Authentic Data Collection in an Untrustworthy Computer Environment

Thomas J. Wilke <tjw@prz.tu-berlin.de>

12 June 2002
This talk is not about

- Cryptographic algorithm analysis
- Secure communication methods or protocols
- Public key infrastructures implementation or operation
- Smart card programming or management
The talk wants to

• motivate why a secure data collection is needed.

• give an idea about the problem of insecure data collection and solution available today addressing the problem.

• present a method how the data collection process can be protected in an trustworthy manner.

• show how this method can be implemented and applied in practice.

• give an outlook for future applications which will base on a secure data collection process.
Contents

• The process of digital signing

• The problem of authentic data collection

• Practical solution: Authentic Data collection Device

• Outlook and future work: E-contracting services

• References and contact
Digital Signing

Digital signing is one of the most demanding applications for trustworthy data collection since:

- it provides a technical base to make binding declarations associated with real monetary or legal values which have exclusive electronic representation.

- some governments have put handwritten signatures par digital signatures.

- it is one key component to establish an e-commerce and e-government completely processed on computer systems.
Digital Signing

Trustworthiness of digital signatures can only be guaranteed if the following conditions can be fulfilled:

- the secret key should only be accessible to the person it has been dedicated to since its represents its digital identity
- the public key distribution has to be trustworthy
- the cryptography used should be adequate to the common security standards
- the process of generating digital signatures has to be done in a trustworthy environment
- the signature verification has to take place in a trustworthy environment
The problem of authentic data collection

To ensure a trustworthy signing process on an insecure desktop computer system the following operation sequence will have to be protected:

- data collection from a trustable device and transfer to a temporary storage
- temporary storage of the collected data
- hash calculation
- public key encryption of the hash value
The problem of authentic data collection

Digital signing is a special case of authentic data collection. A more general way to guarantee a trustable data collection is:

- get the data to be collected from a source
- check the correctness of the collected data
- transform the collected data into a representation that can be proved to be authentic

The whole operation sequence has to take place in a trustable environment (“Trusted Point”).
The problem of authentic data collection

Analogy to the method ensuring an authentic data collection process.

Secure Chamber

= Authentic Data Collection Device

Regent

= User

Knight

= Data

Suite of Armor

= Cryptographic Methods

Data presentation enabling a verification of the authenticity
Authentic Data Collection Device

Common keyboard extended with the following additional units:

- Card reader
- Crypto unit
- Radio controlled clock and GPS receiver
- Video unit to fade in a data display over the regular video signal of the computer
- RS232 interface
Mobile Authentic Data Collection Device

Design issues of the Mobile Authentic Data Collection Device:

- same basic feature as the ADD
- high flexibility in interoperation with different kind of devices
- intuitive and easy to use Man Machine Interface
- providing a trustworthiness environment for different applications
- functional networked services (e-payment, contract supervision)
- approved and standardized hardware based to be used as mobile device
- memory card interface
- optionally: advanced person identification mechanism
Mobile Authentic Data Collection Device

Hardware base is a PDA driven by linux that

- can exchange data with external devices via a bluetooth-, infrared-, keyboard-, serial- and USB-interface.

- can interoperate with man via an LCD-display, microphone, speaker, writing with an stylus an the display or an external connected device (e.g. keyboard)
Mobile Authentic Data Collection Device

Hardware and functional extensions of the Linux PDA are:

- an integrated smart card reader
- integrated radio driven clock and GPS receiver
- optional integrated biometric sensors
- only data with a authentic provable data representation can leave the MADD via any device interface.
- executable code cannot be loaded on the PDA by a user
- verification mechanism to check whether authentic hard- and software function is given or not
- case is protected to detect any mechanical manipulations
Outlook and future work: E-contracting services

1. step: is done by establishing the usage of certificates, smart-cards and authentic data collection!

2. step: processes have to be defined which ensure that e-contracts can be handled like old fashioned ones in respect of law. Therefore secure processes are needed to archive the contracts to be applicable in a legal case.

3. step: these services have to be established to be available for everyone and for every kind of legal declarations.
Contact and References

Contact:  tjw@prz.tu-berlin.de,

http://www.prz.tu-berlin.de/~tjw/

References:

