Blockhub: Blockchain-based Secure Cross-domain Software Development System

Denis Ulybyshev¹, Bharat Bhargava¹, Miguel Villarrreal-Vasquez¹, Aala Alsalem¹, Ganapathy Mani¹, Leszek Lilien¹, Donald Steiner², Jason Kobes², Steve Seaberg², Paul Conoval², Robert Pike², Rohit Ranchal³
¹Computer Science and CERIAS, Purdue University; ²Northrop Grumman; ³IBM

**OBJECTIVES**

- Provide secure software sharing and software access auditing
- Provide integrity of provenance data
- Detect software spillage

**FEATURES**

- Encrypted SM is stored in SB
- Role- and attribute-based access control
- X and Y, can share software via smart contracts running in blockchain network
- Every request and transfer of SM is logged in blockchain’s distributed ledger
- For software transfer authorization needed by both smart contract and policy enforcement engine of the SB

**WAXEDPRUNE ARCHITECTURE**

1. Registration of software attributes and ID information
2. Access Authorization
3. Process Automation

**SOFTWARE SPILLAGE DETECTION**

- SB contains $\text{Enc}[\text{Software}(S)] = \{\text{Enc}_1(SM_1), \ldots, \text{Enc}_n(SM_n)\}$ and Access Control Policies ($P = \{p_1, \ldots, p_n\}$)
- X is authorized to extract and decrypt SM1 from SB
- X leaks Enc(SM1) or SM1 to unauthorized service Y
- When Y tries to decrypt SM1 CM checks policies: whether SM1 is supposed to be at Y
- If plaintext SM1 is leaked: visual watermarks; web crawler checks digital watermarks

**PUBLICATIONS, PROTOTYPE**

https://github.com/Denis-Ulybyshev/alhsa17

**ACKNOWLEDGEMENT**: This research is supported by Northrop Grumman. We collaborated with Donald Steiner, Leon Li, Jason Kobes, Steve Seaberg, Peter Meloy, Paul Conoval.