10 PRINT “V.A.C. - INSECURE”
20 PRINT “DIRECT OBJECT”
30 PRINT “REFERENCE”
RUN

Marinus Kuivenhoven
OWASP Dutch Chapter Meeting
11-03-2010

Commodore 64

SOGETI

Commodore 1541

SOGETI

Asymmetrisch gedrag

SOGETI

Asymmetrisch gedrag

SOGETI

Kopieerbeveiliging

- **Asymmetrisch gedrag verhogen**
  - > **Kosten media maken en media afspelen**

SOGETI

Asymmetrie als kopieerbeveiliging

- **Kosten van media**

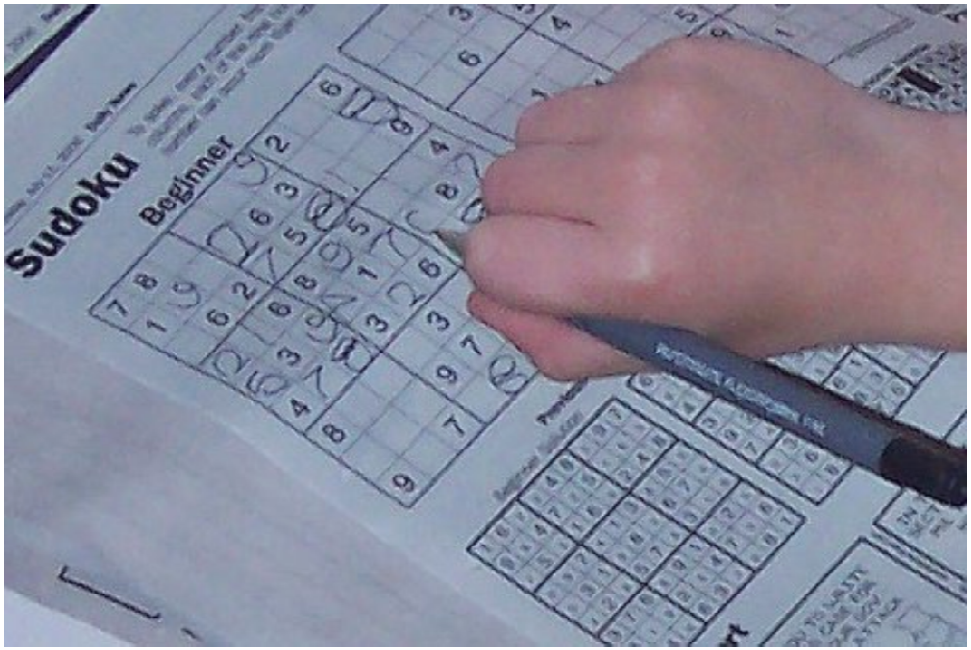
Asymmetrie als kopieerbeveiliging:

