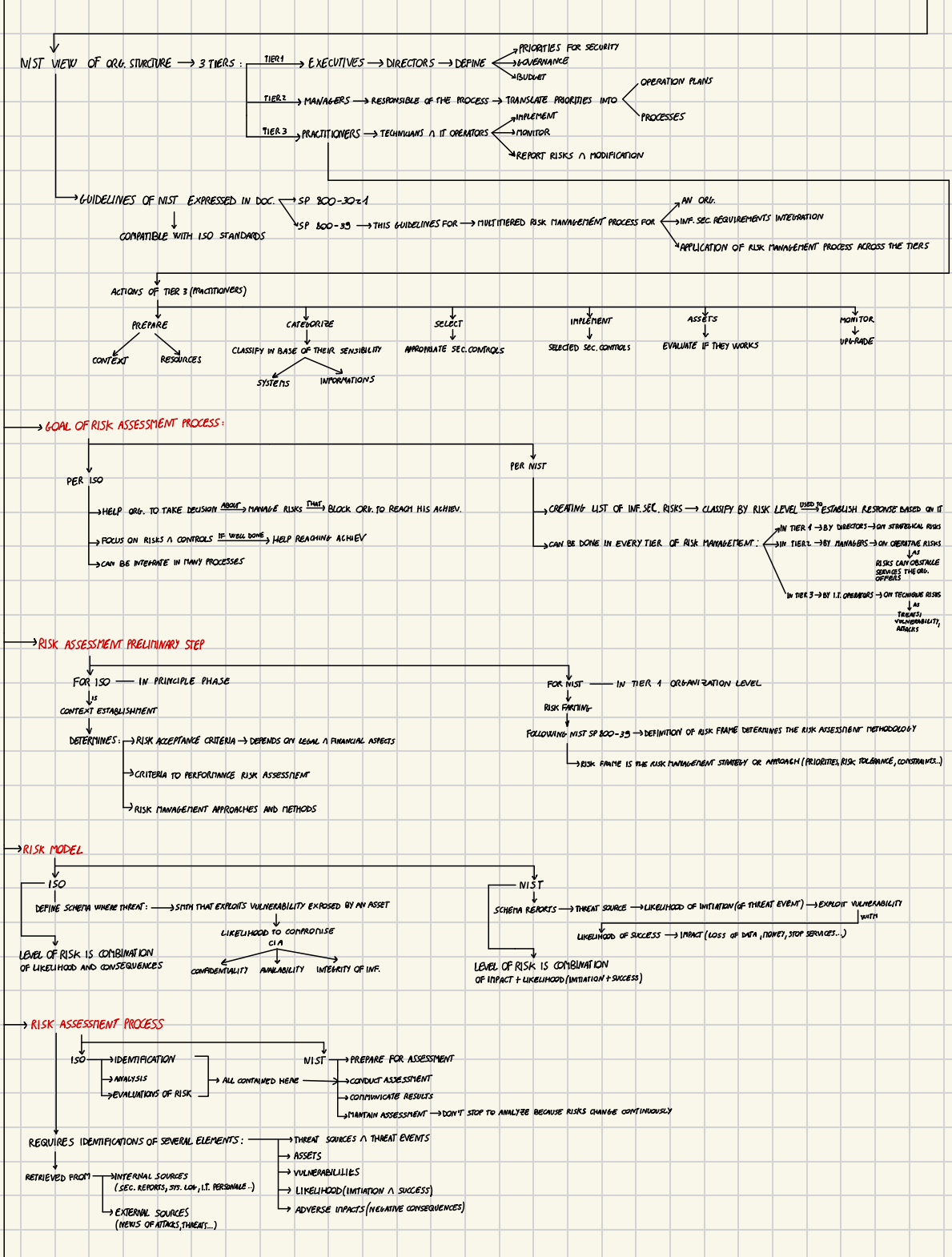
RISK MANAGEMENT

- CONCEPT OF RISK → EXPOSURE TO DANGER — POSSIBILITY SOMETHING UNWELCOME
- RISKS ORGANIZATIONS THAT MANAGE DATA
  - LOSS OF CONFIDENTIALITY
  - INTEGRITY
  - AVAILABILITY OF INFORMATION OR INFORMATION SYSTEMS
- MAIN ACTOR → TO DEVELOP GUIDELINES AND STANDARD → FOR INFORMATION SECURITY RISK MANAGEMENT
  - ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION) → NON GOVERNMENTAL → PUBLISHES INTERNATIONAL STANDARDS
    - ALL ASPECT OF TECHNOLOGY — IS A DOCUMENT — BEST PRACTICES ABOUT DOING SOMETHING (PRODUCTS, SERVICES OR PROCESSES)
  - NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY) → GOVERNMENTAL ORGANIZATION → PART OF U.S. DEPARTMENT OF COMMERCE
    - BEST PRACTICES ON SECURITY AND PRIVACY OF INFORMATION
- DEFINITION RISK
  - ISO → VALID ANY ORG
    - RISK → MEASURE → DESCRIPTION OF EFFECT OF UNCERTAINTY ON OBJECTIVES
      - DESIRABLE
      - UNDESIRABLE
      - POSITIVE
      - NEGATIVE
  - NIST → MEASURE OF RISK AND IMPACT ONLY → FOCUS INFORMATION SECURITY ASPECT
    - RISK MEASURE ENTITY THREATENED BY POTENTIAL EVENT
    - EXPRESSED IN FUNCTION OF
      - LIKELIHOOD OF EVENT'S OCCURRENCE
      - IMPACT OF IT
- ASSET → PART OF ORGANIZATION → NEEDS PROTECTION FROM RISK → TO AVOID EXPLOITATION → FOR MALICIOUS PURPOSES
- RISK MANAGEMENT → KEY ROLE PROTECTING ORGANIZATIONS → ALLOWS TO BALANCE
  - OPERATIONAL AND ECONOMIC COSTS OF PROTECTIVE MEASURES
  - PROTECTION NEEDED
