Marc Vauclair

From: Gorog, Chris (US - Denver) [cgorog@deloitte.com]
Sent: Thursday, July 07, 2011 17:50
To: Marc Vauclair; 'OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG'; Thierry Gouraud; Wim Nuyts; Sami Nassar
Cc: 'Gene Frost'; 'Khera, Rohit'; 'Tom Thomassen'; 'ngreenfield@aep.com'; 'Johannes Lintzen'; 'Steven A Dougherty'; 'James Blaisdell'; 'Hotha, Surya'; 'Sadu Bajekal'; 'David Sequino'; 'jleigh@us.ibm.com'; 'Gallo, Gio'; 'Scott Humphries'; 'Humphrey, Robert B Jr'; 'Mike Ahmadi'; 'Izzo, Bill'; 'Jurijus.Cizas@infineon.com'; 'Thomas Hardjono'; 'mjcooper@us.ibm.com'; 'mark.stafford@infineon.com'; 'Rosenthal, Bruce S.'; 'Bobby Brown'; 'Sorebo, Gilbert N.'; 'Duren, Mike'; 'Freund, Mark C'; 'Dunn, Chris'; 'Chasko, Stephen'; Ward, Mark; Valenzuela David R
Subject: RE: UCA Embedded Systems Security - Device Security

I have used an older but good IEEE reference on the operation of cryptographic operations for hardware systems, called A Survey of Lightweight-Cryptography Implementations.

Google search “A Survey of Lightweight-Cryptography Implementations”

Christopher Gorog, PMP
Manager | Smart Grid Security Practice | Security & Privacy Services
Deloitte & Touche, LLP
Desk: +1 303 298 6580 | Mobile: +1 719 393 3470 or +1 303 229 9561
www.deloitte.com

From: Marc Vauclair [mailto:marc.vauclair@nxp.com]
Sent: Thursday, July 07, 2011 8:32 AM
To: 'OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG'; Thierry Gouraud; Wim Nuyts; Sami Nassar
Cc: 'Gene Frost'; 'Khera, Rohit'; 'Tom Thomassen'; 'ngreenfield@aep.com'; 'Johannes Lintzen'; 'Steven A Dougherty'; 'James Blaisdell'; 'Hotha, Surya'; 'Sadu Bajekal'; 'David Sequino'; 'jleigh@us.ibm.com'; 'Gallo, Gio'; 'Scott Humphries'; 'Humphrey, Robert B Jr'; 'Mike Ahmadi'; 'Izzo, Bill'; 'Jurijus.Cizas@infineon.com'; Gorog, Chris (US - Denver); 'Thomas Hardjono'; 'mjcooper@us.ibm.com'; 'mark.stafford@infineon.com'; 'Rosenthal, Bruce S.'; 'Bobby Brown'; 'Sorebo, Gilbert N.'; 'Duren, Mike'; 'Freund, Mark C'; 'Dunn, Chris'; 'Chasko, Stephen'; Ward, Mark; Valenzuela David R
Subject: UCA Embedded Systems Security - Device Security

Dear all,

- welcome
- collection of names of participants to the call: through a small mail saying “hello I was in the call” with business card information
- agreement on list of topics to be addressed (as listed in minutes of last “Device Management” call):
    - device identity
    - device authentication
    - authorization
    - random number generation
    - key management
    - hardware security
    - what is missing from the list?
        - cryptographic hardware: does it fall under hardware security?
        - ciphers
        - secure protocols
- call for collecting all previous documents/mails… exchanged in random, identity, key management, hardware security… => all to be sent to Marc Vauclair

- call for volunteers to take parts in charge
- way of working suggested:
    - based on all the collected inputs (drafts, mails…), I put all of them in a consolidated document, I circulate the document for comments before next call
    - in next call we discuss the comments
- check on whether it is possible to move next call to Monday July 18th, or Tuesday July 19th (17:00 CET; 8:00am Pacific Time, 11:00am New York).

Regards,
Marc

Marc Vauclair
BU Identification, Group leader a.i. Center of Competence Systems Security Leuven
Senior system architect and Technology Manager Security Applications, Senior Principal
NXP Semiconductors
Interleuvenlaan 80
3001 Leuven, Belgium

Tel. +32 16 390 602 Mobile + 32 475 36 16 82 Fax +32 16 390 855
Email Marc.Vauclair@nxp.com, www.nxp.com
PGP Fingerprint: FACC 4E8F E4A9 7AAA A9E8 F9CF 07B9 79A4 A66B EE0A
I'll sleep when I'm dead