PASSWORD-TRIGGERED TRUSTED DELETION

January 2016

Partner institution :

CONCORDIA UNIVERSITY

BACKGROUND

Data deletion is problematic from both technical and usability perspectives. While governments and businesses generally have policies to safely remove data from devices, proper deletion is currently not proven at a technical level by any solution as we are aware of. NIST guidelines on media sanitization specify a completely manual procedure for generating a "Certificate of Sanitization". Data deletion is particularly difficult in the following situations: (a) when a user is coerced to reveal the disk encryption key or password; (b) when a computer with encrypted disk is lost or stolen, but cannot rely on a remote service for data deletion; (c) when the disk encryption key or other secrets can be retrieved from RAM; and (d) when quick and verifiable deletion is needed in network-connected machines. In all situations, we cannot rely on a trusted, remote service to enforce the deletion mechanisms.

TECHNOLOGY

Our "Trusted Deletion" comprises three components:

- Gracewipe (boot-time data protection/deletion under coercion),
- Hypnoguard (wakeup-time data protection/deletion for lost/stolen devices, with protections against memory extraction attacks), and
- NetworkDelete (under development, quick deletion in a local network).

They provide all of the following features together: triggering the hidden encryption key deletion process in a way that is indistinguishable from unlocking the hidden data; verification of the deletion process; restricting guessing of passwords used for data confidentiality; and full-memory encryption. We rely on the TPM chip, and modern CPU's secure execution modes such as Intel TXT and AMD-V to implement our Trusted Deletion systems.

COMPETITIVE ADVANTAGES

Trusted Deletion uses technologies that are already available in millions of computers, and largely operating system and BIOS independent. Our techniques can be readily adopted with minor tweaks in particular deployment scenarios. We rely only on regular user-chosen passwords, i.e., for better security we do not need really "strong" passwords or USB-stored keys (as in BitLocker).

APPLICATIONS

Quick "erase" of hard disks, triggering deletion in lost/stolen laptops, cold-boot protection, erase hard disk under coercion.

TECHNOLOGY DEVELOPMENTAL STAGE

The main function is fully implemented and tested on few computers. The extension to guard against memory attacks during sleep-wake cycle has also been implemented. The extension for network-based remote deletion is in a preliminary state.

PATENT STATUS

Patent pending

BUSINESS OPPORTUNITY

License available. Strategic partnership for future improvements and new functions.

For Information please contact:
Duc Levan
Senior Director, Business Development
T.: 514 840-1226, ext: 3003 / dlevan@aligo.ca