SafeVanish: An Improved Data Self-Destruction for Protecting Data Privacy

Lingfang Zeng, Zhan Shi, Shengjie Xu, Dan Feng

School of Computer Science and Technology, Huazhong University of Science and Technology
Information Storage Division, Wuhan National Laboratory for Optoelectronics
Motivation: Data Lives Forever (1/2)

Motivation: Data Lives Forever (2/2)

The decapsulation process by compose the encryption key for Vanish0.1.

The improved architecture of Vanish0.2.1.
Motivation: Hopping attack

The hopping process of the malicious nodes in hopping attack.

The push operation in the VuzeDHT network.

Nodes (may flow into and out at any time)
VuzeDHT network

The copy operation for refresh within the Vuze network every 30 minutes

The second hop after the first hop, its coverage after this hop

Nodes (may flow into and out at any time)
VuzeDHT network

The copy operation of malicious node

The coverage for the first attack

Malicious nodes

Hop after 3 minutes, it becomes a new attack node
Motivation: Sniffing

In addition, it’s very dangerous for Vanish to transmit key shares that exposed to the network.
Existing approaches and their shortcomings

- Increase the Vanish threshold $k$ for composing the encryption key
- Switching Vanish to a privately hosted DHT
- Detect the attacker
- Limit the ID distribution mechanism of Vuze
Solution for the hopping attack

Increasing the length of range of key shares
The expanded length range of key shares (1/2)

A Ball class object

Random bytes

Key shares

[16, 51], range size is 35

Simulation of random add operation

[16, 151], the expanded range size is 135
The expanded length range of key shares (2/2)
Solution for the sniffing attack

Using the RSA encryption algorithm
Conclusions

- Discuss the existing state-of-the-art self-destructing data schemes (Vanish) exhibit fragile for hopping attack and sniffing attack in realistic application.
- Propose a new scheme called SafeVanish.