CLOCKWISE

by John Laskey & M. E. Kabay, PhD, CISSP-ISSMP

Another welcome contribution from collaborator John Laskey. This is entirely John's work with minor editorial changes by Mich.

* * *

Have you ever come across a profession that is the opposite of every element taught in information management and security?

I just did. For family reasons, I attended a conference of clock- and watchmakers. Themes included precision and accuracy and the attendees were all serious-minded professionals. Having much the same profile, in fact, as security professionals.

How, then, could this gathering be the antithesis of our profession? I'll highlight the differences, because sometimes it's just fun to compare outlooks from professionals whom you could expect to have much in common.

Complexity

This is a no-no from an information planning and security perspective. Remember Bruce Schneier's aphorism, "…[C]omplexity is the worst enemy of security"< http://www.schneier.com/crypto-gram-0003.html >? Our clock-makers, however, see complexity as absolutely a merit – I was startled early on in the conference by a PowerPoint slide that assessed the complexity of a prototype clock as one of five driving factors behind its design! Not only did this clock feature moving parts fashioned as little animals: the creatures were designed to move in ways that actually increased accuracy, while some of the cogs and wheels were designed so they would move in ways that would draw in the viewer's attention. So instead of concentrating on the end 'product' (i.e., telling the time) the observer is invited to appreciate and enjoy the spectacle of how the 'product' came about.

Openness

There is much debate about openness in security: from reporting vulnerabilities to the secrecy around some security architectures, particularly government ones. All of this is based on an argument that obscurity makes the job of potential attackers more difficult, despite the insistence of educators on Kerkhoffs' Principle< http://www.mekabay.com/nwss/833_lesson_in_a_haystack--kerckhoffs_principle.pdf >. By refreshing contrast, our clockmakers have a completely different perspective of the workings of their new designs. For one particularly complex clock, the presenter gave his audience a complete visual breakdown of how all of the working parts were made and how they would work together. This rather bracing outlook (from the perspective of a security professional and, perhaps, a patent lawyer) probably owed much to the fact that this clock was conceived in 1993, and was not due for completion until 2015. The design and the work put into the project were so complex and time-consuming that plagiarism was unlikely to be a problem. Incidentally I did not see or hear the word 'patent' at any point during the conference.

Retrofitting and Add-Ons

One feature of an IT architect's art is to reduce as far as possible the need for retrofitting, for instance by helping to identify and manage obsolescence in a new IT system and integrating security considerations from the start of the design. But the maker of the complex clock had thought up some pretty fundamental new ideas for its appearance since its original concept, and was adapting them into the design. A prototype of the clock looked a lot different than its drawing board concept, and the audience was invited to applaud the development of the clockmaker's ideas – even though they continued well beyond the implementation stage.

Turnaround Times

A major challenge for security developers is to keep in step with the system designers and the delivery timescales set by the system's owners and beneficiaries. As I have said, out clockmaker thought nothing of working on a design so complex that it would take 23 years from design to full implementation. And, he added, no computer-assisted measures had been used in the design: everything was done by hand, including the long calculations needed to ensure all the moving parts worked.

Obsolescence

IT designers, and security experts are often challenged by the question of obsolescence; a component might cease to be manufactured, or it might be too difficult to service, or be superseded by a better, cheaper, more secure method/component. Our clockmakers however think nothing of designing new, complex mechanical solutions to problems that you might consider already long solved. Some of us may, for instance, wonder why they seek new solutions in gears and wheels at all when there are plenty of electronic answers that are more precise and less prone to wear.

The answer is aesthetics. There are still many who appreciate mechanical timepieces (for some people, it is still a signature of success to show off a mechanical watch, if not necessarily a timepiece that takes 23 years to deliver). But I wonder: might a clock-maker be very good at systems design and security? Or might a professional security person be able to design and deliver a mechanical timepiece?

* * *

John G. Laskey< http://www.linkedin.com/pub/john-laskey/28/b28/b69 > is a US-based security consultant who has worked for the UK government equivalents of DHS and FEMA. As IT Security Officer for the Home Office he was responsible for the security risk management of a number of high profile systems developed to increase government and public security. Recently, John helped launch the CESG Certified Professional scheme for IA consultants seeking UK government contracts. John has advised senior UK government managers on the health of major projects and programs and he is a certified lead auditor for the ISO 27001 security standard. He is a member of BCS – the Chartered Institute for IT – and of the Institute of Information Security Professionals (IISP).

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *