VESZPROG

Vulnerabilities of the usage of digital signature

Dr. Ferenc Leitold
fleitold@veszprog.hu

Pannon University - Veszprog Ltd.
HUNGARY

Vulnerabilities of the usage of digital signature

- NOT related to the mathematical basics
- Related to the typical usage only

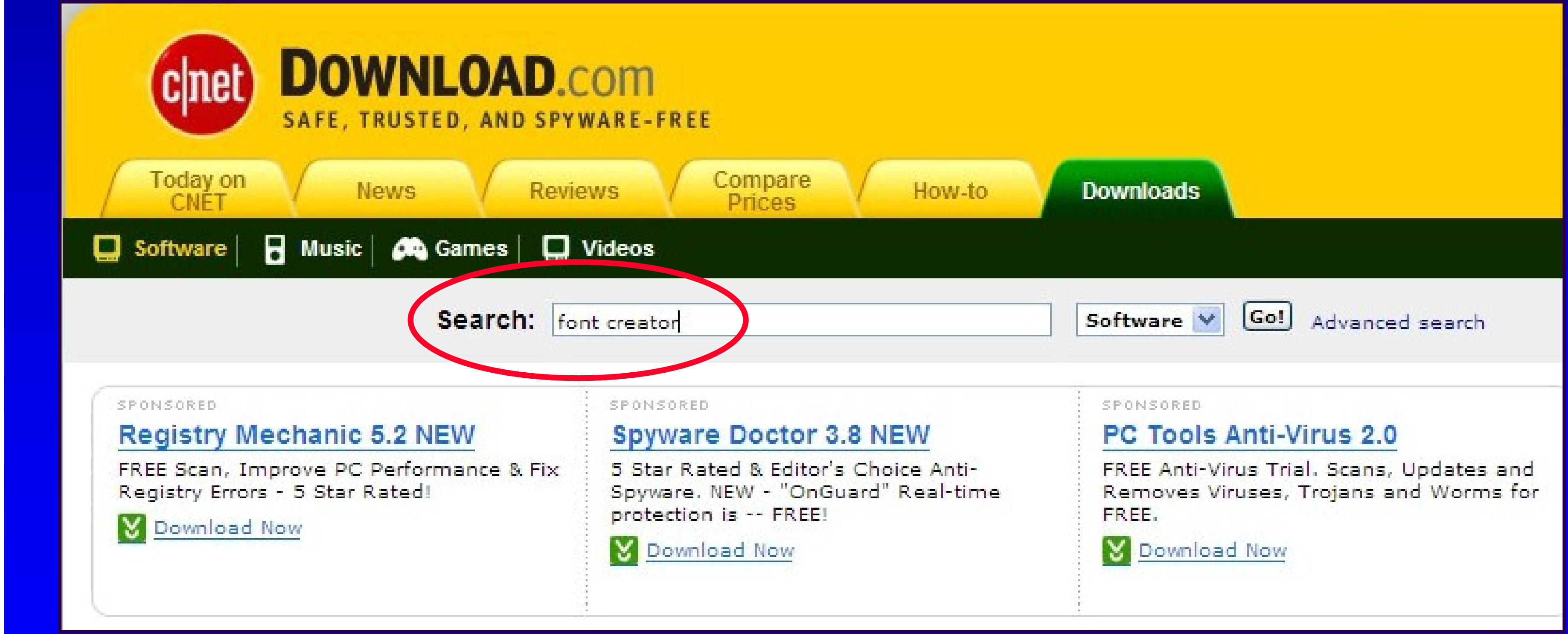
Contents

VESZPROG

- Demonstration
- Traditional signature vs. digital signature
- Attack possibilities
- Transmission of signed documents
- Conlusions

Demonstration

VESZPROG



Search: font creator

SPONSORED

Registry Mechanic 5.2 NEW

FREE Scan, Improve PC Performance & Fix Registry Errors - 5 Star Rated!

Download Now

SPONSORED

Spyware Doctor 3.8 NEW

5 Star Rated & Editor's Choice Anti-Spyware. NEW - "OnGuard" Real-time protection is -- FREE!

Download Now

SPONSORED

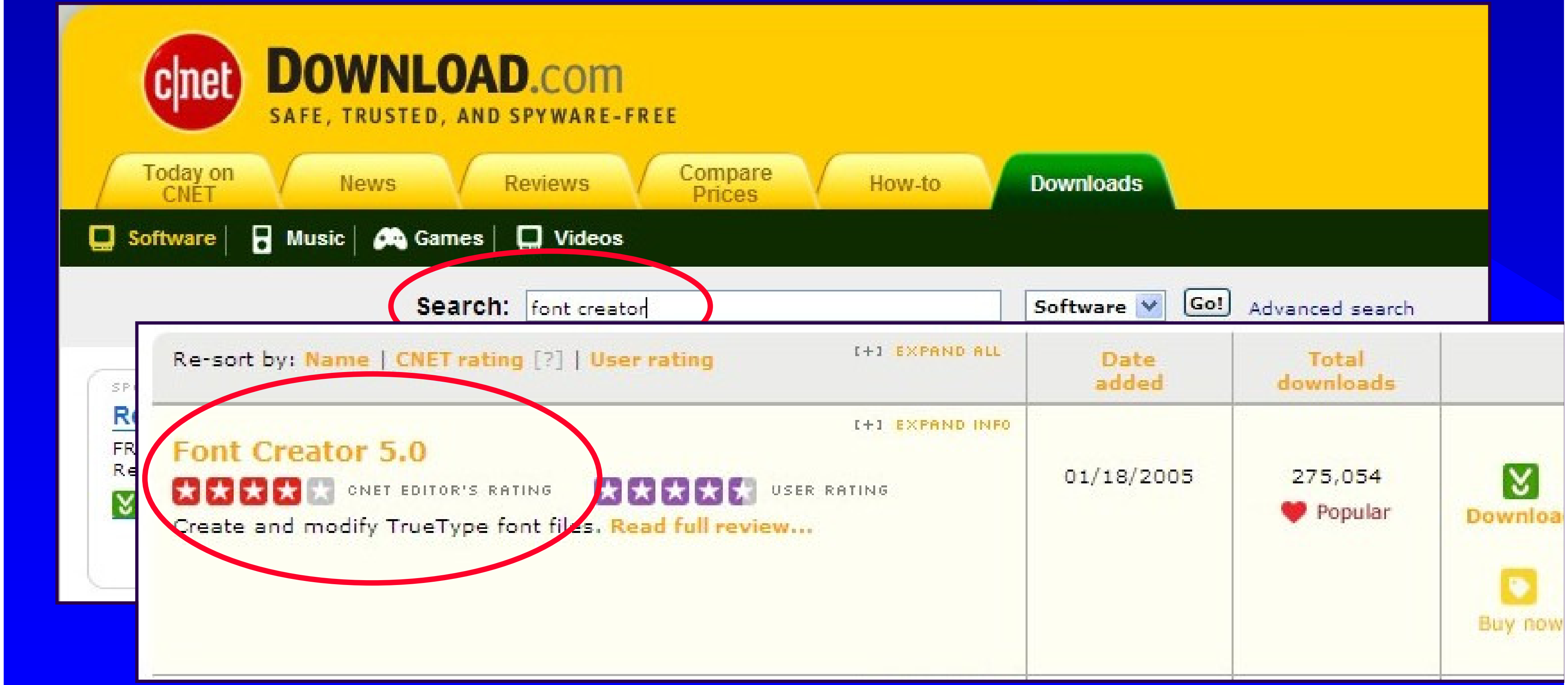
PC Tools Anti-Virus 2.0

FREE Anti-Virus Trial. Scans, Updates and Removes Viruses, Trojans and Worms for FREE.

Download Now

Demonstration

VESZPROG



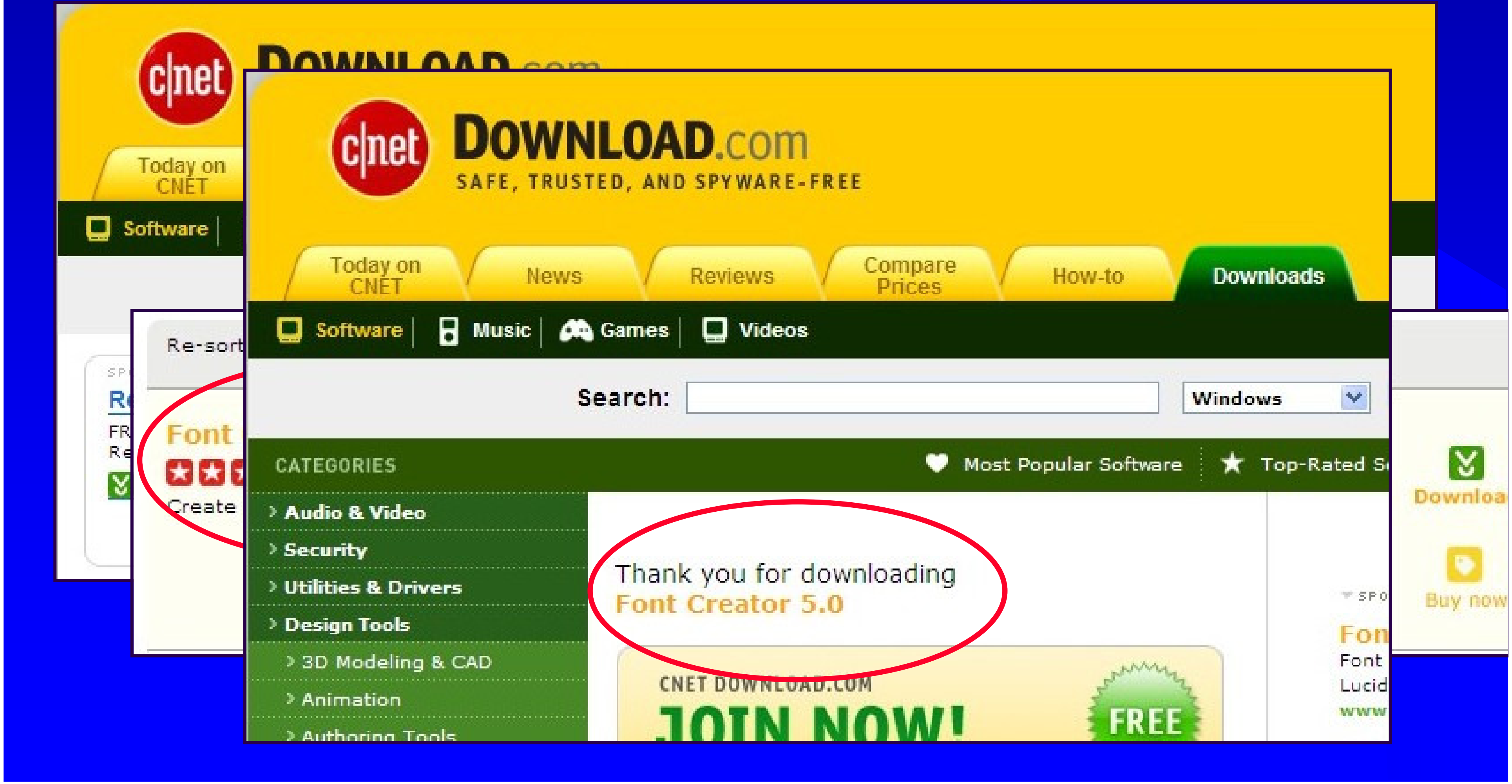
Search: font creator · Software

Re-sort by: Name | CNET rating [?] | User rating [+] EXPAND ALL

	Date added	Total downloads	
[+] EXPAND INFO Font Creator 5.0 ★★★★☆ CNET EDITOR'S RATING ★★★★☆ USER RATING Create and modify TrueType font files. Read full review...	01/18/2005	275,054 ♥ Popular	Downloa Buy now

