

Interview

Silver Bullet Talks with Virgil Gligor

GARY MCGRAW
Cigital

Virgil Gligor is a professor in Carnegie Mellon University's (CMU) Department of Electrical and Computer Engineering. He's also codirector of CyLab (www.cylab.cmu.edu). Gligor serves on Microsoft's Trusted Computing Academic Advisory Board and has consulted with Burroughs and IBM. Gligor has served on many government information security study groups and served on the National Research Council's Panel on Information Security.

Gary McGraw: What are the most important changes in information security over the course of your career?

Virgil Gligor: The most important thing is really the fundamental understanding that every time a new technology is introduced, we introduce new vulnerabilities. The bad comes with the good. As a consequence, we essentially have to watch out for the negative side effects when we introduce technologies and address those and occasionally change our adversary models, or else we end up fighting the last war and perhaps losing even that.

McGraw: Do you think that that understanding is beginning to affect the field of computer security?

Gligor: Absolutely! As a matter of fact, I now see security awareness not just on behalf of the public, but very early awareness of a security implication in software and hardware systems design as well and, of course, in networking. For example, if you talk to any of the computer manufacturers and software producers, they will tell you that security is now a concern that's fairly dominant at the beginning of the design of any system in addition to performance, cost, power, and so on.

McGraw: That's a fairly new phenomenon.

Gligor: It is fairly new—I would say that this phenomenon has taken place only in the last five years.

McGraw: In my opinion, the introduction of the Web in 1993 was a game-changing event for security.

Gligor: No question, you're absolutely right. It was [game-changing] in the sense that it raised the awareness of security in the general public. Clearly, hardware and software vendors were aware of the security problems, but there were no market pressures to produce secure products other than from the DoD [US Department of Defense] and the cop-out [from vendors] was, "Well, the DOD can always buy its own info sec equip-

ment." The Web changed the game in the sense that it exposed security vulnerabilities to the general public, and consequently, started slowly creating demand for security products.

McGraw: It helped to move things in the right direction?

Gligor: It certainly did.

McGraw: Computer security has since become a multibillion-dollar industry. Has the commercialization of the field helped?

Gligor: It's helped a lot, but there's a long way to go. Let me tell you one direction in which I'd like to see security evolve. I'd like to see more usable security—user-friendly security, I might say, for a variety of reasons. One major reason is that, generally, security is invisible and, to some extent, should be invisible to the user. However, we should, to the largest possible extent, enable users and administrators to use security products in a graceful way, namely, without a huge effort and without mistakes. We are not close to that goal.

McGraw: I guess one of the problems with security being invisible is it leads to a real potential for "The Emperor's New Clothes" problem, in which it's invisible because it's nonexistent.

Gligor: Yes, absolutely. This is a somewhat worrisome characteristic, but I think we are making progress.

McGraw: What do you think about some of the commercial products that are available to consumers? Do you think that they're helping with computer security?

Gligor: About 60 to 70 percent of the products—if I were to guess—are helpful. I'd say that some of the products that we have on the market are generally useless. I hate to say this because these products had their use in the past, but now they are becoming obsolete.

I can give you an example. Suppose that I am out of my office with my laptop turned off for 24 hours. In those 24 hours, tens of thousands of new virus variants appear on the Net. Virus scanners cannot keep up with them and have not kept up at this point. We get roughly 100,000 new virus variants per week according to CERT [Computer Emergency Response Team], which is our sister organization at Carnegie Mellon. Consequently, virus scanners at this point have a reasonably limited value, and I believe in the future they'll have somewhat of a limited market once people realize that this is the state of affairs.

McGraw: Part of the impact is this acceleration of time and any sort of delta has a much larger impact than it might have in the past.

Gligor: Absolutely. The acceleration of virus variants in the past three or four years has been phenomenal.

