

Talking with: Security Expert M.E. Kabay

Adaptive attackers, novice computer users, indifferent management ... it's no wonder our defensive mechanisms need continuous refinement.

M. E. Kabay, PhD, CISSP is an Associate Professor of Information Assurance in the Division of Business and Management at Norwich University, where he created and manages the online Master of Science in Information Assurance program

UBIQUITY: Tell us a little about Norwich University.

M.E. KABAY: Norwich University is the oldest private military college in the United States. It was founded in 1819 by Alden Partridge who worked at the U.S. Military Academy at West Point. He believed that military students ought to have a more scientific and engineering orientation than was common at that time. He eventually left West Point and founded Norwich University in Norwich, Vermont.

UBIQUITY: Is it still in Norwich?

KABAY: No. It was moved from Norwich to Northfield in 1866 when the original building burned down.

UBIQUITY: How big is it now?

KABAY: It's a small university with between 1,600 and 1,700 students. About half of those are cadets enrolled in ROTC programs full-time. The concept of ROTC was founded at Norwich. Four of the military disciplines are represented here: the Army, the Navy, the Air Force and the U.S. Marine Corp. Full-time active duty officers work on staff and govern the military education of our students.

UBIQUITY: And the other students?

KABAY: The other half are ordinary civilian university students. In a typical classroom, half the students will be in uniform and half won't.

UBIQUITY: Is everyone is comfortable with this?

KABAY: Yes. It seems to be accepted. There's inevitably some friction but it's a very civil and comfortable place for everyone, regardless of which side they're on.

UBIQUITY: Norwich seems to have a strong online presence.

KABAY: Yes, we do thanks to the efforts of Dean Fred Snow and his fearless leadership in collaboration with the Board of Trustees and support of the President and other officers. Dean Snow has put together a splendid set of programs, starting with the MBA. In January 2002 I was asked to create and manage the Master of Science in Information Assurance, or MSIA program. We were up and running by September of 2002.

UBIQUITY: Tell us more about the online MSIA program.

KABAY: I wanted the program to stand out from other graduate programs in information assurance by having a central role for the students' employers. One of the biggest themes in my thinking was that we should integrate our students' work with their place of employment. To be accepted in the program, our students must have a signed commitment from their employer promising that the employer will allow and encourage the student to do research on the security issues within their working environment and that one or more managers will read the student's end-of-seminar reports.

UBIQUITY: Tell me about your master's students. How many are there? Who are they?

KABAY: The growth in the program has been explosive and exciting. We had 15 students in September 2002, 30 in January 2003, and 60 in September 2003. The other aspect that surprised us in the MSIA is the nature of our students. We require that the students have a minimum of two years of full-time experience in information technology. The reason is that I did not want people with solely a theoretical view of the world in our master's program. But many of the people applying to our program are far more experienced than the two-year cutoff. Some of them have 10 to 20 years of experience in information security, let alone IT. Many of our students have CISSP (Certified Information Systems Security Professional) designations from the (ISC)2, which is the highest professional designation in our field. We also have students with professional certification as auditors or as emergency response specialists. That's been a surprise and a delight because the level of the discussions and the essays has been extraordinary.

UBIQUITY: You mentioned that in order to be admitted, the students must have a promise of cooperation from their employers. What has been the employers' reaction to the program?

KABAY: At the end of every seminar, the students write a 5,000 word or more summary of their findings during the seminar including detailed analysis and practical recommendations. The reports must be submitted to their managers. These reports have been received with tremendous interest and uniformly positive response. Some students have reported that their investigations of security have been so well received by their employers that they have been put in charge of new security task forces. In at least one case, a student was formally promoted because of the work he's been doing in our program.

UBIQUITY: How long does it take to complete the program?

KABAY: Our program follows the overall structure of all of the graduate programs at Norwich. The programs are 18 months long. They have six seminars, each of which is 11 weeks long.