Demonstration

VESZPROG



Thank you for downloading
Font Creator 5.0

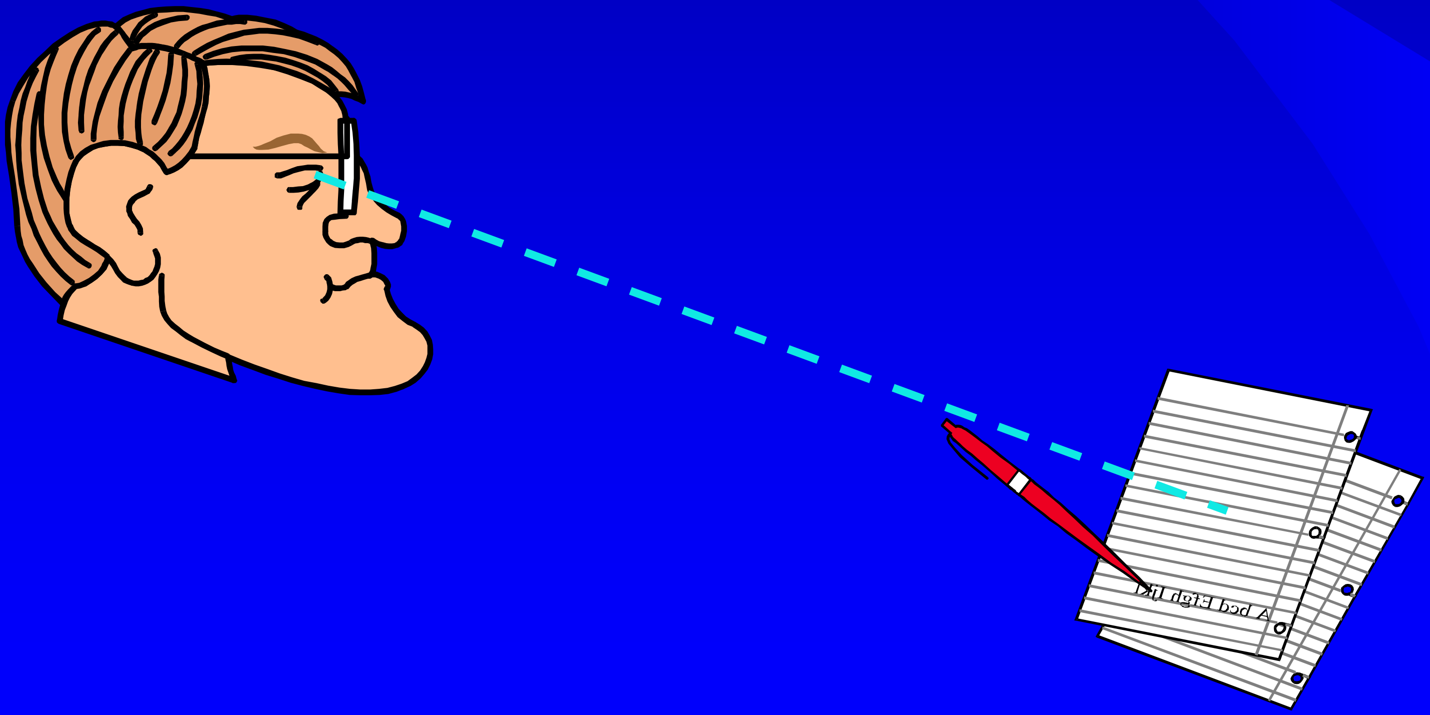
Demonstration

VESZPROG

Is there any additional security problem of digital signature against traditional signature ?

