EE Security & Privacy met with several interesting speakers at the 23rd ACM Conference on Computer and Communications Security (CCS), held 24–28 October 2016 in Vienna. IEEE S&P is highlighting these interviews in its Spotlight department.

This issue features MIT Lincoln Laboratory’s Hamed Okhravi, cryptographer and cryptanalyst Bart Preneel of KU Leuven, and former assistant director for US federal cybersecurity Gregory Shannon. They discuss issues ranging from moving-target defenses to publication models, education, and government regulation.

Hamed Okhravi on Moving-Target Defenses

What are the main topics that MIT Lincoln Lab is interested in, in the context of security and privacy?

Hamed Okhravi: We do work at Lincoln in many different areas, including designing resilient systems, cyberanalytics and data analytics, modeling and simulation, cyberoperations, and cyberassessment. So it’s a very diverse portfolio of work. My work specifically falls under the umbrella of what’s called moving-target defenses that both our memory safety and software-defined networking efforts fall under.

Moving-target defense has been an important research direction for some time, and recently it has become very trendy, with a large number of publications. So how do you see memory protection research? Do you think we’re finished, or is there still room for research?

Okhravi: Let me take a step back, quickly explain the motivation for moving-target defenses. One of the major problems that we have been facing in cyber is that our systems look very similar internally. If you have an instance of software and have another instance of the same software application, they look exactly alike on the inside. So if attackers find a vulnerability, they can exploit all of these applications at once, and that’s the root cause of many of the large-scale attacks.

We’ve had attacks that can compromise millions of machines at once. The idea of moving-target defenses is to randomize, diversify, or dynamically change the system so it won’t be vulnerable to the same type of exploit and will, in a sense, raise the bar for attackers. Memory safety and many of the memory defenses also fall under moving-target because many such techniques use randomization and diversification as part of their defense.

We’re certainly not done by a long shot because the scope of
these attacks and the power that an adversary can have over a system have been underestimated in the community. There have been many defenses that try to block certain types of attacks or paths in the memory safety domain, but attackers have shown that they can go around those defenses and come up with novel ways to bypass them.

Information leakage attacks are a prominent example of this. Many diversification techniques rely on the fact that the attacker doesn’t know how the system has been randomized. But it has been shown that adversaries can use various types of information leakage to learn how a system has been randomized or diversified, and then attack it. Of course, new classes of defenses try to mitigate that, but it’s still an open research problem to find efficient, fast, and complete defenses, particularly for legacy languages like C, C++.

So what happens if we have new languages as efficient as C and C++ and with safety measures that we don’t have in legacy languages? Do you think that’s the direction to go in the language community?

Okhravi: That’s certainly one direction. A lot of the challenges come from the fact that those languages aren’t very close to the hardware and instructions that we have. So in a lot of ways, they rely on environments or virtual machine monitors that are written in lower-level languages, and that’s how those languages are attacked. If you look at the attacks against Java, in many cases they don’t target Java that’s memory safe—they target the Java virtual machine that’s written in a lower-level language.

If one wants to go down that path, the scope can’t be limited to just the language. Maybe we need new architectures that also fit with those languages that are safe and can better defend. So that’s certainly one direction, and there’s active work going on there. There’s also the other direction of augmenting hardware architectures with tags or memory safety checks so that legacy languages could still run on those.

There are multiple dimensions of design. Of course, speed is one that has to be considered and also compatibility with existing code bases. We have billions of lines of code that are already written in these lower-level languages. The question becomes, what should we do with those? Even if we have a language that’s safe today, that still requires porting all these lines of code into the new languages.

Are you also considering these new directions in your work?

Okhravi: We have done work both in the randomization and diversification domains, which is sort of the short-term fix for legacy languages like C, C++. We’re also collaborating with the MIT campus on building new architectures that are tagged so that these properties can be enforced in the processor itself.

Four or five years ago, there were maybe one-third of the number of attendees at CCS; now we have more than 1,000. Is that a good development for a young researcher, or is the competition and pressure so high that you can’t concentrate on publications because of funding and other things?

Okhravi: Rapid growth like this has its advantages and disadvantages. The advantage is, of course, that it’s better that more minds and more smart people are thinking about these same difficult problems. Maybe they can come up with more innovative solutions than the community before, and that’s certainly a promising direction.

The disadvantage is that it’s hard to stay on top of recent developments. As researchers, we have to read the literature every year, and there are at least four top-tier conferences and many papers in each one of them. So it’s difficult to keep up with the literature. It’s also important to ensure that it’s not the same set of ideas being presented in these communities again and again, to ensure that we don’t get tunnel vision.