UBIQUITY: How did you develop the curriculum for the program so quickly?

KABAY: I had just completed a two-year-long project with Senior Editor Sy Bosworth of creating the *Computer Security Handbook, Fourth Edition*, for the Wiley & Sons publication group. It is a complete reorganization and rewrite of the industry standard computer security handbook. The book was redesigned to have an orientation structure along life cycle lines, as opposed to tools. The progression in the book matches how we think about security in a logical way. The textbook is the core of the MSIA. The seminars follow the same sequence as the parts of the handbook that Sy and I designed and the weekly topics are in pretty much the same sequence as the chapters that are within those parts. The curriculum design was ready within a month and a half. It was unheard of, but it is not quite a fair comparison because I started with two years of work on it.

UBIQUITY: Is the program recognized by the National Security Agency?

KABAY: The National Security Agency offers certification for Centers of Academic Excellence in Information Assurance Education. Norwich University was named as a Center of Excellence a few years ago. We just passed the first stage of our re-certification with flying colors.

UBIQUITY: What's happening at the undergraduate level?

KABAY: Our undergraduate students are enthusiastic about the information assurance and criminal justice courses dealing with cyber crime. We have a special interest group on security audit and control that is affiliated with the ACM Student Chapter, and we also have an information warfare laboratory where students do lab work on defensive countermeasures. The cadets will be competing in the military academies information warfare contest held at West Point every year. In September 2004, we will induct the first students in our new major: the Bachelor of Science in Computer Security and Information Assurance.

UBIQUITY: Well, that's the state of security at Norwich. What do you consider the state of security in the country as a whole? Is it horrible? Is it good? Give it a grade.

KABAY: It is difficult to say because we lack a sound statistical base for measuring the nature of the problem. There are two kinds of problems of ascertainment. One is that you can only measure crimes that are noted, and so the criminals who are extraordinarily skilled may escape notice. Secondly, there's no mandatory reporting of computer crimes, so we depend on occasional public information about crimes that are revealed by their victims (or sometimes by the criminals). The third aspect that makes things difficult is that we don't have uniform targets to compare. We have such heterogeneity in networks that it's extremely difficult to come up with uniform statistics. Even if we could isolate them, we'd have to factor in so many other variables. What version of firewall do they have? Do they have intrusion detection systems? Do they have access monitoring? There are so many factors that make systems different that even if we did have accurate statistics on break-ins, attacks and denial of services, we would still have a great deal of difficulty in coming up with actuarially sound statistical information. Finally, the surveys that are popularly discussed tend to have self-selected populations of respondents and lack measures for internal validation, making them hard to use for generalizations about the overall state of security.

UBIQUITY: It seems like we're seeing more frequent and different kinds of security attacks.

KABAY: That is another problem. The kinds of damage and attacks in computing change all the time. They're adaptive. When we descend against one type of attack, the attackers modify their attacks. Like everyone else in the field today, I tell my students that they should think of security as a process, much like quality

assurance, because the attacks or threats change. Our vulnerability changes as our systems evolve and as new products are put into place.

UBIQUITY: How do you illustrate this point to your students?

KABAY: I ask them to think of an analogy to a house with a door and the door has a lock on it. Somebody comes to your house and uses a lock pick to open your door and leaves a note in your house that says, "You lamer. You only have a lock on your door. Ha, ha. I got in." And so you put on a dead bolt. The next day you come by and the hacker has used a forged key and has opened your dead bolt and left another note that says, "Ha, ha, I got in anyway, you lamer." At this point, you put an iron grill in front of your door in the hope of dissuading the hacker from entering, so he goes into the window and says, "You idiot, you reinforced your door but you forgot the windows." So you put bars on the windows. The hacker drives up with a truck, attaches a chain to the iron bar, rips it off the wall, goes in through the window and leaves a note that says, "Ha, ha. I got in." You put up iron fences with spikes and a 23 centimeter Howitzer outside your house. The attacker comes by with a tactical nuclear missile, blows your defenses to smithereens and in the smoldering ruins of your house, leaves a note saying, "Ha, ha. I got in anyway, you lamer." No matter what we do, somebody has fun challenging the defensive mechanisms.

