is secure is secure *for some group* (for example, the blessings of liberty are secured for the people of the U.S.);[5]
- That which is secure is secure from some negative condition (loss, danger, injury, etc.); and
- That which is secure is so by some means (for example, policemen, locked doors).

Although the above ordinary language definitions and examples do not indicate it, we know there is more to be said about security. For example, what is secure is secure *to some degree*; and what is secure is so *relative to some particular environment*. But this paper seeks only to articulate the "joints" visible from ordinary language; this articulation will enable us to educe a basic definition of "IT security." This basic definition will reflect both ordinary language and, as will be seen, ordinary life.

Syntactically, then, "secure" is a polyadic operator: for some group *G*, some thing *T* is *secure* from some negative condition *c* by some means *m*:

secure (T,G,c,m)

3.3: Basic Definition of "IT Security," Part 1

As a species of security, IT security will have the same basic syntax. If we determine appropriate values of the variables in the formula "secure (T,G,c,m)," we shall know the semantics of IT security, too. The following are reasonable assignments:

- That which is primarily to be secured is some set of information,

[4] In light of the previous paragraph, it seems more natural to say that security is the absence of a (negative) condition.

[5] In the sense intended here, a group may consist of a single person.

represented in IT.[6]

- They for whom information is to be secured are some group of humans.[7]

- The means of securing information are variously termed IT security mechanisms, safeguards, countermeasures, etc.

The last statement is a tautology, and will remain so until specific security mechanisms are named. This is left to the reader to do.

But what are the values of 'c'? That is, *what are the negative conditions which can befall information, and which it seems reasonable to expect IT security to protect against?*

Because information has been around for millennia, so, too, have the negative conditions which occur to information. The answer to our question, then, can be found even in the period of human history which antedates the invention of computers, as well as among the non-IT aspects of contemporary human life.

4: Information in Human Life

Living as we do in an imperfect world beset with scarcity of goods and resultant competition for them, the success, even the survival, of a group of humans depends upon its ability to act effectively. Effective action is, roughly, action which results in the satisfaction of the group's needs. Humans' ability to act effectively is grounded to a great extent in their ability to model external reality, to accurately represent the surrounding world in language and to communicate it to one another.

Examples of such representations include:

- "That kind of mushroom will make you sick."
- "$E = mc^2$"
- "Our enemies are located 27 miles north-northeast."

Such representations have truth-value (i.e., are either true or false); and humans who believe true representations (ones which represent reality) tend to have an advantage over humans who believe false representations.

In their competition for scarce goods, human groups have competed *with one another*. It makes sense, therefore, that a key component of each group's competitive strategy has been the attempt to control other groups' access to true representations of reality.

For most humans, no less than three groups of humans are distinguished:

- Our closest group ("we")
- Our allies, who share some of our important interests and who tend to cooperate with us in achieving them
- Our adversaries, who tend to oppose

---

[6] This assignment represents the view of ordinary IT users. Service providers, who charge for the use of IT resources (e.g., CPU cycles, storage space), will justly say that IT resources, too, are to be secured. It is arguable that the value of these resources is secondary, deriving from the value of the information they make available.

[7] This is a provincial view. After a 'close encounter of the third kind', we must change this to include those nonhumans, too.

some of our important interests and who act to prevent us from achieving them

Each of these three groups possesses information concerning its own plans, actions, possessions, etc.; and each also comes to possess some of the other groups' information. As a necessary condition of its fulfilling its plans, each group both seeks to control its own information and to acquire some control over the other groups' information.

These attempts to control information commonly take the following forms:

- We **conceal** certain information (our **secrets**) from adversaries and, to a lesser extent, from allies
- We **reveal** certain information to our allies and, to a lesser extent, to our adversaries[8]
- We **probe** the secrets of our adversaries and, to a lesser extent, of our allies[9]
- We **lie** to our adversaries and, to a lesser extent, to our allies; and we attempt to detect their lies to us[10]

We are here in very familiar territory--in the ancient realm of secrets and lies. Each of us has kept secrets and told lies for as long as we can remember; indeed, they are integral to human existence.[11]

And here is the beginning of an answer to our question, posed at the end of the previous section: **the negative things which can occur to information are various kinds of failure of human groups to conceal, reveal, and probe secrets, and to lie and detect lies.** We shall examine these failures more closely in Section 4.2. But first, to better understand the importance of these failures, and of protecting against such failures, let us remind ourselves of the importance of secrets and lies in our lives.

