

# Ensuring TANGO Control System

Sergi Blanch-Torné<sup>1</sup>, Ramiro Moreno Chiral<sup>2</sup>

<sup>1</sup> Escola Politècnica Superior, Universitat de Lleida. Spain.  
sblanch@alumnes.udl.es

<sup>2</sup> Departament de Matemàtica. Universitat de Lleida. Spain.  
ramiro@matematica.udl.es

June 9, 2013

github.Papers: 2013-06-09 (revision 8079e7c)

**Abstract.** <sup>3</sup>

- **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:** “*TANGO as a Supervisory Control and Data Acquisition (SCADA) and/or Industrial Control System (ICS)*”
- **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).*”
- 

---

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

## 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*”
- 

### 2.1 Ensuring presentation layer

- **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*”
- 

### 2.2 Ensuring domain layer

- **TODO:** “*Trusted Computing and Hardware protections*”
- **TODO:** “*multicast, events and the other features that must be secured. Perhaps secret sharing?*”
- 

### 2.3 Ensuring data layer

- **TODO:** “*TANGO database access control*”
- **TODO:** “*Ensuring between instrumentation and the agents out of the scope of this paper*”
- 

### 2.4 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.*”
-

## 2.5 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 session 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.