



Experiences of establishing trust in a distributed system operated by mutually distrusting parties

Scott Crawford

Enterprise Management
Associates
Boulder, CO

David Chadwick

University of Salford
Salford, UK



Introduction

- ⌘ Subject organization: Engaged in worldwide environmental monitoring
- ⌘ Observed contaminants/events could result from accidents as well as events of international political significance
 - ⌘ Examples: Bhopal 1984, Chernobyl 1986
- ⌘ Detection could have an impact on international relations



Introduction

- ⌘ Participants therefore represent interests of participating nations who don't always fully trust each other
- ⌘ Monitoring data must therefore **assure integrity and trust**
- ⌘ But, it must be trustworthy to organization as a whole, not too greatly influenced by any one party or a minority



Organizational structure

- ⌘ Representative policy-making bodies, with policy-making working groups focusing on specific aspects
- ⌘ Operational organization and staff representative of participants
- ⌘ Distribute responsibility for implementation among representative groups; limit influence of individual participants or hosting nations where possible
- ⌘ Thus, distribution of trust in implementation on many levels



Data collection and monitoring regime

- ⌘ Data collected from over 300 sites worldwide in multiple scientific disciplines
- ⌘ "Continuous" (waveform) and "segmented" data (discrete messages)
- ⌘ Sites networked to central international data collection facility
 - ⌘ Raw data
 - ⌘ Data analysis services also provided at central site: supplementary information, not conclusion-drawing
- ⌘ Participants' national data repositories also collecting some or all data or data subset(s)



Principles of distributed trust in data collection

- ⌘ Organization's operations division collects and provides data impartially, allowing each participant to draw their own conclusions
- ⌘ Principles:
 - ⌘ Data, operations open to scrutiny
 - ⌘ Distribute trusted responsibilities among a group
 - ⌘ No individual should be a single point of trust
 - ⌘ "Preponderance of data" from multiple collection points, disciplines



Data authentication

- ⌘ Authentication to be incorporated in the data itself
- ⌘ Digital signature applied to data at collection point
- ⌘ Algorithm of choice: DSA (DSS)
- ⌘ Key management centered on X.509v3 certificates
- ⌘ Conflict between distribution of CA trust functionality and single signing key



Distributed trust in certificate signature

- ⌘ X.509v3 certificates issued by a single certificate authority (CA)
- ⌘ Need to distribute trust in certificate signature (CA private key)
- ⌘ Investigated solutions: functional/role-based distribution, threshold cryptography



Investigation of threshold cryptography

- ✦ “M out of N” key components cryptographically distributed
- ✦ Components must be combined for operations (e.g. signature generation)
- ✦ Impractical for signing data at collection point, but a possible certificate-signature solution



Previous threshold implementation studied

- ✦ Identrus: Cooperative peers at high level of banking, building a trust architecture between participants and their customers
- ✦ An original Identrus participant: CertCo
 - ✦ Held threshold cryptography patents



Drawbacks to threshold cryptography

- ✧ Then-current threshold RSA had some susceptibilities (Langford '96)
- ✧ No practical threshold DSA/DSS scheme at time of system design (Desmedt '97)
- ✧ Limited solution providers
- ✧ So ruled out



Chosen solution

- ✧ Retain M-out-of-N distribution of responsibility for certificate issuance in operational distribution of roles (RAO/CAO in Baltimore terminology)
- ✧ DSA certificate signing algorithm
- ✧ Enforce >1 person access to sensitive components (key stores, etc.)



Implementation summary

- ✦ Preliminary design, laboratory pilot, initial deployment design, initial field implementation
- ✦ Testbed trials of lab and field systems
- ✦ "Continuous" data: DSA signature field (40 bytes)
- ✦ "Segmented" (message-format) data: S/MIME
- ✦ LDAP namespace rooted on organization ID



Example: Keypair initialization

- ✦ Keypair generation at the monitoring site:
 - ✦ >1 onsite personnel witness, sign output, send back to data center
- ✦ Certificate issuance
 - ✦ >1 RAO verify received signed message from the field



Proposed command-and-control solution

- ✍ Digital signature of command/control messages
- ✍ Only holders of command-and-control certificates are empowered to issue commands
- ✍ Issues:
 - ✍ Monitoring site access to CA certificates, CRLs:
Network vs. local cache
 - ✍ Logging/auditing of control messages



Limiting aspects of system

- ✍ Certain components limited in capability or not amenable to addition of signature functionality
- ✍ Limitations on PKCS#10 certificate request generation
- ✍ Tamper-evident measures at sites but sensors could be physically moved during network or power outages (suggested adding GPS receivers but it was too costly, complex or too large for the equipment footprint)



Initial results

- ⌘ Human involvement is considerable
 - ⌘ Multiple participants, "M-out-of-N" carried into all operations where possible/applicable
- ⌘ Knowledge, skill burdens are significant
 - ⌘ PKI, trust, security, OSs etc.
- ⌘ "Ease of use," user interaction issues
- ⌘ PKI components, systems still maturing



Summary and conclusions

- ⌘ Began as a technology exercise, but deployment is heavily dependent on human factors
 - ⌘ (Trust is, after all, a human perception)
- ⌘ Trust distribution is wider than at the CA alone
 - ⌘ "Preponderance of data," number of collection sites, openness of data to scrutiny
 - ⌘ These factors were present prior to system deployment; thus, while system adds significant trust measures, it is still dependent on these other attributes
- ⌘ A qualified success, reflective of the organization
 - ⌘ Data verification systems successful
 - ⌘ Participants highly motivated, educated, skilled
 - ⌘ Like Identrus (international banking), organization has necessary resources to support the system