  - EACH ORG DECIDES WHEN RISK ACCEPTABLE → BASED ON INFORMATIONS → AFTER DATA ANALYSIS
- ISO 31000 STANDARD → COMMON APPROACH → MANAGE ANY KIND RISK → (NOT SPECIFIC INF.SEC.)
  - APPLICATION CUSTOMIZED X ANY ORG
  - STRUCTURE:
    - PRINCIPLES → GOAL
      - CREATE VALUE INSIDE THE ORG.
      - PROTECT VALUE
    - FRAMEWORK → GUIDE LINES HOW RISK IS MANAGED
      - ITS EFFECTIVENESS DEPENDS ON GOVERN ∧ SUPERVISION
    - PROCESS → ITERATIVE PROCESS 3 PHASES:
      - RISK IDENTIFICATION → ANALYZE
        - ASSETS
        - THREATS
        - OPPORTUNITIES
      - RISK ANALYSIS → EVALUATE
        - CONSEQUENCES
        - LIKELIHOOD RISK HAPPENS
      - RISK EVALUATION → DECIDE IF RISK BASED ON RISK'S LEVEL IS ACCEPTABLE OR NOT
- ISO PROVIDES SOME STANDARDS MORE SPECIFIC FOR INF.SEC. MANAGEMENT SYSTEMS (ISMS):
  - ISO/IEC 27000:2018
    - IS VOCABULARY CONTAINING MAIN DEFINITION:
      - ASSETS → EVERYTHING VALUE AND REQUIRES PROTECTION
      - CONTROL → A MEASURE → ACTS TO MODIFY RISK
      - VULNERABILITY → WEAKNESS OF ASSETS V CONTROL → CAN BE EXPLOITED BY THREATS
  - ISO/IEC 27005:2022
    - ISO STANDARD FOR INF.SEC, CYBER SEC., PRIVACY PROTECTION
    - GUIDE LINES FOR RISK MANAGEMENT IN INF.SEC.
    - IT IDENTIFY 2 KIND OF INF. ASSETS:
      - PRIMARY/BUSINESS ASSETS → INF. V PROCESSES OF VALUE (INTELLECTUAL PROPERTIES; FINANCIAL INF.; INF ABOUT CUSTOMERS...)
      - SUPPORTING ASSETS → COMPONENTS OF INF.SYS. ON WHICH BUSINESS/PRIMARY ASSETS ARE BASED (HARDWARE, SOFTWARE, APPLICATION...)


