;login:

THE MAGAZINE OF USENIX & SAGE

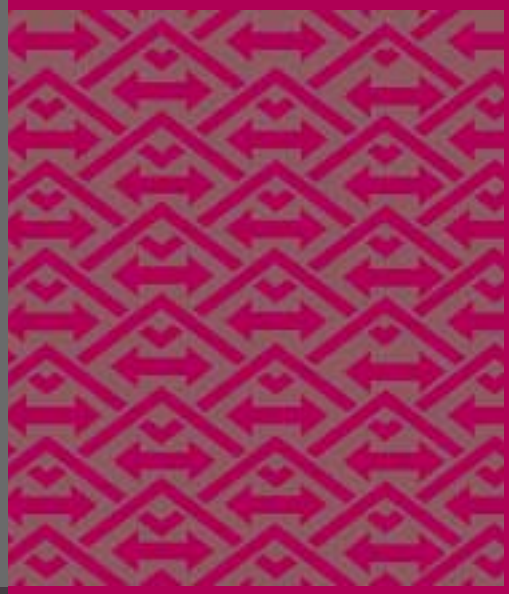
November 2000 • volume 25 • number 7

THEME ISSUE: SECURITY

edited by Rik Farrow

inside:

AN INTERVIEW WITH
BLAINE BURNHAM



USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

an interview with Blaine Burnham

by Carole Fennelly

Carole Fennelly is a partner is Wizard's Keys Corp, a company specializing in computer-security consulting. Carole also writes for www.sunworld.com.

<fennelly@wkeys.com>

Dr. Blaine Burnham is Director of the Georgia Tech Information Security Center.

We have all heard the design model "Keep It Simple, Stupid" (KISS). In his keynote address at the USENIX Security Conference in August, Dr. Blaine Burnham expanded on this concept of common-sense security architecture by demonstrating his points using examples that everyone could easily identify with.

I found many of Dr. Burnham's points to be quite clear and inarguable. In discussing the principle of Acceptability, he stressed that a security solution that is too difficult to use will invite people to go around it or not use it at all. I couldn't agree more.

Some of Dr. Burnham's statements were thought-provoking and invited further discussion. He graciously agreed to take time out from his busy schedule to answer a few questions.

Design Principles of Simplicity: Followup Questions

Carole Fennelly: There was a reference to code that is not open source as providing security by obscurity. While relying on obscurity as the sole means of providing security is foolhardy, isn't some obscurity necessary? There was a comment later in the talk that "it takes a secret to keep a secret." Isn't this a form of obscurity? Isn't privacy also a form of "security through obscurity"?

Blaine Burnham: "Security by obscurity" speaks to the notion that you are basing the security of the system on the assumption the bad guys are unable to discover the internal working of the security system. Historically this has been a very bad assumption. We always tend to underestimate the ability and persistence of the bad guy. This is not to say that one should aggressively market one's security architecture to the bad guy. The only safe assumption is to assume the bad guy has a complete and accurate copy of your security solution.

Regarding the "it takes a secret to keep a secret" statement: It simply means that the solution is designed in such a fashion that the introduction of secret content enables the system to propagate the ability to keep a secret. There is nothing obscure about the secret – usually everything about the secret – except its actual content is known. For example, the DES algorithm is widely available. The details of generating DES keys are openly available. However, a secret (a specific instance of a key known to only one party) DES key can reliably protect – keep secret – a great deal of information.

I don't see privacy as a form of security through obscurity. To me privacy is a global system property/behavior in which the system has access to the private information but it does not divulge the information in violation of the privacy policy. The system knows it doesn't tell. Part of the problem has been the absence of meaningful privacy policies – hence an open season on personal/private information, a behavior that argues that personal information is the property of the holder, not the referent – and therefore the referent has no control/stake in the information. In addition, we have to deal with the fundamental weakness of the systems to enforce any meaningful privacy policy in the face of anything more than casual attempts to assault the system.

Carole: Actually, what I was referring to with regard to privacy fits in with your explanation of "security by obscurity." I may not aggressively advertise where I live and my bank account numbers to the public at large, but I don't rely on that "obscurity" to protect myself.

