The UMBC Cyber Defense Lab presents

How Signing Protocols Fail: An Analysis of the Secure Evidence Attribution Label

Carson Kegley, William Bowman, Michaela Finazzo
Undergraduate Students, UMBC

Joint work with Enis Golaszewski and Edward Zieglar

12:00noon–1pm ET Friday, September 11, 2026
Remotely via WebEx: https://umbc.webex.com/meet/sherman

AI image generation is a powerful accelerant in the existing mis/disinformation crisis, leaving governments and firms scrambling for solutions. We analyze one such proposed solution, the *Secure Evidence Attribution Label (SEAL)*, a protocol designed to establish provenance of digital media. SEAL allows signers to attest the provenance of media cryptographically by signing a hash of a digital asset, then distributing the public key used to verify the signature in a DNS TXT record. The name of the domain, where the public key is stored is hashed with the asset and protected under the signature, giving cryptographic proof of file integrity and the identity of the signer.

We perform the first independent security analysis of the SEAL protocol, in which we assess the specification for structural weaknesses. We also test for implementation errors in its two first-party signature verifiers: *SEAL-C* and the online *SEAL Validator*. We identify and formalize SEAL's stated security goals (record integrity, file integrity) and define an additional necessary security goal (domain authentication). Using the *Cryptographic Protocol Shapes Analyzer (CPSA)* we model the protocol and determine whether the model meets the stated security goals. Additionally, we evaluate whether the two signature verifier reference implementations adhere to the specification.

Our investigation concludes that SEAL currently neither satisfies record integrity, file integrity, nor domain authentication goals. Because SEAL relies on a DNS root of trust and does not attempt to mitigate the unsecured nature of DNS over UDP, it is vulnerable to simple *man-in-the-middle (MITM)* and DNS cache-poisoning attacks. Additionally, SEAL allows signers to sign only parts of a file yet have the signature validated as if they had signed the entire file. This property permits a malicious actor to sign only certain parts of a file and change the content of unsigned portions without detection. We propose and formally verify several mitigations to address these challenges.

About the Speakers.

Carson Kegley (ckegley1@umbc.edu) is an UMBC undergraduate student majoring in computer science. He is also a veteran of the United States Air Force, where he worked in defensive cyber operations. Kegley is a researcher in the UMBC *Protocol Analysis Lab (PAL)*.

Michaela Finazzo (michaef1@umbc.edu) is an undergraduate computer science student and Cyber Scholar at UMBC. She is a member of PAL, where she works on the SEAL project. In the *Data Management & Semantics (DAMS)* research group, she is building a knowledge graph for sensors in assisted living communities. Her current research projects include analysis of the *Agent Payments Protocol (AP2)* for INSuRE+E.

William Bowman (wbowman4@umbc.edu) is a computer science undergraduate at UMBC. They are a researcher in PAL, where they have worked on projects including the *Coalition for Content Provenance and Authenticity (C2PA)* protocol and SEAL. Their current research projects include analysis of the AP2 in CMSC 691. Bowman is a UMBC Cyber Scholar.

Host: Dr. Alan T. Sherman, sherman@umbc.edu

Support for this event is provided in part by the NSF under SFS grant DGE-2438185.

The UMBC Cyber Defense Lab meets biweekly on Fridays 12-1pm. All meetings are open to the public.