4.1: Benefits and Costs of Secrets and Lies

Successful concealment of one of our group's secrets can be the means by which we do ourselves (and our allies) great good, and our adversaries much harm. For

---

[8] Although IT security professionals speak relatively little about "revealing," they speak quite often of "sharing" information.

[9] As the terms are used here, we reveal and others probe our secrets; either case can result in the disclosure of our information to others.

[10] The importance of these acts is evidenced by the multitude of words which we possess to name them. The following is a partial list.

Conceal: obfuscate, suppress, hide, withhold, encode.

Reveal: confide, divulge, leak, tattle, blow the whistle, inform, insinuate, hint, intimate.

Probe: steal, gather covertly, eavesdrop, tap, pry, rifle, snoop, spy, pirate.

Lie: fib, fabricate, invent, counterfeit, falsify, misrepresent, distort, adulterate, exaggerate, embellish, inflate, magnify, overstate, stretch, flatter, calumniate, libel, slander, defame, delude, deceive, foist, mislead.

[11] In my discussion of lies and secrets, I am much indebted to the two important books of Sissela Bok, [2].

example, when Odysseus contrived the Wooden Horse, hiding inside with the other Greek warriors, in order at last to end the ten-year war, it was critical to the Greeks' success that they conceal the plan from their adversaries. Successful concealment of this secret meant victory for the Greeks and death for the Trojans.

Had a Greek traitor revealed the secret prematurely to the Trojans, or had a Trojan spy successfully penetrated the secret of the Wooden Horse, Odysseus and the other warriors inside the Horse would likely have been killed,[12] and the victory might have gone instead to the Trojans. Note that if we imagine ourselves to be Trojans, we see that probing can be the means of achieving benefits for ourselves.

On the other hand, revelation of your secrets, confiding them to allies, is a way to arm them and thus to better your own chances. It is also one of the means by which you establish intimacy with a friend, and is a benefit to you both.

Lies are one of the means by which we conceal our secrets. But lies have other uses as well. Sissela Bok writes:

> "Deceit and violence--these are the two forms of deliberate assault on human beings. Both can coerce people into acting against their will. **Most harm that can befall victims through violence can come to them also through deceit**....Even Othello, whom few would have dared to try to subdue by force, could be brought to destroy himself and Desdemona through falsehood."[13]

People's actions are, roughly, a function of their wants and beliefs.[14] For example, if a person wants to eat some pizza; and if s/he believes that s/he can achieve that by calling Domino's and ordering one; then s/he will want to call Domino's and order a pizza. But if s/he can be made to believe that Domino's has gone out of business, then s/he will not want to call Domino's. Thus one can, as Bok says, "coerce people into acting against their will" by changing their beliefs, through lies. Bok elaborates:

> "A lie, first, may misinform, so as to obscure some *objective*, something the deceived person wanted to do or obtain. It may make the objective seem unobtainable or no longer desirable....
>
> Lies may also eliminate or obscure relevant *alternatives*, as when a traveler is falsely told that a bridge has collapsed [and as in our pizza example]....Similarly, the estimates of *costs and benefits* of any action can be endlessly varied through successful deception.
>
> Finally, the degree of *uncertainty* in how we look at our choices can be manipulated through deception. Deception can make a situation falsely uncertain as well as falsely certain."[15]

---

[12]See Homer's *The Odyssey*, Book VIII.

[13]Bok, [2] (*Lying*), Ch. II, p. 19; boldface added.

[14] See, e.g., [4]. The example which follows is also Goldman's; see p. 102.

[15]Bok, [2] (*Lying*), Ch. II, pp. 20-21. As Bok remarks in a footnote (p. 312, note 4), her discussion here "draws upon the framework [namely, objectives, alternatives,

A final, important point about lying, which Bok again points out (Ch. II, pp. 21-32): each of us is both liar and lied to; and our interests vary as we adopt the point of view of liar or deceived.

4.2: Information's Negative Conditions; Basic Definition of "IT Security," Part 2

We are now in a position to fully answer the question posed at the close of Section 3.3: what are the negative conditions which can befall information, and which it seems reasonable to expect IT security to protect against? By answering this question, we can complete the basic definition of "IT Security" begun in Section 3.2.

