From:	Kelsey, John M. (Fed)
To:	Apon, Daniel C. (Fed); Vassilev, Apostol T. (Fed)
Cc:	Celi, Christopher T. (Fed); Moody, Dustin (Fed); Scholl, Matthew A. (Fed); Bassham, Lawrence E. (Fed); Sonmez Turan, Meltem (Fed); Davidson, Michael S. (Fed); Chen, Lily (Fed); Mouha, Nicky W. (Assoc); Waller, Noah D. (Fed); Cooper, David (Fed); Chang, Donghoon (IntlAssoc); McKay, Kerry A. (Fed); Barker, Elaine B. (Fed); Miller, Carl A. (Fed); Kang, Jinkeon (IntlAssoc); Perlner, Ray A. (Fed); Lichtinger, Jacob T. (Fed)
Subject:	Re: SCA Discussion (longer-form follow-up)
Date:	Tuesday, August 17, 2021 7:08:14 PM

My sense (I am definitely not an expert) is that:

a. It makes sense to split these between timing and other (power/EM) side-channels, since the timing side-channels have security implications for a much wider range of applications.
b. We can actually test constant-time implementations and be pretty sure we've closed any timing side-channels.
c. Resistance to power/EM side-channels is probably not ever absolute, but instead is based on the number of operations the attacker can observe, the sensitivity of his equipment, the specific techniques he's using, etc. Whatever test we use for this is going to give us only limited assurance. Also, this seems to be very dependent on specific technology.
d. We care a lot about whether or not an algorithm is inherently hard/easy to secure against timing and power/EM side-channels, but we probably don't need to care as much about the details of every power/EM side channel attack on an implementation.

--John

From: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
Date: Monday, August 16, 2021 at 16:08
To: "Vassilev, Apostol T. (Fed)" <apostol.vassilev@nist.gov>
Cc: "Celi, Christopher T. (Fed)" <christopher.celi@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>, "Bassham, Lawrence E. (Fed)" <lawrence.bassham@nist.gov>, "Sonmez Turan, Meltem (Fed)" <meltem.turan@nist.gov>, "Davidson, Michael S. (Fed)" <michael.davidson@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Mouha, Nicky W. (Assoc)" <nicky.mouha@nist.gov>, "Waller, Noah D. (Fed)" <noah.waller@nist.gov>, "Cooper, David A. (Fed)" <david.cooper@nist.gov>, "Chang, Donghoon (IntlAssoc)" <donghoon.chang@nist.gov>, "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>, "Barker, Elaine B. (Fed)" <elaine.barker@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Kang, Jinkeon (IntlAssoc)" <jinkeon.kang@nist.gov>, "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, "Perlner, Ray A. (Fed)" <ray.perlner@nist.gov>, "Lichtinger, Jacob T. (Fed)" <jacob.lichtinger@nist.gov>
Subject: SCA Discussion (longer-form follow-up)

Hello all,

Thank you for coming to the meeting this morning and sharing your thoughts on side-channel attacks and analyses! =)

I wanted to recap a couple take-aways I had myself (but *definitely* not a comprehensive list -- a ton was raised in the meeting that I won't repeat here, but others may want to!).
Please feel free to share your ongoing thoughts, or raise points that I'm not including in this first email.

1. The area of side channel attacks and analyses seems to be a very broad area, with room for work from multiple people in multiple projects and from multiple backgrounds. We have had some historical effort in this area around a decade ago, but the field is very broad now (much broader than our current work in the area).

   Simultaneously, we need to consider whether validation/certification is realistic, given the many constraints; e.g. budget costs or talent acquisition at testing labs.
   Note that the EU-based Common Criteria effort has some successes in this space, and seems (to me) to be beyond what we are doing at the moment.

2. Historically, the existence of side-channel attacks against standardized cryptographic algorithms has been very surprising to many people. A key, early example is the cache-timing attack against AES, but a multitude of SCA flavors persist today: invasive vs non-invasive, including (among the non-invasive category) timing attacks, SPA/DPA power analysis, EM analysis, cold-boot attacks, and issues about device-specific "combinatorial explosions" (do you need to be secure for every device, every model, every program compiler, every architecture, etc?).

3. The Threshold Crypto project has a focus on this area specifically through their "Masked Circuit" track, but it may not solve the problem so ideally as hoped for. In particular, the regime of AI-based power analysis attacks, it seems that the historical notion of Threshold Implementations (TI) doesn't resolve the concern like one would like.

   Along these lines, I wanted to point out a couple things:

   a. A talk at DEF CON 27 (2018) by Google's Security&Privacy Research Lead: https://www.youtube.com/watch?v=Db8mj5KFz8E
   b. This talk was mostly replicated at the keynote talk at WAC 2021 (an associated workshop with CRYPTO 2021, going on this week), where I asked him "How do you defend against this, just in theory?" and he replied "Yikes, I don't know!" (Hopefully the Youtube video for that will come online soon)
   c. Intersecting this new avenue for SCA with the Post-Quantum Crypto project, the recent paper: https://eprint.iacr.org/2021/849.pdf

4. Hopefully in the next weeks/months, we will have a few external speakers to give tutorials on the modern state-of-the-art in side-channel attacks and analyses for the Crypto Reading Club (that Meltem is organizing). If all goes as planned, there should only be further, very interesting questions raised in this space for us to discuss.

Anyway, I'm sure I left off about a good 60%+ of the conversation in this email. Please bring up anything that you found interesting from the discussion, or any other issue that was on your mind that you didn't get to bring up.

Thanks everyone!
--Daniel