George Mason University,
Office of Technology Transfer
Seeks partners to license ...

CIPHER X-RAY

Tech ID # GMU 11-027 **Patent No. 9,160,524**

Description of Technology:

Whether or not (and to what extent) cryptographic operations and secrets can be effectively recovered from potentially obfuscated binary executables will have a far reaching impact on both malware analysis and the security of legitimate binary executables.

CypherXRay is a binary analysis framework that has unprecedented capabilities to expose the cipher operations, their internals and secrets of cryptographic algorithms. Using the avalanche effect, CypherXRay is able to detect and pinpoint public key cryptographic operation, block cipher and hash operation. Additionally, it can accurately recover the input (plaintext), the output (decrypted plaintext) and the secret key (e.g. 256-bit AES) and the private key (e.g. 1024-bit RSA) used in the identified cipher operation.

A proof of concept prototype has been developed in Linux.

Primary Investigators:

Dr. Xinyuan (Frank) Wang is an associate professor of computer science in the Volgenau School of Engineering at George Mason University. Xin Li worked as a graduate student on this technology with Dr. Wang.

Advantages:

- Unprecedented capabilities to recover hidden code and secrets of sophisticated malware
- Able to pinpoint exact timing of decryption into plaintext
- Can be used to reveal potential security weaknesses of existing software systems

George Mason University, Office of Technology Transfer

Contact

George Mason University
Office of Technology Transfer
4400 University Drive, MS 5G5
Fairfax, Virginia 22030
Phone: 703-993-8933
Fax: 703-993-9710
Email: hmehta4@gmu.edu