We do need diversity of ideas, which is challenging because researchers might be unconsciously biased toward the opinions and ideas that they have worked on. It’s important to have diversity in the program committees as well, so that we can really bring a variety of opinions and ideas into the conference.

If I gave you all the funding that you needed, what problem would you want to solve?

Okhravi: I would like to design our architecture and programming languages from scratch. I think many of today’s challenges have historical causes. A lot of these modern systems are modeled after historical systems like PDP-11 for no better reason than historical succession, and a lot of the security problems are inherited from those systems. For example, the memory model of PDP-11 is very similar to the

---

About the Speakers

Hamed Okhravi is a senior staff member at MIT Lincoln Laboratory. Contact him at hamed.okhravi@ll.mit.edu.

Bart Preneel is a full professor at imec-COSIC KU Leuven. Contact him at bart.preneel@esat.kuleuven.be.

Gregory Shannon is the former assistant director for Cyber Security Strategy in the White House Office of Science and Technology Policy. Contact him at shannon@sei.cmu.edu.
memory model of our current processors, and that has been the root cause of many of the problems. If we redesign these systems with security built in, both languages and the processor, we could do a much better job. That doesn’t mean that it will solve every problem in cybersecurity, but it’s a major step toward achieving better security.

Do you think we’ve become better at solving real-world security problems, or have you not seen much progress outside academia?

Okhravi: I certainly think we’ve become better; both our understanding and the level of expertise that’s required to mount an attack have grown significantly over the past decades. Before, it used to be the case that you could easily find the vulnerability in the most popular operating systems or software applications and exploit it. Nowadays, it’s significantly more difficult. Also, we see a lot of commercial technologies that deploy some of these defenses that have been proposed in academia, in terms of hardware architectures, program safety, web security, all of these domains.

Having said that, the domain itself has also grown significantly. So before, we were dealing with desktop sorts of applications and maybe embedded systems. Now we have all these IoT [Internet of Things] devices; now we have cyber-physical systems. Now we have significantly more connectivity and diversity of targets, which makes it a more challenging problem. So progress has been made, although I’m not sure if it’s at the same level as the growth in the computing environment.

You said that if you had the time and the funding, you’d design systems from scratch because we have learned from our past failures. Somebody has to make the systems and invest money. Do you think that industry would?

Okhravi: If the idea is promising and if they see that it’s going to make a major difference, sure. We’ve seen in the past that when an idea is really polished and promising, of course everybody adopts it. Having said that, we have to make sure that all the system components and the infrastructure are in place.

We have to think about issues like compatibility and performance. In a lot of research projects, the work is done on one dimension of this problem. But to gain widespread deployment, we have to connect all the dots. We can’t sweep anything under the rug. We have to figure out all the necessary components. If we do that, I believe that the chances of it being adopted are promising.

Bart Preneel on Journal-Based Publishing and Public-Key Cryptography

How do you see the development of cryptographic research in an international sense?

Bart Preneel: Because cryptography has very strong ties to mathematics and theoretical computer science, as a scientific discipline, it’s much more rigorous. And it has matured faster than computer security, which is still struggling with its foundations and long-term contributions, although there’s a lot of exciting work being done.

On the other hand, as cryptography develops, there is a growing disconnect between some of the theory research and the applications. I enjoyed the first crypto conferences because there were talks about not only theory but also RSA chip designs and practical systems. In the early 1990s, cryptography became more widely used, but at the same time, the research community shifted more to theory—that was considered the foundational work, and the rest was seen as more heuristic and less relevant. So while our community was integrated, we gradually pushed out the applied work from our main conferences. The crypto community responded by creating new, more practical events such as FSE [Fast Software Encryption] and CHES [Cryptographic Hardware and Embedded Systems]. But most applied crypto papers are now published in computer security venues.

The nice thing about crypto research is that deep theory work can lead to breakthroughs in applications. While multiparty computation was seen as an exotic research topic, today it’s being used by major players to compute on sensitive data to get valuable information without revealing the data to one another; this was considered science fiction in the 1980s. The IACR [International Association for Cryptologic Research] has been working to strengthen the connections between the theory and applications communities.

Do you think that we, as a research community, are doing substantial research? Or are there too many “delta” ideas, too much marginal research?

