E-SECURITY & PKI: Towards an effective Arab-African Cooperation

(Hammamet, Tunisia, 22 September 2014)

X.509 in a changing world

Dr. Bilel Jamoussi

Introduction

- E-Security and PKI are fundamental building blocks that enable trusted transactions
- Basis for e-commerce, IoT, Smart Grid, Mobility
- Enables economic grown among Arab-African countries
- Based on International Standards

Rec. ITU-T X.509 until now

- The base specification for pubic-key infrastructure (PKI)
- First edition in 1988
- Seventh edition in 2012
- Widely deployed in the world
  - Banking
  - E-government
  - Health
  - Etc.

What is PKI about?

PKI is about:

- Trust (trust anchor concept)
- Validation of authenticity of information
- But also:
  - Privacy and confidentiality
  - Non-reputiation
- Tools and procedures for above

Today's PKI

- Technically X.509 PKI works and is ubiquitous
- Most common use of PKI is SSL/TLS for secure communication with millions of web servers
- But most RPs (users) do not have certificates or relationships with any CAs
- Over 600 commercial CAs in existence – From many different countries
- How can an RP know if all of these are trustworthy? – Reading their CPs/CPSs is not practical
- How can an RP get damages if CA is untrustworthy or careless or is hacked etc.
- – When it has no formal relationship with CA – Taking into account cross border legal issues

A changing world

- New countries are entering the PKI world
- Cloud computing
- Mobile technology
- Machine-to machine (M2M) communications
- In particular: Smart Grid with millions of entities

A changing environment

- Constrained environments:
  - Memory constraints
  - Processing capacity
  - Bandwidth constraint
  - Time constraints
  - Economic constraints
- Mobile applications
- Huge networks

Other requirements

- Higher level of security by adaptability to different applications
- Protection of the users
- Ease of PKI establishment
- Ease of PKI maintenance

What about Rec. ITU-T X.509?

Rec. ITU-T X.509 must respond to these changing conditions to allow for secure networks also in the future

Future of Rec. ITU-T X.509

- Eighth edition is a significant update expected in 2016:
  - Removal of ambiguities
  - Consistent and current terminology
  - Whitelists (fast validation)
  - Trust broker (secure validation)
  - Machine readable policies (user assistance)
  - Etc.

Supplementary specifications

- X.509 needs supplementary specifications:
  - Profiles and best practices (planned for 2016)
  - Automated PKI establishment and maintenance (planned for 2016)

Summary

- X.509 PKI is now ubiquitous
- The PKI technology is pretty robust and secure – providing the algorithms are kept up to date and – the implementations are complete and correct
- The trust framework, policies, and procedures are the weakest areas
  - This is where most of the standards work is now focused, and where most of the successful attacks are
- New application domains are continually been found, with new requirements
  - New/revised/enhanced standards are required for these

Conclusions and Recommendations

- The intension is to enhance X.509 to meet future challenges
- We need to develop a new generation of PKI experts
- An educational project should be established

Acknowledgment

- **Erik Andersen,**
  - **Andersen's L-Service, Denmark**
  - **era@x500.eu**

- **David Chadwick**
  d.w.chadwick@truetrust.co.uk