We have already said that these negative conditions are various kinds of failure of human groups to conceal, reveal, and probe secrets, and to lie and detect lies. The specific kinds of failure fall into two general classes, depending upon whether we are talking about our group's information or about the information of another group (for example, an adversary). (Using the formula stated at the end of Section 3.2, we are here varying the value of 'T'.)
Regarding *our own* information, the failures against which we wish to defend are:

a. Our information being revealed[16] to someone from whom we wish to conceal it
b. Its being concealed from someone to whom we wish to reveal it
c. Its being probed by someone from whom we wish to conceal it
d. Its being false, due to deception and/or our not detecting that it has been falsified)

The first three failures concern secrets; the fourth, lies.

Regarding the information *of another group* (for example, an adversary), the failures against which we offensively strive are:

a. Their information being revealed only to those (excluding us) which the other group wishes to reveal it to
b. Its being concealed from exactly those (including us) which the other group wishes to conceal it from
c. Its resistance to our probes
d. Its resistance to our attempts to falsify it and/or their detecting our attempts or successes in falsifying

With this second set of failures, we touch upon what is lately termed "offensive information warfare." But humans have sought to avoid such failures throughout their history. It's just that now, with IT, some of these failures can occur in new ways. In the final section we shall look at one.
First, though, to complete our basic definition:

> **IT Security** is that discipline which, for groups of humans, protects sets of electronic information against the eight negative conditions just stated, by means of IT safeguards.

5: How To Fail Like a God; How Not To

---

etc.] provided by decision theory for thinking about choice and decision-making."

[16] See footnote 9 above.

Before computers and before writing, humans stored their information in their brains, their memories; and they communicated it (concealing, revealing, probing, and lying) via the spoken word (and gestures). All of us are familiar with the protective means they used, for we continue to use them in our everyday lives. To conceal, we are silent or lie. To selectively reveal, we sequester ourselves in rooms, whisper, etc. To probe we pay keen attention to body language, check for consistency in what we are told, etc. And to lie—we know very well how to lie, don't we?

Writing and IT have extended the human brain, including memory. They have also extended the means of communication. These extensions introduce new ways for the above-listed failures to occur. One is discussed here.

In ordinary human life, where we communicate verbally, our lies can cause another to accept falsehoods, which are then recorded in her/his memory. Note these two aspects of the process:

- our coercion, via lies, of the other's assent, and
- the recording in memory of the accepted falsehood.

In ordinary, unextended human life, lies pertain to the first aspect; they are designed to deceive the belief-acceptance criteria of the one lied to. They do not pertain to the second aspect; we are not able with verbal lies to overwrite the memories in another's organic brain.

Since the appearance of IT, however, our lies pertain to the second aspect as well: we are now able to 'utter what is false' directly into the extended memories of our adversaries. We have means to directly falsify the contents of the primary and secondary storage in their AISs and of messages in their networks. *Nota bene*: by this means we circumvent entirely the first aspect, our adversaries' belief-acceptance criteria.

In the 18th century Bishop Berkeley argued that the external, material, reality in which humans believe does not exist at all, and that the true cause of this appearance (for there does appear to be a world) is God, who at each instant places in human minds the ideas which constitute that appearance.[16] With IT, incredibly, humans have become possessed of this truly godlike power; we can now lie on a scale previously imagined only by Bishop Berkeley.

That *should* give us pause. But it won't. We are talking, after all, about lying, and about keeping secrets; and these are integral to the life of our species. There is no question of eliminating them; we must have both. We will naturally use IT to lie and conceal, probe and reveal, better than ever before.

And what if IT should enable us to lie so well that no one any longer knows the truth? Why, then effective action will be impossible (see Section 4). Or what if it enables probing of secrets so well that all secrets are revealed? Then effective competition will no longer be possible. Since human survival depends upon our ability to compete and act effectively, human

[16] See [1].

life will, under these circumstances, cease.

It will cease, that is, if there is nothing to keep lying and concealing, probing and revealing, *within their accustomed bounds*. "Nothing too much" in human life, the Greeks warned us. Some lies, some secrets, some revelations—this is as it should be with us. But all lies, or no lies, all or no secrets, all or no revelations—these for us are death. IT security provides the needed limits, restores the time-honored bounds.

Without protective means by which we can protect information against the negative conditions listed above, the apocalypse; with them, continued life.

Now: do you *still* want to cut the security budget?

Postscript: Relation of the C-I-A View and ISO 7498-2 to Secrets and Lies

The C-I-A view and ISO 7498-2 are so much a part of today's IT security world that any proposed new definition of "IT security" which cannot address the issues they do is *ipso facto* suspect. This postscript therefore briefly considers how the security objectives and services of these two relate to the basic "IT security" definition offered above.

