Privacy-Preserving Log Audits for CALEA Wiretaps

Adam Bates and Kevin Butler – Computer and Information Science Department, University of Oregon

with Micah Sherr and Clay Shields (Georgetown U), Patrick Traynor (Georgia Tech), and Dan Wallach (Rice U.)

Modern lawful access wiretapping was established in 1994 with the Communications Assistance for Law Enforcement Act (CALEA). However, CALEA infrastructure is subject to a number of vulnerabilities that wiretap targets can exploit to create gaps or corruption of wiretap transcripts. Wiretaps are unable to demonstrate their own correctness, which is troubling because the violation of regulatory laws could lead to their inadmissibility in criminal trials. This is troubling to law enforcement, but citizens also deserve assurances that wiretaps are being used lawfully and correctly.

We are investigating and addressing the challenge of enabling secure auditing in existing federal wiretapping deployments. We enhance these systems by adding a privacy-preserving, tamper-evident logging mechanism. Our architecture uses an untrusted storage service that augments existing CALEA deployments without requiring costly modification to the service provider’s infrastructure. We introduce a single component, the Encryptor, that augments existing CALEA deployments without requiring costly modification to the service provider’s infrastructure. It sends to a Remote Audit Log that acts as an untrusted central database. Two auditors interact with the log, a Court that can access cleartext wiretap records and an Accountant that can only access coarse-grained wiretap usage statistics.

We enhance these systems by adding a privacy-preserving, tamper-evident logging mechanism. Our architecture uses an untrusted storage service that augments existing CALEA deployments without requiring costly modification to the service provider’s infrastructure. We introduce a single component, the Encryptor, that augments existing CALEA deployments without requiring costly modification to the service provider’s infrastructure. It sends to a Remote Audit Log that acts as an untrusted central database. Two auditors interact with the log, a Court that can access cleartext wiretap records and an Accountant that can only access coarse-grained wiretap usage statistics.

For our preliminary evaluation, we performed microbenchmarking of each step in the wiretap record generation process. The speed of a single event’s creation is bottlenecked by the encryption of our aggregate block.

For further information…
Contact Adam Bates (amb@cs.uoregon.edu),