From:	Perlner, Ray (Fed)
To:	Romine, Charles H (Fed)
Cc:	Lennon, Elizabeth B. (Fed); Smith,Daniel C (daniel-c.smith@louisville.edu); Petzoldt, Albrecht R. (IntlAssoc)
Subject:	RE: ERB Reminder
Date:	Wednesday, August 30, 2017 5:20:00 PM
Attachments:	CryptSRP_final.pdf

We agree with the suggested change. Here's an updated version, which has also been uploaded to NIKE

Thanks,
Ray

From: Lennon, Elizabeth B. (Fed)
Sent: Monday, August 28, 2017 4:04 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Cc: Marron, Jeffrey A. (Fed) <jeffrey.marron@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>; Marth, Lisa D. (Fed) <lisa.marth@nist.gov>; Shields, Kaitie (Fed) <kaitlin.shields@nist.gov>
Subject: FW: ERB Reminder

Ray, see Chuck's comments below and please respond to him directly, ccing me.

Thanks. Liz

Elizabeth B. Lennon
Writer/Editor
NIST Information Technology Laboratory
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
301 975-2832 telephone
301 975-2378 fax

From: Romine, Charles H (Fed)
Sent: Monday, August 28, 2017 3:56 PM
To: St Pierre, James A. (Fed) <james.st.pierre@nist.gov>
Cc: Lennon, Elizabeth B. (Fed) <elizabeth.lennon@nist.gov>; Shields, Kaitie (Fed) <kaitlin.shields@nist.gov>; Marth, Lisa D. (Fed) <lisa.marth@nist.gov>
Subject: Re: ERB Reminder

Colleagues,

I like this paper a lot; however, I'm concerned about the following statement early in the paper:

"Our attack therefore shows that combining several multivariate schemes into one brings no extra

security into the system."

I don't think that's a supportable statement. Their attack shows that combining ***these particular*** multivariate schemes in ***this particular way*** brings no extra security into the system, right? Does their attack rule out any value in combining several multivariate schemes, or just this one? Perhaps a better phrasing would be

"Our attack shows that this attempt to combine several multivariate schemes into one brings no extra security into the system."

An even broader statement could read

"Our attack shows that seeking to provide extra security into a system by combining several multivariate schemes into one is fraught with challenges, and may not even be possible."

Even better, I like the clear statement at the end of the Conclusion of the paper:

"… our attack shows that the security of a weak multivariate scheme like Square is not automatically increased by combining it with another (secure) scheme."

Please check with the authors on whether they'd like to stand by their original wording, or would prefer to change it as above (or in some other way).

Thanks!

Chuck

--

Charles H. Romine, Director
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8900
Gaithersburg, MD 20899-8900
Phone: 301-975-2900, FAX: 301-975-2378
Email: cromine@nist.gov
www.itl.nist.gov

Executive Assistant:
Lisa Marth, 301-975-2900, lisa.marth@nist.gov

From: "St Pierre, James A. (Fed)" <james.st.pierre@nist.gov>
Date: Monday, 28August 2017 at 15:22
To: Charles Romine <charles.romine@nist.gov>
Cc: "Lennon, Elizabeth B. (Fed)" <elizabeth.lennon@nist.gov>, "Shields, Kaitie (Fed)"

<kaitlin.shields@nist.gov>, Lisa Marth <lisa.marth@nist.gov>
Subject: FW: ERB Reminder

Chuck,
I have reviewed this paper and have no comments.
Jim

James St. Pierre, Deputy Director
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8900
Gaithersburg, MD 20899-8900
email: jimstp@nist.gov
phone: (301)-975-4124

From: Lennon, Elizabeth B. (Fed)
Sent: Monday, August 28, 2017 11:40 AM
To: St Pierre, James A. (Fed) <james.st.pierre@nist.gov>
Subject: FW: ERB Reminder

Jim, here it is. Liz

Elizabeth B. Lennon
Writer/Editor
NIST Information Technology Laboratory
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
301 975-2832 telephone
301 975-2378 fax

From: St Pierre, James A. (Fed)
Sent: Monday, August 28, 2017 10:27 AM
To: Lennon, Elizabeth B. (Fed) <elizabeth.lennon@nist.gov>
Cc: Marth, Lisa D. (Fed) <lisa.marth@nist.gov>; Shields, Kaitie (Fed) <kaitlin.shields@nist.gov>
Subject: RE: ERB Reminder

Thanks – can you resend the Perlner paper? I can't find the email.

James St. Pierre, Deputy Director
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8900
Gaithersburg, MD 20899-8900
email: jimstp@nist.gov

phone: (301)-975-4124

From: Lennon, Elizabeth B. (Fed)
Sent: Monday, August 28, 2017 8:17 AM
To: St Pierre, James A. (Fed) <james.st.pierre@nist.gov>
Cc: Marth, Lisa D. (Fed) <lisa.marth@nist.gov>; Shields, Kaitie (Fed) <kaitlin.shields@nist.gov>
Subject: ERB Reminder

Jim, these papers are awaiting your review:

G2017-1631, Ray Perlner, Total Break of the SRP Encryption Scheme
G2017-1572, Pat O'Reilly, CSD Annual Report
G2017-1494, Keith Stouffer, Cybersecurity Framework Manufacturing Profile

Thanks. Liz

Elizabeth B. Lennon
Writer/Editor
NIST Information Technology Laboratory
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
301 975-2832 telephone
301 975-2378 fax