

“Security in GDPR”

Giuseppe F. Italiano

University of Rome Tor Vergata

giuseppe.italiano@uniroma2.it



[@GFIItaliano](https://twitter.com/GFIItaliano)

6 Privacy Principles of GDPR

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Kept in a form which permits identification of data subjects for no longer than is necessary
6. Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage

6 Privacy Principles of GDPR

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner (**Lawfulness, fairness and transparency**)
2. Collected for specified, explicit and legitimate purposes (**Purpose limitations**)
3. Adequate, relevant and limited to what is necessary (**Data minimisation**)
4. Accurate and kept up to date (**Accuracy**)
5. Kept in a form which permits identification of data subjects for no longer than is necessary (**Storage limitations**)
6. Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage (**Integrity and confidentiality**)

6 Privacy Principles of GDPR

1. Lawfulness, fairness and transparency
2. Purpose limitations
3. Data minimisation
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality

Security as a “principle”:

Security is not “nice add on” but a “must”!

Article 32 GDPR

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

A Shift in Paradigm

“Functional” Security:

The goal is not only to defend yourself and your organization from possible attacks but to make sure that security guarantee that your services, systems and applications work properly!

Security at the foundation of data quality, reliability, interoperability, etc...

Limits of Traditional Approach

- In my own experience, most organizations take a “defensive” security approach
- I.e., defend only against possible attacks
- In the research community (and not only) we have been talking about security by design for a long time
- But in practice, most fail to address it

Are we ready?

2017 Survey by Global Cyber Security Center & Europrivacy:

- “Are you currently applying any security/privacy by design principles when defining your new services?”
- Yes: 58.1%
- No: **41.9%**

Open survey, 160 Italian respondents:

36.9% ICT, 13% Financial, 10% Manufacturing, 8.8% Public Admin, 5% Telecom, 2.5% Energy & Transportation)


Limits of Traditional Approach

- Why should I invest in security?
- We do not deal with sensitive data... (Esp. SMEs)

Limits of Traditional Approach

- Why should I invest in security?
- We do not deal with sensitive data... (Esp. SMEs)

Company Size	Apr '17 (1 in)	Mar '17 (1 in)
1-250	409	566
251-500	358	622
501-1000	488	650
1001-1500	950	1049
1501-2500	362	693

Email Malware by Organization Size 

Company Size	Apr '17 (1 in)	Mar '17 (1 in)
1-250	5502	8304
251-500	6337	9864
501-1000	6012	9752
1001-1500	13128	17670
1501-2500	7791	12767

