



# ITU- AICTO Regional workshop

Policy Advocacy on Data Privacy and Security

05 – 06 December 2016

## Data Protection: Stack of Rules, Policies and Tools

Dr. Nizar Ben Neji

Faculty of Sciences of Bizerte (FSB)  
University of Carthage

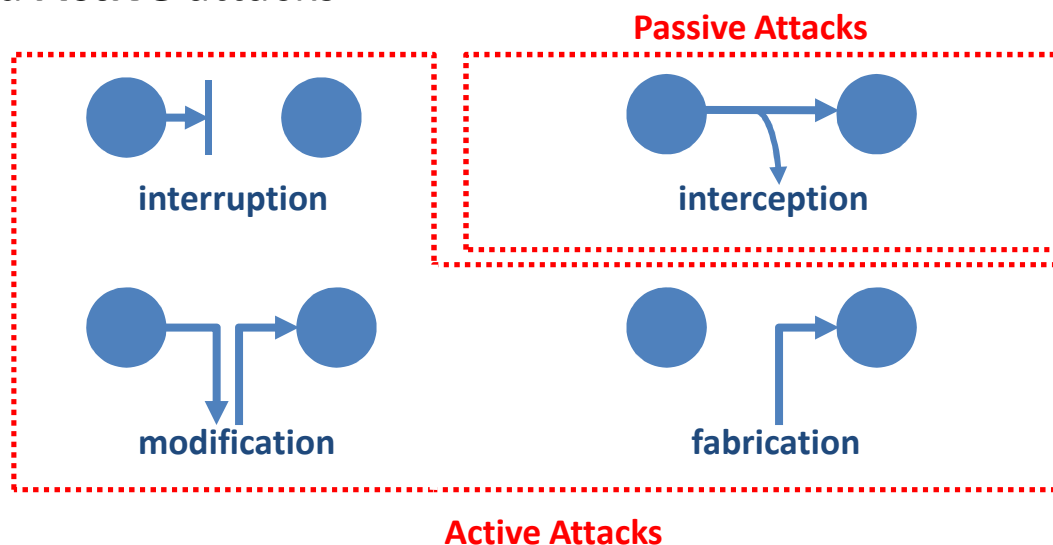


December, 5<sup>th</sup> 2016 - Elgazala Technopark

# Data Security

## BASIC NOTIONS

- **Data security** means protecting data from the **illegal actions** of unauthorized users and from the **unwanted actions** of the authorized users
- **Intentional** and **Accidental** Threats
- **Security objectives** (Authentication, Confidentiality, Integrity, Availability, ...)
- **Internal** and **External** attacks
- **Passive** and **Active** attacks



- **Data Security** is different from the **protection of the use of personal data**

