File 20110822.1300: Notes from a phone call from Michael I. Schwartz, who called me today about the MG-03529 disclosure. He noted that 303-932-4720 doesn't work; it goes to someone else now.

Mr Schwartz is in LM Denver. He is reviewing the disclosure for Dr. Chiang. He noted that Adobe introduced nested digital signatures in version 9; we need to check whether the method Adobe uses is similar or different, superior or inferior to the method I described. Mr Schwartz asked many questions about why I did things the way I did, e.g., why exactly three slots for signatures? In the U.S. the law is first to invent, not first to file, so it is still worth persuing even if Adobe has been able to do multiple digital signatures on a file since 2005 or so.

I think Mr Schwartz is in IS&GS Security. He worked on Radiant Trust before he had to go on medical leave shortly before I started on that project.

He mentioned Dr Albert Levi, a researcher in Turkey, who has published extensively on nested certificates [1, 4, 2, 5, 3]. I looked briefly at those papers and Dr Levi's PhD thesis, and it seems to me they are concerned primarily with the problem of nesting CA certificates in case the primary CA is unreachable due to intermittent network connectivity.

Mr Schwartz is going to look at it in more detail this week. I don't really have time. We are looking for something 'different' in the method I described, preferably done better than what Adobe claims for their secure workflow solution, but if I anticipated Adobe's method, that could be very interesting in the USPTO.

I argue that any method that skips over troublesome portions of the source file (NITF, in the original embodiment), is less secure than mine, which was designed to be foolproof. The purpose to which the present method was put was nonrepudiation.

We talked about other applications in NGA and DCGS; I mentioned HIPAA.

Mr Schwartz also pointed out Steven Savage's work on tracing the spam value chain in `;login` and USENIX. We have similar experiences with patents; it sounds like he holds three; I asked if I could interview him with respect to RTG 1.0 later on, after I get past confirmation of status in a few weeks.

References

[1] Albert Levi and M. Ufuk Çağlayan. A multiple signature based certificate verification scheme. In *Proceedings of the Third Symposium on Computer Networks (BAS'98)*, pages 1–10, Izmir, Turkey, 25–26 June 1998.

[2] Albert Levi and M. Ufuk Çağlayan. NPKI: Nested certificate based public key infrastructure. In *Advances in Computer and Information Sciences '98—Proceedings of the Thirteenth International Symposium on Computer and Information Sciences (ISCIS XIII)*, pages 397–404, Turkey, October 1998. Concurrent Systems Engineering Series, IOS Press. Vol. 53.

[3] Albert Levi and M. Ufuk Çağlayan. Analytical performance evaluation of nested certificates. *Performance Evaluation*, 36–37:213–232, August 1999.

[4] Albert Levi and M. Ufuk Çağlayan. Integrity control in nested certificates. In *Proceedings of the Fourth Symposium on Computer Networks (BAS'99)*, pages 149–157, Istanbul, Turkey, 20–21 May 1999.

[5] Albert Levy. *DESIGN AND PERFORMANCE EVALUATION OF THE NESTED CERTIFICATION SCHEME AND ITS APPLICATIONS IN PUBLIC KEY INFRASTRUCTURES.* PhD thesis, Boğaziçi University, 1999.