Preneel: Initially there was plenty of high-impact research, even if the technical quality of the papers (in terms of formalism) would be judged weak by today’s standards. Today, we see much more rigorous work but not always the same creativity or impact. And the competition is tough. It’s a very inefficient enterprise. In terms of submissions, you accept maybe 15 or 20 percent, and then what happens to the rest of the papers? There’s always re-reviewing happening, which is okay if researchers have the time to rewrite their papers but, unfortunately, that doesn’t always happen. Moreover, because of time pressures, I’m not sure that the quality of reviews is always equally good.
In the 1980s, there were good reasons for computer science, as a new and fast-developing field, to publish mostly at conferences. But as the field matures, I believe we should switch to a journal model. A good way to do this seems to be a conference–journal hybrid model, which encompasses the best of both worlds: there are three to four submission deadlines per year, there is a multiround journal-style review process with strict deadlines, and the papers are presented at conferences. This transition has been pioneered by PVLDB (Proceedings of the VLDB Endowment), PoPETS (Privacy Enhancing Technologies Symposium), and now Fast Software Encryption (IACR Transactions on Symmetric Cryptology).

I’ve served on the editorial board of PoPETS and am now co-chair the Transactions on Symmetric Cryptology. What I like about this model is that the review process is much more positive. Reviewers try to find the good aspects of papers, advising authors, “If you will make the following changes, then we will accept it next time.” They try to nurture and improve [the papers]. So, in general, there’s a more positive attitude, and it’s more efficient because if you resubmit, at least two of the reviewers will be the same.

The risk in the model is that reviewers who are very critical have more power to stop a paper from appearing. So the community must consider how to ensure that the model is fair.

For that you have chairs?

Preneel: Yes, but it’s still difficult, given the scale, to manage this. I’m not saying this model is perfect. I just think it’s more positive and more encouraging. One of the arguments for a conference model is fast dissemination. But in the conference–journal hybrid model, we manage to publish papers online within three to four months after submission, which is faster than in many conferences. Also with ePrint servers and archives, the speed argument is no longer relevant. Of course, the social element of conferences is very important.

Do you think for a huge conference, like CCS, a conference–journal hybrid model would be applicable?

Preneel: I think the people in charge should consider it; with careful planning it’s definitely possible. At the same time, the community should also reflect on what it values. A journal model also means no longer rushing your paper. We don’t want last-minute and incremental papers; we should encourage more rendered papers that reflect a complete effort. A journal or hybrid model will help to achieve this.

Consider [the September 2016] DDoS [distributed denial-of-service] attack on IoT [Internet of Things] systems with a default password inside. The attack exploited default passwords, a problem that’s been well understood for decades. On the other hand, we have very “fancy” research in the crypto and security community, such as machine learning for intrusion detection and postquantum cryptography. What’s your view of future challenges? Where would you advise young researchers to put their efforts?

Preneel: Your question touches on two things. There’s a very big gap between the average deployment and the research that’s happening, but I’m not sure that researchers can do much. Maybe senior people can be more outspoken in the policy area, because these solutions clearly have economic and policy components. They’re not to be dealt with as research problems, although we could study them more and make it clear what the solutions are.

As a young person, you’re not in a position to change the game. I think it’s, again, up to the senior people to see how can we make sure that this community progresses and that we reward people working toward long-term solutions. As academics, we should look at current systems and point out weaknesses and find new cool attacks, but we should also try to develop long-term solutions. This balance is difficult.

What I found has worked very well for practice in cryptography are challenges, such as the hash function competition (SHA-3) and the authenticated encryption competition (CAESAR). Earlier, there were competitions for block ciphers (AES) and stream ciphers (eSTREAM). Perhaps this model could be extended to other areas in which the community focuses on requirements and solutions, and hopefully in a few years, it comes up with an answer. It’s very good to focus research on real problems inspired by applications. As a community, we should develop a research agenda. There are different initiatives for this but no integrated community agenda such that everybody understands, for example, that these are the 10 problems we want to work on as a community for the next 10 years. With the EU H2020 project ECRYPT-CSA (www.ecrypt.eu.org), we are working on such a road map for crypto.

---

Our systems look very similar internally, so attackers can exploit all of these applications at once. —Hamed Okhravi
Currently, most schemes are based on public-key cryptography, but we still have the practical problem of public-key infrastructures, at least on the global level. Do you think we need a paradigm change?

Preneel: In 1992, [Whitfield] Diffie, [Paul] van Oorschot, and [Michael] Wiener invented forward secrecy—the station-to-station protocol—for which they did not get enough credit; only after the Edward Snowden revelations did the broader community realize how important this was.