UBIQUITY: What are some of the other problems you encounter in achieving security?

KABAY: I would summarize them by saying our users don't take security seriously. Management does not take security seriously. The technical environment changes so fast, it's difficult to implement anything effectively. There are some evolving legal issues.

UBIQUITY: Why don't users take security seriously?

KABAY: We have had explosive growth of the Internet and of computer usage in general, worldwide. The number of people using computers who have been on the 'Net for less than, say, a few months is constantly increasing. Given the weaknesses of the infrastructure, we rely on the users as a fundamental bulwark against attack. This is a bit like selling people automobiles that don't have brakes and then expecting them to remember to wear iron-shod shoes so they can put their feet through the holes in the baseboard and drag their feet to stop the car. We give people dangerous, unprotected tools and expect novices to install and configure

them. For example, Windows XP comes with a firewall but it's not configured. The typical 75-year-old novice computer user will not know what to do with the Windows XP firewall. It's not that these are bad or stupid people, it's that we don't have a mechanism for keeping up with the hordes of unaware, untrained people.

UBIQUITY: What are some of the consequences of this generation gap between older and younger users?

KABAY: In many cases, parents and teachers know less than their children or students about the technical aspects of computers. Adults violate intellectual property laws and then act surprised when the RIAA spawns 216 lawsuits for millions of dollars each. Children are victimized because their parents don't know to warn them about dangers on the Internet. The Internet is not a place; that's a metaphor. Cyberspace is a word. It doesn't mean the Internet is a place with its own laws and rules. It's just a means of communication. But some people treat it as if the rules of civility and normal human behavior don't apply. It's as if you were to tell somebody that when they're talking on the telephone, they no longer have to be truthful because they're in telephone space. And in telephone space, imagination wants to be free and you don't have to be truthful or kind, because after all, it's telephone space. So in cyberspace, you don't have to be honest, truthful, or avoid stealing other people's property because, after all, it's cyberspace.

UBIQUITY: Some people like to make a distinction between hackers and crackers.

KABAY: I make a distinction because the press took over the words. You notice I never talk critically about hackers. I always say criminal hackers to distinguish. I say criminal hackers because I want to make it clear that I'm talking about people who break the law using technical resources. Being interested in how things work and thinking up new ways of using technology is not in itself bad. I've been a hacker in the old sense of the word since I was 15 years old, in 1965.

UBIQUITY: Many hackers pride themselves on invading systems but doing it with good intentions.

KABAY: That's absolutely irrelevant. The ones who claim that they're beneficial by entering systems without authorization don't understand the fundamental principals of security. Any breach of security, any use of a trusted system without authorization, destroys the trusted computing base.

UBIQUITY: How do you teach this point to your students?

KABAY: Say that somebody broke into your house and opened the bottles of food in your refrigerator and then put the bottles back and left a note saying, "I opened the bottles to see what was in them but I didn't do any harm." Do you think anybody in his or her right mind would eat or drink the food in the bottles? That would be nuts. A stranger has entered a region of trust, your refrigerator, and done unknown things without your permission and observation to your food. Criminal hackers should understand that if an organization trusts the data and the program on a computer for business critical functions, then once a stranger has entered the system without permission the program or data are no longer trustworthy. I use that example for my students when I'm teaching to get over this profoundly ignorant perception or statement by the criminal.

UBIQUITY: Getting on to another subject, what are your thoughts on electronic voting. Is it hopeless in your view?