NIST VIEW OF ORG. STRUCTURE → 3 TIERS :
TIER 1 → EXECUTIVES → DIRECTORS → DEFINE → PRIORITIES FOR SECURITY
→ GOVERNANCE
→ BUDGET
TIER 2 → MANAGERS → RESPONSIBLE OF THE PROCESS → TRANSLATE PRIORITIES INTO → OPERATION PLANS
→ PROCESSES
TIER 3 → PRACTITIONERS → TECHNICIANS ∧ IT OPERATORS → IMPLEMENT
→ MONITOR
→ REPORT RISKS ∧ MODIFICATION
→ GUIDELINES OF NIST EXPRESSED IN DOC. → SP 800-30r1
→ SP 800-39 → THIS GUIDELINES FOR → MULTITIERED RISK MANAGEMENT PROCESS FOR → AN ORG.
→ INF. SEC. REQUIREMENTS INTEGRATION
→ APPLICATION OF RISK MANAGEMENT PROCESS ACROSS THE TIERS
COMPATIBLE WITH ISO STANDARDS
ACTIONS OF TIER 3 (PRACTITIONERS)
PREPARE → CONTEXT
→ RESOURCES
CATEGORIZE → CLASSIFY IN BASE OF THEIR SENSIBILITY → SYSTEMS
→ INFORMATIONS
SELECT → APPROPRIATE SEC. CONTROLS
IMPLEMENT → SELECTED SEC. CONTROLS
ASSETS → EVALUATE IF THEY WORKS
MONITOR → UPGRADE
→ GOAL OF RISK ASSESSMENT PROCESS :
PER ISO
→ HELP ORG. TO TAKE DECISION ABOUT → MANAGE RISKS THAT → BLOCK ORG. TO REACH HIS ACHIEV.
→ FOCUS ON RISKS ∧ CONTROLS IF WELL DONE → HELP REACHING ACHIEV
→ CAN BE INTEGRATE IN MANY PROCESSES
PER NIST
→ CREATING LIST OF INF. SEC. RISKS → CLASSIFY BY RISK LEVEL USED TO → ESTABLISH RESPONSE BASED ON IT
→ CAN BE DONE IN EVERY TIER OF RISK MANAGEMENT : → IN TIER 1 → BY DIRECTORS → ON STRATEGICAL RISKS
→ IN TIER 2 → BY MANAGERS → ON OPERATIVE RISKS
→ AS RISKS CAN OBSTACLE SERVICES THE ORG. OFFERS
→ IN TIER 3 → BY I.T. OPERATORS → ON TECHNIQUE RISKS
→ AS THREATS, VULNERABILITY, ATTACKS
→ RISK ASSESSMENT PRELIMINARY STEP
FOR ISO → IN PRINCIPLE PHASE
IS → CONTEXT ESTABLISHMENT
DETERMINES : → RISK ACCEPTANCE CRITERIA → DEPENDS ON LEGAL ∧ FINANCIAL ASPECTS
→ CRITERIA TO PERFORMANCE RISK ASSESSMENT
→ RISK MANAGEMENT APPROACHES AND METHODS
FOR NIST → IN TIER 1 ORGANIZATION LEVEL
→ RISK FRAMING
→ FOLLOWING NIST SP 800-39 → DEFINITION OF RISK FRAME DETERMINES THE RISK ASSESSMENT METHODOLOGY
→ RISK FRAME IS THE RISK MANAGEMENT STRATEGY OR APPROACH (PRIORITIES, RISK TOLERANCE, CONSTRAINTS...)
→ RISK MODEL
ISO
DEFINE SCHEMA WHERE THREAT : → SMTH THAT EXPLOITS VULNERABILITY EXPOSED BY AN ASSET
→ LIKELIHOOD TO COMPROMISE CIA
CONFIDENTIALITY
AVAILABILITY
INTEGRITY OF INF.
→ LEVEL OF RISK IS COMBINATION OF LIKELIHOOD AND CONSEQUENCES
NIST
SCHEMA REPORTS → THREAT SOURCE → LIKELIHOOD OF INITIATION (OF THREAT EVENT) → EXPLOIT VULNERABILITY WITH
→ LIKELIHOOD OF SUCCESS → IMPACT (LOSS OF DATA, MONEY, STOP SERVICES...)
→ LEVEL OF RISK IS COMBINATION OF IMPACT + LIKELIHOOD (INITIATION + SUCCESS)
→ RISK ASSESSMENT PROCESS
ISO → IDENTIFICATION
→ ANALYSIS
→ EVALUATIONS OF RISK
→ ALL CONTAINED HERE
NIST → PREPARE FOR ASSESSMENT
→ CONDUCT ASSESSMENT
→ COMMUNICATE RESULTS
→ MAINTAIN ASSESSMENT → DON'T STOP TO ANALYZE BECAUSE RISKS CHANGE CONTINUOUSLY
REQUIRES IDENTIFICATIONS OF SEVERAL ELEMENTS :
→ THREAT SOURCES ∧ THREAT EVENTS
→ ASSETS
→ VULNERABILITIES
→ LIKELIHOOD (INITIATION ∧ SUCCESS)
→ ADVERSE IMPACTS (NEGATIVE CONSEQUENCES)
RETRIEVED FROM
→ INTERNAL SOURCES (SEC. REPORTS, SYS. LOG, I.T. PERSONALE :)
→ EXTERNAL SOURCES (NEWS OF ATTACKS, THREATS...)

