Informatics and Sustainability

Internet and Reality – The real and the fake in the digital age
HS2015 / Prof. Dr. M. Hilty

Hernani Marques Madeira <h2m@access.uzh.ch>
Matthias Scherrer <matthias.scherrer@uzh.ch>
Florian Schüpfer <flo.schuepfer@bluewin.ch>
Digital Image Doctoring
Digital Image Doctoring
Cloning

- Technique
  - copy and pasting of objects
- Artifacts
  - repeating patterns in image
- Detection
  - find similar and spatially coherent image regions
Lighting

- Technique
  - move objects from one setting to another

- Artifacts
  - inconsistent light direction

- Detection
  - estimate direction of light by brightness distribution on surfaces
  - detect inconsistencies
Re-touching

- Technique
  - adjusting colors / contrast / white balance, sharpness, noise, removing elements or visible flaws on skin or materials

- Artifacts
  - distorted correlations in color-sensor array

- Detection
  - detect wrong correlations
Negative Effects

Propaganda
(for / against persons or topics)
Negative Effects

Alteration of history (removing objects or persons from historical images)
YouTube views – fake or real?
Advertisment on YouTube

- Enable AdSense on the account (account monetization)
- 45/55 split of all YouTube advertising
  - 45% for Google
  - 55% for the content creator
- Average cost per thousand YouTube views (2013): $ 7.80
Winners and Losers of fake views

- Advertisers are charged on the basis of how many times their advertisements are viewed.
- Winners:
  - (Google that charges for the advertisement)
  - Content creators who get a part of these revenues and probably more popularity than they would without boosting their view count.
- Losers:
  - Advertisers who pay for fake views → click fraud or “invalid traffic” as Google prefers to call it
How to fake YouTube views?

- Low-wage work force
- Purchase fake YouTube views
- Purchase or program a bot/algorith to increase the traffic figures:
  - $250 billion spent by advertisers for marketing each year from which they probably lose $6 billion to such bots/algorithms
Not only YouTube views . . .

– . . . can be bought, also comments, likes, etc.
– A lot of other services can be bought as well.
Conclusion on digital frauds

- Advertisers lose a lot of money through fake YouTube views and other digital frauds.
- Google tries to filter this “invalid traffic” in order to not lose their credibility.
- How much trust should we – the people – put in what digital service providers tell us?
Malware and (computer) trust
Types of malware

- Computer viruses (or worms)
- Trojan horses (when for governments: (euphemistically) GovWare)
- Scareware
- Spyware
- Adware
- Ransomware
Example: scareware business

- Software which scares users and creates incentives to carry out payments (e.g. to buy fake Anti-Virus (AV) software).
- Three main ways of infection
  - Social engineering
  - Drive-by downloads
  - Installation via botnets
- In an investigation (Stone-Gross et al. 2011) of three fake AV criminal networks, following figures emerged, for observation times of 3 months (AV1), 16 months (AV2) and 30 months (AV3):

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Prices</th>
<th># infections</th>
<th># sales</th>
<th>income/month</th>
</tr>
</thead>
<tbody>
<tr>
<td>AV1</td>
<td>$ 50–70</td>
<td>8.4 millions</td>
<td>189k</td>
<td>$ 3 millions</td>
</tr>
<tr>
<td>AV2</td>
<td>$ 50–90</td>
<td>6.6 millions</td>
<td>137k</td>
<td>$ 313k</td>
</tr>
<tr>
<td>AV3</td>
<td>$ 60–100</td>
<td>91.3 millions</td>
<td>1.97 millions</td>
<td>$ 3.9 millions</td>
</tr>
</tbody>
</table>
Example: Trojans / GovWare lowering IT security

Swiss Federal Department of the Environment, Transport, Energy and Communications (DETEC) created (disclosed) malware to intercept Skype calls (Mini-/MegaPanzer); showing e. g. ways to undermine IT security.
Example: Trojans / GovWare fabricating evidence

Hacking Team’s Galileo Trojan Horse for Governments (GovWare) was leaked; showing e. g. ways to fabricate evidence.

```python
ELEM_DELIMITER = 0xABADCODE

def content(*args)
    hash = [args].flatten.first || {}

    process = hash[:process] || ['Explorer.exe\0', 'Firefox.exe']
    process.encode!("US-ASCII")

    path = hash[:path] || ['C:\\Utenti\\pippo\\pedoporno.mpg']
    path = path.to_utf16le_binary_null
```
How to trust trust?

– Pre-infected hardware (infected chips, firmware etc.)
– Pre-infected operating systems (system level backdoors)
– Backdoor-containing compilers
  – Cf. Ken Thompson (1984) on “Reflections on Trusting Trust” describing a compiler level backdoor, inserting (and such preserving) itself when compiling future compiler versions.
Example: Spyware appearing in App repositories

XcodeGhost: Manipulated Software Development Kits (SDKs) introduced malware into Apple’s App Store (and Google Play).

Apple Bans 100s Of iPhone Apps For Stealing Personal Data

Apple announced yesterday that it had pulled hundreds of apps from its App Store because they violated the App Store’s review process by collecting unapproved kit of data.

A third-party analytics service called SourceDNA discovered that apps using a software developer kit (SDK) from a Chinese advertising platform called Youmi, were collecting personally identifiable data, including email addresses, Apple IDs,
End
Questions & Comments?
Discussion questions

- What are other possibilities to fake and distribute digital information?
- What are (further) possibilities to prove/check/detect the correctness of digital information?
- What is really provable by technology (trust/control over the technology), or: can a computer be trusted in general terms?