Alex Iliev <alexander.h.iliev@dartmouth.edu> on 04/18/2005 11:06:10 PM

To: submissions@nspw.org
cc: "Alexander H. Iliev" <sasho@cs.dartmouth.edu>, Sean Smith <sws@cs.dartmouth.edu>
Subject: NSPW 2005 submission

Title: Tiny Trusted Third Parties

Authors: Alexander Iliev and Sean Smith; {sasho,sws}@cs.dartmouth.edu

Category: research paper

Attendance statement: We would both like to attend if accepted.

Attached: paper pdf and cover/justification letter

Thanks very much!

Title: Tiny Trusted Third Parties
Category: research paper

There has been much work, mostly from the theory of cryptography community, on
Secure Multiparty Computation (SMC). They define the security of a multiparty
protocol by its similarity to a protocol where a universally trusted third party
(TTP) performs the computation and distributes the outputs to the players.
However, they then proceed under the assumption that such trusted parties do not
exist, and need to be simulated by a protocol involving only the players. This
is in essence the thinking which we wish to challenge.

Advances in secure hardware technologies in the last decade have produced
devices which are designed to be trustworthy, even for relying parties at remote
locations, and against an adversary with physical access. Both physical security
and software protocols are used to provide assurance to the relying party

that
the device is a real one and is running a known program.

Having a trusted space at remote locations enables applications which would otherwise be inefficient, or require the development of a new specialized protocol for every problem. We have already investigated the feasibility of hardware-assisted Private Information Retrieval, and will be turning to the more
general problem of two-party secure computation, especially of algorithms which
have a large overhead in the standard oblivious circuit evaluation solution.

Perhaps inevitably, trusted devices with a sufficiently high level of physical
security tend to have limited computational power and memory size. So, effectively using such hardware of a TTP is not just a matter of moving the computation into such a device. Instead, we must carefully consider how to arrange these devices into networks connected by encrypted channels, in order to
ensure that the adversary observing the interaction of the devices still cannot
learn (or modify, without detection) the internal details.

The new paradigms we are proposing include a new approach to constructing TTPs,
taking advantage of the fact that they spend a lot of time engaged in a small set of operations; the idea that such TTPs should be considered as useful tools
in constructing practical multiparty protocols, especially over large data sets;
and the suggestion that more theoretical attention should be given to what can
be computed securely with such "oblivious" networks or circuits of tiny TTPs.

- iliev-smith.pdf