"zkSBOM: Privacy-Preserving SBOM Sharing with Zero-Knowledge Sets"

Tom Sorger, KTH

Software Bills of Materials (SBOMs) are increasingly mandated by regulators, yet existing sharing mechanisms impose a binary choice between full disclosure and full opacity. This exposes software suppliers to attacks that can be deduced from the SBOM only, such as the presence of a vulnerable dependency. Conversely, software consumers can be fooled by software suppliers who modify or misrepresent published SBOMs. We present zkSBOM, a privacy-preserving SBOM sharing mechanism designed to address these threats. zkSBOM uses zero-knowledge sets to cryptographically commit to the components within an SBOM. Software consumers can query for known vulnerabilities and receive a cryptographic proof confirming whether the artifact described by the SBOM is affected, without revealing any additional SBOM content. We conduct a security analysis of zkSBOM by quantifying expected leakage from inclusion and exclusion proofs. We demonstrate real-world feasibility by applying it to realistic scenarios and evaluating its operation requirements. Our evaluation demonstrates that zkSBOM is a strong, secure, and privacy-preserving mechanism for SBOM sharing, protecting software suppliers and software consumers from one another.