McGraw: My own work focuses on software security where I think we've made some tangible progress. I've been tracking the software security space for several years and in 2008 revenues

from tools and services companies passed \$450 million. That's exciting because that's when the middle market begins to emerge and the analysts come in and start covering the space. Do you think that software security is here to stay?

Gligor: Software security will be with us forever as far as I'm concerned, and I'll tell you why. Software development, by and large, is a creative process. Don't let anybody tell you that formal methods account for more than 10 to 15 percent of the software development. It hasn't happened in the last 30-plus years, and it probably will not happen in the future either.

McGraw: Especially in the US.

Gligor: Well, anywhere—let's admit to that fact. No matter what we academics would like the world to be, the world is not that way in the sense that formal methods have had very miniscule penetration so far. But things are improving. Starting from the premise that there will always be bugs, and so consequently, there is always going to be room for improvement in the software development process just because it's a creative endeavor.

Engineering actually helps mitigate the consequences of the errors that we introduce, of course, because our creativity sometimes exceeds our ability to do things correctly. I believe that from that perspective, software security as a discipline is extremely important. By the way, we at Carnegie Mellon teach bits and pieces of software security in all our courses.

McGraw: That's great.

Gligor: You [students] don't see a single software security course, but it starts from Introduction to Security, and it goes to Network Security, and then goes to Software Systems to System Software Secu-

ity and so on. As a matter of fact, even in Applied Cryptography we talk about software security.

McGraw: We know that's important, having looked at the results of the latest NIST [US National Institute of Standards and Technology] call for algorithms and some bugs that were in those submitted algorithms.

Gligor: We [CMU] have the benefit of having the Software Engineering Institute and the Institute for Software Research and, of course, the computer science department, that teach a number of courses in the security aspects of software. Clearly, model checking, which is the only formal or semi-formal method to apply on a larger scale is being taught by one of the most recent Turing Award winners, Professor Ed Clarke.

McGraw: When I was starting in the computer security field roughly 23 years after you started, I was at a meeting at NIST where they were bemoaning the problem of sharing information about actual exploits. I remember someone there—I think it was Andersson—who was talking about, "Oh, software security is a fad. It's kind of like a sine wave, and it comes and it goes, and it's just coming again, but it's gonna go again." You don't believe that?

Gligor: Actually, I don't believe any of that, but I can explain where that thought came from. Essentially, in the early days the idea was that we can build security kernels which were formally verified. In other words, the software security of these kernels was assured formally, but these kernels were very small, and the thought was that if we have the small kernels which are formally verified, then application software and the rest of the operating system soft-

ware could have as many bugs as possible and will do no damage to the system.

Of course, I'm exaggerating this view to make a point, but essentially that was the view. That view, unfortunately, never materialized.

McGraw: It seems like there's a—what would you call it—a “ripple” of that view in this notion of security coprocessors in laptops and whatnot.

Gligor: The security coprocessors help to actually do things—so they help to check things faster—so they help to a significant extent to make security usable from a performance point of view. But basically doing all sorts of traces and checking traces and backing up computations essentially will turn out to be good Band-Aids.

McGraw: I want to switch gears a little bit. You grew up under Nicholae Ceaușescu [president of Romania, 1974–1989], and escaped during his regime.

Gligor: I grew up before his time, although I spent about four years under his power. Actually, I did not escape, although the story would have been a lot more exciting if I did. I was actually sent to study abroad.

It was essentially a cover-up of the Romanian government that sent Ceaușescu's oldest son to study at the Imperial College in London. To make that look like a national program as opposed to a favor to a dictator's son, they gave a national competition for scholarships abroad to most Western European countries and the US. I was one of the lucky ones who spoke some English, and I made it to the US.

McGraw: How did those early formative years influence your thinking about freedom in security?

About Virgil Gligor



Virgil Gligor is a professor of electrical and computer engineering at Carnegie Mellon University. During the past 29 years, Gligor's research interests have ranged from access control mechanisms, penetration analysis, and denial-of-service protection to cryptographic protocols and applied cryptography. He was a consultant to the Burroughs and IBM Corporations, and is currently serving on Microsoft's Trusted Computing Academic Advisory Board.

