Internet Maladies (Partie Deux)

Ronald L. Chichester

HIPLA Conference

Galveston, Texas

October 1, 2010

Last Year...

* **Identity Theft**

* **Phishing Scams**

* **Botnets**

* **Designer Botnets (coming)**

This Year...

- **Designer Botnets (arrived)**

- **Cloud Computing**

- **PDF Exploits**

- **Flash Exploits**

- **Social Network Exploits**

Botnets

Designer Botnets

Point

Click

Exploit!

Cloud Computing

Cloud Computing

* **Security**

* **Who owns the data?**

* **Bailment**

* **Proprietary Format**
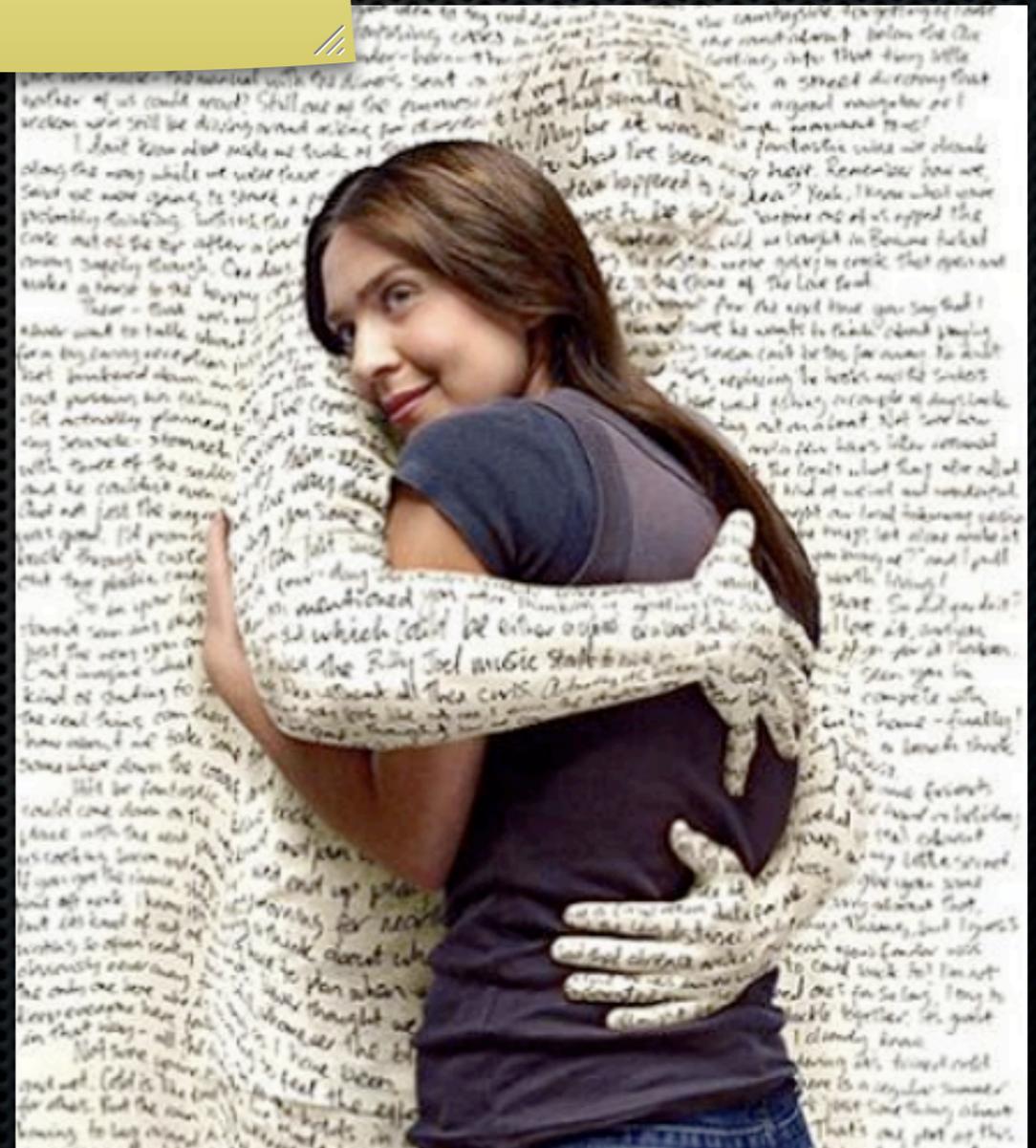
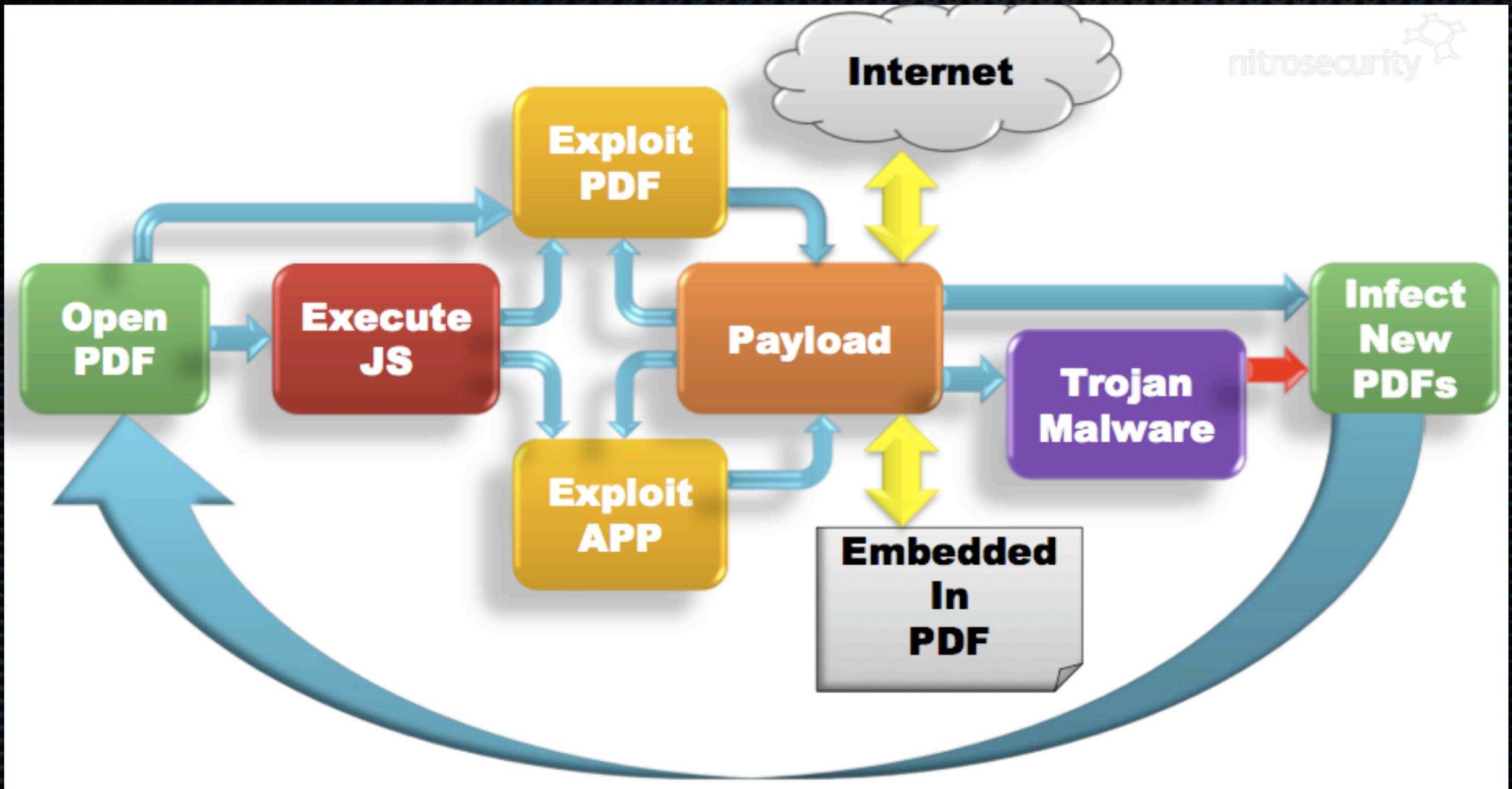 * **IP** (pre and post)