Blaine: This is a good working example of my point. You don't have to advertise and otherwise aid and abet the bad guy. On the other hand, these measures in and of them-

selves cannot provide you the real protection you may need. Some mechanism(s), usually of a completely different nature, will have to be employed to provide the protection you may demand.

Carole: A comment was made that script kiddies create so much "noise" that it is difficult to track the real criminals. Isn't some of this relatively harmless noise necessary to raise awareness of security in the corporate world?

Blaine: I would not like to argue that this noise is harmless. In fact it is very harmful – depending on who you read – latest numbers put the cost in the trillions. Further, as distressing as it is, the observation that the security awareness of the corporate world has been significantly increased as a result of this noise appears to be true, at least to a first approximation. I find this whole "motivational" discussion tremendously upsetting because it shouldn't have to happen. There has been any amount of discussion and ample demonstration, for years, pointing to the encroaching risk to information systems. I find it unbelievable that we have done so little, really, to address the problems. I suspect that something like a consumer-protection agency is going to come about to deal with the problem. This will be a solution that no one will like.

Carole: I certainly don't endorse the activities of script kiddies and I agree they are a major annoyance. But aren't many reports of "damages" grossly exaggerated? Such as reporting the damages as including the cost of installing a firewall and redesigning a Web site?

Blaine: I haven't spent much time trying to validate the legitimacy of the damage claims. I know the impact of any of these DDoS attacks can be very substantial.

Carole: You mentioned that insurance companies will become an incentive for improving security. Do you think they will have a different picture of actual damages? Won't they hold organizations liable for not adhering to industry best practices?

Blaine: I think the insurance industry will have consistent measures for assessing the damage. What those measures are has yet to be determined. But over time insurance firms have demonstrated the ability to home in on the correct measures. I don't exactly see how the insurance industry will hold organizations liable. I think it will work more along the lines that failure to adhere to best practices may void a company's insurance policy. Sort of like – as I recall – skydiving can void a personal injury/life insurance policy. However, in addition, the interdependencies of e-mumble will create situations such that if a particular business fails to adhere to best practices and the consequent damage propagates to the e-mumble business partners, the insurance representatives of the damaged parties will come at the nonadhering business for compensation. This could have *enormous* consequences. For example, if you are running some mom-and-pop telecommuting engineering function for a major toy company and you are networked into their whole just-in-time manufacturing – for the Christmas rush – toy production facility, and you don't take sufficient protection measures while you are sitting on the beach somewhere while you put the finishing touches on your design, and the bad guy (today he may be in the employ of a competing toy company, tomorrow who knows) is able to gain access to your system and alter the design you upload to the JIT plant, and the plant manufactures the toy with a lead-based paint (this is the bad guy's modification) that causes the toys to all be recalled the day after Thanksgiving. I would hope you had paid up liability coverage – *a lot of it*.

Carole: You stated that "hostile and malicious code are the real problems." What about badly written code?

Probably one of the more significant overlooked notions is the word "personal" in the phrase "personal computer."

Blaine: The Greeks built the Trojan horse after spending tremendous energy exploring for a more direct access to the city of Troy. It is fair to observe that the Trojans were probably fairly disciplined in their walls and gates and windows maintenance. Had they not been, the Trojan horse would not have been necessary. Look at it from the bad guy's point of view: Take advantage of the target's mistakes; these mistakes lower the cost of the effort to achieve the objective. Badly written code is a tremendous advantage to the bad guy. He doesn't have to work so hard.

Carole: You stated that "security is not an add-on." How do we enforce this? If you look at the white paper for the proposed Simple Object Access Protocol (SOAP), security is certainly considered to be someone else's problem.

Blaine: I cannot argue for or against better alternatives for the SOAP; however, at least the SOAP does not claim to support security services. There is no confusion about this. Don't look to SOAP for security services. Q.E.D.

Carole: How can we make security attractive to the "bottom line"?

