Contribution ID: **13** Type: **Poster**

Checking Grid Certificate Profile Compliance

Monday, April 12, 2010 5:06 PM (3 minutes)

Digital certificates are used to secure international computation and data storage grids for e-Science projects in EGEE. The International Grid Trust Federation has defined a set of guidelines for digital certificates used for grid authentication. We have designed and implemented a program and test suites to check X.509 certificates against profiles and policies relevant for use on the Grid to assist implementers and users of PKI to reach appropriate trust decisions.

Detailed analysis

The IGTF has defined the Grid Certificate Profile for X.509 digital certificates used for grid authentication. As certificates are machine-readable and the Grid Certificate Profile is relatively well-defined, there is clearly scope for automation in checking compliance of certificates to the profile, which we believe is important for grid PKI scalability. We designed a practical tool for CA operators and grid sys-admins based on Perl and OpenSSL, both widely used in the target community. We investigated several approaches to defining tests and different certificate access libraries. We made use of the Perl Test / TAP framework to define the certificate test suites and added necessary functionality to Crypt::OpenSSL::X509 to allow us to implement the tests, which was a challenge due to poor OpenSSL documentation. We encountered some parts of the Grid Certificate Profile that pose difficulties for automatic testing.

Conclusions and Future Work

Some bug fixes and complete coverage of the Grid Certificate Profile are necessary. Test suites for other requirements are desirable, as is an online certificate status or validation service. As the grid CA certs are easily available a web application could present current test results for all known CAs. In closing, the current version is a useful practical tool for grid PKI implementers and users, and indeed IGTF reviewers now make use of it when assessing CAs for accreditation

Impact

The Grid Certificate Profile contains 88 distinct provisions, 8 of which were not implementable as automatic tests as they require comparing multiple certs, online checks, or subjective judgement. 69% of Grid Certificate Profile provisions were implemented as tests. Only 22 out of 91 IGTF CAs fully passed the test suite, although most failures were against recommendations rather than requirements. Compliance may be increasing over time but even some recently accredited CAs are not strictly compliant. This work is of considerable interest in IGTF where it is seeing use in the accreditation process. There exists complementary work in evaluating policies against requirements but there does not appear to be any well-known alternative to our work, which bridges the gap between policy and the practice of issuing certificates.

Keywords

PKI, X.509, Trust, Authentication

URL for further information

http://grid.ie/wiki/CheckCerts

Author: Dr O'CALLAGHAN, David (Trinity College Dublin)

Co-authors: Dr COGHLAN, Brian (Trinity College Dublin); Ms DORAN, Louise (Trinity College Dublin)

Presenter: Dr KENNY, Stuart (TCD)

Session Classification: Poster session

Track Classification: Support services and tools for user communities