PDF Exploits

PDF Exploits

Javascript is the underlying mechanism for the exploits
- Open PDF
- Execute Javascript
- Exploit PDF
- Payload

* **Javascript**
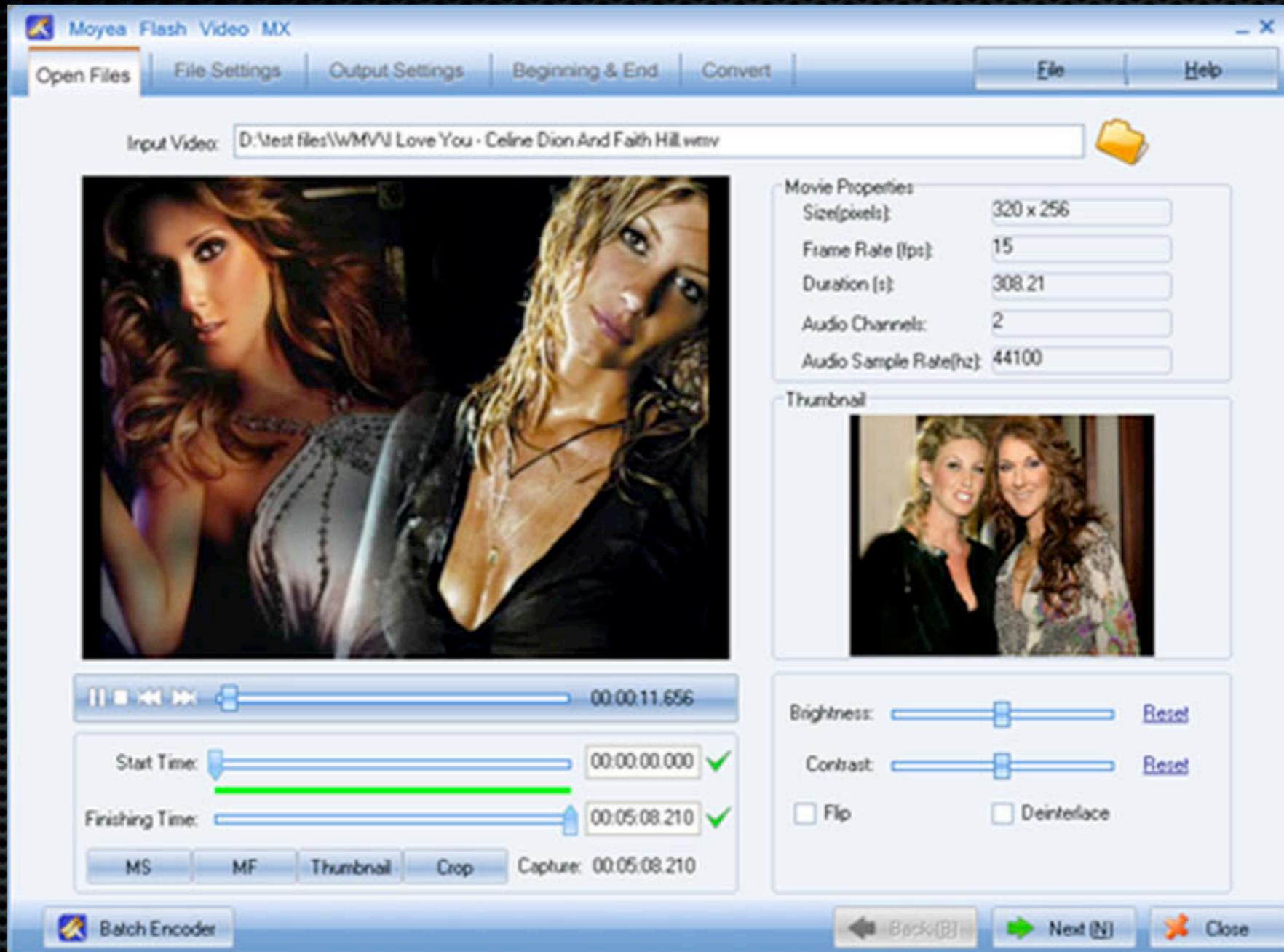
* **Incremental Updates**

