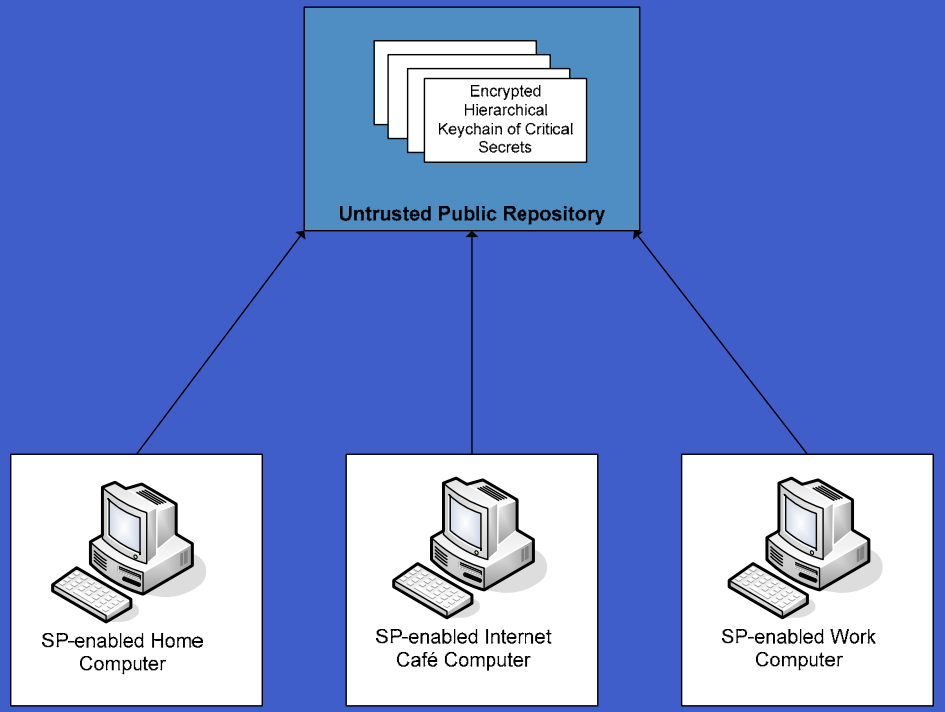
Architecture for Protecting Critical Secrets in Microprocessors

Lee, R.B., et al., Architecture for Protecting Critical Secrets in Microprocessors.
ACM SIGARCH Computer Architecture News, 2005. 33(2): p. 2-13.