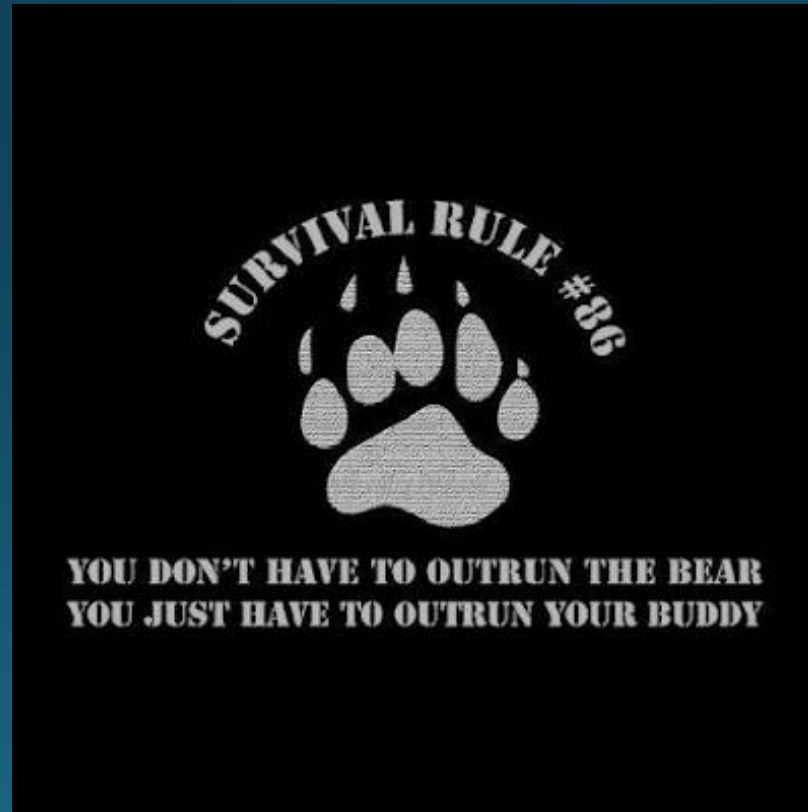
Email Phishing by Organization Size 

Limits of Traditional Approach

- Why should I invest in security?
- I'm not going to win this war... (Esp. SMEs)

Limits of Traditional Approach

- Why should I invest in security?
- I'm not going to win this war... (Esp. SMEs)



Limits of Traditional Approach

- Why should I invest in security?
- Where is my return? (Esp. SMEs)
- I don't have time to read 400-page documents, answer 500 questions, carry out 20 or 50 control checks, and insert them in my risk management. How will this help my business? Strength relationships with my customers? ...

Limits of Traditional Approach

- Why should I invest in security?
- Where is my return? (Esp. SMEs)
- I don't have time to read a 500-page document, answer 400 questions, carry out 20 or 50 control checks, and insert them in my risk management. How will this help my business? Strength relationships with my customers? ...
- If I were an investor, I'd like to be reassured that you're doing your best to protect your digital assets and infrastructures, ensuring a level of security appropriate to the risks, and that also digital risks are monitored and well integrated with risk management!

A Shift in Paradigm

- Several techniques have been around for quite some time now in the research community (cryptography), e.g.,
 - Searchable encryption
 - Homomorphic encryption
 - Multiparty computation
 - Differential privacy
 - Privacy preserving computations
 - Zero Knowledge
 - ...
- Need to make them more practical and technology-ready

A Shift in Paradigm

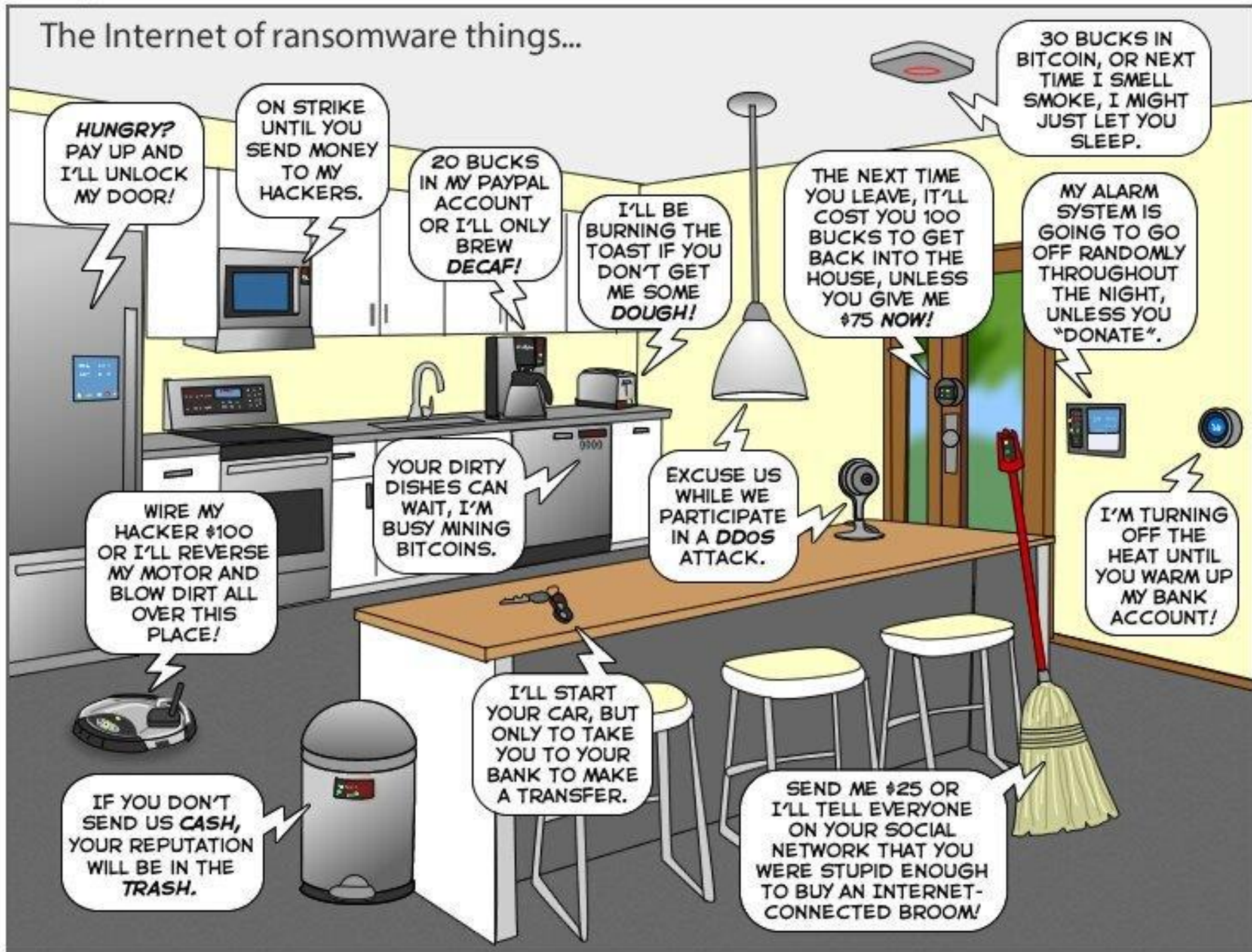
- Urgent to do something now, as things are already getting more complicated (Big Data, Internet of Things, etc...) ...