# Protection of the use of Personal Data

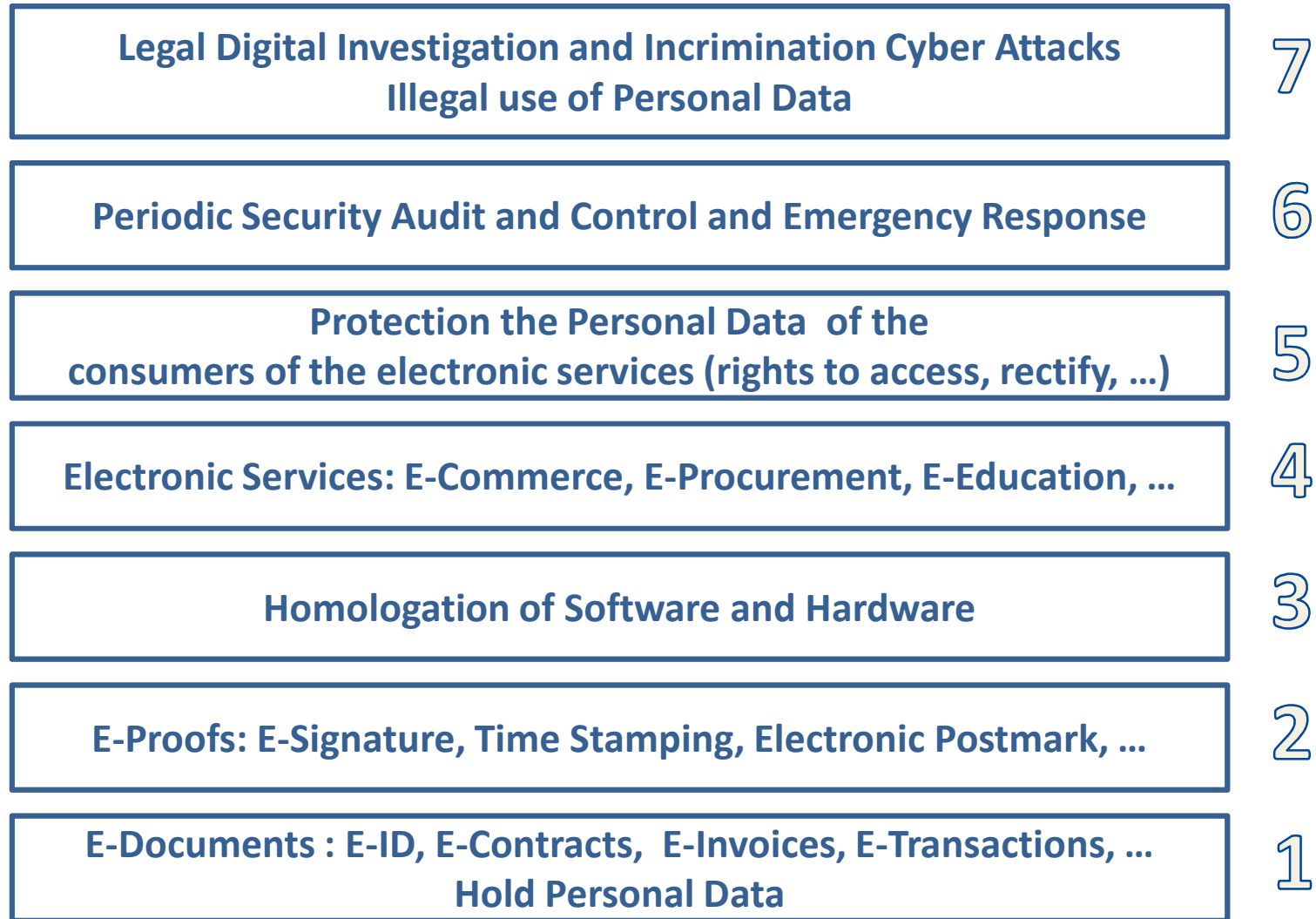
## NOT ONLY ABOUT TECHNOLOGY

- Protection of personal data means protecting it from the **illegal use**
- Protection and Security of personal data is **not only about technology**
  - ✓ Regulation texts (Laws, Decrees, Ministerial orders, ...)
  - ✓ Security Policies (Information System, Network, Password, Privacy, ...)
  - ✓ Technical and Administrative Procedures
  - ✓ Awareness and trainings (academic, recycling, ...)
  - ✓ ...