RISK IDENTIFICATION

- ISO
  - TWO APPROACHES
    - EVENT BASED → STRATEGIC SCENARIOS ARE EXPRESSED
      - WHAT COULD HAPPEN?
      - RISK IDENTIFIED ∧ ASSESSED
      - FOCUS CONSEQ. OVER PRIMARY/BUSINESS ASSETS
      - (CLIENT DATA, SERVICES)
    - ASSET BASED → WHAT HAS TO BE PROTECTED?
      - IN TERMS OF SUPPORTING ASSETS, VULNERABILITIES, THREATS
      - IDENTIFIES OPERATIONAL SCENARIOS THAT COULD THREATEN THESE ASSETS
  - ASSIGN TO EACH THREAT A SOURCE TYPE:
    - DELIBERATE
    - ACCIDENTAL
    - ENVIRONMENTAL
    - CAN GROUP THEM INTO BIGGER CATEGORIES (NATURAL THREATS, HUMAN THREATS...)
- NIST
  - TYPES OF ANALYSIS ORIENTED TO:
    - THREAT SOURCES ∧ EVENTS ∧ DEV OF THREATS
    - ASSETS/IMPACT ON CRITICAL ASSETS → HOW IMPORTANT ASSETS GET DMG?
    - VULNERABILITY OF INF. SYS. V ENVIRONMENTS
      - WHERE ARE WE VULNERABLE? (WEAK PW, NON-UPDATED SW, ...)
  - FOUR SOURCE-TYPE:
    - ADVERSIAL
    - ACCIDENTAL
    - STRUCTURAL
    - ENVIRONMENTAL

THREAT IDENTIFICATION "THREAT MODELLING"