- **Metadata van media**

SOGETI

Asymmetrie als kopieerbeveiliging

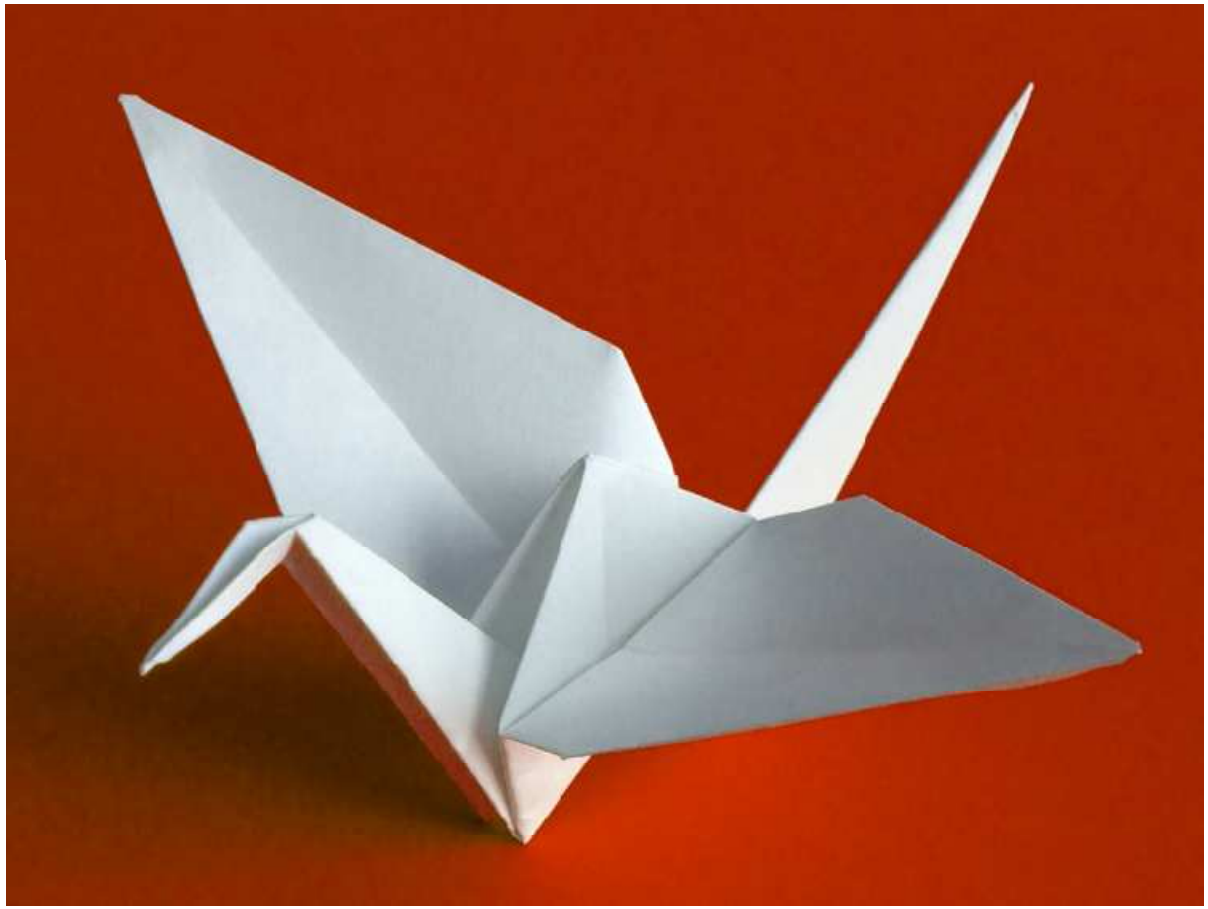
- **Integriteitscontrole in software**



SOGETI

Asymmetrie als kopieerbeveiliging

- **Hardware-afhankelijkheid**



SOGETI

Kopieerbeveiliging C64 #1

- **Bad Sector (1983)**
  - > **Opzettelijk maken van errors**

SOGETI

Kopieerbeveiliging nu

- **Playstation 2 (2000)**
  - > **Opzettelijk maken van errors**

SOGETI

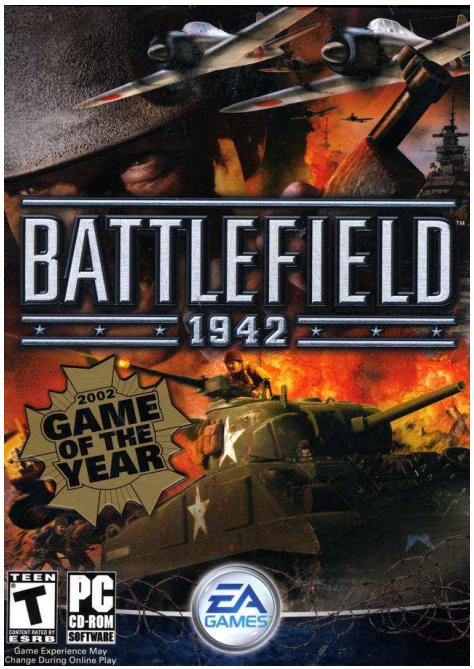
Kopieerbeveiliging C64 #2

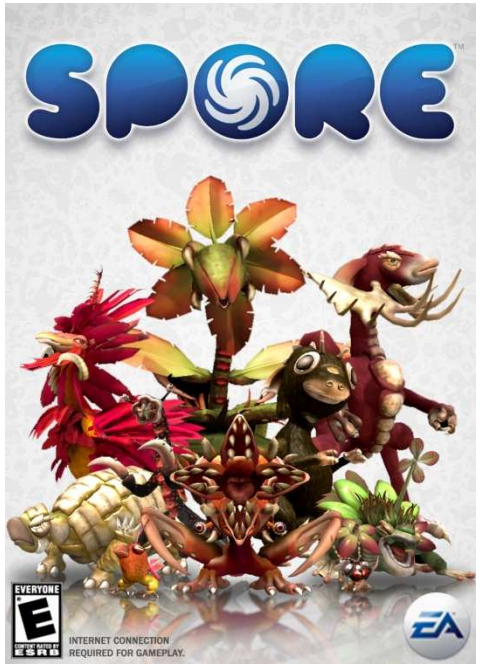
- **Gap Bytes (1985)**
  - > **Tussenruimten vullen**