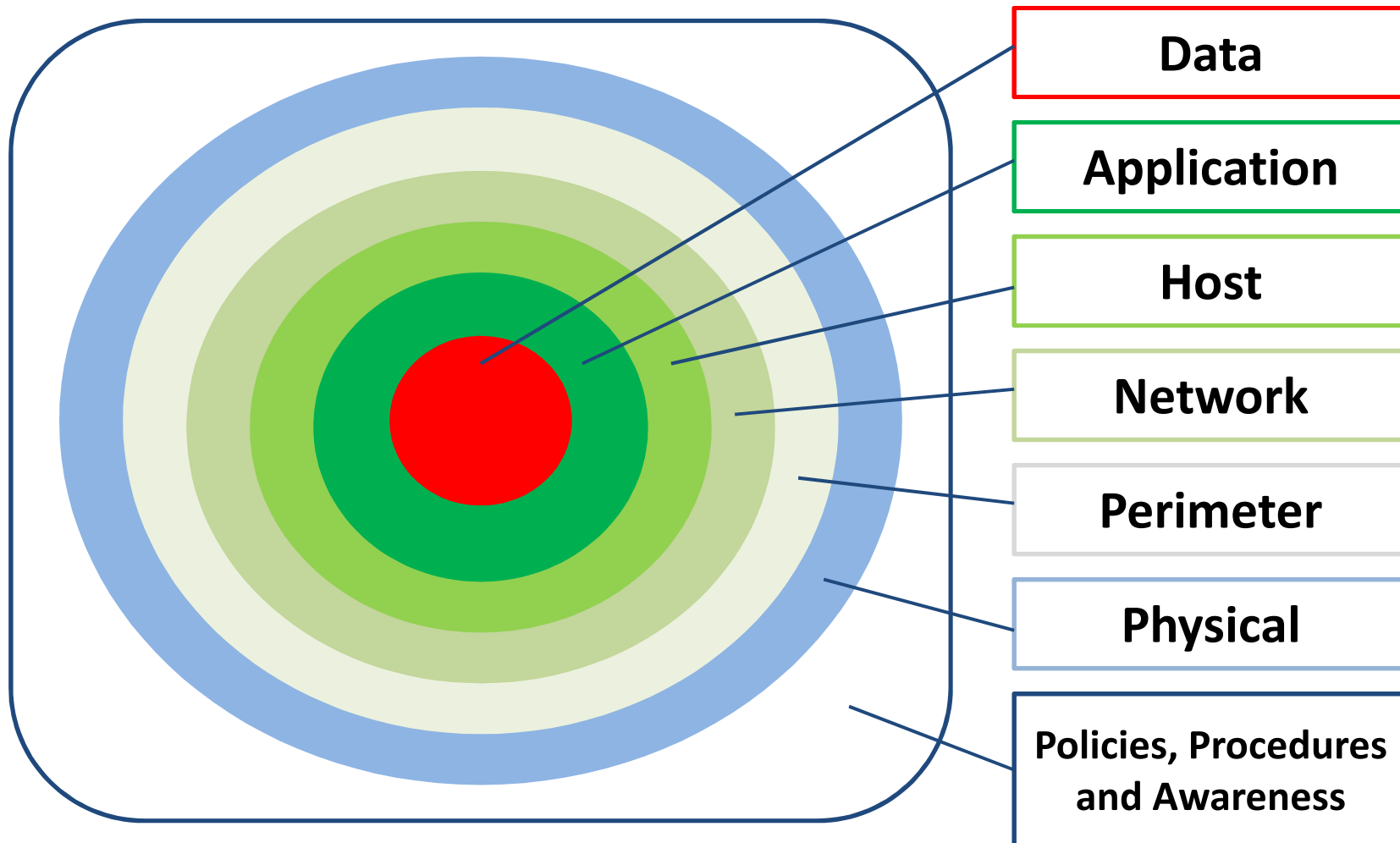
# Stack of Rules

## REGULATION TEXTS



# Stack of Tools

**DEFENSE IN DEPTH**



# Stack of Security Policies

## PRIVACY POLICY

- **Privacy Policy** is a public document specifying how **client's data** are **gathered, used, disclosed and managed and deleted**
- **Client's data** (name, address, date of birth, marital status, contact information, level of study, financial records, medical history, ...)
- **Period** of retention of data
- **Purpose** of use and retention and whether it is **kept confidential, shared** with partners, or **sold** to other firms
- Other security policies:
  - ✓ System Information Security Policy (PSSI)
  - ✓ Physical Security Policy
  - ✓ Network Security Policy
  - ✓ Password Policy
  - ✓ ...



# Protection of Personal Data

## PERSONAL DATA

- **Personal data** refers to data, whether **true or not**, about an individual who can be identified from that data
- **Digital** and **paper** format
- **Stored, archived, processed** or **transferred**
- **Automated** and **non automated** processing
- Personal data:
  - ✓ Identifiers
  - ✓ Quasi-identifiers
  - ✓ Sensitive data
  - ✓ General information



# Protection of Personal Data

## PERSONALLY IDENTIFIABLE INFORMATION (PII)

**Identifiers** are data used to identify and distinguish individuals according to the National Institute of Standards and Technology (NIST):

- National identification number
- Social security number
- Passport number
- Vehicle registration plate number
- Driver's license number
- Credit card numbers
- Home address
- Telephone number
- Email address
- IP address
- Face, fingerprints, or handwriting
- Digital identity
- Genetic information
- Login name, screen name, nickname, ...
- ...