APPROACH TO THREAT IDENTIFICATION

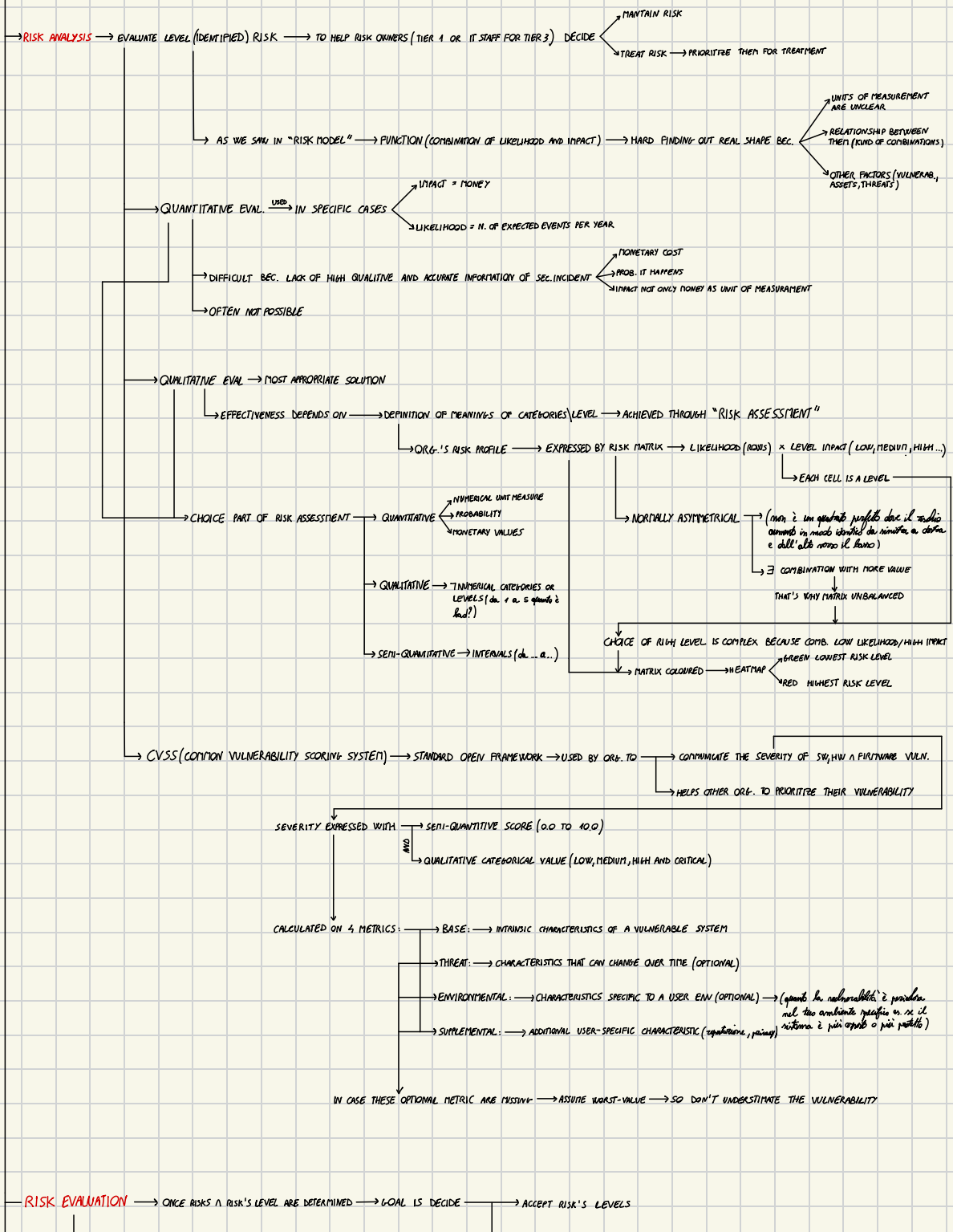
WITH GRAPH-BASED TECHNIQUES

- ATTACK TREES → DESCRIBE EVENT CAUSED BY ADV. THREAT SOURCE
  - ROOT NODE → GOAL ATTACKER
  - LEAF NODES → ACTIONS ATT. CAN MAKE
  - OTHER NODES → INTERMEDIATE GOALS
  - UNDERSTAND ALL POSSIBLE ATTACK PATH
- FAULT TREES → TOP-DOWN LOGIC DIAGRAM → IDENTIFY ∧ ANALYZE ALL ELEMENTS CAUSE UNDESIRED EVENT (NOT ONLY HUMAN ATT.)
  - ROOT → TOP EVENT
  - LEAF → BASE EVENTS (BASE CAUSES)
  - OTHER NODES → CONNECTION BETWEEN EVENTS → LOGIC PORTS (AND, OR ...)
- THREAT TREES → APPLICATION OF FAULT TREES SPECIFIC FOR SEC. INF. → ¬USE LOGIC PORTS
  - IDENTIFY ALL POSSIBLE EVENTS COMBINATION → CAN VIOLATE SEC. POLICY
  - VISUALIZE SIMILARITIES BETWEEN ATTACK PATHS → UNDERSTAND IF MANY USE SAME VULNERAB.
  - ROOT NODE → MAIN EVENT
  - LEAF NODES → BASE EVENTS
  - OTHER NODES → ¬INTERMEDIATE EVENTS → THEY ARE THREATS CATEGORIES
- DIFFERENCES TREES
  - ATTACK → EXCLUSIVE INTENTIONAL → HOW HE ATTACKS (ALL PATHS)
  - THREAT → NOT ONLY INTENTIONAL → ALL PATH FROM WHERE THREAT CAN COME FROM

VULNERABILITY IDENTIFICATION

VULN. OCCURS IN EACH LEVEL OF ORG. → THIS PHASE IS VALID
- ISO
- NIST → EX. OF INF. SOURCES FOR VULN. IDENTIFICATION AT INF.SYS (TIER 3):
  - CVE → COMMON VULNERABILITY EXPOSURE → PROVIDES LIST OF KNOWN CYBER.SEC. VULN.
  - NVD → NATIONAL VULNERABILITY DATABASE → MANAGED BY NIST
  - CWE → COMMON WEAKNESSES ENUMERATION → LIST OF COMMON WEAKNESS
    - SW., HW., FIRMWARE
    - OTHER COMPONENTS OF INF.SYS. THAT CAN BECOME VULN.

