A Trusted Open Platform

England, P.; Lampson, B.; Manferdelli, J.; Willman, B.
Computer, Vol.36, Iss.7, July 2003
Pages: 55- 62

Presented by Richard Paul

The Problem

- "*Computers are entrusted with more personal and valuable data everyday, and local and remote users need mechanisms to safe guard this data against misuse*."

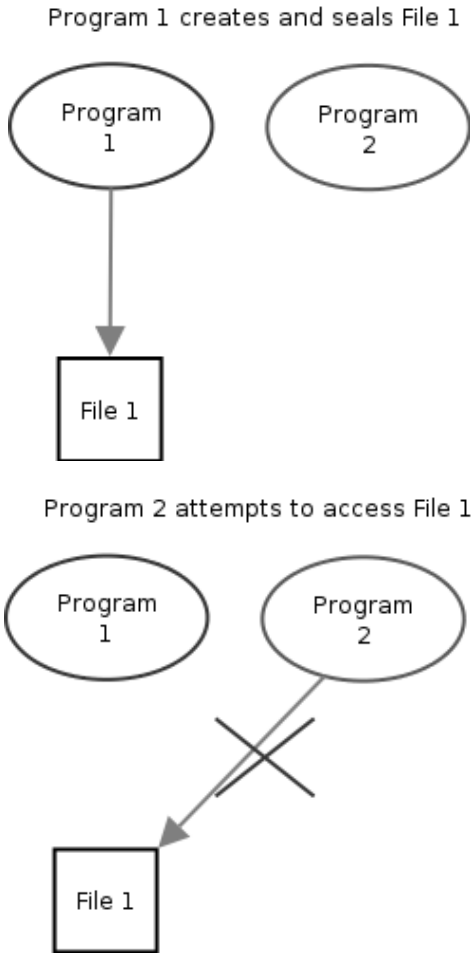
  - User data is vulnerable to viral and Trojan attacks.
  - Passwords, credit cards and other personal information may be susceptible to key sniffers.
  - Personal or business information may be accessible by a Trojan that scans a hard disk for information.

A Possible Solution

- Microsoft's *Next-Generation Secure Computing Base* (NGSCB).
- The NGSCB "…*extends personal computers to offer mechanisms that let high-assurance software protect itself from the operating systems, device drivers, BIOS, and other software running on the same machine.*"

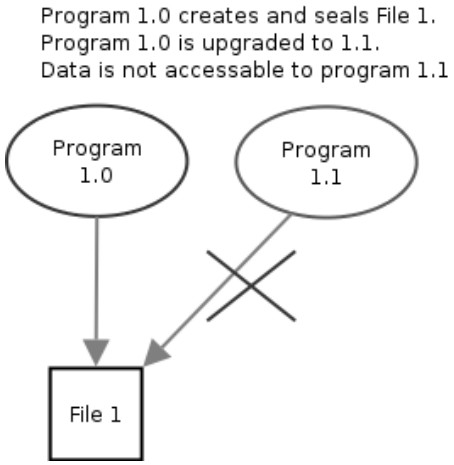
Sealed Storage

- Data is sealed and encrypted.
- Based on cryptographic hash (code ID) of the program executable.
- Sealed data can only be unsealed by a program with the same code ID



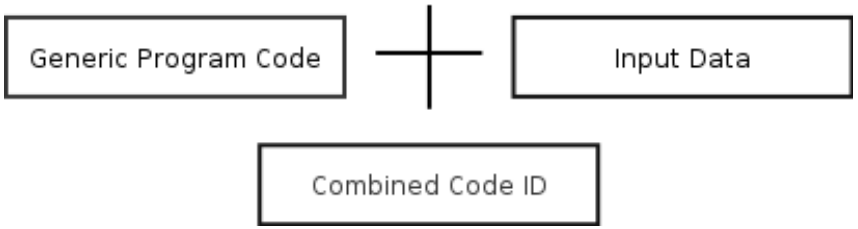
Program/Kernel Upgrade

- Problem arises when the code ID changes for a program.
- Eg. During an upgrade or authorised patch.
- Un-patched program seals data with the patched programs code ID.
- Must know the code ID before the upgrade.
- If corruption occurs in a program the data becomes inaccessible.



Generic Program Code

- Various programs perform different operations based on their input.
- E.g. Scripting Languages, Java, Python.
- Create a code ID based on the combination of the interpreter and the input data.
- If the interpreter gets updated, all code IDs for programs run by the interpreter become invalid.



Attestation

- Programs can authenticate themselves to remote computers using public key encryption.
- Microsoft encourages the formation of third-party "*identity service providers to act as trusted intermediaries between service providers and their customers.*"
- Users only reveal their platform ID to a limited number of 'trusted' providers.
- These providers return secondary attestation tokens to the users for everyday web use.

Appreciative Comments

- NGSCB creates highly secure data that is protected against unauthorised access.

- Strong application in rights managed data.
  - Users can share data between trusted machines through attestation.
  - Data is stored securely on the machine.

Critical Comments

- Performance Trade-Off
  - All secure information must be encrypted and decrypted.
  - Randomisation is added to the files resulting in higher file sizes and time spent writing to the disk.

Questions

- How could updating an interpreter (generic program code) be dealt with?
- Will the average home user embrace the high security levels of the NGSCB?

Generic Program Code

- Separate the code ID in to 2 segments.
  - Generic Program Code
  - Input Data

NGSCB for the average user.

- Needs to be transparent.
- May prove difficult when installing new programs or upgrading existing programs.

- Difficult for users when things ‘go wrong’
  - If a program file becomes corrupted the associated data is inaccessible.