IJITSA is very pleased to include an interview with Professor Gene Tsudik in this special issue. Gene is a “Lois and Peter Griffin” Professor of Computer Science at the University of California, Irvine (UCI). He obtained his PhD in Computer Science from USC in 1991. Before coming to UCI in 2000, he was at IBM Zurich Research Laboratory (1991-1996) and USC/ISI (1996-2000). Over the years, his research interests included most topics in security and applied cryptography. He currently serves as Director of Secure Computing and Networking Center (SCONCE) and Vice-Chair of the Computer Science Department. Since 2009, he is the Editor-in-Chief of ACM Transactions on Information and Systems Security (TISSEC).

When it comes to Gene’s research, one observation a researcher in security, privacy and applied cryptography would make is Gene’s lack of cryptonecrophilia. A common trait of a cryptographer is their persistence in attacking insecure and rotten protocols, yet this feature is absent in Gene’s work; on the contrary, Gene seems to gallop into new challenges and attempts to tackle problems before they manifest.

Professor Katos: You have been involved in security research for over 20 years. Do you think the agenda and priorities have changed if so have the users’ and stakeholders’ needs and expectations of security controls changed too?

Professor Tsudik: Twenty years ago security had relatively few “users”; they were confined to fairly professional types. Today, security is germane to a huge number of users most of whom are not technology-savvy. Viruses and malware were a quaint curiosity at the time of the Morris Worm. They are clearly an everyday problem affecting most people, even those who are not direct computer or Internet users.

Professor Katos: Privacy seems to be moving to the foreground of the security research agenda. A few years ago it was quite common to encounter the term “Security” in isolation but nowadays we often pair “Security & Privacy”. What does this coupling mean to you?

Professor Tsudik: Privacy is, depending on whom you ask, either a separate topic in its own right or a subset of security. I haven’t

DOI: 10.4018/jitsa.2011070106
made up my mind on this issue. Privacy used to mean “the right to solitude, or the right to be left alone”. Today, its meaning has changed to something much more amorphous. Many in our society have enthusiastically embraced the exhibitionism and voyeurism of blogs, tweets and Facebook pages. This has led to the deliberate erosion of privacy; it thus seems quite disingenuous when the same people (e.g., those with a few hundred “friends”) vociferously complain about lack of privacy. On the other hand, increasing digitalization has led to some real concerns about privacy that weren’t there a decade ago. This includes medical and employment records as well as a host of other sensitive information. There is, I believe, a lot left for the research community to do in terms of facilitating average users’ control of their private data.

Professor Katos: Some feel that Cryptography does not really solve problems but transforms them into more manageable forms so they can be addressed by other non-cryptographic means. Given the large scope and wide adoption of modern information systems, do you think that a cryptographer would have faith towards the non-cryptographic security controls deployed on large systems where cryptography is now a small, albeit vital part of the security puzzle?

Professor Tsudik: Cryptography is, indeed, not the solution to security problems— it is almost never a panacea. It’s often a major component of the solution. Non-cryptographic security is likewise not the solution (unless we’re talking about physical security). I think a rational cryptographer familiar with the real world would have to agree that cryptography alone is an excellent fodder for research papers. It needs to be accompanied by (either or both) secure hardware and software. Also, when human users are involved, usability is a key ingredient lack of which typically results in ineffective solutions.

Professor Katos: There have been attempts for setting out grand challenges in information security in the past. Would you consider that it is worth investigating and establishing grand challenges in Security and Privacy?

Professor Tsudik: I am leary of lofty and catchy phrases like «grand challenges». They are usually spouted by self-serving politicians or researchers who have turned into politicians. If such things exist, they are a moving target.

Professor Katos: In your recent work presented at ESORICS 2010, you coined the term “provably forget”, referring to a type of secure update that highlighted the need for a device to wipe a previous configuration and start with an assured clean slate. To my understanding this requirement could be related to trusted computing, reliability and robustness which if placed in the modern mosaic of different and plenty pervasive computing devices and embedded systems (and operating systems), there may emerge a lot more “provably do” requirements and operations. I mean, many information systems are part of critical infrastructures and assurance may be required in many levels.

Professor Tsudik: My use of the term “provably forget” was meant as the opposite to “provably know” in the sense of “proof-of-knowledge” concept popular in cryptography. Since it is possible to prove knowledge of something while revealing essentially no information about it, e.g., using zero knowledge techniques, it would be nice to prove non-knowledge of something. For example, I would like a computer that I used to log in to my webmail account to provably “forget” my password. The ESORICS paper you mentioned shows how to an embedded device (e.g., a sensor) can provably forget all of its prior state (e.g., old code). However, it seems very hard to extend this approach to a general-purpose computing device.

Professor Katos: With the proliferation of cyberattacks on information systems and increased concerns on infrastructure and user
protection, could we argue that we are heading towards a state of “security at any price”?

Professor Tsudik: First off, I have no clue where we are headed. Internet infrastructure security is clearly a hot-button issue, however, it is not a new one. I don’t believe in fairy tales promising malware-free future and guaranteed infrastructure protection. I do believe in measured progress. Historically, Internet security has not made great big strides. Instead, progress has been made in baby steps: security improved gradually in lock step with new malware and attacks. I expect this piece-meal reactive process to continue.

ENDNOTE

1 Cryptonecrophilia (noun): an act of repeatedly finding “holes” or “bugs” in a long-dead (broken) cryptosystem, scheme or protocol (http://www.ics.uci.edu/~gts/words.html)