KASTEL - Institut für Informationssicherheit und Verlässlichkeit
Lehrstuhl Prof. Dr. J. Müller-Quade
https://crypto.kastel.kit.edu

Forensic Analysis of MATE Threats to Deniability in E-Voting Systems

Bachelor's/Master's Thesis

Modern e-voting systems aim to guarantee coercion resistance and voter deniability, ensuring that voters cannot prove how they voted even if they want to. These properties are critical to prevent voter intimidation and vote selling. Although the cryptographic community has extensively studied deniability from a protocol and proof perspective, comparatively little attention has been given to realistic endpoint threats, especially Man-At-The-End (MATE) attackers who control the voter's device or execution environment. A MATE adversary might instrument, modify, or observe the voting client at runtime and after the act of voting. This makes it possible to extract both persistent and volatile digital traces that may reveal the voter's true choice or other sensitive behavior. Such traces can exist in main memory, the file system, or in network traffic, and they may allow post-hoc event reconstruction inconsistent with the system's intended deniability guarantees.

Goals: The goal of this thesis is to systematically analyze e-voting software under a MATE threat model using digital forensics methodologies to determine whether the identified traces impact deniability, coercion resistance, or related security goals.

Scope of the work

The work should experimentally determine which traces real-world implementations leave behind and to what extent these traces undermine voter deniability and coercion resistance. To do so, the student is expected to:

- Develop an automated virtualized test environment for reproducible collection of file-system, main memory, and network data.
- Extract and analyze digital traces created during the voting process and classify their relevance for reconstructing voting actions.
- Evaluate how the identified artifacts impact deniability, coercion resistance, and related security goals.
- Formulate corresponding threat models and propose recommendations for more MATE-resilient e-voting implementations.

Requirements

- Solid understanding of the fundamentals of digital forensics
- Experience with black box and white box approaches to application forensics (reverse engineering, binary instrumentation, differential analysis, etc.)
- Familiarity or willingness to become familiar with e-voting protocols and systems.
- A keen curiosity and interest in the topic are required!

Contact

In case of interest or for further information, please contact Dr. Jan Gruber, jan.gruber@kit.edu (Room 276, Building 50.34), and/or Marc Nemes, nemes@fzi.de (Room 276, Building 50.34).