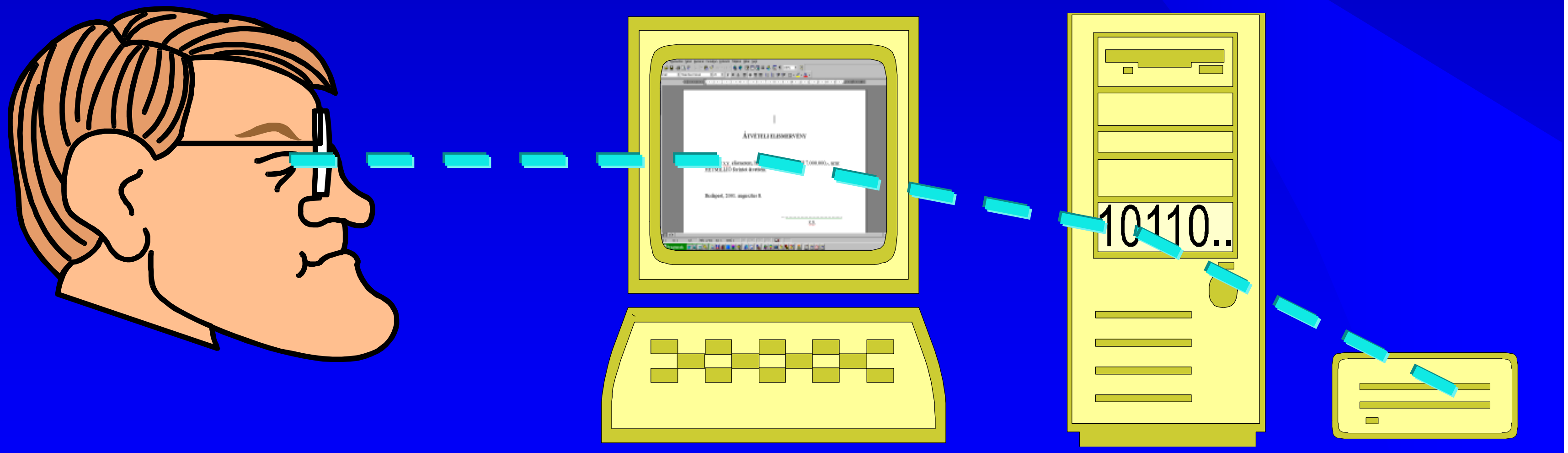
➔ YES

Traditional signature



Digital signature

VESZPROG



Some attack possibilities

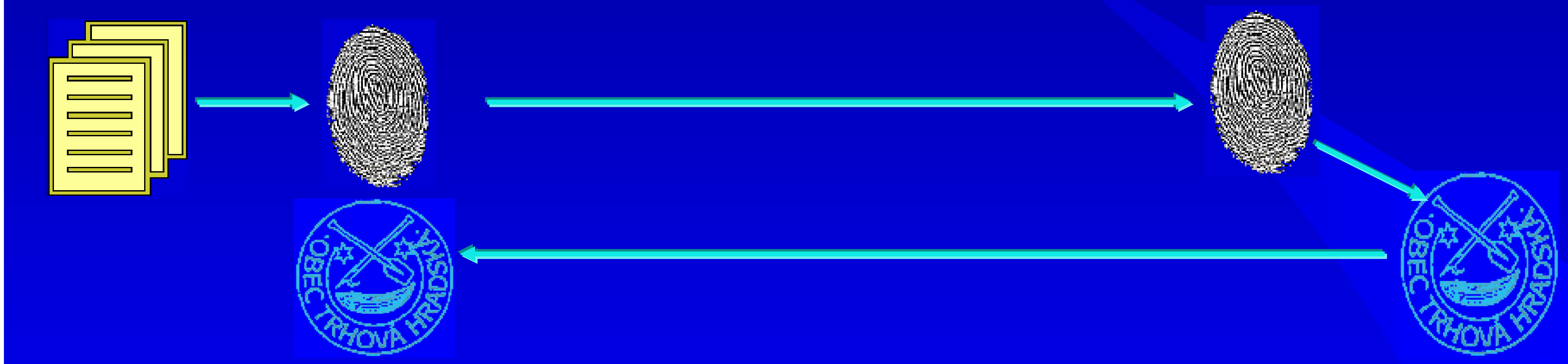
VESZPROG

- Manipulate the visualization
- Manipulate the signing process
- Using incorrect algorithms

Manipulate the visualization

- Modifying fonts
  - Windows, X: font files
  - VGA: downloading new fonts
- Automatically executed programs attached to documents (macro)
- Modifying the presentation process

