Dealing with Trust in eGov Services

Vassily Kritis

Intrasoft International, Chief Operation Officer, 40, rue Montoyer straat,
B-1000 Brussels, Belgium
Vassily.Kritis@intrasoft-intl.com

Public Organisations are generally concerned with delivery of services to taxpayers and members of a sovereign state, or with delivery and maintenance of frameworks that benefit the general public (traffic networks, protection against criminals, education, protection from foreign perpetrators, etc.). Traditionally and in most states, Public Organizations have been early adopters of Information and Communication Technologies (ICT) in their effort to increase efficiency and quality of services delivered to the public.

Typically, trust in general purpose public sector Computerised Information Systems is established by ensuring integrity, confidentiality, availability, authentication and non-repudiation of the various constituents. This applies to software, communications, data, hardware, as well as the physical/environmental aspects, staff, and remaining administrative/organisational aspects. It must however be observed that, in recent years, contemporary Public Sector Information Systems increasingly expand their scope into the management of public funds. In this particular area though, the process of establishing trust in related Public Information Systems must extend beyond the five trust elements mentioned above, and also address the prevention of fraud.

Fraud detection is the first step in building a Public Organisation's Information System fraud-prevention shield. Intelligent fraud detection is necessary so that additional overhead introduced, that might have a damaging effect on the relationship between citizens and the State, is kept to the minimum. Also, continuous fraud detection is necessary to identify (a) new cases previously unknown, (b) variants of previously detected frauds, or (c) cases which ceased to be relevant to the organisation. Fraud may have many guises, be that of (a) individual public administrators abusing their access authority on potential system loopholes, (b) multiple public administrators colluding in an institutionalised privilege, or (c) collusion between public administrators and outsiders.

In order to deal with fraud, a Public Organisation must identify and evaluate which fraud cases could be potentially conducted through its Information Systems. We address the need to monitor and fight fraud in an intelligent and continuous way by employing the process of Data Mining. By analysing information within an Information System, data mining helps identify patterns, relationships and recognisable indicators of fraudulent activities. To fight fraud successfully requires an understanding of both, (a) the fraud mechanisms themselves and (b) the potential of data mining in an Information System. Data mining techniques may be used proactively to review a business process to identify anomalies or operational risks and reactively to assist law enforcement agencies in their investigations.

By building data mining based fraud-detection systems within Governmental Information Systems we increase fraud deterrence and therefore enhance trust. We can further prevent fraud which cannot be easily deterred and promptly detect fraud which cannot be obviously prevented. Additionally we enable analysis and investigation of detected fraud to substantiate legal action against those responsible.