Supporting Unconditionally Secure Authentication within e-Government Infrastructure based on QKD

Sufyan T. Faraj Al-Janabi (Ph.D., Prof.)
College of Computer Science and IT
University of Anbar, Ramadi, Iraq
saljanabi@fulbrightmail.org
Problem Statement

- It has been noticed that the speed of ICT advancement in developing, deploying, and using e-government infrastructures is much faster than the development and deployment of security services.
- Therefore, government organizations are still suffering from the existence and emerging of security risks.
- All available security solutions are only computationally-secure!
The aim of this work is to show the importance and validation of including unconditionally-secure authentication services within e-government infrastructure based on QKD.

The work highlights the basic requirements for a general framework that facilitates such inclusion and also introduces sample protocol modification.
Authentication Techniques

Mathematical Authentication Techniques

Message Authentication Codes (MACs)

A-Codes

Digital Signatures
MACs and A-codes can provide data integrity and data origin authentication.

It is important to emphasize that MACs are only proven to be computationally secure while the security of A-codes is unconditional.

Thus, MACs are suitable for short-term security but they are not useful for long-term (say 20 years) requirements, especially when considering new technologies like quantum computers.
Digital signatures are very widely used technology for ensuring unforgeability and non-repudiation of information.

Digital signature schemes can be constructed for both computational security and unconditional security.
eGMMs vs. ISMMSs

General Convergence Maturity Model

A-Codes, etc..
The proposed N-Tier framework architecture

- Presentation Tier
- Business Logic Tier
- Security Tier
- Data Access Tier
- Data Tier
Basic security-related functions

- Signature-creation
- Signature-verification
- Info-box access
- Session certificates
- Session encryption
- Session decryption
- Key-synchronization
Typical deployment of key bank agents
Proposed key management and distribution approaches

**Courier-based approach:**
- This is the most traditional approach

**Quantum cryptographic-based approach:**
- Recently, there have been significant advancements in Quantum Key Distribution (QKD)

**Hybrid PKI-based approach:**
- Properly combining QKD with public-key based authentication
Why QKD?

- QC delivers cryptographic keys whose secrecy is guaranteed by the laws of physics.
- QC offers new methods of secure communications that are not threatened even by the power of quantum computers.
- In quantum cryptography, physically secure quantum key distribution can be combined with the mathematical security of the OTP cipher and/or information-theoretically secure authentication (based on universal hashing).
Stand-alone QKD PTP link

Key Distribution
Optically switched QKD network
Trusted relays QKD network

Link Encryption

Private Enclave

QKD Endpoint

Trusted Relay

Encrypted Traffic via Internet

QKD Endpoint

Trusted Relay

Private Enclave
“Full” quantum network

End-to-End Key Distribution

Private Enclave

QKD Endpoint

Untrusted QKD Switch

Untrusted QKD Switch

QKD Endpoint

Private Enclave

Encrypted Traffic via Internet
Tightly-coupled protocol stack strategy; secret random bits obtained from QKD (which is mainly a physical layer technology) are merged directly somehow into a conventional higher-layer security protocol suite. Thus, the consumer security protocol has to be modified to enable the integration of QKD within it.

Loosely-coupled protocol stack strategy; the focus here is to develop original multi-layer protocol infrastructures that are dedicated to QKD networks. In such a case, the QKD network infrastructure can be viewed as a "new cryptographic primitive".
<table>
<thead>
<tr>
<th>Message Type</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1- start-quantum-transmission</td>
<td>null</td>
</tr>
<tr>
<td>2- start-acknowledgement</td>
<td>null</td>
</tr>
<tr>
<td>3- end-quantum-transmission</td>
<td>null</td>
</tr>
<tr>
<td>4- end-acknowledgement</td>
<td>null</td>
</tr>
<tr>
<td>5- synchronize-quantum-channel</td>
<td>timing information</td>
</tr>
<tr>
<td>6- receiver-sifting</td>
<td>indices of detected pulses, detection bases</td>
</tr>
<tr>
<td>7- sender-sifting</td>
<td>pulses' indices, transmission bases</td>
</tr>
<tr>
<td>8- receiver-error-correction</td>
<td>reconciliation technique dependent</td>
</tr>
<tr>
<td>9- sender-error-correction</td>
<td>reconciliation technique dependent</td>
</tr>
<tr>
<td>10- set-equality</td>
<td>hashes of chosen sets</td>
</tr>
<tr>
<td>11- equality-acknowledgement</td>
<td>null</td>
</tr>
<tr>
<td>12- privacy-amp-parameters</td>
<td>parameters of the privacy amplification method</td>
</tr>
<tr>
<td>13- privacy-amp-acknowledgement</td>
<td>null</td>
</tr>
<tr>
<td>14- receiver-discussion</td>
<td>situation dependent</td>
</tr>
<tr>
<td>15- sender-discussion</td>
<td>situation dependent</td>
</tr>
</tbody>
</table>
Conclusion

- Using A-codes can offer additional security benefits especially in situations when long-term and/or significantly high level of security is required.

- We advise A-codes based services for G2G and G2B settings only in the first adaptation stage.

- It is possible in next stages to include e-democracy (especially e-voting)
Future Work

- Since our current implementation is mainly limited to simulation. Future work might consider prototype implementation on Intranet level.

- Further investigation of hardware and software requirements of such systems for wired and/or wireless settings can also be considered.
Thank you