Manipulate the signing process



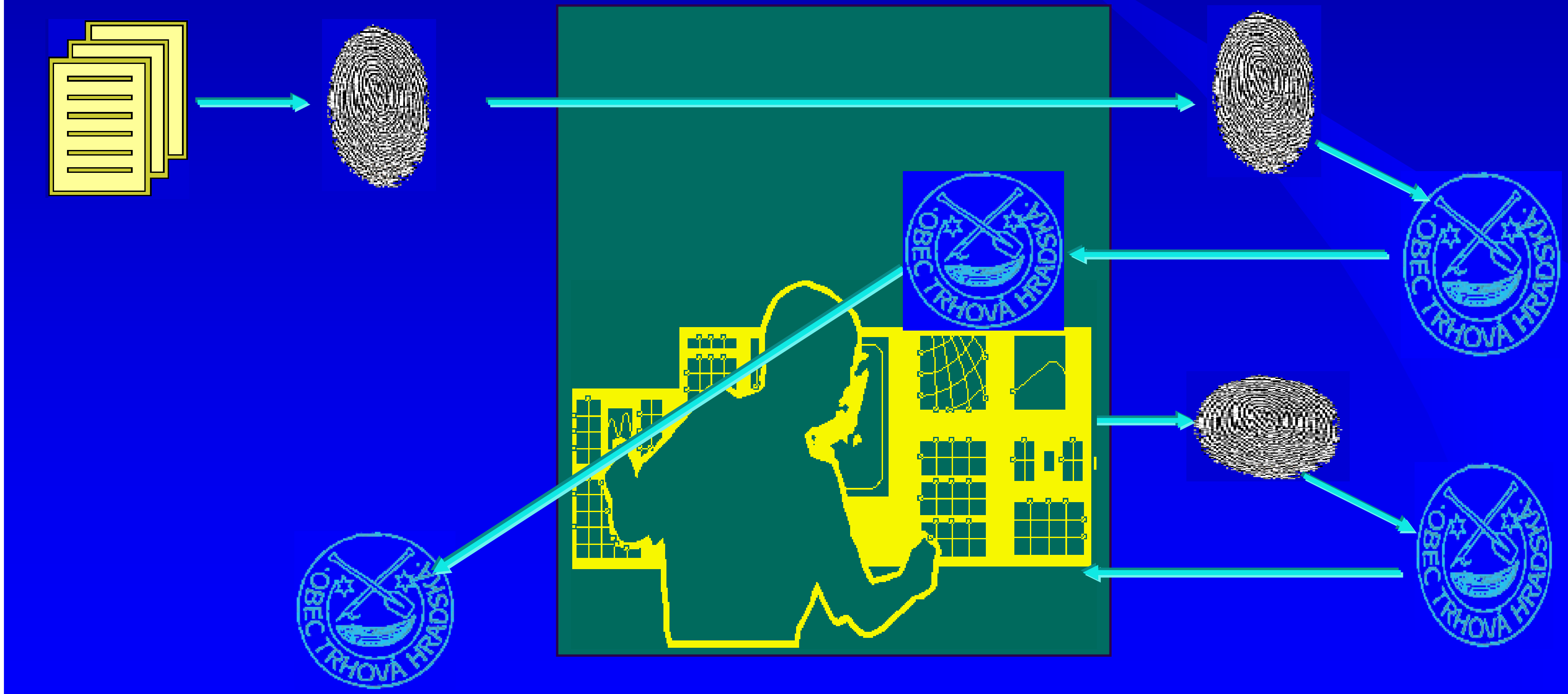
User interface

OS
(Windows)

External device

Manipulate the signing process

VESZPROG



User interface

OS
(Windows)