He was a member of several US government information security study groups that set research agendas in information security, and served on a National Research Council panel on information security. Gligor was awarded the National Information Systems Security Award in 2005.

Gligor has BSc, MSc, and PhD degrees from the University of California at Berkeley.

Gligor: I'm somewhat biased in that sense because I grew up in a very controlled environment. The first thing that you notice when you come out, although I traveled before coming to the US to a certain extent, is exactly that—freedom. I strongly believe in that, and I think that security cannot be an excuse for compromising individual and institutional freedom in general.

McGraw: It's a real danger. I think that those of us who grew up free have a tendency not to know what we've got.

Gligor: Absolutely! Let me give you a real example from our field about freedom versus security. I bet that if we had a lot of security in the early [developmental] stages of the Internet we would not have the Internet the way it is right now. In fact, we'd have a very small network, probably with lots of government controls in all sorts of countries, and the Internet would not have taken the shape that it has. People in the US don't quite appreciate that, and we all criticize the Internet as it is right now, but the way it developed is because of the freedom to expand without much administrative and bureaucratic control.

McGraw: It certainly helps that

some people believe information wants to be free and this provides a channel for that.

Gligor: Precisely, and it should be free. Of course, security should be enforced and control only the things that have to be controlled to enable those freedoms.

McGraw: What role, if any, do you think computer security practitioners should play in the politics of security?

Gligor: Practitioners always play a very important part in the sense that they educate policy makers in what is possible and what's not, what's practical and what's not, and influence policy in that way because essentially, policy makers have to be informed to maintain a balance between the possible, the useful, the prudent, and the impossible.

McGraw: I'm thinking about three cases in particular where I'd kind of like your opinions, if you don't mind rendering them.

The first is electronic voting. What is your view on the security conundrums involved with electronic voting, and what do you suppose we should do about it?

Gligor: What we should do about it in what sense? Should we ban it? Should we allow it with no scru-

tiny? What are the parameters of the question?

McGraw: No parameters whatsoever. Make it up.

Gligor: Let's take two extremes. Essentially, the era of electronic voting is with us at all levels. We vote in professional organizations electronically, like the IEEE and the ACM. We vote electronically in other areas. When we rank books and movies and things like that. That's one extreme.

There is technology pressure and political pressure and administrative pressure to extend electronic voting to local, regional, and national elections. Electronic voting is with us, and it's by and large a very good thing. Now having said that, I believe that we have made a huge mistake, which we keep repeating, of introducing a new technology without looking at the bad side effects.

McGraw: My goodness! You said that earlier.

Gligor: Right. What happened was the technology was introduced with very little scrutiny, and we all noticed the consequences. The problem is that this technology has to gain credibility, and it hasn't had much credibility so far. Luckily, we had very good people who raised a lot of red flags reasonably early. That's really a testimony to the strength and the depth of the interest of security technologies in public policy. I'm hopeful that a lot of those bugs that cause a lot of consternation to many designers will, in fact, be removed within the next five, possibly seven years.

McGraw: Interesting. The second channel in this intersection of computer security and politics is the Foreign Intelligence Surveillance Act (FISA).

Gligor: Yes, I'm quite familiar with FISA, and I know even where they are located in Washington.

McGraw: We're going to do a panel on FISA at RSA this year [The panel took place in April —*Ed.*]. I'm interested in your opinions about this.

Gligor: Actually, the idea of FISA as originally envisioned was brilliant, and I still think it's an extremely good idea. I think that the role of FISA should be strengthened in the sense that government actions should be under legal scrutiny, and FISA is really the first line of handling that.

McGraw: Because of the court system set up by FISA.

