Personal Information Leakage by Abusing the GDPR 'Right of Access'

Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax, Wim Lamotte, Ken Andries

▶▶ UHASSELT EDM

General Data Protection Regulation (GDPR) and ‘Right of Access’

GDPR

- European framework, in effect since May 2018.
- European consumers and businesses.
- Generated a lot of startups.
- Substantial monetary penalties (20 000 000 euros or 4% of turnover).

Right of Access

- Permits subjects to request all their personal information.
- For free and within a month (max. 2 months)
- Subject Access Request or Data Request (in our paper).

Research questions: Data Requests under ‘Right of Access’

- What information is requested by the organization to verify the identity of the consumer ?

- How is the requested information verified by the organization ?

- Can the requested information be forged by an adversary or can the organization be persuaded through social engineering to obtain personal information from someone else ?

- How can we improve the identity verification?

Setting up experiment

- Impersonating 2 targeted individuals as an adversary to obtain their personal information by forging data requests.
- Targeted individuals = 2 authors.
- Contacted 55 organizations, primarily based on Alexa top 50. Independently from each other.
- Classified each organization in categories: Financial, Retail, News Outlet, Entertainment, Transport & Logistics and others.

What credentials are requested or verified by the organization ?

Combinations of the following:

- Login credentials
- Email address ownership
- ID card
- Home address
- Calling subject
- Specific user data

Can we forge or extract the requested credentials ?

Email address: Forgeable

- Create similar looking email. Old concept in phishing.

mariano.dimartino@yahoo.com
mariano.dlmartino@yahoo.com

mariano.dimartino@gmail.com
mariano.dimartino@gmaíl.com

Can we forge or extract the requested credentials ?

Home address: Forgeable

- Apply some OSINT: Found for both individuals.
- Sometimes, only the city is required: social media.

Can we forge or extract the requested credentials ?

ID card

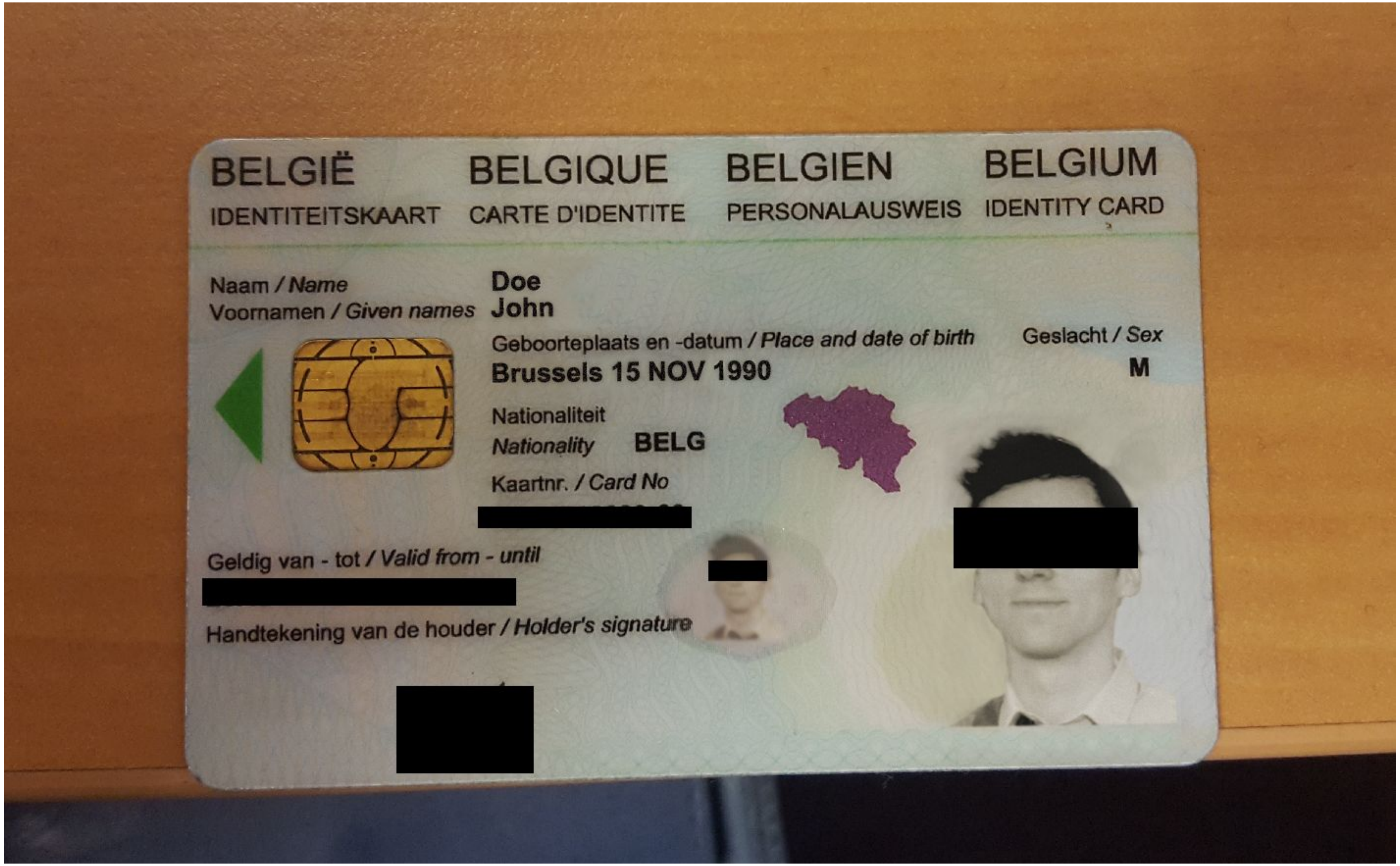
- Take picture of own ID card and photoshop name, date of birth and portrait photo of the targeted individual.

