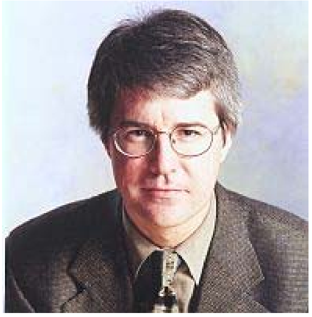
BOB BLAKLEY TALKS TO THE OPEN GROUP



Bob Blakley, Chief Scientist, IBM Software Group

Bob addresses current and future information exchange security concerns, speaks about possible solutions, discusses the possibility of expanding the use of security design patterns from technology into business, and shares his plans related to his involvement in The Open Group Security Forum.

Q: From a practical point of view, and with the exception of viruses, what are the top security issues that electronic information exchange brings?

A: Viruses, of course, would be the number one concern. Number two would be confidentiality and privacy. If you are exchanging information that has any business sensitivity or privacy sensitivity, you have to consider that the communication can be intercepted on the wire, and also that the information might be stored at many different places along the way. For example, if you are sending an email, the message is stored at the various intermediate mail transfer agent servers. You either have to do something for protection or you have to understand what policies and protections the intermediate servers have in place.

The other problem that you might have to worry about if you are exchanging business information is the issue of timeliness. If you have anything that is time-critical – for example, a contract with a fixed deadline – you have to be careful about timely delivery of the information. In the email context, you don't exactly know how long the delivery of information will take: it depends on how much traffic there is, how the servers are feeling, and on the connectivity path. For session-oriented communications, when you are doing direct transfers – ftp or relay chat, or something like that – you don't have to worry so much about unpredictable latency, but you do have to worry about the machines themselves not being available.

So, if you are getting ready to have some critical communication, you need to make sure that your infrastructure is capable of supporting availability, and that the services are online.

Q: How do you see this changing in the future?

A: In the near future, the most important change in person-to-person communication will be that more and more is going to be carried over IP networks: think voice over IP, streaming video for video conferencing, and other similar technologies. Moving all of those on IP infrastructure aggregates risk.

Today, risk to the IP routing backbone, for example, could disrupt email, web access, and a number of other protocols. But it normally doesn't cause a lot of disruption in television reception, in telecommunications over the telephone, or in wireless communications to your handheld devices.

If we move more and more of these services for even a part of their travel onto the IP backbone network, then suddenly any major outage in the IP network will create significantly more disruption than it does now.

So we ought to think about either having parallel backbones for those services, or building enough redundancy into the system to give us confidence that we are not going to get very widespread outages.

Q: So you don't foresee any big problems with wireless …

A: We already have big problems with wireless! Wireless number spoofing already happens – it's more difficult now than it used to be because the GSM standards are more difficult to hack than the old analog phones used to be, but you can still do that. It's easier to do if you can get your hands on somebody's chip, the SIM. But really the more serious concerns in the wireless environment right now are related to the security of the communication itself – being able to listen in on communications, for example. This is a particular problem for the 802.1X family of protocols. It is logistically difficult to intercept a targeted voice communication from a cell phone because you have to be close enough to the person with a handset, to be within transmission range of that handset. People are relatively mobile; they tend to move around. So listening in on a business executive's cell phone conversations might require you to follow him with an antenna, which is hard. On the other hand, it is not difficult to listen around office buildings, they tend to stay in one place – so in the short term, the wireless technology is a much more serious concern than cell phone handset security. But that equation will change as more and more functions get aggregated onto the handset, and as more of the computing and text and data communications move from desktops to wireless handsets.

> **The concept of Boundaryless Information Flow™ is itself the biggest security challenge … to achieve the goal of moving information around more freely, we are going to have to be more creative in developing appropriate security mechanisms to make that happen … security is going to become an emergent property of networks or … we'll end up designing networks differently than we do today.**

Q: We spoke about challenges to communications at present and in the future; what do you see as the biggest security challenge to The Open Group's concept of Boundaryless Information Flow™?