How does the C-I-A view relate to the basic definition of "IT Security" presented above?

"Confidentiality" and "secrecy" are synonyms. So it is both tautologous and redundant to say that people generally want to keep their secrets confidential. Confidentiality thus maps neatly to our concealing, selectively revealing, and resisting others' probes of, our secrets.

Integrity pertains to lies, more exactly, to our preventing or detecting others' attempts to falsify our extended memories; and to our attempts to falsify others' extended memories without being detected.

If unauthorized withholding is at a metalevel relative to confidentiality and integrity (see Section 2), then it is presumably also at a metalevel relative to both secrets and lies. The unauthorized withholding of authorized reading maps nicely to:

b. our information's being concealed from those [including ourselves] to whom we wish to reveal it

if that concealment is caused by malicious persons. Protection against denial of service includes protection against this negative condition.

Unauthorized withholding of authorized reading also pertains to the corresponding negative condition regarding the information *of another group* (see Section 4.2).

However, the withholding of authorized writing does not map to either of the two negative conditions which address lies.

This should not surprise us, since the basic definition of "IT security" given in Section 4.2 articulates only "the 'joints' visible from ordinary language" (Section 3.2). In ordinary, unextended human life, the condition of a person's being unable to 'record' memories in her brain is so rare that ordinary language does not acknowledge it.

The biography of the Marquis de Sade, for example, reminds us that in earlier times men sometimes attempted to deny authorized 'writing' by imprisoning a person

in a cell containing neither paper nor writing utensils. But this condition, too, is not reflected in ordinary language uses of "secure," "security," etc.

In any case, if we would extend the basic definition of "IT security" offered above, this condition of unauthorized withholding of authorized writing is a good candidate to add to the list of eight negative conditions.

How do the five security services of ISO 7498-2 relate to the basic definition of "IT Security" presented above?

Data confidentiality and data integrity relate in the manner described just above.

Authentication pertains to lies. The object of authentication is to prevent a subject from lying about her/his/its identity. (This one lie is so consequential that a security service is devoted to preventing just it.) The mechanism used to effect authentication may involve a secret (e.g., a password, a cryptographic key); but having a secret is not the object of authentication.

Non-repudiation, too, relates to lies. Its object is to prevent either party to a communications exchange from successfully lying about having been a party to it. (Of the many kinds of lies, this particular class of lies is thought to have sufficiently deleterious effects that a security service is devoted to preventing just it.)

Thus, while data integrity relates to lies generally, authentication relates to one specific lie, and non-repudiation to a particular class of lies.

Access control apparently pertains to both secrets and lies. For it supports both data confidentiality and data integrity, which, as we have recently seen, relate to secrets and lies, respectively. Access control is a means both to regulate the concealment, selective revelation, and probing of secrets and to prevent the falsification of extended memories.

References

1. Berkeley, George. *Three Dialogues Between Hylas and Philonous*. Liberal Arts Press, Inc., 1954.
   --*A Treatise Concerning the Principles of Human Knowledge*. Bobbs-Merrill Co., 1970.

2. Bok, Sissela. *Lying: Moral Choice in Public and Private Life*. Vintage Books, 1978.
   --*Secrets: On the Ethics of Concealment and Revelation*. Vintage Books, 1983.

3. Brinkley, Donald L. and Schell, Roger R. "Concepts and Terminology for Computer Security," in *Information Security: An Integrated Collection of Essays*, edited by Marshall Abrams, Sushil Jajodia, and Harold Podell. IEEE Computer Security Press, 1995, pp. 40-97.

4. Goldman, Alvin. *A Theory of Human Action*. Princeton University Press, 1970.

5. *Information Technology Security Evaluation Criteria (ITSEC)*, Version 1.2, 28 June 1991.

6. ISO 7498-2, *Information Processing Systems—Open Systems Interconnection—Basic Reference*

Model—Part 2: Security Architecture, 1989.

7. Parker, Donn B. "An Essay: Restating the Foundations of Information Security." *ISP News*, May/June 1991.

8. Pfleeger, Charles. *Security in Computing*, 2nd edition. Prentice-Hall, Inc., 1997.

9. Storey, Neil. *Safety-Critical Computer Systems*. Addison Wesley Longman Limited, 1996.

10. *Webster's Ninth New Collegiate Dictionary*. Merriam-Webster, Inc., 1990.