

Marc Vauclair

From: Mike Ahmadi [mike.ahmadi@granitekey.com]
Sent: Thursday, July 07, 2011 17:40
To: Marc Vauclair
Subject: Fwd: UCA Embedded Systems Security - Device Identity Sub Group Meetings
Attachments: BAS Security.pdf; ATT00001..htm

Forwarding for consolidation

Begin forwarded message:

From: "Rosenthal, Bruce S." <BRUCE.S.ROSENTHAL@saic.com>
Date: May 30, 2011 10:34:32 AM PDT
To: Mike Ahmadi <mike.ahmadi@granitekey.com>, "OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG" <OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG>
Subject: RE: UCA Embedded Systems Security - Device Identity Sub Group Meetings

Here is that whitepaper I spoke about earlier in the call. The authors propose some security related extensions to building automation and control protocols that are widely used throughout the EU (BACNet, LONWorks, KNX/EIB). They develop their approach around symmetric encryption (AES) with key management schemes implemented apparently using the existing hierarchical architecture of the KNX/EIB protocol and application framework.

Don't know if there is anything we can use or build on in this proposed approach, but here it is.

Bruce Rosenthal: Principal Consultant
Critical Infrastructure Security & Protection Practice Lead

SAIC Energy, Environment & Infrastructure, LLC (SEE&I)

Real-time Systems and Communications Division

+011 505.507.5830: primary mobile
e-mail: bruce.s.rosenthal@saic.com

Energy | Environment | National Security | Critical Infrastructure | Health

When you come to a fork in the road - take it

From: OpenSG SG Security WG Embedded Systems Security Task Force [<mailto:OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG>] **On Behalf Of** Mike Ahmadi
Sent: Monday, May 30, 2011 9:25 AM
To: OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG
Subject: Re: UCA Embedded Systems Security - Device Identity Sub Group Meetings
Importance: High

Marc,

I made some comments and edits (tracking enabled) to your document. It is attached.

Mike Ahmadi