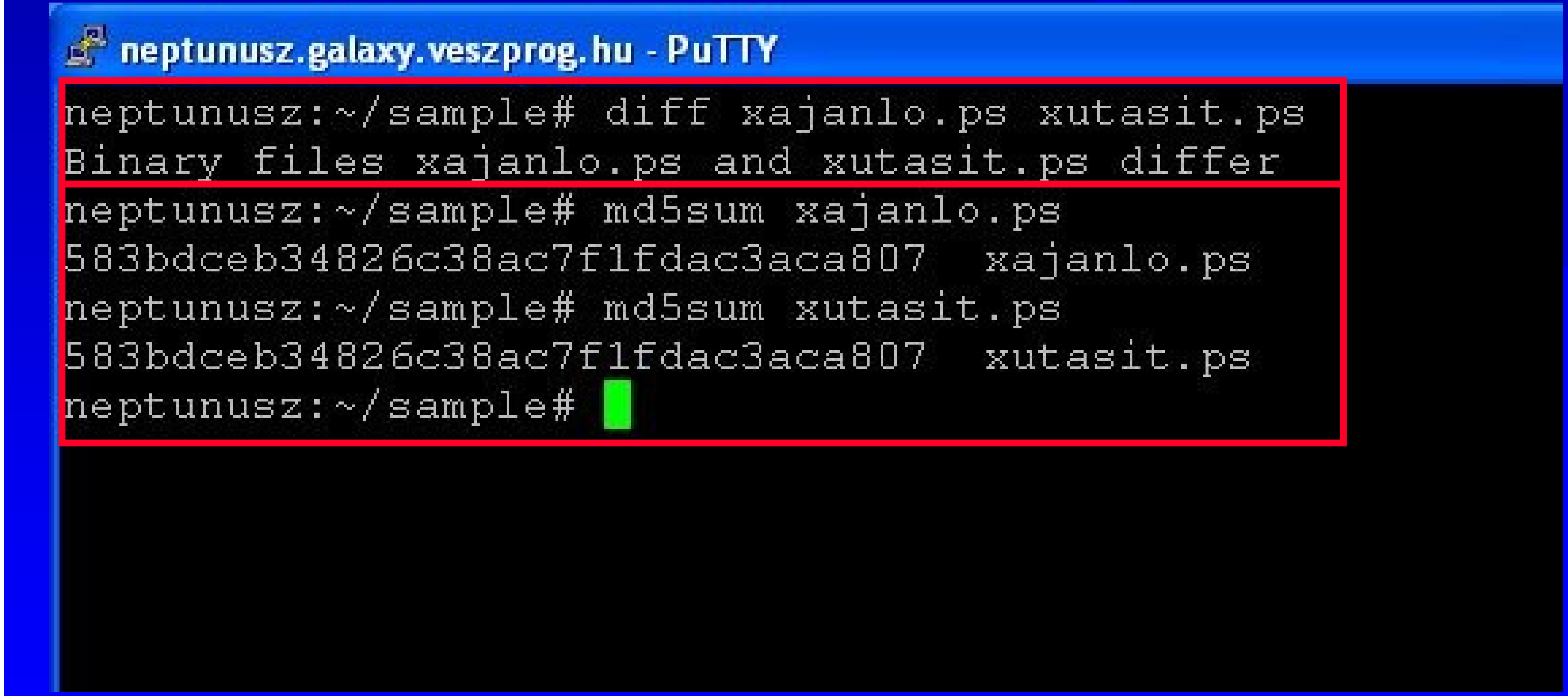
External device

Manipulate the signing process

VESZPROG

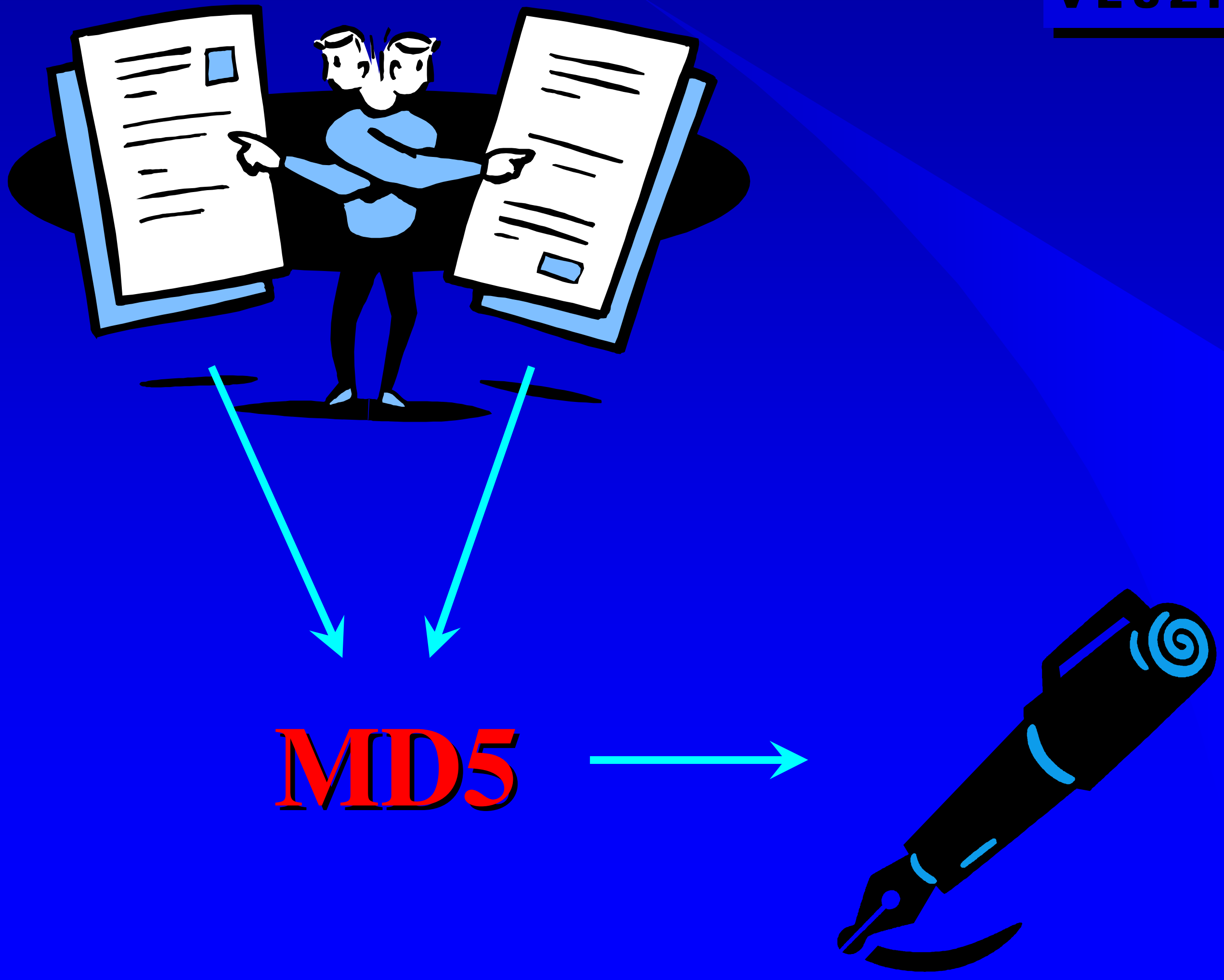
- Signing program patch
- Supervision of the communication between the application and the external device