SOGETI

Kopieerbeveiliging

- **PC games met SafeDisc (2002-….)**
  - > **Tussenruimten vullen**





SOGETI

Kopieerbeveiliging C64 #3

- **Trackalignment (1987)**
  - > **Afwijkend na elkaar plaatsen**

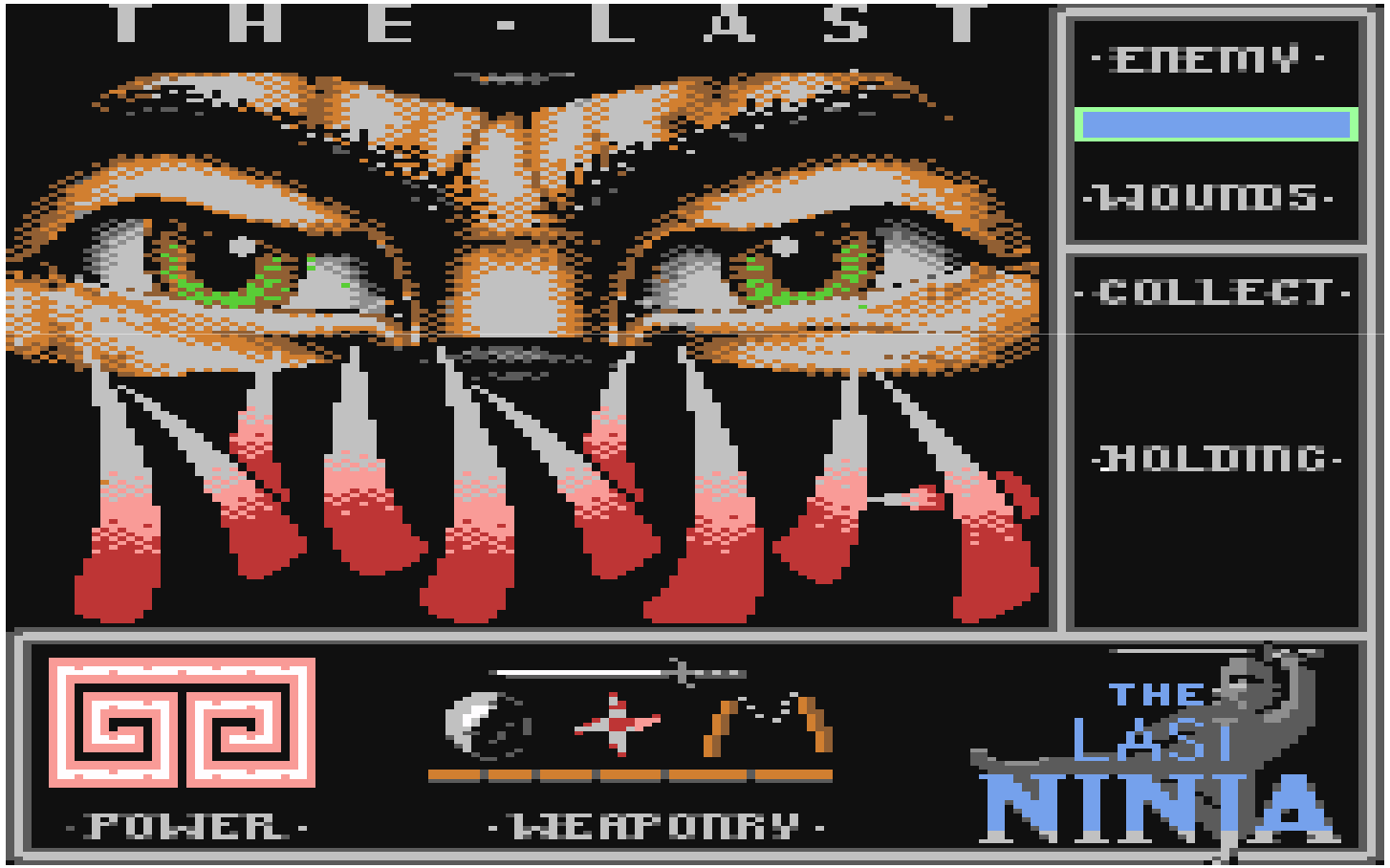
SOGETI

Kopieerbeveiliging nu

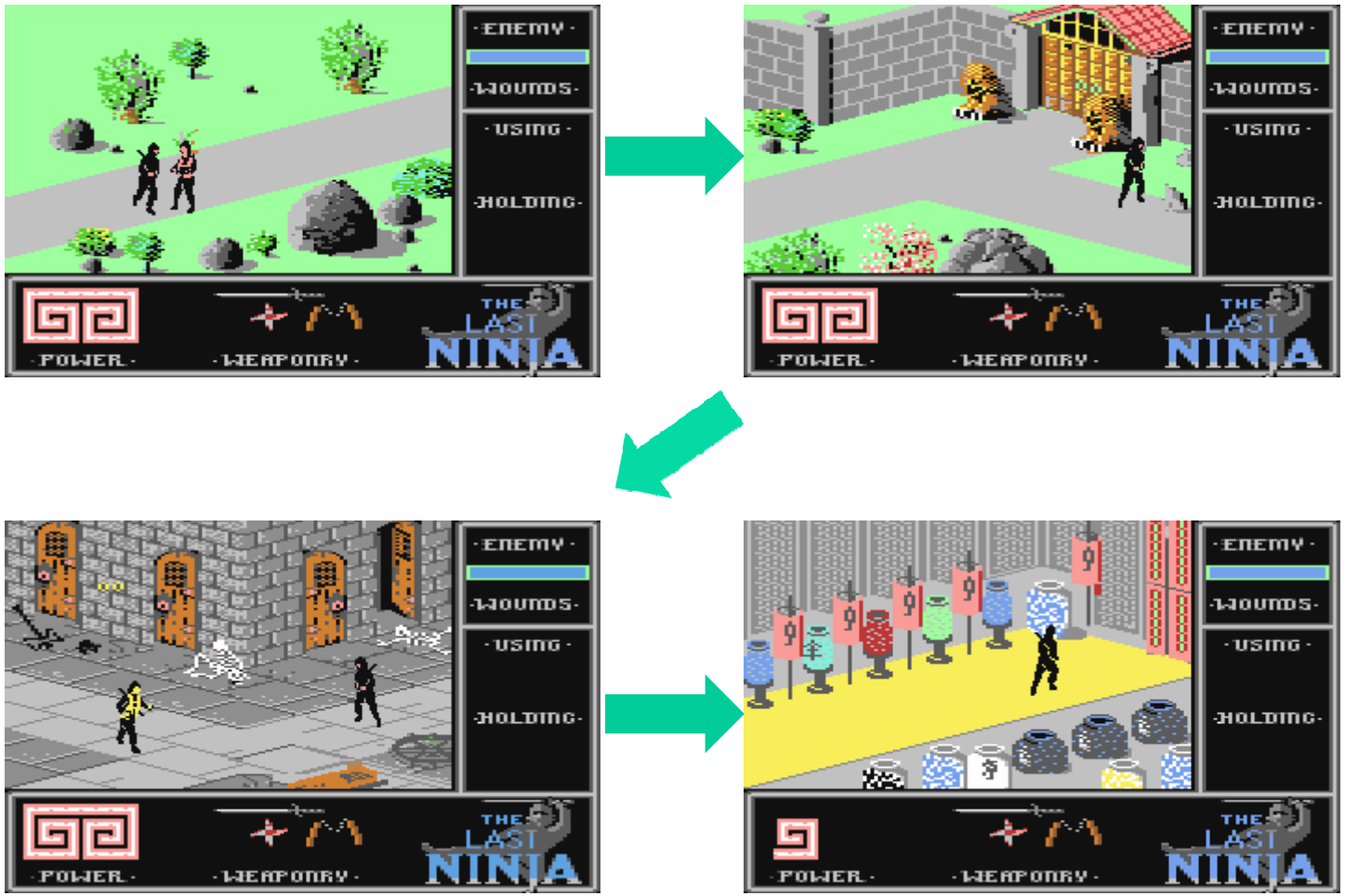
- **XBOX 360 (2005)**
  - > **Afwijkend na elkaar plaatsen**

SOGETI

Last Ninja


THE LAST NINJA
ENEMY
WOUNDS
COLLECT
HOLDING
POWER
WEAPONRY
THE LAST NINJA

Last Ninja



SOGETI

Last Ninja

SOGETI

Last Ninja

SOGETI

Vulnerability:IDOR

Insecure Direct Object Reference

:

Input

zorgt voor

(een deel van)

een naam

van een resource.