This was a major contribution toward creating secure channels. We will still need to do more work on this basic problem. We have about 10 billion devices using public-key crypto. The largest application is for secure updates. So every time we update an app, or an operating system, digital signatures are used.

The second largest application of public-key crypto is credit cards, following the EMV [Europay, MasterCard, and Visa] specs. Even the US is now adopting this standard. There are close to four billion cards in use today. And if you look at large deployments, the third big one is TLS/SSL. There is also public-key crypto in pay-TV systems, electronic identity cards, and passports. Securing these applications without public-key crypto would be very difficult.

Where it went wrong with TLS/SSL was governance of the Certification Authorities—this is where we have very big problems. In the global credit card business, the governance works fine—there’s an infrastructure with 40 million terminals, and the key management seems to work. The Internet, of course, is a much more open and complex ecosystem whereby many different things play a role. The TLS/SSL ecosystem had a very convenient trust model to kick-start e-commerce, and it made some people rich very quickly. But managing the trust relations is challenging, and end users are confused. There are too many Certification Authorities, but also browser vendors, mobile platform vendors, and app developers. There’s a track record of abuse by nation states and malicious actors who exploit the weaknesses in governance. It’s amazing that 20 years later we’re still struggling with this problem. More transparency is clearly part of the answer (such as Certificate Transparency developed by Google), but there are many forces with other interests. Governments have been reluctant to intervene. I’m not generally in favor of government control, but some regulation is needed because the ecosystem has gotten completely out of hand. Of course, it’s complex; it also has connections with economic power, censorship, and control of the Internet.

**What I like about the conference—journal hybrid model is that the review process is much more positive. —Bart Preneel**

Gregory Shannon: In Government and Adversarial Thinking

What are you doing with regard to cybersecurity?

Gregory Shannon: I’m the assistant director for Cyber Security Strategy at the White House Office of Science and Technology Policy, National Security and International Affairs Division. And my role is to advance the policy around research and development for cybersecurity as it applies not only within cybersecurity but also within other domains like privacy, resilience, accountability.

So why are you here at CCS?

Shannon: I’m here because CCS is one of the top academic conferences in cybersecurity. The fact that it’s in Europe this year is particularly attractive because it’s important to understand the international aspects of cybersecurity research. And this gives us a wonderful opportunity to do that. Of 1,000 attendees, 150 are from the US. So it’s clearly a forum where the US research community is very active, even when it comes overseas to Europe. Part of my goal is to get a sense of what the European community is doing and how that relates to the US’s R&D priorities.

Did you foresee this growth of interest in cybersecurity research?

Shannon: Yes, but it’s certainly been slow. I remember back when SIGGRAPH [Special Interest Group on Computer Graphics and Interactive Techniques] grew from fairly specialized graphics algorithms to the point where those algorithms were helping movies win Academy Awards. There are other technical areas that started off slow but now have a large following and impact. SIGGRAPH provides more of an industrial view now, but I think it’s important that the cybersecurity research community is growing in this way, and I think it shows that there continue to be challenges worthy of investigation.

We have here 4 x 4 tracks with sub-disciplines between information and security. What is your view on the results that these researchers are producing?

commerce, the growth of the Internet, and secure communications was nothing short of profound. And then we have Ross Anderson using security constructs to help fight poverty in the sub-Sahara.

This is amazing work, and it goes back to very important security principles that have been learned over the years and aggregated through conferences like this. There’s a quote by Linus Pauling along the lines of, “If you want to have a good idea, have a lot of ideas.” The fact that we’re having more ideas means we’re going to have more good ideas. Not every idea is going to be great, but I think they all help inform the investigation, identify promising ways of looking at problems, and actually help identify ways that aren’t going to be fruitful and effective. And that’s an important part of it.

You are also involved with cybersecurity strategic aspects. Do you think that there’s pressure in the academic community to generate publications? And there are initiatives to change the way we publish. Do you see this pressure among researchers because they need funding?

Shannon: That’s a hard question. I’ve heard concerns expressed about two issues, at least in the cybersecurity community. One is continuity of funding—the notion that every year, or every 18 months, you’re having to write your next big grant. As your program grows, it gets more and more challenging.

And two, the opportunity to do multidisciplinary work is exceptionally challenging. We have to look to our peers in the medical and biology and physics communities who’ve established large science projects, large enterprises—whether it’s telescopes, or the LHR (Large Hadron Collider), some of the collaborative cancer research that’s going on now, some of the big medical data mining research that’s going on, where results are being shared and such.