Gligor: That's right. I think the FISA law, as originally anticipated, is something that I give as an example to Eastern Europe—the Czech Republic, Hungary, Romania, Serbia, and so on. I think that they should actually copy that model. I think that all intelligence services should be under the scrutiny of the judicial system. I'm a big supporter of that idea.

McGraw: Very interesting. The third is, what are your opinions about the leadership of cybersecurity in the nation?

Gligor: This is a very good question because, unfortunately, I don't think that we have had much.

McGraw: We have an opportunity to get some, though.

Gligor: Yes, I think that we have neglected this area perhaps because it's too hard to solve in a politically successful way. People just ignored it until the last two or three years. I believe that security now has a lot of visibility within the national government, and consequently, I

think that we'll get good leaders. Good leaders, of course, have to be trained and are not necessarily going to be 100 percent politicians, nor are they going to be 100 percent technical people.

McGraw: You need to find some sort of bizarre hybrid, like a platypus.

Gligor: Possibly, or you need to have basically several people working in a collaborative fashion.

McGraw: Awhile ago, you instructed me to read Morrie Gasser's book [*Building a Secure Computer System*, 1988, Van Nostrand Reinhold] from the '80s.

Gligor: Yes, now I remember. I even remember promising to send you a copy of it—a photocopy of it.

McGraw: What are the top two forgotten papers in the literature, assuming that we've all read Saltzer and Schroeder?

Gligor: It really depends in which area you are talking about.

McGraw: Let's talk about software security. Is that too narrow?

Gligor: If you talk about software security, I think there were a number of papers written in the early days. I hate to admit having written the first paper on a penetration analysis model and tool for C, and that was in 1991 ["Towards a Theory of Penetration-Resistant Systems and its Applications," 1991; <http://dx.doi.org/10.1109/CSFW.1991.151571>]. That was the first published paper that showed that you don't have to rely on the flaw hypothesis methodology, which is basically glorified hacking. You don't have to rely on that 100 percent. We still do that. In fact, Clark Weissman, who with

Dick Linde started the flaw hypothesis methodology, was very appreciative of the fact that we put some engineering discipline into that. That's not a paper for the layman, but it's really the first one.

Of course, we did the first covert channel analysis tool for C in 1987 ["A Formal Method for the Identification of Covert Storage Channels in Source Code," 1987, <http://doi.ieeecomputersociety.org/10.1109/SP.1987.10014>].

Let me stop there with my own work because this is not about my work. This is in general. I'll tell you what [you] should do. One could actually purchase a book which I think is quite good in an overview of the early days of se-

curity. That's Matt Bishop's book [*Computer Security: Art and Science*, 2002, Addison-Wesley] which is essentially a historical handbook. I think it presents fairly accurately what was done by whom and when and why it mattered.

McGraw: Lastly, what's your favorite breakfast cereal?

Gligor: I actually don't eat breakfast cereal. I'm really sorry to admit it. Maybe I should start now.

You can find additional podcasts in this series, including those featuring Matt Blaze, Kay Connelly, Bill Brenner, and Laurie

Williams, at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet/. □

Gary McGraw is Cigital's chief technology officer. His real-world experience is grounded in years of consulting with major corporations and software producers. McGraw is the author of *Exploiting Online Games* (Addison-Wesley, 2007), *Software Security: Building Security In* (Addison-Wesley, 2006), *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), and five other books. McGraw has a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him at gem@cigital.com.

Lower nonmember rate of \$32 for *S&P* magazine!

IEEE Security & Privacy magazine is the premier magazine for security professionals. Each issue is packed with information about cybercrime, security & policy, privacy and legal issues, and intellectual property protection.

Top security professionals in the field share information you can rely on:

- SilverBullet podcasts and interviews
- Intellectual Property Protection and Piracy
- Designing for Infrastructure Security
- Privacy Issues
- Legal Issues and Cybercrime
- Digital Rights Management
- The Security Profession

Subscribe now!

www.computer.org/services/nonmem/spbnr

