返回首页

Does Helios ensure ballot secrecy?

http://www.firstlight.cn   2010-12-06

Helios is an open-source web-based end-to-end verifiable electronic voting system, suitable for use in low-coercion environments. In this paper, we analyse ballot secrecy and discover a vulnerability which allows an adversary to compromise voters' privacy. This vulnerability has been successfully exploited to break privacy in a small election using the current Helios 3.0 implementation. Moreover, the feasibility of an attack is considered in the context of French legislative elections and, based upon our findings, we believe it constitutes a real threat to ballot secrecy in such settings.

存档文本