THIS PHASE INVOLVES CONSEQ. ∧ IMACTS OF
- THREAT EVENTS
- INF. SEC. EVENTS


RISK ANALYSIS → EVALUATE LEVEL (IDENTIFIED) RISK → TO HELP RISK OWNERS (TIER 1 OR IT STAFF FOR TIER 3) DECIDE
MAINTAIN RISK
TREAT RISK → PRIORITIZE THEM FOR TREATMENT
AS WE SAW IN "RISK MODEL" → FUNCTION (COMBINATION OF LIKELIHOOD AND IMPACT) → HARD FINDING OUT REAL SHAPE BEC.
UNITS OF MEASUREMENT ARE UNCLEAR
RELATIONSHIP BETWEEN THEM (KIND OF COMBINATIONS)
OTHER FACTORS (VULNERAB., ASSETS, THREATS)
QUANTITATIVE EVAL. USED IN SPECIFIC CASES
IMPACT = MONEY
LIKELIHOOD = N. OF EXPECTED EVENTS PER YEAR
DIFFICULT BEC. LACK OF HIGH QUALITIVE AND ACCURATE INFORMATION OF SEC. INCIDENT
MONETARY COST
PROB. IT HAPPENS
IMPACT NOT ONLY MONEY AS UNIT OF MEASUREMENT
OFTEN NOT POSSIBLE
QUALITATIVE EVAL → MOST APPROPRIATE SOLUTION
EFFECTIVENESS DEPENDS ON → DEFINITION OF MEANINGS OF CATEGORIES\LEVEL → ACHIEVED THROUGH "RISK ASSESSMENT"
ORG.'S RISK PROFILE → EXPRESSED BY RISK MATRIX → LIKELIHOOD (ROWS) x LEVEL IMPACT (LOW, MEDIUM, HIGH ...)
EACH CELL IS A LEVEL
CHOICE PART OF RISK ASSESSMENT → QUANTITATIVE
NUMERICAL UNIT MEASURE
PROBABILITY
MONETARY VALUES
QUALITATIVE → NUMERICAL CATEGORIES OR LEVELS (da 1 a 5 quanti è bad?)
SEMI-QUANTITATIVE → INTERVALS (da ... a ...)
NORMALLY ASYMMETRICAL → (non è un quadrato perfetto dove il rischio aumenta in modo identico da sinistra a destra e dall'alto verso il basso)
∃ COMBINATION WITH MORE VALUE
THAT'S WHY MATRIX UNBALANCED
CHOICE OF RISK LEVEL IS COMPLEX BECAUSE COMB. LOW LIKELIHOOD/HIGH IMPACT
MATRIX COLOURED → HEATMAP
GREEN LOWEST RISK LEVEL
RED HIGHEST RISK LEVEL
CVSS (COMMON VULNERABILITY SCORING SYSTEM) → STANDARD OPEN FRAMEWORK → USED BY ORG. TO → COMMUNICATE THE SEVERITY OF SW, HW ∧ FIRMWARE VULN.
HELPS OTHER ORG. TO PRIORITIZE THEIR VULNERABILITY
SEVERITY EXPRESSED WITH → SEMI-QUANTITIVE SCORE (0.0 TO 10.0)
AND
QUALITATIVE CATEGORICAL VALUE (LOW, MEDIUM, HIGH AND CRITICAL)
CALCULATED ON 4 METRICS:
BASE: → INTRINSIC CHARACTERISTICS OF A VULNERABLE SYSTEM
THREAT: → CHARACTERISTICS THAT CAN CHANGE OVER TIME (OPTIONAL)
ENVIRONMENTAL: → CHARACTERISTICS SPECIFIC TO A USER ENV (OPTIONAL) → (quanto la vulnerabilità è percepita nel tuo ambiente specifico or se il sistema è più esposto o più protetto)
SUPPLEMENTAL: → ADDITIONAL USER-SPECIFIC CHARACTERISTIC (reputazione, privacy)
IN CASE THESE OPTIONAL METRIC ARE MISSING → ASSUME WORST-VALUE → SO DON'T UNDERSTIMATE THE VULNERABILITY
RISK EVALUATION → ONCE RISKS ∧ RISK'S LEVEL ARE DETERMINED → GOAL IS DECIDE → ACCEPT RISK'S LEVELS

- NIST → ¬INCLUDE EXPLICITY THIS STEP → INCLUDES IT IN → RISK ASSESSMENT / RISK TREATMENT
- ISO → ESTABLISH A PHASE FOR IT IN RISK ASSESSMENT
- ¬ACCEPT → DECIDE WHICH RISKS TREAT BEFORE

RISK TREATMENT

- GOAL ∧ FUNDAMENTALS → THIS PHASE START IF ORG CHOOSE TO TREAT
  - INPUT: PRIORITIZED SET OF RISKS
  - GOAL: MODIFY THE ACTUAL INFORMATION SEC. PLAN OF AN ORG. → SO THAT MEET THE ESTABLISHED ACCEPTANCE CRITERIA
  - OUTPUT: SET OF INFORMATION SEC. CONTROLS → THAT NEED BE IMPROVE AND DEVELOPED → DESCRIBED IN A RISK TREATMENT PLAN

- HOW IT WORKS:
  - FORMULATION ∧ SELECTION OF RISK TREATMENT OPTIONS → WITH CORRESPONDING CONTROLS → EACH CONTROL IS A MEASURE THAT → MAINTAIN THE RISK / MODIFY THE RISK
  - PLANNING ∧ IMPLEMENTATION
  - EVALUATION OF THE CHOSEN TREATMENT PLAN
  - IF RESIDUAL RISK → ACCEPTABLE → PROCESS ENDS / ¬ACCEPTABLE → START A NEW CYCLE