A: The concept of Boundaryless Information Flow is itself the biggest security challenge.

The reason the boundaries were there in the first place is to preserve organizational integrity and to make sure that information doesn't get to people or organizations that are not supposed to have it.

So the boundaries are fences, and the fences are designed to protect what is inside. Moving information freely across boundaries means that we are subjecting the information to types of risk that it has not been subjected to in the past. The reason that we didn't subject it to those risks was largely that we didn't know how to protect it against those risks. So, in order to achieve the goal of moving information around more freely, we are going to have to be more creative in developing appropriate security mechanisms to make that happen.

Q: How should we go about it? What would be your suggestion?

A: There are basically two approaches that hold out some promise. One of them is the approach that Phil Venables, CTO for Goldman Sachs, talks about under the title of 'emptying security architecture'. Essentially, his argument is that security is going to become something like an emergent property of networks. So, when you put the components of networks together, the pool of the network and the characteristics of the information artifacts, which travel over the network, will be designed in such a way that either people will have incentives not to cheat or damage information, or it will essentially be impossible, or very, very difficult to cheat in any way. That's a plausible argument. We know about ways to design networks of autonomous entities with rules designed to make sure that people respect them – for economic reasons or other kinds of reasons. So that's one possibility.

Possibility number two is that we'll end up designing networks differently than we do today. Today networks consist mostly of: (a) networking hardware itself, which is typically what you think of as routers that are responsible almost exclusively for moving traffic; and (b) very high function end points, which do processing and presentation and interact with units and all that sort of stuff. I think the networks will consist of three kinds of components instead of only two kinds. There will be: (a) the network infrastructure components, which are responsible for moving the traffic around; (b) the high function end points for the clients and servers; and (c) a set of dedicated special-purpose security devices, which sit around the network, and without which the network itself would be unimaginable. Every time you design a network there would be a population of these things living in it and they would be doing security things.

Q: You co-authored a book on security design patterns that was recently published. Understanding your expertise in technology and security, do you think the security design patterns approach could be broadened from technology into business?

A: Yes, and we are already doing that at IBM. IBM has a set of business security patterns that were developed based on interviews with more than thirty of our largest enterprise customers. We examined what these customers were doing both functionally and in respect to protecting information and we boiled it down to five business security patterns. That was an analytical exercise; we were essentially doing data mining on the customer set. We have subsequently used the business security patterns in a couple of customer occasions through IBM Global Services. I've been involved in some of those engagements and have continued to refine the business security patterns, so in the future I believe that we will publish them in some form; a more polished form than what exists today.

I think that what we as an industry will naturally end up with is a set of business patterns and a set of architectural patterns at a high level that refine them, which is more or less what we've been working on in The Open Group.

Then we'll also develop more detailed implementation patterns that will show people how to transform the architectural elements that they've selected into individual devices or product choices or code that they generate.

Q: You are an active member of The Open Group Security Forum. What are your future plans – on what do you want to focus your work within the Forum?

A: We want to continue to work on the security design patterns. The Open Group has recently published the first edition of the Security Design Patterns guide[1], and the book explicitly says that we anticipate that additional work will take place and revisions will be made in the light of experience. We have gone to the design patterns community and reviewed with them one set of our patterns – we learned a lot. We expect to revise not only the pattern that we reviewed, but also some of the other ones based on that feedback. We plan to go to other pattern community conferences to review the other patterns. We are also aware that there are functional security areas that are not covered by the existing patterns catalog, and so we've got some more work to do there in terms of adding elements to the toolkit. So, security patterns is activity number one.

Activity number two that I am hoping to work on is along the lines of your earlier question: I would like to involve the Security Forum in working on architectures based on these special-purpose security devices that we talked about earlier. We'll have the first session on that topic and we will discuss with the membership if that is a project that they wish to take on.

[1] To get a copy of the Security Design Patterns guide, please visit www.opengroup.org/bookstore/catalog/g044.htm.