Matt Bishop responde a la revista Sistemas

Su voz es una de las más autorizadas en el mundo sobre Seguridad Informática.

El científico e investigador, reconocido a nivel mundial como experto en los aspectos de mayor impacto de la Seguridad Informática, aceptó la convocatoria para dar respuesta a varias de nuestras inquietudes.

Matt Bishop recibió su grado como doctor Ph.D en Ciencias de la Computación en Purdue University, en 1984. Fue científico e investigador del Instituto de Investigaciones Avanzadas en Ciencias de la Computación, del Dartmouth College, y formó parte del grupo de profesores de la misma institución, antes de vincularse al Departamento de Ciencias de la Computación de la Universidad de California, en Davis, Estados Unidos.

Sus áreas de investigación han girado en torno al análisis de vulnerabilidades en sistemas de computación, en el marco del diseño, la construcción de herramientas para la detección y disminución de riesgos, estudios que contemplan el manejo de todo tipo de lógica maliciosa.

Su actividad es permanente alrededor de la seguridad en redes, el estudio de los ataques de denegación de servicio, modelaje de políticas, aseguramiento y pruebas de software, como también modelaje formal de controles de acceso.

El doctor Bishop participa activamente en educación sobre seguridad de la información. Es coeditor de la columna de Educación del IEEE Security & Privacy; y, miembro del capítulo Del Colloquium de Educación en Seguridad de los Sistemas de Información.

Es autor de uno de los libros más importantes sobre seguridad informática, denominado "Computer Security: Art and Science", publicado con Addison-Wesley.

Además, lidera los cursos de Ingeniería de Software, Arquitectura de Computadores, Sistemas Operativos y Programación en la Universidad de California.

Revista Sistemas: ¿What's critical competencies that an information security professional must develop to face new insecurity challenges in 2020?

Matt Bishop: All security is based on assumptions. So, the most critical competency for an information security professional is the ability to analyze a situation, system, or site and determine what assumptions the security protocols, procedures, and mechanisms are making. This involves asking questions as well as analyzing systems. Knowing these assumptions, the information security professional can determine how best to protect the system. Other critical competencies are a knowledge of computer systems that store information, networks over which the information flows, and how to apply cryptography to protect the information and systems. Finally, an often-overlooked set of competencies involve understanding the social milieu in which the issues of security arise. For example, disallowing anonymity in some countries would not be possible, because people would find it repugnant. Similarly, authenticating using DNA would require people's DNA be stored in a database that was available to any system the person was to have an account on. From the purely technical point of view, this may be a great idea; from the social point of view, many would consider it a horrendous violation of peoples' privacy. Being able to devise countermeasures that are appropriate in a given social and political environment is as important as understanding the technology.

Security is about people first, and technology second.

RS: ¿Do you consider that information security could be a "service commodity" in 2020? This is, information security will be an standard service that could be deliver to a third party?

MB: Yes, information could well be a "security commodity". In fact, some companies in the United States have already done this; for example,

Symantec (among others) will provide around-the-clock managed security services, including incident response, intrusion detection, and improving a site's or an organization's security. I suspect that, as systems become more and more complex, we will see security services being offered by more third parties.

One advantage to this is the offerers may have experience with the same security systems in many different environments. They will also be able to correlate information from all their clients, thereby feeding information about attacks against one into the defenses of all. A danger is that the provider may not learn the client's needs, and instead assume the defenses used by its other clients will suffice to protect the new client. Security is an individual service, and even though there is much commonality in the systems to be protected and the tools to protect them, how to configure the tools, and which tools are most appropriate to use, will differ from client to client -- as will the threats and countermeasures.

RS: ¿How do you see the evolution of Information Security Area (as organizational structure) in next 10 years?

MB: I'm not sure I understand this question. Do you mean the organization of the knowledge and disciplines in the field, or how organizations will be structured to deliver security services?

If the former, I suspect the field will undergo a number of attempts to organize the information in the next 10 years, and none of them will be particularly successful. Eventually, we will reach a consensus of core aspects to the discipline, but I suspect it will take more than 10 years, due to the variety of constituencies involved in defining such a core.

If the latter, I believe that governments and industries will try to develop ways to work together and share information about security, and academic institutions will continue to try to increase funding for fundamental research. I am not sure how successful they will be. I hope they are successful at working together, rather than coming into conflict.

RS: ¿What's the focus of information security research agenda in next 10 years? ¿Universities and Industries could be working together in this agenda?

MB: The big focus is going to be assurance -- specifically, "secure" programming (I hate that term for a variety of reasons, but everyone uses it …) Industries can help guide this part of the curriculum by providing examples, information about what they see as important, common

problems, and tools to help students examine code for problems. Assurance in general will also become more emphasized, and industries can work with academic institutions to provide support in courses that emphasize this. One way is to have employees act as mentors for students; instructors, or guest teachers, or as "teaching assistants" who will show the students how their systems or tools work and help the students examine the tools and systems for problems.

Other foci will be on securing the infras-tructure, such as routers and gateways, and also SCADA technology -- the security of that technology is woefully lagging. Also, human factors -- how to design security mechanisms so that people can use them easily, and they can be configured and installed correctly -- is becoming a very "hot topic", deservedly so.

RS: ¿Which are the recommendations that you give to information security professionals and academics in Colombia, to face information security challenges in next 10 years?

MB: I would give the following recommendations:

a. Learn as much as you can about how people and society work. This basically means partaking of life, and learning about your own and other cultures, societies, and governments. What security is permissible depends a lot on all of those, and the more you know about them, the better.

b. Know limits -- those of the technology, those of the policies and procedures, and your own. A large part of security is determining the limits of effectiveness of the security mechanisms and policies, and not extending them beyond what can be done. And knowing your own limits will help you determine what you need to learn!

c. Ask questions. You learn a lot by asking questions. And when you are examining security data, or working with security mechanisms, ask what the information *really* means and the tool *really* does. Sometimes you find that what "everyone" says is wrong, in some cases.

d. Do not forget basic principles. Technology changes, but not the principles. Using them enables you to get to the heart of problems, and design and build better systems.

e. Be willing to explain security, and why you make recommendations. The more non-security folks learn about security, the better for everyone.