Using incorrect algorithms



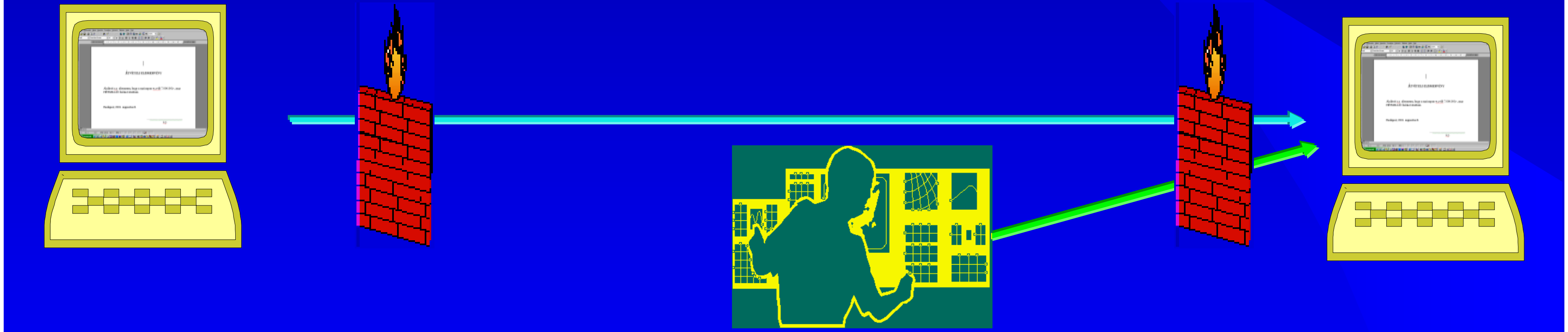
```
neptunusz:~/sample# diff xajanlo.ps xutasit.ps
Binary files xajanlo.ps and xutasit.ps differ
neptunusz:~/sample# md5sum xajanlo.ps
583bdceb34826c38ac7f1fdac3aca807  xajanlo.ps
neptunusz:~/sample# md5sum xutasit.ps
583bdceb34826c38ac7f1fdac3aca807  xutasit.ps
neptunusz:~/sample# 
```

Using incorrect algorithms



MD5

Transmission of signed documents



Using encryption or not ?

Does the firewall forward the encrypted message ?

Conclusion

VESZPROG

It is very important to know:

- exactly which document(s) will be signed,
- what kind of device is used,
- what is our purpose of the usage.

?