 An Interview with Walter Fumy, Chairman of ISO/IEC JTC 1/SC 27, IT Security Techniques

Walter Fumy discusses the importance of IT security standards in today's world and the role that SC 27 plays in this field.

Q: Why are international standards important in the area of cybersecurity and how would you describe SC 27's role?

Well, why is any standardization important? Of course, I like to think that security is a very special topic – data security has always been an issue for governments, the military, and the financial sector. In the last 25 years, with the migration of much human activity from the physical world – from person-to-person contact – into the electronic world and cyberspace, we have increasingly needed to deal with the impact on security and privacy. IT brings a new level of challenges, which are of concern to individuals and enterprises, as well as to administrations.

So, why are standards important for cybersecurity? Like with any standard, by sharing best practices and by specifying state of the art techniques and mechanisms, they can assist improving the quality of processes and also the quality of solutions – cybersecurity standards can help businesses, administrations, and individuals. What is special is that security is a horizontal area in that it applies to basically everything and should be considered basically everywhere. For this reason the customer base of SC 27 are not only the aforementioned businesses, administrations, or individuals, but also other standards committees that apply our work in their respective work area.

We at SC 27 see ourselves as an internationally recognized center of information and IT security standards expertise. Our work covers the development of standards for the protection of information and communications technology (ICT) and includes generic methods, techniques, and guidelines, to address both security and privacy aspects. These methods, techniques, and guidelines fall into five important areas that our five working groups are structured after. The first area is information security management systems (ISMS), including requirements, controls, conformance assessments, accreditation, and auditing requirements in the area in information security. We have a working group on cryptographic mechanisms, one on security evaluation criteria and methodology, one on security services, and the final one is on security aspects of identity management, biometrics, and privacy.

From our point of view, SC 27 more-or-less sits in the center of many security activities and we like to think that we are quite successful in what we do. We currently have 135 publications by SC 27, 52 P members and 18 O members, which add up to 70 national bodies from all over the world participating.

When we were founded in 1990, we started with only 18 P members. Today, we cover almost the whole globe, and our membership is still growing year by year. In addition, we maintain a large number of liaisons to other standards developing bodies, internal and external to ISO. The participation of so many organizations in SC 27 distinguishes our subcommittee as an international center for standards-setting in the IT security realm, while also providing us with the responsibility of promoting a more secure IT world.

Q: There are many JTC 1 subcommittees and many organizations beyond JTC 1 interested in and affected by cybersecurity standards. How does SC 27 interact with relevant committees and organizations?

Absolutely true – many JTC 1 subcommittees and other organizations beyond JTC 1 are interested in or affected by cybersecurity. This is due to the horizontal nature of security, and also to the increasing awareness over the years. We have many strong liaisons both within JTC 1 and beyond JTC 1. In total we have almost 70 liaisons, which is of course a huge challenge, to maintain so many liaisons. Those other committees typically apply or profile our work in their respective areas. In many instances we learn about specific requirements those committees might have and give it a greater focus – for example, regarding various security aspects.

Sometimes, it's the case that SC 27 does the profiling; two examples of this are ISO/IEC 27015 *Information technology – Security techniques – Information security management guidelines for financial services*, which is a profile of ISO/IEC 27002 *Information technology – Security techniques – Code of practice for information security controls*, for the financial sector. ISO/IEC 27015 provides ISMS for the financial sector, which we did in liaison with TC 68 and other bodies interested in or active in this sector. A second example is ISO/IEC 27017 *Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002*, a code of practice that is also a profile or extension of the basic ISMS standard. This code of practice standard for information security controls for cloud computing services is currently under development, in the committee draft (CD) stage.

Sometimes we will also, one could say, develop standards on demand by other SDOs. An example of this is ISO/IEC 27018 *Information technology – Security techniques – Code of practice for PII protection in public cloud acting as PII processors*, which is currently at the draft International Standard (DIS) stage. I say on demand, but of course the normal processes of getting new work items adopted do apply. And in some cases, as a final example of cooperation, we do joint publications. The main instance here is working with ITU-T, where we have a number of co-published standards. But overall, if you look at the total number of liaisons, doing joint publications is more the exception than the rule.

There are also two other ways that liaisons contribute: via liaison statements, but also by active participation in our meetings. So they would send experts to our meetings to contribute, and in other cases we send experts to their meetings. It always depends where the focus on the work is: whether it's more focused on security itself or whether it's more focused on the area of application.

In general, the standards put out by SC 27 tend to be applicable to a wide range of areas within the IT security realm. Other organizations with an interest in security can then use these standards and apply them to their specific area of concern. In this way, SC 27 addresses both the demand arising from the horizontal nature of IT security, as well as some of the specific concerns voiced by liaison organizations or governments.

Q: There have been allegations that intentional weaknesses may have been inserted in some cryptographic standards. How does this affect SC 27?

Unfortunately, we have to assume that these claims are true, even though we don't have proof in the strong sense. Since last September, when these allegations were published first, experts within and outside SC 27, as well as journalists, had a closer look and found a number of indications that support these allegations.

What we know today is that one mechanism in one standard is affected. The standard is ISO/IEC 18031 *Information technology – Security techniques – Random bit generation*, which was published in 2011. The mechanism is the random number generator called Dual_EC_DRBG. The name indicates that it's based on elliptic curve (EC) technology, and DRBG stands for deterministic random bit generator. This random bit generator is ridiculously inefficient I would say – inefficient by a factor of about 1.000 compared to other mechanisms in the same standard, according to experts. Nevertheless, it has been widely implemented in cryptographic libraries, including the BSAFE library of the RSA company, a Microsoft library which is called SCHANNEL, and some versions of the OpenSSL implementation. BSAFE made this mechanism the default mechanism; so if nothing is changed, that's how the random numbers are generated.