SOGETI

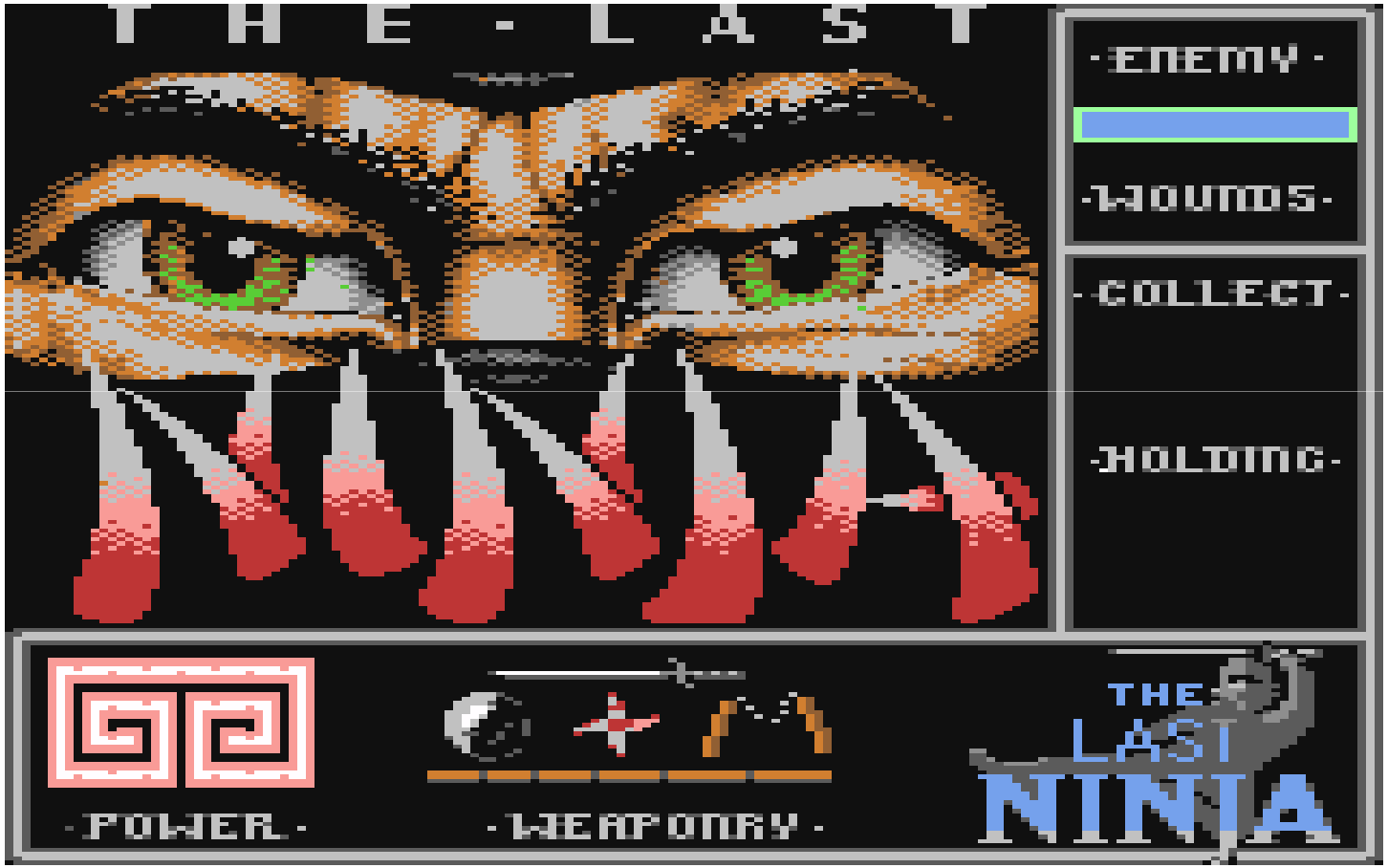
Assessment:IDOR

/genpage.php?picture=party5.jpg

/txt2pdf.jsp?filepath=\txt\doc.txt

/myaccount.asp?account=273635

Last Ninja



Autorisatie

SOGETI

Last Ninja 2

Validatie

SOGETI

Last Ninja 3

Referentie

SOGETI

Countermeasure: IDOR

- **Controleer autorisatie op objecten**
  - **Gebruiker, in rol, in fase, ect.**
- **Valideer aangeleverde parameters**
  - **Whitelist middels een map**
- **Voorkom blootstelling**
  - **Geen PK's, bestandsnamen, ect.**

Countermeasure: IDOR

CLIENT:

```
<select name="dropBoxFiles">
    <option value="S6bn03j">Vergadering_met_Ma</option>
    <option value="83HJse3">Rapportage_wk14</option>
    <option value="x9Sdr21">Overzicht_nieuweklanten</option>
</select>
```

SERVER:

Gebruiker: X, Rol: Y, Proces: Z, Stap: A

S6bn03j => /u01/files/vergadering_met_ma.doc
83HJse3 => /u01/files/Rapportage_wk14.wrt
x9Sdr21 => /u01/files/overzicht_nieuweklanten.pdf

SOGETI