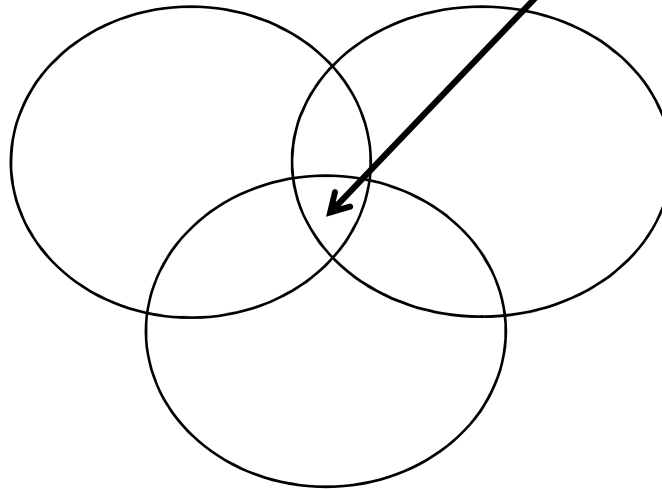
# Protection of Personal Data

## POTENTIALY PII

**Quasi-identifiers** are shared by many people and if combined together they may identify an individual :

- First or last name
- Country, state, postcode or city of residence
- Workplace, School, University, ...
- Age
- Date of birth
- Birthplace
- Gender or race
- Job position, Grades, ...
- Geographic location, ...
- ...

**multiple quasi-identifiers  
may uniquely identify an  
individual**



# Protection of Personal Data

## SENSITIVE DATA

- Personally Identifiable Information (ID Numbers, Contact Information, ...)
- Healthcare records
- Judicial or criminal record
- Financial assets and transactions
- Contents of the communications
- Personal life and daily activities
- Personal information that the individual prefer that it remains secret
- Any information that poses a risk to a person or a company
- ...



# Protection of Personal Data

## TECHNIQUES OF ACCESS TO DATA

- Elements of access(Authentication, authorization, administration and audit)
- Techniques of access to data
  - ✓ Authentication factors:
    - Something you have,
    - Something you know,
    - Something you are,
    - Something you can do,
    - Where you are.
  - ✓ PKI Technology and authentication keys
  - ✓ One Time Password (OTP)
  - ✓ Single Sign On (SSO)
  - ✓ VPN Authentication
  - ✓ TLS Authentication
  - ✓ M of N authentication, ...
  - ✓ ...



# Protection of Personal Data

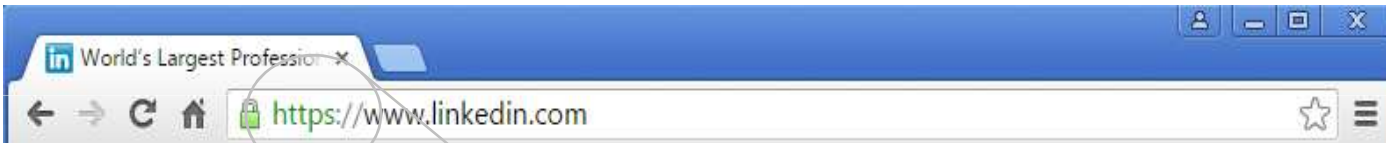
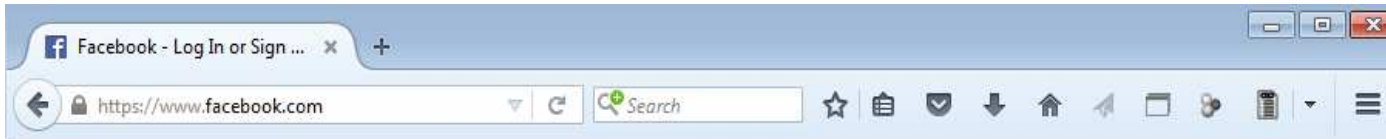
## TECHNIQUES OF DATA PROTECTION

- Types of access (Read, Write, Execute)
- Techniques of data **confidentiality**
  - ✓ Encryption
  - ✓ One way functions
  - ✓ Splitting data
  - ✓ Data anonymization
  - ✓ ...
- Techniques of data **integrity**
  - ✓ Digital signature (Types, Standards, Validity, ...)
  - ✓ Time Stamping
  - ✓ ...



# Protection of Data

## PRACTICAL EXAMPLE: CASE OF SSL/TLS



**Never introduce your personal data in this case for several reasons**

# Conclusion

- Involve universities and research labs
  - ✓ we are dealing with unknown problems or known problems but not solved yet
  - ✓ our students are future professionals: invest on them instead of recycling them later
- Protection of data is not only about technology
  - ✓ Regulation texts
  - ✓ Policies, procedures, training and awareness
  - ✓ Technical solutions

# Thank you for your Attention

Dr. Nizar Ben Neji  
Cybersecurity Expert  
FSB, University of Carthage

[nizar.benneji@fsb.rnu.tn](mailto:nizar.benneji@fsb.rnu.tn) / [nizar.benneji@gmail.com](mailto:nizar.benneji@gmail.com)

(+216) 99 207 377