

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



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

Demonstration

A screenshot of the cnet DOWNLOAD.com website. The page has a yellow header with the cnet logo and the text "DOWNLOAD.com SAFE, TRUSTED, AND SPYWARE-FREE". Below the header are navigation tabs for "Today on CNET", "News", "Reviews", "Compare Prices", "How-to", and "Downloads". A dark green bar contains icons for "Software", "Music", "Games", and "Videos". A search bar is highlighted with a red circle, containing the text "font creator". To the right of the search bar are buttons for "Software", "Go!", and "Advanced search". Below the search bar are three sponsored software listings: "Registry Mechanic 5.2 NEW", "Spyware Doctor 3.8 NEW", and "PC Tools Anti-Virus 2.0". Each listing includes a brief description and a "Download Now" button with a green checkmark icon.

cnet **DOWNLOAD.com**
SAFE, TRUSTED, AND SPYWARE-FREE

Today on CNET | News | Reviews | Compare Prices | How-to | **Downloads**

Software | Music | Games | Videos

Search: font creator | Software | Go! | Advanced search

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



cnet **DOWNLOAD.com**
SAFE, TRUSTED, AND SPYWARE-FREE

Today on CNET | News | Reviews | Compare Prices | How-to | **Downloads**

Software | Music | Games | Videos

Search: Software Advanced search

Re-sort by: Name CNET rating [?] User rating	[+] EXPAND ALL	Date added	Total downloads	
Font Creator 5.0 CNET EDITOR'S RATING USER RATING Create and modify TrueType font files. Read full review...	[+] EXPAND INFO	01/18/2005	275,054 Popular	Download Buy now

Demonstration



A screenshot of the CNET Download.com website. The page has a yellow header with the CNET logo and "DOWNLOAD.com" text. Below the header is a navigation bar with buttons for "Today on CNET", "News", "Reviews", "Compare Prices", "How-to", and "Downloads". A secondary navigation bar includes "Software", "Music", "Games", and "Videos". A search bar is present with a "Windows" dropdown menu. On the left, a "CATEGORIES" sidebar lists various software types. The main content area displays a message: "Thank you for downloading Font Creator 5.0", which is circled in red. Below this message is a "JOIN NOW!" button with a "FREE" badge. On the right, there are "Download" and "Buy now" buttons. The overall layout is clean and organized, typical of a software download portal.

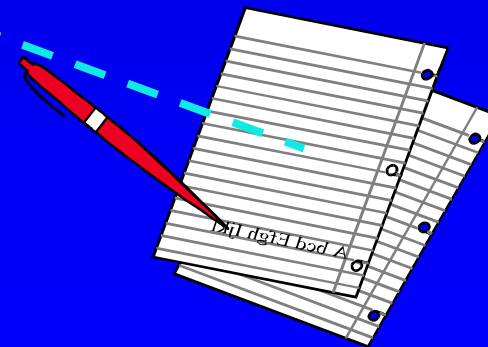
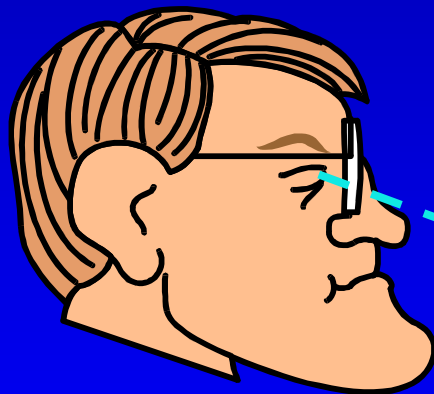
Demonstration



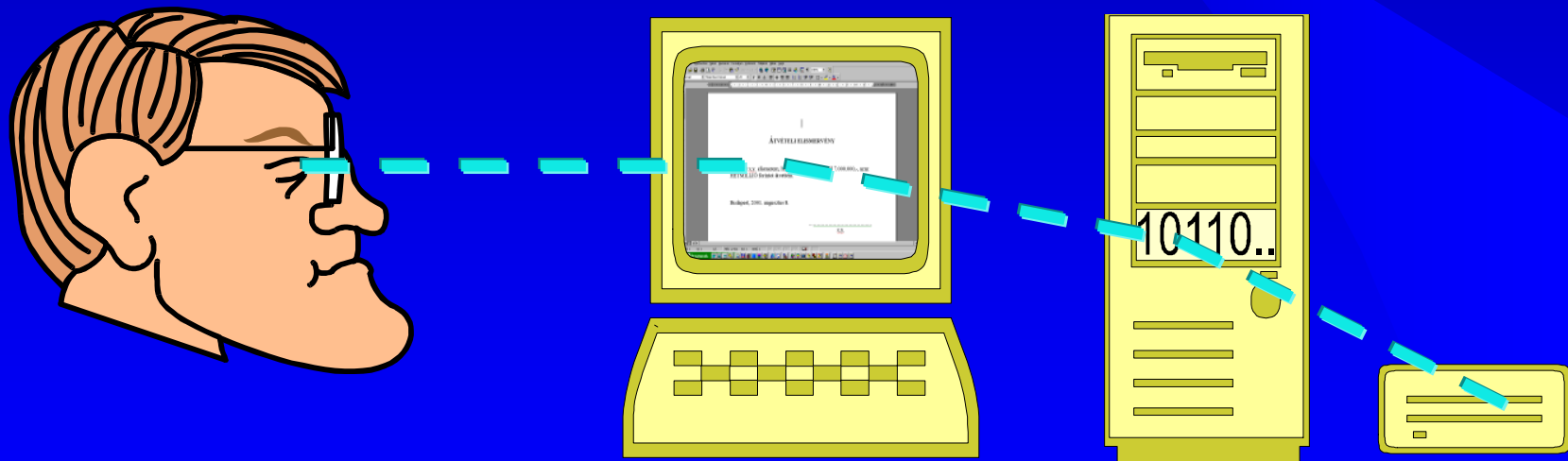
Is there any additional security problem of digital signature against traditional signature ?

→ YES

Traditional signature



Digital signature



Some attack possibilities



- **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



User interface

OS
(Windows)

External device

Manipulate the signing process



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

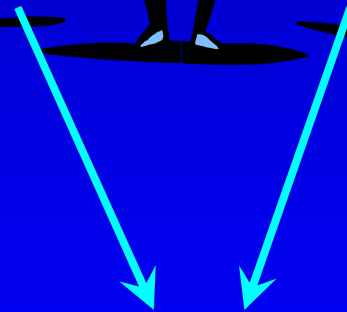
Using incorrect algorithms



neptunusz.galaxy.veszprog.hu - PuTTY

```
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



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.**