* **Worms/Viruses**

PDF Exploitation Process

PDF Exploits

Helpful tools:
  pdf-parser.py
  Malzilla
  Script-Fu
  pdftk
  Hex-editor
  Spider Monkey

- **Free Tools**

- **Linux / OS X**

- **Trust PDF's ???**

Flash Exploits

Flash Exploits

- **Very Capable SDK**
- **Video & Microphone**
- **Flash Cookies**

Social Networking

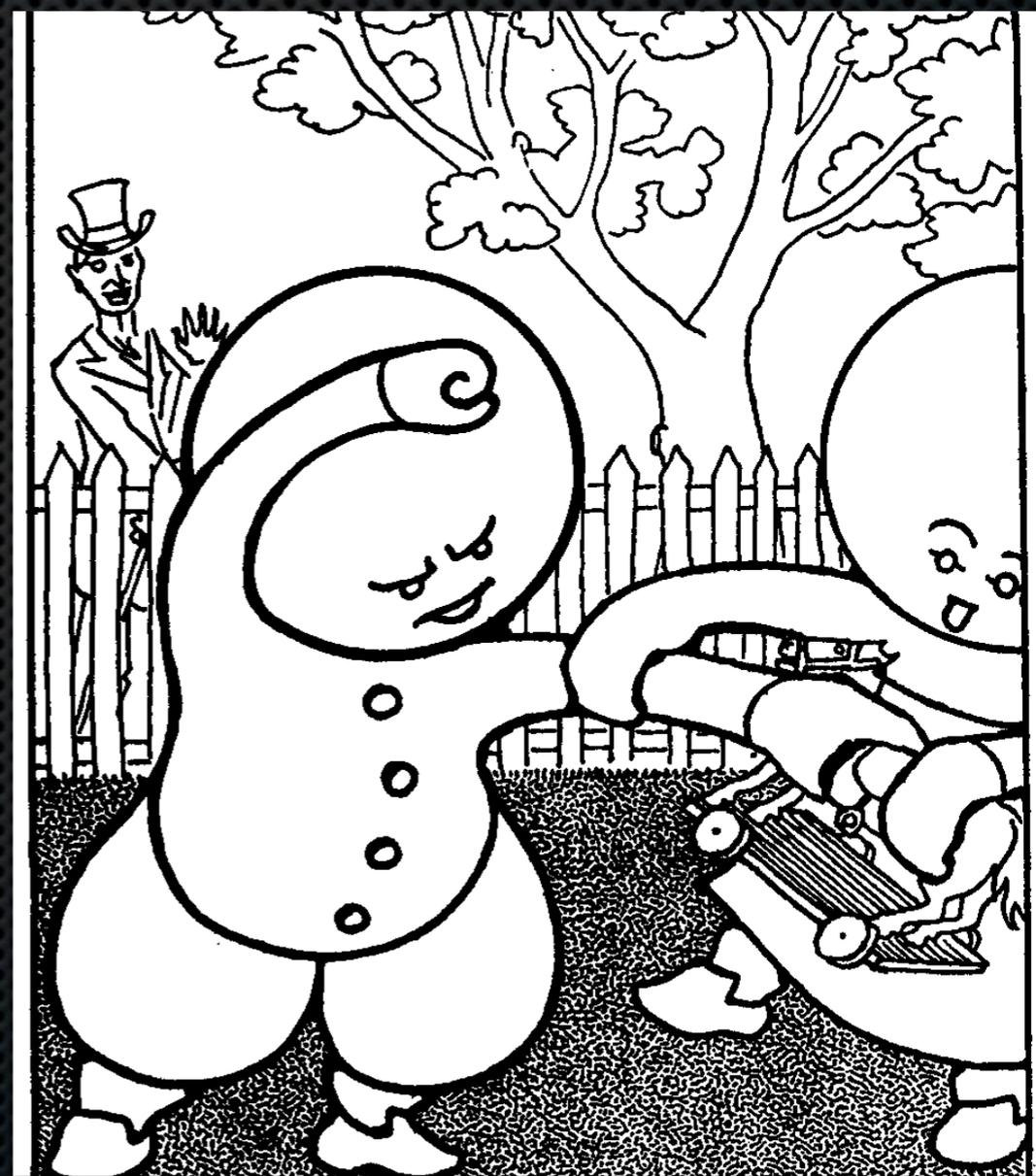# Social Networking Exploits

- **Clickjacking**

- **Much More...**

© Hank Grebe
www.mediaspin.com

Attacked website is transparent

Fake input controls positioned under the hijacked web controls

User provides username and password.