Internet of Things



Mirai botnet, a DDoS nightmare
turning Internet of Things
into Botnet of things

The Internet of ransomware things...



HUNGRY?
PAY UP AND
I'LL UNLOCK
MY DOOR!

ON STRIKE
UNTIL YOU
SEND MONEY
TO MY
HACKERS.

20 BUCKS
IN MY PAYPAL
ACCOUNT
OR I'LL ONLY
BREW
DECAF!

I'LL BE
BURNING THE
TOAST IF YOU
DON'T GET
ME SOME
DOUGH!

THE NEXT TIME
YOU LEAVE, IT'LL
COST YOU 100
BUCKS TO GET
BACK INTO THE
HOUSE, UNLESS
YOU GIVE ME
\$75 NOW!

30 BUCKS IN
BITCOIN, OR NEXT
TIME I SMELL
SMOKE, I MIGHT
JUST LET YOU
SLEEP.

MY ALARM
SYSTEM IS
GOING TO GO
OFF RANDOMLY
THROUGHOUT
THE NIGHT,
UNLESS YOU
"DONATE".

WIRE MY
HACKER \$100
OR I'LL REVERSE
MY MOTOR AND
BLOW DIRT ALL
OVER THIS
PLACE!

YOUR DIRTY
DISHES CAN
WAIT, I'M
BUSY MINING
BITCOINS.

EXCUSE US
WHILE WE
PARTICIPATE
IN A DDOS
ATTACK.

I'M TURNING
OFF THE
HEAT UNTIL
YOU WARM UP
MY BANK
ACCOUNT!

IF YOU DON'T
SEND US CASH,
YOUR REPUTATION
WILL BE IN THE
TRASH.

I'LL START
YOUR CAR, BUT
ONLY TO TAKE
YOU TO YOUR
BANK TO MAKE
A TRANSFER.

SEND ME \$25 OR
I'LL TELL EVERYONE
ON YOUR SOCIAL
NETWORK THAT YOU
WERE STUPID ENOUGH
TO BUY AN INTERNET-
CONNECTED BROOM!



What to do next?

- **Policy makers** should keep on supporting incentive mechanisms for privacy-friendly services (from policies to concrete implementations)
- **Researchers** need to further investigate practical privacy enhancing technologies and make their utmost efforts to disseminate their research results.
- **Industries** and the **research community** should offer tools that enable natural implementations of privacy properties.
- **Research funding agencies** should support more this process.
- **Policy makers** and **media** should promote more those activities.