Ensuring TANGO Control System

Sergi Blanch-Torné[1], Ramiro Moreno Chiral[2]

[1] Escola Politècnica Superior, Universitat de Lleida. Spain.
sblanch@alumnes.udl.es
[2] Departament de Matemàtica. Universitat de Lleida. Spain.
ramiro@matematica.udl.es

May 29, 2013
github.Papers: 2013-05-29 (revision 1fe20c3)

Abstract. [3] TODO: "*embedded cryptography*"
TODO: "*Ensuring* TANGO *must be like https. Transparent as possible from the current usage.*"

Keywords: Cryptography, Elliptic Curves, Distributed Systems, SCADA, Controls system, Synchrotron

1 Introduction

TODO: "*What is* TANGO *?*"

TODO: "*Distributed systems transparencies [1] that* TANGO *complains, and which are not*"

TODO: "*Go further that the Locking/Access control*"

TODO: "*Why to secure it? Trust in a peripheral firewalls is not enough.*"

TODO: "*Embedded in instrumentation, limited calculation capacity (it must behave indistinguishable if it's a huge server or an embedded board), limited bandwidth (Don't increase the current needs significantly): very good candidate for elliptic curves, generalized Rijndael and stream cipher.*"

TODO: "*The price of the information and the balance between the cost to ensure and the value of the ensured goods. Security levels: Open, confidential, Secret, Top Secret. (remember the German standard on this levelling).*"

2 Identifying scenarios

TODO: "*In terms of security threads, which is more representative from [2] for the current use case? Hospital, Bank, Military Base. Practical paranoia [3]*"

TODO: "*Key distribution protocols [2] sec.3.7.2*"

[3] Partially supported by grants MTM2010-21580-C02-01 (Spanish Ministerio de Ciencia e Innovación), 2009SGR-442 (Generalitat de Catalunya).

2.1 Access Control

TODO: "*Agent authentication in a distributed system*"
TODO: "*Ensuring communication between agents and between those agents with the user interfaces.* Command, read *and* write *operations;* Properties *modifications and changes application. This can be compared with* RFID *communication between card and readers, but adding communication in between the agents*"
TODO: "TANGO *database access control*"
TODO: "*Ensuring between instrumentation and the agents out of the scope of this paper*"
TODO: "*Trusted Computing and Hardware protections*"

2.2 Secret sharing

TODO: "*multicast, events and the other features that must be secured*"

2.3 Brainstorming attacks

Passive attacks TODO: "*Eavesdropping (Passive attacks) and Men-in-the-middle (active attacks) between agents.*"
TODO: "*Noise to block an alarm transmission*"

Active attacks TODO: "*Break the public face, web site or gui*"
TODO: "*Supplant agents.*"

2.4 Intrusion Detection

3 Zero-knowledge proof for authentication

TODO: "*The agents in the distributed system must be authenticated to be sure that they hasn't been supplanted*"

4 Protocols

TODO: "*protocol layers [4]*"

4.1 Communication hybrid schema

TODO: "*Pubkey to agreed a season key as the usual hybrid systems*"
TODO: "*Use the Symmetric key to seed a shared PseudoRandomGenerator as a key for a stream cipher of transmitted data and listened data between talkers*"
TODO: "PseudoRandomGenerator *(PRG), can be use the KeyDerivation of the Rijndael or better other possible alternatives*"

5 Conclusion

References

1. A. S. Tanenbaum and M. van Steen, *Distributed systems, Principles and Paradigms.* Prentice Hall, 2002. International Edition.
2. R. J. Anderson, *Security engineering - a guide to building dependable distributed systems (2. ed.).* Wiley, 2008.
3. N. Ferguson and B. Schneier, *Practical Cryptography.* New York, NY, USA: John Wiley & Sons, Inc., 2003.
4. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* New York, NY, USA: John Wiley & Sons, Inc., 2nd ed., 1995.