- Censor everything else.

- National Register Number and Passport ID number are rarely required, so censor it.

Can we forge the requested credentials ?

ID card: Photoshopped



BELGIË IDENTITEITSKAART

BELGIQUE CARTE D'IDENTITE

BELGIEN PERSONALAUSWEIS

BELGIUM IDENTITY CARD

Naam / *Name* Doe

Voornamen / *Given names* John

Geboorteplaats en -datum / *Place and date of birth*

Brussels 15 NOV 1990

Geslacht / *Sex*

M

Nationaliteit

Nationality BELG

Kaartnr. / *Card No*

[redacted]

[redacted]

[redacted]

Geldig van - tot / *Valid from - until*

[redacted]

Handtekening van de houder / *Holder's signature*

[redacted]

Can we persuade the organizations ?

Org: “Please send a request with an email address that is known to us.”
Adversary: “Sorry, lost access to my account due to hackers. This is the reason why I am sending a data request. Trying to get a view of all personal information that may be leaked...”
Success: 1 / 5

Org: “We sent your personal data to an email address known to us.”
Adversary: Wait until a few days before deadline -> “Didn’t receive response to data request. Deadline has almost passed.”
Success: 1 / 2

Can we persuade the organizations ?

Org: “Please send proof A,B and C to verify your identity.”
Adversary: Wait until a few days before deadline -> “Okay, here is proof A and C.”
Success: 2 / 2

Overall strategy: pressure and legal talk.

Results:

- From **55** organizations:
    - **37** accepted manual data requests
    - **14** provided an online platform to request data.
    - **4** didn’t answer at all.

- **12** out of **37** organizations leaked the personal data of the targeted individual. Falsified credentials were never questioned.
- **3** out of **37** organizations leaked the personal data of someone else.

Results:

- **Leaked data consists of:**
  - **Financial**: Timestamped financial transactions, account numbers, services bought, ...
  - **Retail**: serial numbers of products, delivery dates, products bought, …
  - **Entertainment**: profile preferences, products bought, …
  - **T&L**: Timestamped GPS locations, saved routes, purchased tickets, customer ID, …
  - **News outlets**: browsing history, profile preferences, …

Recommendations:

- **Consumers:**
  - Basic hygiene

- **Organizations:**
  - Require login credentials: significantly reduces risk (also, suggested by GDPR).
  - Strictly verifying ownership of email address.
  - Call subject and request specific user data.
  - Don’t ask for IDs!

Ethics:

- Prior written permission of University Ethical Research Committee and targeted individuals.

- Vulnerable organizations were notified of research and recommendations.

- Organizations are anonymized.

- All organizations responded positively. 3 organizations requested a meeting to discuss the recommendations.

Thank you.

Questions ?

References:

Related work

Type of credentials: Boniface et al. (https://hal.inria.fr/hal-02072302/document)
Risks of SARs: Amber Welch (https://youtu.be/FAYGZ9COrto)

Future work

Cagnazzo et al. (https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2019/08/05/ESORICS19-GDPiRated.pdf)

Urban et al. (https://www.ei.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2019/08/05/DPM19-SAR-Study.pdf)

Interesting cases (1)

We requested personal information of our targeted individual:

Ley Johnson

We received the data of another individual:
Name: **Lesley John**
Address: **Sonarstreet nr.15**