We’re a young discipline, so we’re still trying to figure this out.

There’s an opportunity to incorporate ‘adversarial thinking’ into computational thinking education. —Gregory Shannon

We’re definitely pushing the boundary of the social need for diverse research groups to get together and do work right now. Society wants answers to some of the cybersecurity challenges we have. It’s not going to be just normal theory. It’s not going to be just formal methods. It’s not going to be a fancy piece of hardware. It’s not going to be an easy-to-use interface only. It’s going to be all of these things coming together, understanding that whole dynamic. It is going to require a lot of different perspectives. There are opportunities for inspiration from philosophers, from artists, from musicians, from a wide range of areas to help advance the field.

What other specific topics within cybersecurity would you like to see more research on?

Shannon: I’ll give you a copy of the “Federal Cybersecurity Research and Development Strategic Plan” [www.nitrd.gov/Publications/Publi-cationDetail.aspx?pubid=61] that came out in February 2016 as part of [Former President] Barack Obama’s Cybersecurity National Action Plan. You asked what my particular approach is, and the things I care about are in there. The importance of metrics—the ability to characterize how much more difficult some protection makes it for an adversary. The notion of threat models—so that we can use more structured tools. The notion of sustainable security—and by “sustainable” I mean it uses secure designs, secure implementation, verifying the security, and then having secure updates. The notion of defensive deterrence—that we can deter adversaries with our defense if it’s sufficiently robust. We can rely on that if we can characterize how hard we’ve made it for the adversary. Today, we can’t characterize that, so our fellow citizens and policymakers are left with no certainty about whether this will protect the country or their personal information. And I think that’s a real challenge for the R&D community. That’s embodied in the plan.

Many governments, although they finance security research projects, experience security breaches within their organizations. How do you see this development? Is it something that’s generating new challenges, both for government and researchers?

Shannon: It’s exciting. There are going to be a lot of interesting challenges. You called out government vulnerabilities and incidents with governments, but the challenge is that the government relies on commercial off-the-shelf [COTS] systems. So the challenges they face are no different from those faced by citizens and private industry. And that’s the more concerning thing: it’s pervasive. But it also shows that there’s not a specialized solution that’s going to solve the problem.

There’s not going to be a government-specific or critical infrastructure-specific solution, because they’re all relying on COTS. And COTS infrastructure doesn’t have sufficient security—it’s still leaves things vulnerable. The other important reason to have security incorporated in COTS, to the tool chains, is because today’s
academic, graduate student special project is tomorrow’s start-up, which is tomorrow’s budding company, which is tomorrow’s hundred billion dollar infrastructure company.

If security wasn’t part of that development from the beginning, at what point do you stop and make it secure, make it private, make it accountable, make it resilient? We could be stuck when we innovate in a broad way.

So the real challenge is, how do we make it so that even when you’re just doing a simple coding exercise as part of a course, there’s good security as part of that tool chain you’re using. It’s built into the compiler. It’s built into the infrastructure you use. Tests and evaluations are automatically included so you know that even with the very first program you write, you’ve got something with some robustness to it—and that doesn’t exist today.

Do you have any specific message for IEEE Security & Privacy readers?

Shannon: [Former President Barack Obama] has been advocating computer science for all, which is a profound impetus for our education system to add computational thinking to the curriculum, so that all US citizens will be able to do computational thinking. It’s also an opportunity to incorporate “adversarial thinking” in a healthy, respectful, ethical way. As you do computational thinking, you recognize that while your computations create value, there are going to be adversaries out there who want to thwart you, want to compromise what you have, and want to take what you have. You have to be mindful that in today’s computational digital world, there’s now a capable adversary. And you have to be aware that your good intentions aren’t enough to protect what you’re doing—you need to think about how an adversary might look at it.

That’s different from a lot of the engineering disciplines because they’ve had the physical isolation of systems. Physics has ensured that the safety of systems would be effective, because once the centrifugal force gets to a certain level, the flywheel kicks off and the system shuts down. In the digital world, you don’t have the luxury of the enforcement of physics. So it’s a harder problem, and requires engineers to think differently.

Ahmad-Reza Sadeghi is a computer science professor at Technische Universität Darmstadt and editor in chief of this magazine. Contact him at ahmad.sadeghi@trust.cased.de.

Shaza Zeitouni is a research assistant and PhD candidate at Technische Universität Darmstadt. Contact her at shaza.zeitouni@trust.tu-darmstadt.de.