

Toward a Security Ontology

There comes a point in the life of any new discipline when it realizes that it must begin to grow up. That time has come to the security field, as this magazine's founding indicates. Many things come with adulthood—some desirable and some less so. If we're to establish a

ones are modified, and both have new vulnerabilities. Attacks are developed that exploit these vulnerabilities, letting bad guys wreak a certain amount of havoc before we can mobilize and close them off. Some of these exploits are not conceptually new: we've seen them before and we can classify them with other like things. This helps us predict outcomes and set expectations. Other things truly are new: we must name them so that we can talk about them later. What's missing is a broader context that we can use to organize our thinking and discussion.

What the field needs is an ontology—a set of descriptions of the most important concepts and the relationships among them. Such an ontology would include at least these concepts: data, secrecy, privacy, availability, integrity, threats, exploits, vulnerabilities, detection, defense, cost, policy, encryption, response, value, owner, authorization, authentication, roles, methods, and groups. It should also contain these relationships: "owns," "is an instance of," "acts on," "controls," "values," "characterizes," "makes sets of," "identifies," and "quantifies." A good ontology will help us organize our thinking and



MARC DONNER
Associate
Editor in Chief

place in the engineering community for ourselves as practitioners with expertise in security and privacy issues, we must be clear about what it is that we do and what we don't do; what can be expected of us and the boundaries of our capabilities.

Today, far too much security terminology is vaguely defined. We find ourselves confused when we communicate with our colleagues and, worse yet, we confuse the people we're trying to serve. Back in the bad old days, it seemed clearer. The Orange Book (see the related sidebar) was new and seemed relevant, and the industry agreed on the nature of the security problem. Today, we find the Orange Book, developed near the end of mainframes' golden age and before the widespread networking of everything with a program counter, less helpful.

In the midst of a security incident, we have a responsibility to communicate clearly and calmly about what's happening. We must be able to explain during incidents (and at other times) to fellow security experts, to other technologists, and to the general public in a clear and effective way just what it is that we do, how we do it, and how they benefit from our work. For this conversation, simple appeals for better secu-

rity are too trivial, but detailed analyses of cryptographic key lengths are too fine-grained.

There have been several attempts at assembling glossaries of terms in the field. Although these have been useful contributions, glossaries are inherently unable to give form and direction to a field. A glossary is generally a collection of known terms and should be inclusive in scope. This means that it naturally includes contradictory or subtly overlapping terms, leaving it to the reader to decide which to use and which to discard. Independent practitioners will innocently make different choices, and suddenly we're in `comp.tower.of.babel`.

It is the nature of an active technical field that there be continuing change. New systems are built, old

The Orange Book

Widely called the "Orange Book" in the industry, US Department of Defense's Standard DOD 5200.58-STD has established key definitions for computer security professionals for two decades. The work to produce the standards began in the late 1960s and concluded in the late 1970s. As a result, the Orange Book essentially misses all of the issues raised by the networking of vast numbers of computers. You can find a copy of the standard online at www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html.

EDITOR IN CHIEF

George Cybenko • Dartmouth College • gvc@dartmouth.edu

ASSOCIATE EDITORS IN CHIEF

Marc Donner • Morgan Stanley • marc.donner@morganstanley.com
Carl E. Landwehr • US National Science Foundation • clandweh@nsf.gov
Fred B. Schneider • Cornell University • fbs@cs.cornell.edu

writing about the field and help us teach our students and communicate with our clients. A great ontology will help us report incidents more effectively, share data and information across organizations, and discuss issues among ourselves. Just as students of medicine must learn a medical ontology as part of their education, to avoid mistakes and improve the quality of care, so ultimately should all information technologists learn the meanings and implications of these terms and their relationships.

There has been a substantial amount of good work along the lines of developing an ontology, starting at least with the Orange Book. However, recent rapid growth in the field has left the old ontology behind; as a result, it increasingly feels like we're entering the precincts of the Tower of Babel. We need a good ontology. Maybe we can set the example by building our ontology in a machine-usable form in using XML and developing it collaboratively. Is there a Linnaeus, a father of taxonomy, for our field waiting in the wings somewhere? □

Errata

For the March/April 2003 "On the Horizon" department issue, author Gary McGraw acknowledges that Microsoft Research and the US National Science Foundation supported the workshop under grant 0302708 to Rutgers University. He expresses his thanks for this support.