KABAY: It's not hopeless but it is very difficult. The difficulties are, number one, identification and authentication of the voters. Then there's the question of the reliability of the machinery. There's also a question of how you ensure that the voter data cannot be tampered with. That's critically important. We must make sure that all of the voting machine companies use proper cryptographic check sums and digital signatures that will prevent modification of the records. We also need to prevent tampering with the software that would, for example, convert a vote for A into a vote for B without letting anybody know and then recording it permanently in the voting records. Can these problems be solved in a way that is cost-effective for the nation, increases voter participation and increases accuracy? The answer is yes but we're not there yet.

UBIQUITY: Talking in general about security issues, is there unanimity among the security experts or are there great divisions in the way they think? Are there any real controversies within that community?

KABAY: There are certainly controversies about specifics. I think there is consensus that we have some major problems in security today. I think there's a consensus that much of the commercial off-the-shelf software has had little attention to security and inadequate quality assurance. We might even argue that some of what is being sold should be qualified as beta test versions, in an older terminology, that is being sold as if it were production software. Other issues are that the fundamental designs are flawed: they're poorly thought out, and they put

too much responsibility on users. I don't like having to rely on users to protect corporate information technology. Why should we be asking *users* to update their anti-virus product? It doesn't make sense.

UBIQUITY: We should end up by telling our readers who you are. What is your background?

KABAY: I come from Montreal, Canada. I grew up in a home where I was forced like a hothouse flower into more advanced education than my age would have made appropriate. I was reading adult books by age five and reading surgery textbooks at age seven. I finished high school math by the time I was nine. I taught math to high school seniors when I was 13. They called me "Slide Rule" because I carried a slide rule, which still hangs on the side of my monitor. I was a strange and unpopular child with the vocabulary of a college student when I was very little.

UBIQUITY: Why did you study surgery? Were your parents doctors?

KABAY: My father was an engineer and my mother was interested in journalism. I think my father, who survived the Holocaust, believed that a doctor would always have something to do, even in times of war and travail, so we'd never starve. I guess that's why I got interested in medicine at that time. One of my favorite stories is of the day a famous cardiologist visited our home. I was nine years old, and he turned to me with a very patronizing air and said, "I saw a *blue baby* today." I suppose he thought that I would express amazement but I said, "Oh, the Tetralogy of Fallot?" And he practically had a heart attack. He said, "You know the Tetralogy of Fallot? And I said, "Oh yes, enlargement of the aorta, mitral stenosis, atrial-ventricular septal defect and patent ductus arteriosus." At that point, he nearly did have a heart attack. That was the kind of kid I was.

UBIQUITY: Where did you go to school?

KABAY: I went to McGill University and then to Dartmouth College where I took the Doctorate in Invertebrate Zoology and Applied Statistics. Although I've taught many courses in computing, I've never taken a university course in computing.

UBIQUITY: What do you enjoy most?

KABAY: What I most enjoy in life is doing anything with my wife, Deborah Black. Not only do we enjoy all the usual wonderful stuff -- walks in the countryside, our family, our pets -- we often laugh as we slave over some

distasteful job and say things like, "There's no one I'd rather do _some horrible task_ with." Doing things with Deborah is the best thing in the world.

UBIQUITY: What does she do?

KABAY: She's a behavioral neurologist. She's interested in frontal lobe issues like epilepsy and Tourette's syndrome and anosognosia (people not recognizing their own illness), memory loss and other fascinating, complicated things.

UBIQUITY: Do I remember correctly that you are musical?

KABAY: Yes, I'm a bass baritone. A couple of years ago I gave a recital of Winterreise at the Barre Opera House. My wife is a concert cellist. She has been soloist with the Montreal Doctor's Orchestra on many occasions. She gives an annual recital at her hospital, which is called Bach 'n' Black.

Links:

Norwich University history: <http://www.norwich.edu/about/who/history.html>

NU Graduate Programs: <http://www3.norwich.edu/grad/>

MSIA: <http://www3.norwich.edu/msia/>

Mich Kabay Web site: <http://www2.norwich.edu/mkabay/>

END