Leuchtfeuer

A Unified Agreement Protocol for Mix-nets

No Author Given

No Institute Given

Abstract. We describe the structure of the deployed mix-net systems, and examine the security implications that arise when user behavior is influenced by the node reliability and availability data provided by independently-operat362(s42(inform)1(atio)1(n)-343(s)-1(ervic)1(e)-1(s.)]TJ0-11.006Td[(W)85(e)-483(prese)-1(r

mixes in the mix-net. The security of the system is based on the premise that a user's traffic may be safely routed through nodes which the attacker controls, as long as the user's client has selected a path through the network that includes a sufficient number of honest nodes. Multiple distributed-trust mix-net variants have been deployed on the Internet since the early 1990's.

The components of the extant mix-nets are operated on a volunteer basis, often by parties unknown to the users. Since many volunteer operators lack the resources to offer the same level of high-availability access assurance as com-

3 Anonymity set attacks based on pinger data

A mix network in which users obtain their view of the network's heath and status

the worst they can do is to crash – is rather hard, and a significant amount of research has been put into securing a distributed systems against faulty par-

only a binary value. As there is a (potentially) infinite universe of possible values, a multivalued Byzantine agreement protocol can no longer guarantee that the output of the protocol is the input of some honest party – this would only be possible if all honest parties propose the same value. It is, however, possible

Update set of mixes. The main functionality of our protocols is to maintain a consistent set of mixes. Furthermore, a client should easily be able to obtain that

mix also needs to maintain a serial number, so that all parties can be assured