In the "Interface" section of the March/April 2003 issue (European privacy, p. 9), we edited Alessandro Lofaro's comments incorrectly. His explanation: "My phrase about Benjamin Franklin meant he took concepts he knew (written constitution as base of the state; republic; judiciary, executive and legislative powers) and managed to "force" them on a group of British colonists to which such concepts were mostly foreign. Conversely, when these concepts were used in Europe they were already part of a long tradition—"constitutio rei publicae" (constitution of the Republic) is a phrase and concept pre-dating Christianity, like "demos cratos" (democracy), the three-legged structure was "designed" by J.J. Rousseau...).

It is not by chance since 1789 and the French Revolution (but the origin of the tradition is again going back centuries before the year zero) the first articles of Europe's constitutions contain the rights of the individual, while the equivalent Bill of Right is of 1791, four years after the Constitution."

IEEE Security & Privacy regrets this error. —Ed.

EDITORIAL BOARD

Massoud Amin, University of Minnesota
 Ross Anderson, University of Cambridge
 Jim Davis, Iowa State University
 Anup K. Ghosh, Defense Advanced Research Projects Agency
 Peter Honeyman, CITI at University of Michigan
 Thomas F. Keefe, Oracle Corporation
 David Ladd, Microsoft Research
 Ruby Lee, Princeton University

DEPARTMENT EDITORS

Application Security

Marty Stytz, Air Force Research Laboratory, and James Whittaker, Center for Information Assurance

Attack Trends: Iván Arce, Core Security Technologies, and Elias Levy, Symantec

Biblio Tech: Marc Donner, Morgan Stanley

Digital Rights: Michael Lesk, Internet Archive

Education: Matt Bishop, University of California, Davis, and Deb Frincke, University of Idaho

Global Perspectives: Jim Hearn, independent consultant

On the Horizon: Nancy R. Mead, Carnegie Mellon University, and Gary McGraw, Cigital

Secure Systems: S.W. Smith, Dartmouth College

COLUMNISTS

Michael A. Caloyannides, Mitretek Systems
 Bruce Schneier, Counterpane Internet Security

CS MAGAZINE OPERATIONS COMMITTEE

Jean Bacon (chair), Thomas J. Bergin, Pradip Bose, Doris L. Carver, George Cybenko, John C. Dill, Frank E. Ferrante, Robert E. Filman, Forouzan Golshani, Rajesh Gupta, Warren Harrison, Mahadev Satyanarayanan, Nigel Shadbolt, Francis Sullivan

CS PUBLICATIONS BOARD

Rangachar Kasturi (chair), Jean Bacon, Laxmi Bhuyan, Mark Christensen, Thomas Keefe, Deependra Moitra, Steven L. Tanimoto, Anand Tripathi

SUBMISSIONS: Submit one copy of your article to *IEEE Security & Privacy*, Magazine Assistant, 10662 Los Vaqueros Circle, Los Alamitos, CA 90720-1314; phone +1 714 821 8380; security@computer.org. Manuscripts should be approximately 7,200 words long, preferably not exceeding 15 references. For editorial guidelines, visit <http://computer.org/security/>.

EDITORIAL: Unless otherwise stated, bylined articles as well as products and services reflect the author's or firm's opinion; inclusion does not necessarily constitute endorsement by the IEEE Computer Society or the IEEE.

TASK FORCE

Deborah M. Cooper
 independent consultant
 Charles J. Holland
 US Deputy Undersecretary of Defense
 Richard A. Kemmerer
 University of California, Santa Barbara
 J. M. "Mike" McConnell
 Booz-Allen
 Francis Sullivan
 IDA Center for Computing Sciences

STAFF

Lead Editor: Kathy Clark-Fisher
 kclark-fisher@computer.org
 Group Managing Editor: Gene Smarte
 Staff Editors: Scott L. Andresen, Jenny Ferrero, and Steve Woods
 Production Assistant: Monette Velasco
 Magazine Assistant: Hazel Kosky
 security@computer.org
 Contributing Editors: Keri Schreiner and Joan Taylor
 Original Design: Kraus & Assoc. and Larry Bauer
 Graphic Design: Robert Stack and Alex Torres

Publisher: Angela Burgess
 Assistant Publisher: Dick Price
 Membership & Circulation Marketing Manager: Georgann Carter
 Business Development Manager: Sandra Brown
 Assistant Advertising Coordinator: Marian Anderson