Deterring Attacks against Critical IT Infrastructure

Researchers

Dan Brownstein
danbr@cs.bgu.ac.il

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Dr. Niv Gilboa
gilboan@bgu.ac.il

Results

Development is in progress. Several algorithms are needed for developing the protocol of which only a few are already constructed. Among these algorithms are: construction of a small DFA that verifies signatures, construction of an efficient scheme for functional encryption for Cascade Mealy Machine (extension of the currently known functional encryption schemes for regular languages). In addition, there is a team of fourth-year Communication Systems Engineering students who implement the scheme.

Goals

In our previous work the notion of arbitrators in a Peer-to-Peer (P2P) network was used to enforce the client-server agreement for the limited case of conditional anonymity. Arbitrators are P2P semi-trusted entities that function as a jury in the technology court of law. The communicating parties, users and servers, agree in the initial phase on a set of arbitrators that they trust (reputation systems may support their choice). Then, the user divides its identity into shares and sends each share to one arbitrator, such that only a large enough number of arbitrators can reveal the identity of the user. The CA signs the shares that the user distributes to the arbitrators, vouching for their authenticity. The communication between the user and the server is performed in an undeniable manner, which means that the server can convince the arbitrators that the user misbehaved. In the event that the server finds a violation of the terms of the policy, the server proves to the arbitrators that a violation took place and the arbitrators reconstruct the user's identity.

An important objective of this research is the construction of schemes that encourage commitment to a policy and enforcement of this commitment, even without a third party. In this approach, a client commits to a certain policy or agreement and in return receives service from a server. The client's commitment includes hidden information such as the client's identity or a signed financial instrument such as a check or a bond. If the client breaches the terms of the agreement then the server can expose the hidden information without assistance from external parties, such as arbitrators.

Description

Attacking critical IT infrastructure is almost always risk-free. Whether targeting government services or financial institutions, an attacker can sit in the comfort and safety of his home and mount one attack after the other. Protected from identification by the virtual anonymity of the Internet and from legal proceedings by being in a different jurisdiction than the target, the greatest risk for most attackers is that their attack may fail.

The technology can be used in critical IT infrastructures as another cyber security measure.