- TREATMENT OPTIONS INCLUDE:
  - ACCEPTANCE/RETENTION: → DEPENDS ON ORGANIZATION'S RISK TOLERANCE → EX: federal agencies shared sensitive information of individuals for preventing terroristic attacks with the risk of compromising data confidentiality
  - AVOIDANCE/ELIMINATION: → BLOCK THE ACTIVITY THAT INTRODUCES THE RISK → EX. after natural disaster such as an earthquake a workstation location there need to be blocked because the availability and integrity of controls are not longer sufficient
  - MODIFICATION/MITIGATION/REDUCTION: → CONTROLS THAT REDUCE → LIKELIHOOD / CONSEQUENCES / IMPACT
    - WHEN CAN'T BLOCK THREAT U MITIGATE IT → EX: cannot prevent environmental disaster, a mitigation option could use cryptographic techniques or server duplication in areas exposed to risk or do regular backup.
      - IT'S NOT ONLY FOR ENV. THREATS
    - THIS OPTION IS FOR ALL RISK THAT → CAN'T DELETE / DON'T WANT DELETE / ¬CONVENIENCE TO DELETE
  - SHARING/TRANSFER: → RESPONSABILITY OR LIABILITY → GIVEN TO ANOTHER ORG. MORE QUALIFIED TO MANAGE THE RISK
    - GIVEN ENTIRELY (TRANSFER)
    - GIVEN PORTION OF IT (SHARING)
  - DIFFERENCES → RESPONSIBILITY → DUTY TO DO SOMETHING → NO FAULT IF SOMETHING HAPPENS
    - LIABILITY → LEGALLY RESPONSIBLE FOR SOMETHING
  - TAKING OR INCREASING THE RISK → BECAUSE IS SEEN AS BUSINESS OPPORTUNITY NOT ONLY AS A THREAT → (IT'S A OPTION ACCEPTED BY ISO)
  - IS POSSIBLE A COMBINATION OF THESE STRATEGIES AND CHOICE DEPENDS ON FUNCTION → HOW MUCH A CONTROL COST / BENEFITS OF REDUCING THE RISK

- ISO 27005 CLASSIFY THESE CONTROLS IN 3 CATEGORIES: → PREVENTIVE → AVOID RISK HAPPENS (strong password, firewall...)

- SHOULD REDUCE CORRECTIVE CONTROL
- DETECTIVE → NOTIFY IF SOMETHING STRANGE IS HAPPENING (intrusion detection system, log, monitoring)
  - SHOULD MITIGATE RISK IF PREVENTING CONTROLS FAIL
- CORRECTIVE → CORRECT OR LIMIT DAMAGE AFTER ACCIDENT (backup, encryption...)
  - SHOULD MITIGATE RISK IF DETECTIVE CONTROLS FAIL

- MANY FRAMEWORK → RELATED TO INF.SEC. → BASED ON A RISK MANAGEMENT APPROACH.
  - CSF (CYBERSECURITY FRAMEWORK) → CREATED BY NIST → FOCUS:
    - MANAGE CYBER SEC. RISKS
    - PROTECT CRITICAL INFRASTRACTURES
    - INCREASE INF. SEC.
    - 3 MAIN COMPONENTS:
      - CORE → A HIERARCHICAL STRUCTURE OF ELEMENTS DESCRIBE ALL INF.SEC. ACTIVITIES
        - ORGANIZED IN 6 FUNCTIONS:
          - IDENTIFY → ASSETS Λ THREATS
          - PROTECT → ASSETS
          - DETECT → EVENTS V. ANOMALIES
          - RESPOND → TO EVENTS
          - RECOVER
          - GOVERN → MANAGE OF RESPONSABILITY OF SECURITY
        - THEN MORE DIVIDED INTO CATEGORIES
      - PROFILES → USED TO EVALUATE
        - "CURRENT PROFILE" → CURRENT LEVEL OF SEC.
        - "TARGET PROFILE" → ESTABLISH THE TARGET TO REACH
      - TIERS → LEVEL OF RISK MANAGEMENT OF AN ORG:
        - TIER 1 "PARTIAL" → KNOWLEDGE OF RISKS LIMITED → PROCEDURES ¬WELL-STRUCTURED
        - TIER 2 "RISK INFORMED" → ORG. KNOWS RISKS → MANAGE THEM BUT ¬STANDARD WAY
        - TIER 3 "REPEATABLE" → SEC. PROCEDURES ARE STANDARDS Λ REPEATABLE
          - ORG. APPLIES CONSTANTLY RISK MANAGEMENT
        - TIER 4 "ADAPTIVE" → ORG. LEARN FROM ACCIDENTS → ADAPT FAST
          - CONTINOUSLY UPGRADE THE SEC.
  - NATIONAL CYBERSECURITY FRAMEWORK (ITALY) → NATIONAL FRAMEWORK FOR CYBERSECURITY → BASED ON NIST CSF → ADAPTED TO ITALIAN CONTEXT
  - CIS (CENTER FOR INTERNET SECURITY) CONTROLS → 18 SEC. CONTROLS → CREATED BY INTERNATIONAL COMMUNITY OF IT PROFESSIONAL
    - ALLIGN WITH RISK MANAGEMENT FRAMEWORKS
    - COMPATIBLE WITH NIST CSF
    - ONE OF MOST USED FRAMEWORKS → TO RAPIDLY INCREASE THE CYBERSECURITY
    - COVER FOLLOWING AREAS:
      - CONTROL'S ACCESS
      - VULNERABILITIES MANAGEMENT
      - BACKUP
      - LOGGING
      - NETWORK SEC.
      - SEC OF HW AND SW
  - OWASP (OPEN WORLDWIDE APPLICATION SECURITY PROJECT) → GLOBAL COMMUNITY FOR APP. SEC. → INCLUDES:
    - LIST OF VULNERABILITIES
    - INSTRUMENTS