All these clicks are hijacked by the invisible frame.
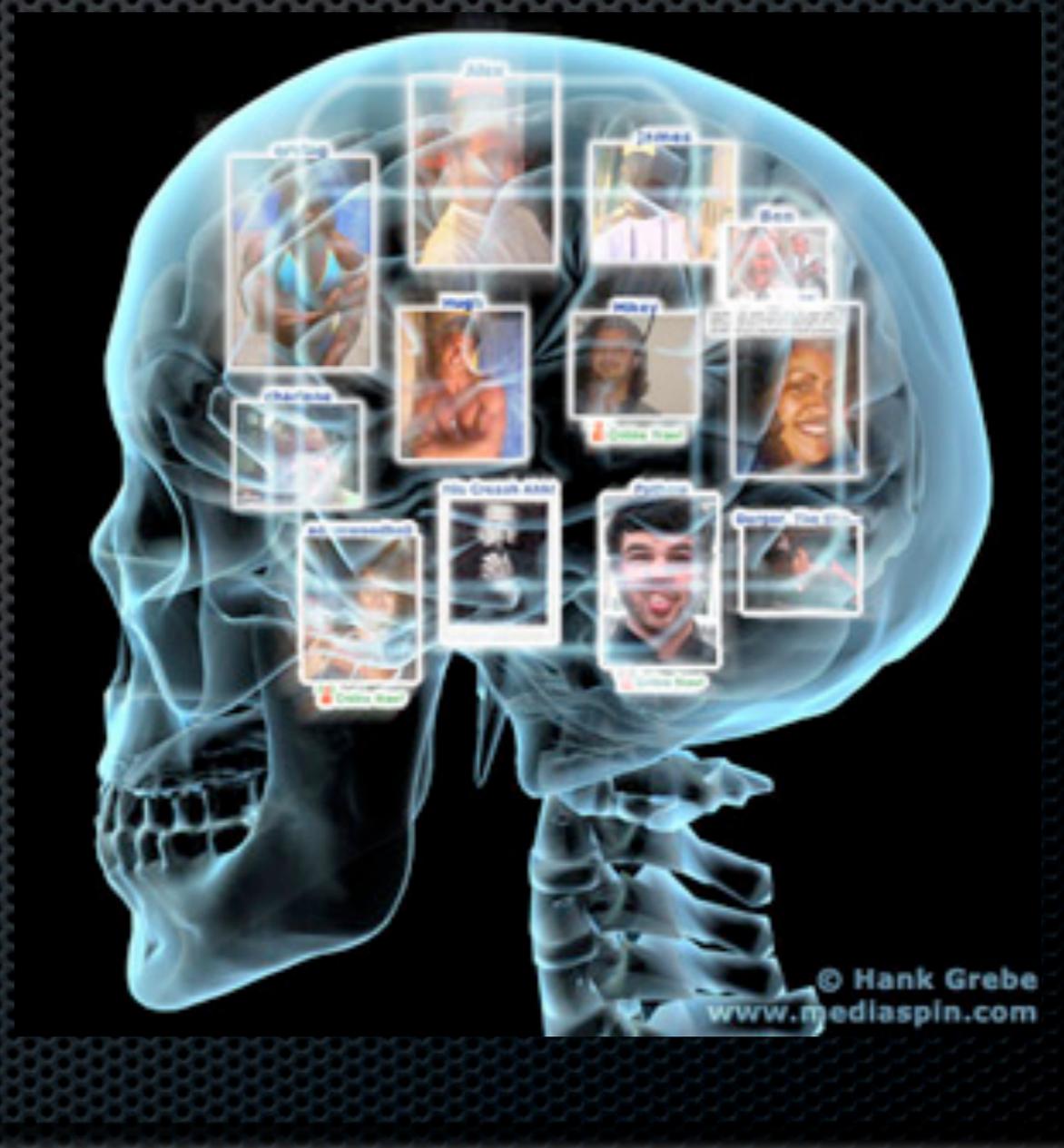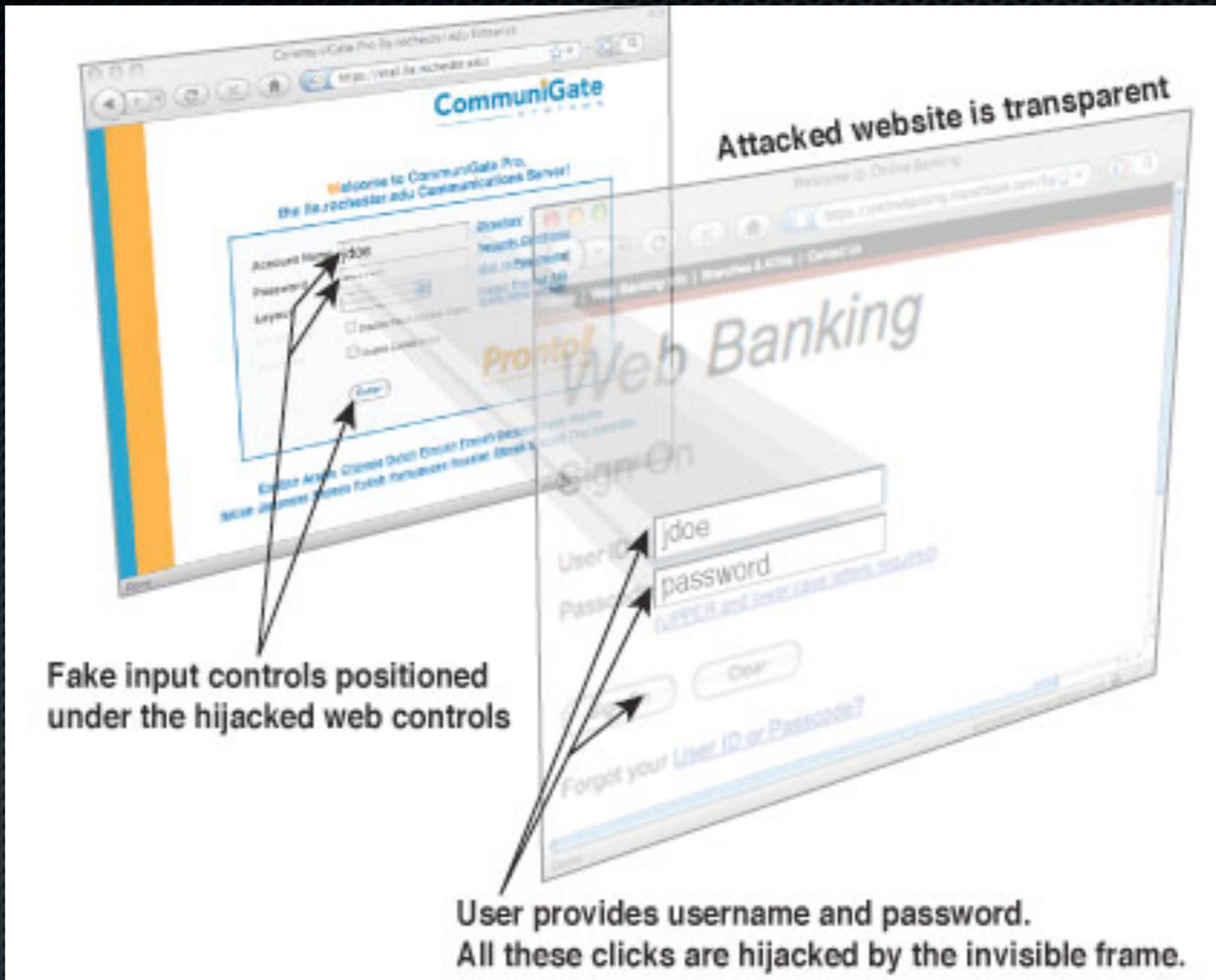
Clickjacking

Social Networking Exploits

- **Account Hijacking**

- **Numerati / Privacy**

- **SPAM / Malware**

- **Cyberbulling**

- **Social Engineering**

- **Crimes**

www.txcomputerlaw.com