

Position Paper for the “*Towards a Roadmap for Future Research*” Workshop

Foundations / Design and Analysis tracks

Can we still avoid Protocol Security *meltdown?*

Brian Monahan

Trusted Systems Lab, HP Labs, Bristol, UK

What is the Internet made from?

It is a tangled web of communications across many different networks, all of which share a common set of protocols based around TCP/IP. One might quite honestly say that the Internet is built out of communications protocols. Such protocols are an essential part of the information infrastructure that makes the Internet and E-commerce happen and are fundamental to their success.

The initial requirement for ARPANET (the precursor to the Internet) was to provide a robust operating network that could function even in the face of severe routing breakdowns. End-to-end user security was de-emphasised there – getting something that worked robustly was considered sufficient achievement in itself.

However, once the Internet was opened for general commercial use, it quickly became a victim of its own success. The communications protocols it uses were designed at a time when security was not a priority. Any security that is provided was not intrinsic to the original design, but has been added afterwards by further protocols.

Before criticising the early Internet pioneers for ignoring security issues, it should perhaps be recognised that users of these original networks were linked to officially supported participating organisations, such as Universities and the military. Thus, most users were generally known to some responsible entity or organisation – they tended to behave themselves. There were no script-kiddies and little risk of malicious insider hacking. It is only with the arrival of the broader, more open and commercial Internet that these threats have emerged in any numbers.

In parallel with the rapid expansion in the number of general Internet users, the uses that this connectivity is put to have also broadened. With applications including online financial services, E-government and general E-commerce and trade having a potentially worldwide user base, distributed transactions need more than ever to be efficient, robust and secure. Accordingly, there is an ever-increasing need to develop new protocols or to adapt old ones.

The academic protocols and crypto communities have understandably been somewhat wary of making changes to systems that have notionally served well in the past. However, this academic reticence will not prevent the entrepreneurial and adventurous developer from taking existing standards and shoehorning them to fit their bright new, shiny applications. They will do it anyway without concern for the academic niceties of debate (c.f. WAP, 802.11).

De facto standards are established when corporations and other large user communities have adopted them as routine operational practice. This can happen in spite of there being serious concerns from some parts of the community. Unfortunately, if such concerns do turn out to be well founded, then

this often leads to a collapse in confidence and trust in those standards and so then to a potentially substantial loss of investment.

We suggest that there may be an emerging crisis in protocol design mirroring the so-called Software Crisis of the 1970's and 80's. Protocol design is taken by software engineers to be a complex, high-risk activity, which only a handful of well-known people appear qualified to practice. Admittedly, although the scientific rigour of such practice is undoubtedly high, this will equally not meet the increasing demands placed upon engineers to implement highly distributed applications. The problems here often come down to unclear or even unstated security requirements.

Given this, the main risk from poor protocols may not come from "brand new" protocols as such, but from radical misuse of existing protocols, with subtle variations and modifications that were not envisaged by their original creators.

There is an obvious need today for improved protocols that are better simply because their security properties and requirements can be more widely appreciated and understood. But far more than this, we need to urgently bring forward ideas, concepts and tools that can help engineers to develop skills for analysing and understanding protocols, making the design process more assured, more routine and less demanding upon the availability of certain well-known individuals.

There is some hope (see References) that the emerging discipline of Protocol Security Engineering can yet help to avoid Protocol Security meltdown – but only time will tell.

References

[A01] R. Anderson, *Security Engineering*, Wiley, 2001

[AL00] R. Amadio and D. Lugiez, On the reachability problem in cryptographic protocols, in *CONCUR* (2000), vol. 1877 of LNCS, Springer-Verlag, 380-394.

[CS02] H. Comon and V. Shmatikov, Is it possible to decide whether a cryptographic protocol is secure or not?, To appear in *Journal of Telecommunications and Information Technology*, 2002.

[CDMLS] I. Cervesato, N. Durgin, J. Mitchell, P. Lincoln, A. Scedrov, Relating Strands and Multiset Rewriting for Security Protocol Analysis, In *Proc. 15th IEEE Computer Security Foundations Workshop* (2000), 35-51.

[DLMS] N. A. Durgin, P. D. Lincoln, J. C. Mitchell, and A. Scedrov, Undecidability of bounded security protocols, In *Proc. FLOC Workshop on Formal Methods in Security Protocols*, Trento, Italy, 1999.

[FA01] M. Fiore, and M. Abadi, Computing symbolic models for verifying cryptographic models, in *14th IEEE Computer Security Foundations Workshop* (2001), pp. 160-173.

[L96] G. Lowe, Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR, In *TACAS* (1996), vol. 1055, LNCS, Springer-Verlag, 147-166.

[P98] L. Paulson, The inductive approach to verifying cryptographic protocols, *Journal of Computer Security*, 6, 1(1998), 85-128.

[RT01] M. Rusinowitch, and M. Turuani, Protocol Insecurity with Finite Number of Sessions is NP-complete, In *Proc. 14th IEEE Computer Security Foundations Workshop* (2001), 174-187.

[S99] D. Song, Athena: a new efficient automatic checker for security protocol analysis, In *12th IEEE Computer Security Foundations Workshop* (1999), 192-202.

[SRI] J. Millen and V. Shmatikov, Constraint solving for bounded process cryptographic protocol analysis, in *Proc. 8th ACM Conference on Computer and Communications Security*, ACM, 2001.

[TFHG99] F. J. Thayer Fábrega, J. C. Herzog, J. D. Guttman, Strand Spaces: Proving Security Protocols Correct, in *Journal of Computer Security*, 7:191-230, 1999.