

Preface

Another year, another workshop. Here are the proceedings of the seventh Cambridge International Workshop on Security Protocols. All very well, you may think, but can there really still be anything genuinely new to say? Is it not just the same old things a tiny bit better?

Well, perhaps surprisingly, this year we discovered some radically new things beginning to happen. The reasons in retrospect are not far to seek: advances in technology, changes in the system context, and new types of consumer devices and applications have combined to expose new security requirements. This has led not only to new protocols and models, but also to known protocols being deployed in delicate new ways, with previous fragilities of watermarking and mutual authentication, for example, becoming desirable features. At the workshop we identified several of these developments and began to map out some lines of enquiry.

This volume brings you a selection of deliberately disputatious position papers, followed by not-quite-verbatim transcripts of the discussions which they provoked. As always, our purpose in making these proceedings available to you is the hope that they will move your thinking in an unexpected direction. If you find your attention caught by something here, if it makes you pause to reflect, or to think “why, that is just *so* wrong”, then good. We’re waiting for your mail.

Thanks to Stewart Lee and the University of Cambridge Centre for Communications Systems Research, for acting as hosts for the workshop, and to Roger Needham and Microsoft Research Limited (Cambridge), for providing us with the use of their meeting room and coffee machine.

Thanks also to Dorian Addison of CCSR and to Angela Leeke and Margaret Nicell of MSRL for keeping us organized, and our especial gratitude to Lori Klimaszweska of the University of Cambridge Computing Service for her Promethean transcription of the audio tapes, which this year featured “echo kickback as well as the usual distorted sound”.

Finally, each of us takes full responsibility for the accuracy and completeness of the material contained in these proceedings. Errors and omissions, on the other hand, are the responsibility of the other three fellows.

February 2000

Michael Roe
Bruce Christianson
Bruno Crispo
James Malcolm

Introductory Remarks

Michael Roe: We always try and have a theme and then people submit papers. The usual thing that happens when you're running a conference is that people resolutely submit a paper on the research they're doing that year, regardless of whether it's got anything to do with the theme or not.

What I thought was going to be the theme — because I'd been deeply buried in it for the previous year — was entertainment industry protocols. We're seeing a great shift in the use of the Internet from the kind of educational, military, and industrial use of networking towards home users buying entertainment, and this causes you to completely redesign protocols. I've been particularly looking at copy protection and digital watermarking, and when you look at those kinds of protocols you discover they're just not like the usual authentication and crypto key exchange we've been trying to do for the last fifteen years. They're fundamentally different, even the kind of asymmetric properties you want in a digital watermark — that anybody can verify it and see that this is copyrighted data and nobody knows how to change it — you think, oh that looks like public key cryptography, but then you discover, no it's not public key cryptography, it's something that's similarly asymmetric but it's different.

And so I thought a theme for the workshop could be how these completely new application areas cause us to come up with protocols that are completely different from what we previously discussed. But from people's submissions this didn't look to be what everybody else was doing.

The second theme that Bruce suggested was auditability of protocols: What do we need in a protocol in order to audit it? What does it mean to have audit support in a protocol? Bruce, it was your idea . . .

Bruce Christianson: Well when something goes wrong, sometimes the question is, what actually happened? And then you work out what state you ought to be in. But I think we know that in the protocol world there's often not a fact of the matter about what actually happened. So we need instead to have some way of agreeing a story we're all going to stick to, about what we're prepared to say happened. Some kind of integrity property for restoring the state. It seems to me that several different pieces of work have each got one corner of that particular problem, and it might be interesting to discuss some of the relationships between those approaches that aren't usually discussed.

Michael Roe: So it's going to be a mixed bag this workshop. A general overall theme still might be the changing environment and the changing application areas, it's just things have changed so much and become so diverse that they exceed my ability to predict what the papers are going to be about.

Une Mise en Thème

an exchange of e-mail

stardate February 1999

From: B.Christianson@herts.ac.uk Fri 3 February 1999 14:45
To: E.S.Lee@ccsr.cam.ac.uk, m.roe@ccsr.cam.ac.uk
Subject: protocols workshop

there is some discontent with the present 'theme':

> one of the strengths of the earlier workshops was that they didn't
> concentrate upon a particular application area and so encouraged
> people with different interests to come together.

how do we feel about 'making protocols auditable' as an alternative?

this theme includes the issues of how a protocol may be audited against more than one policy, what audit records are required and how they are to be kept, the nature of the criteria for success etc.

bruce

===

From: Prof E Stewart Lee <E.S.Lee@ccsr.cam.ac.uk> Fri Feb 5 1999 15:08
To: B.Christianson@herts.ac.uk, m.roe@ccsr.cam.ac.uk
Subject: Security Protocols Workshop

> this theme includes the issues of how a protocol may be audited against
> more than one policy

This is unwise. Generally, a protocol can enforce more than one policy iff one the policies is a subset of the other. This is a well-known result of composition theory. Policies are even more difficult to compose than objects. Two policies that do not satisfy the subset criterion can sometimes be enforced iff there is a requirement that one be enforced before the other -- e.g.: Mandatory Access Control before Discretionary Access Control. For another example, Bell LaPadula is a policy. So is Non-interference. Their composition is extremely difficult (because NI doesn't have DAC, amongst other more technical reasons).

Stew

===

From B.Christianson@herts.ac.uk Fri Feb 5 1999 15:06
To: E.S.Lee@ccsr.cam.ac.uk, Michael.Roe@ccsr.cam.ac.uk
Subject: security protocols workshop

i think you are the first to submit a position paper, stew ;-}.

i'm not welded to those particular issues, but the better to inflame
debate:

policy A: (laundry) no payment implies no laundry
policy B: (customer) no laundry implies no payment

neither policy entails the other.

bruce

===

From Michael.Roe@ccsr.cam.ac.uk Fri Feb 5 1999 15:23
To: Prof E Stewart Lee <E.S.Lee@ccsr.cam.ac.uk>
Subject: Re: Security Protocols Workshop

Hmmm ... we're starting to jump into the discussion that should be held
at the workshop here.

It is a fact of life that many protocols involve communication between
parties who have conflicting interests. Each party, if given sole
authority to set policy, would define a policy which conflicts with that
of the other party. Reconciling these conflicts *is* an important issue in
protocol design, even though we know that there is no *mathematical* tool
which will cause real conflicts of interest to magically vanish.

I vote we keep Bruce's original sentence.

Mike