Dual_EC_DRBG is not only an ISO standard, it's also a NIST standard (it came to SC 27 via NIST), and an ANSI standard. The mechanism is contained in NIST Special Publication 800-90, which was published in 2006, and also in ANSI X9.82. Triggered by the allegations and their own investigations, today NIST recommends that the mechanism should no longer be used. In our case, SC 27 first has issued a cautionary note on the use of this mechanism, and initiated a study period to carefully review the security issues for this mechanism. The study period finally resulted in a proposed Technical Corrigendum to ISO/IEC 18031:2011 with the effect to remove Dual_EC_DRBG from the standard.

How does this affect us? What we face is some damage to trust. Both trust in the process, and trust in the players. We have to ask ourselves why the publication of this mechanism was not stopped, since there had been early warnings in the crypto community about potential flaws in the mechanism when it was first published in the NIST document. And there's some lost trust in the players, and in the editors of this standard in particular. So that's certainly not a good thing. As we all know, trust is hard to build, but very easy to break. So reestablishment of trust is a challenge for us, and we aim at being very transparent and open about any findings we might have in this respect. I believe one of the main lessons we should learn from this is that we must always ensure there's a sufficient amount of independent cryptographic research involved when we publish crypto standards.

Q: What are the main challenges you see for SC 27 in the years ahead?

I'd like to group the upcoming challenges into two areas. The first is to handle size and growth and to *remain as productive and attractive* – a considerable challenge. Effective management and coordination are absolutely essential. In our situation we maintain internal coordination functions in the form of two special working groups: one on management aspects and one on cross-working group topics, i.e. topics that may affect more than one working group. Both of those SWGs were established last year. Also, we maintain our own internal management guidelines in a form of a standing document to help manage the growth and the size. More voting members also means more comments on ballots – we shouldn't underestimate this. For example, in the case of the recent revision of our most popular standard ISO/IEC 27001 *Information security management systems – Requirements*, and the accompanying ISO/IEC 27002 *Code of practice for information security controls*, the editors had to deal with several thousand comments – hard to imagine, isn't it? Hosting our meetings also becomes more and more of a challenge, but so far we have been lucky always finding generous hosts able to provide the infrastructure required for a SC 27 meeting.

The second area is that the topic itself is a challenge. Security is such a complex topic – and the demands change rapidly. Partly, this is due to developments in IT and IT systems; the cloud is an example. Today, we have the Internet of Things coming, and machine-to-machine communications, which is another IT development that affects security. Partly, this is also due to new forms of attack that are arising. I'd like to give you a small number of examples. For the Internet of Things challenge, we need to provide lightweight crypto – that is, cryptographic mechanisms which are designed for restricted platforms that only have very limited computing power, or memory, or energy available for performing their operations. Examples of such platforms are tags or sensors. The challenge is that the mechanisms need to be lightweight in that they don't need a lot of resources, but they'll need to be secure, at least to some degree. SC 27 has published an important milestone in that direction which is ISO/IEC 29192 *Information technology – Security techniques – Lightweight cryptography*. The second example is the cloud. There's a vision among cryptographers of homomorphic encryption schemes, schemes where the cloud service can operate on encrypted data without ever decrypting it, so nobody has to worry about trust of the cloud service. That, as I said, is more of a visionary dream at this point, preliminary schemes are being discussed, and SC 27 has established a study period going trying to identify first steps we could take in this direction.

And then, in cybersecurity we live in this race where we see new forms of attack that either already happened or that we envision coming. One example here is quantum computing. If quantum computers become a reality that's a whole new dimension of how to calculate, how to compute, and also how you could break cryptosystems as we know them, in particular, public-key systems. So if quantum computing becomes a reality, we really would have to replace many of the techniques which we consider secure today; that would be a huge challenge. And those are just a few of many examples of challenges SC 27 is facing or will be expected to face in the near future.

All these "challenges" are actually part of the fun – we still are attracting new members, crypto is an evolving adventure, even the criminals make sure we keep growing our knowledge.

Q: Please tell us about your background in cybersecurity; how did you become interested in standardization?

Oh, my interest goes back a long way. As a Ph.D student, I was working in the field of error correcting codes, which is mathematically and technically somewhat related to crypto. At that time, I attended one of the first ever open workshops on cryptography, organized by Tom Beth, in Germany, almost exactly 32 years ago: March 29 – April 2 in 1982. At this workshop, I got hooked on the topic partly because of the underlying mathematics, partly because security and data protection seemed a good thing – but mostly, I would say, because of the brilliant people that were active in that field and had joined the workshop. For example, I met Adi Shamir there, who is the "S" in the RSA scheme – coinventor of the RSA scheme. I also met Whit Diffie who is the coinventor of public-key cryptography in general. They're both just very remarkable people, and they and many others made a huge impression on the young Ph.D. student. That was my initiation into the field, and since then I've never really left it. That makes for 32 years of experience in security and crypto.

A few years later, in 1986, I started to work with Siemens doing research and development in the area of data security in the manufacturing sector. They had a plant nearby the university where I graduated, and in particular they worked in the car industry, in automation. In the early days for this sector, we designed, among other things, network encryption devices and smartcard based solutions for access and copy protection. We wanted to base those solutions as much as possible on international standards. This intention at the time was new to me, as a scientist fresh from university, but it was absolutely normal for the company.

That's why in September 1987 I attended my first international standards meeting, which was SC 20 *Data security techniques*. I stayed with SC 20, which was disbanded a few years later due to the crypto debate and was in a way replaced by SC 27. In SC 27 then, I became an editor of several crypto standards, later the head of the German delegation, and in 1996 I was elected chair, which is my current position. I love the job; I love working in an intercultural environment, and it's a good feeling to do something so useful.