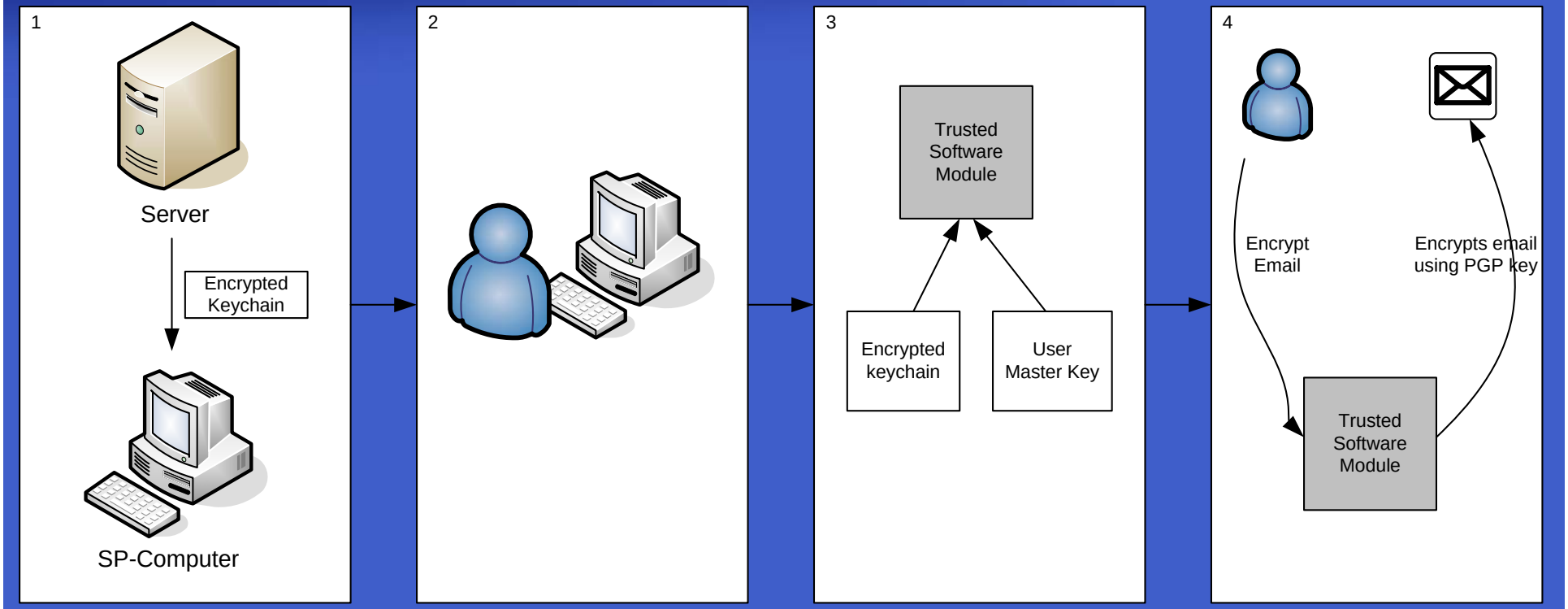
Gene Tang

What is the paper about?

This paper proposes an extension to the current microprocessor architecture that allows us to safely access any of our Critical Secrets, from <u>any</u> "Secret-Protected" Computer. Critical Secrets are cryptographic keys that are used to sign files, messages, data and programs.



So how do I use it?



Download our encrypted keychain from third party

User enters "User Master Key" password into computer

Trusted Software Module decrypts the keychain with User Master Key

Call functions on the TSM when we want to perform an action using keys on the keychain. TSM completes action on behalf of user

What's good about the paper?...

- Addresses a problem common in the financial and military industries, where data is commonly encrypted for security. The SP architecture means users are not limited a single location or the need for auxiliary hardware like a smartcard.
- Provides a broad view of the system, not just a description of the implementation. For example, the paper also proposes a new threat model and performs performance analysis.

What's not so good?...

- Requires a public untrusted repository to hold each encrypted hierarchical keychain of critical secrets. These repositories are susceptible to attack, for example denial of service attacks.

- The system is ‘brittle’ since a small insecurity breaks the entire system. That is, the architecture hinges on a single user password to decrypt and access the user’s critical secrets.

The problem with Passwords...

- Passwords selected by the user should string 14 characters of upper and lower-case letters with numbers, or 60-70 lower-case characters, to be secure.
- Good Password Security means the owner must use non-obvious passwords, change them monthly, and not write them down – a rule very rarely followed[1].
- Passwords are susceptible to simple attacks such as Dictionary and Brute Force Attacks.
- CERT/CC has found that 80% of network security problems are due to bad passwords, and up to 50% of passwords can be guessed using Dictionary/Guessing attacks[1].

The problem with Passwords... (cont)

- The Secret-Protected Architecture, requires the user to enter a password so they can utilise the critical secrets in the keychain.
- This means that the architecture is susceptible to the drawbacks of passwords and password attacks resulting in the architecture becomes worthless if passwords are exposed and proper password procedures aren't followed.
- It is unlikely that all users will follow the safe password practices correctly placing their critical secrets at risk.
- The paper also mentions other forms of authentication, e.g. biometrics. However these are still susceptible to false positives and negatives.

My Question...

- Would you trust placing all your critical secrets under the control of a single password?

References

[1] Password Cracking (2005), retrieved from: http://en.wikipedia.org/wiki/Password_cracking