Blaine: This has been tough. I have tried to picture/market security as a business enabler. This sometimes works – sort of. I think the issue of "due care" will eventually work its way into the auditing and insurance side of the business and businesses will have to respond. I don't see this approach delivering the technology we really need for the information age that is upon us.

Carole: There was a reference to home schooling using the Internet. While the Internet can be a great source of information to children, isn't physical socialization also important?

Blaine: Probably, but I think it will be *way oversold* by the folks that Internet-enabled home schools will threaten the most. For the most part children today can have/get as much "socialization" as they can schedule/stand, outside of the conventional school environment. Internet-enabled home schooling will allow families to choose the socialization they want, rather than have to deal with the "socialization" being forced upon them. For a lot of reasons we have let our schools degenerate into war zones in which bullies reign. Additionally, many, many parents feel the schools have abandoned any notion of a wholesome, family-centered system of values. For them and for many others, particularly families with talented children who are buried in a degenerate school system and can't get out, the option is quickly emerging for parents to simply opt out. Not play and not have to deal with a broken system. I think we are on the verge of seeing many of our schools and even whole systems degenerate into being holding tanks/warehouses for truly dysfunctional youth with the rest opting for some form of neighborhood-based Internet-enabled home schooling.

Carole: I've seen ads that entice people to "find out if your spouse is having an online affair! Find out if your kids are surfing porn sites!" Any thoughts on the type of spyware that is used in the home?

Blaine: There is really not much difference between "home spying" and "corporate spying." It amounts to the bad guy wanting to violate a policy, and a system that is not adequate to support the policy. Probably one of the more significant overlooked notions is the word "personal" in the phrase "personal computer." The expectation of any protection in the out-of-the-box PC way outstrips the ability of the technology, particularly from an insider who has intimate access to the machine. Mostly this points to a serious lack of understanding of the technology. It really reduces to a fairly simple dictum: If

you care about the information and the consequences of its misuse then, to the extent possible, eliminate the shared resource.

Carole: You stated that there are no "silver bullets." What is your opinion of vendors who are offering "one-stop shopping" for security services?

Blaine: The notion of "no silver bullet" is the notion that thus far there does not appear to be a single technology or single point of application for a technology that completely resolves the security challenge of most information systems. By that, I intend to point out that an IDS by itself is not, typically, a complete solution; PKI by itself is not a complete solution. The point is that security is a *system* problem and typically is not resolved through the introduction of a particular security service. Some vendors market a single product. Be cautious of vendors who argue that the single product is a complete solution. On the other hand, there are vendors who market suites of products that tend toward providing system-level solutions. These vendors are trying to provide one-stop shopping to their clients and, arguably, this could be a constructive approach. Arguably to the extent that the one-stop shops are dealing with the interactions and dependencies of the assorted products and understand the completeness of the solutions they offer. It's not a lot different from the notion of buying a car by the piece or as an integrated system. By the piece, one might get on the whole very high-quality individual parts, but one is now committed to dealing with the problem of assembling the parts into a whole. A great deal of energy will go into that effort and will require an organizational commitment to the continual maintenance of the whole parts-assembly business model. And it is not clear that all the parts go together to make something. However, by the car, one gets an integrated system that provides transportation, which is the overall objective.

Carole: What are your plans for the future?

Blaine: I would like to say something about this. The University of Nebraska at Omaha has offered me the opportunity to establish, build, and lead a Center for Information Assurance. We are committed to the mission of developing very skilled information-assurance professionals at both the undergraduate and graduate level. The center will be part of UN Omaha's College of Information Science and Technology and be housed in the University of Nebraska's Peter Kiewit Institute. We will develop a comprehensive undergraduate Information Assurance program targeted at supporting the Critical Infrastructure Protection Cybercorp initiative and developing the MS-level Information Assurance area of specialization. We are in the process of instrumenting a Security Technology Emulation and Assessment Lab. We are committed to developing the highly skilled and educated people, new knowledge, and appropriate technology to achieve a safe, secure, and reliable Information Age.

Security is a *system* problem and typically is not resolved through the introduction of a particular security service.