NUJIA Hits the Web

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

As information security grows in importance and recognition, security practitioners can sometimes feel overwhelmed by the flood of information available through published journals, magazines, and the Web. For example, my favorite information security portal <http://www.infosyssec.com> is packed with resource links. The SecurityTraq section lists 60 white papers and magazines in management of security, networks and systems, most of which are free to professionals.

Many fine security publications rely on their editors and editorial boards to suggest or select writers for new topics or to evaluate proposals for or drafts of articles. Most of these publications also have columnists who publish regularly. Funding this usually through advertising. Although articles often include references for further reading in these commercial publications, the style is largely relatively informal and easy to read. In addition, the simple editorial review process makes for speedy publication and highly topical reading.

Another category of security periodicals is the peer-reviewed scholarly journals. In addition to editorial review, these publications rely on a system known as peer review: typescripts are sent to a number of reviewers with expertise in the subject area. These referees comment on the substance and style of the writing, make suggestions for improvement, and offer their judgment of whether the paper should be published at all. To avoid bias resulting from friendships or animosity, this process is sometimes refined by removing identifying information about the author(s) from the typescript; this process is known as blind peer review. Typically, a scholarly journal requires every assertion of fact to be backed up by direct observation or by reference to published sources.

Scholarly journals are mostly sponsored by commercial publishing houses, associations, government agencies or universities. Many of these journals cost hundreds of dollars for a subscription. Examples of scholarly journals in information assurance (and their publishers and yearly cost in US dollars) include

_Computers & Security_ (Elsevier, $800)
_Computer Security Journal_ (Computer Security Institute, $110)
-The John Marshall Journal of Computer & Information Law_ (J.M. Law School, $97.50)

As I have written before in this column <http://www.networkworld.com/newsletters/sec/2005/0207sec1.html>, my colleagues and I have created the Norwich University Journal of Information Assurance as a peer-reviewed journal that is available to all at no cost. Our editor, G. Will Milor, MSIA, CISSP, ISSMP, is funded through the MSIA program and the journal is particularly interested in publishing work from MSIA students and instructors. We also welcome submissions from the entire security community. We publish our documents as PDF files that are freely downloadable and printable and (unlike many journals) our authors keep their copyright on their material so they can freely use their own writing later without having to ask for permission from anyone.
Our first issue is up on the Web at <http://nujia.norwich.edu/> and includes a valuable case study by Damon Small, MSIA, CISSP, GSCEC on identifying, localizing and neutralizing a network worm infestation. Courtney Falk, a graduate student at Purdue University’s Center for Education and Research in Information Assurance and Security <http://www.cerias.purdue.edu>, has published a thoughtful article challenging hackers on ethical grounds. John Orlando, PhD, the MSIA’s original Administrative Program Director, addresses weaknesses in the conventional approaches to ethical decision making (including mine!) and provides fascinating and valuable insights into more effective approaches to applying ethical reasoning to information technology questions.

Come and visit – and please feel free and encouraged to submit ideas for articles to our editor <mailto:nujia@norwich.edu> or to me directly.

___

ERRATUM:

In the article “Thesis spells out threats to VoIP” <http://www.networkworld.com/newsletters/sec/2005/0718sec1.html> I sent the editor a draft that contained the sentence “I was able to reach Thalhammer and he pointed me to additional VoIP research that he has published.” Unfortunately, this was a _placeholder_ in my draft and I should have taken it out before sending it in! I never was able to contact Dr Thalhammer (his e-mail addresses were dead). I apologize to everyone for this error and hope that Dr Thalhammer will eventually hear that I am trying to reach him. If I do, I shall report on his further research if I can. And I won’t put placeholders in my drafts any more.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.