- OWASP RISK ASSESSMENT FRAMEWORKS ALLOWS TO:
  - ANALYZE APP.
  - TEST SEC.
  - FIND VULN.
  - EVALUATE RISKS
  - FOLLOWS STANDARD METHODOLOGIES
  - GUIDE FOR DEV.
  - TESTING METODOLOGIES
- USED ON
  - SW. DEVELOPMENT
  - SECURITY TEST

- GDPR (EUROPEAN LAW) → ABOUT PROTECTION OF PERSONAL DATA AND THEIR FREE MOVEMENT (OF DATA)
  - INTRODUCE CONCEPT AS:
    - PRIVACY BY DESIGN
    - DATA PROTECTION BY DEFAULT
  - BASED ON A FORM OF RISK MANAGEMENT

CERTIFICATIONS

- A THIRD-TRUSTED PART ATTESTATION → VERIFY A (PERSON / PRODUCT / SERVICE OR PROCESS) → RESPECT REQUIREMENTS
- TWO KINDS OF CERTIFICATION IN CYBERSECURITY
  - PROFESSIONAL → ATTESTING PEOPLE QUALIFICATIONS → IT VALIDATES THE PROFESSIONIST
  - PRODUCT, PROCESS AND SERVICE → ATTESTING THE PRESENCE OF CERTAIN FEATURES → IT VALIDATES THE TECHNOLOGY AND THE ORG
- MAIN ACTORS OF CERTIFICATIONS:
  - CERTIFICATION SCHEME → STRUCTURE THAT DEFINE HOW CERTIFICATION WORKS → (RULES ∧ REQUIREMENTS)
  - ACCREDITATION BODY → ENTITY THAT ESTABLISH IF AN ORG. IS AUTHORIZED TO CERTIFICATE
  - CERTIFICATION BODY → ENTITY WHO EXAMINES ∧ RELEASE THE CERTIFICATE
- STANDARDS FOR CERTIFICATION:
  - ISO 17000 → FOR VOCABULARY ∧ GENERAL PRINCIPLES → (STANDARDIZE LANGUAGE ∧ DEFINITION)
  - ISO 17024 → RULES TO CERTIFY PEOPLE
  - ISO 17065 → RULES TO CERTIFY PRODUCTS, PROCESSES ∧ SERVICES
- PROFESSIONAL CERTIFICATIONS — ORGS THAT PROVIDES THEM:
  - ISC2 (INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM
  - ECSF (EUROPEAN CYBERSECURITY SKILLS FRAMEWORK)
- CISSP (CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL) → PROFESSIONAL CERTIFICATION IN CYBERSECURITY → RELEASED BY ISC2 → IN LINE WITH ISO17024
  - REQUIREMENTS → 5 YEARS OF PAID FULL-TIME WORK → IN AT LEAST 2 OF THE FOLLOWING AREAS:
    - SEC. ∧ RISK MANAGEMENT
    - ASSET SEC.
    - SEC. ARCHITECTURE ∧ ENGINEERING
    - COMMUNICATION ∧ NET. SEC.
    - IDENTITY ∧ ACCESS MANAGEMENT
    - SEC. ASSESSMENT ∧ TESTING
    - SEC. OPERATIONS
    - SW DEV. SEC.

    → PASSING AN EXAM ON ALL DOMAINS
- ECSF (EUROPEAN CYBERSECURITY SKILLS FRAMEWORK) → DOESN'T RELEASE CERTIFICATES → IT'S EUROPEAN STANDARD THAT HELPS TO

- IDENTIFY ROLES IN CYBERSECURITY
- DESCRIBE SKILLS & ABILITIES FOR THESE ROLES

- IDENTIFIES 12 PROFILES → DEFINED BY THEIR:
  - RESPONSABILITIES
  - TASKS
  - REQUIRED KNOWLEDGE
  - SKILLS
  - TYPICAL ACTIVITIES
  - INTERDEPENDENCIES WITH OTHER PROFILES

A PROFILE IS A CATEGORY THAT GROUPS MANY ROLES

EX: "THREAT INTELLIGENCE" PROFILE includes job like:
- Cyber Threat Intelligence Analyst
- OSINT Specialist
- Malware Intelligence Researcher

- PRODUCT CERTIFICATIONS → ATTEST THE QUALITY OF A CERTAIN PRODUCT → "SECURITY CERTIFICATION" FOR A PRODUCT MEANS: → PRODUCT TESTED & PROVIDE:
  - PROB. OF ASSURANCE OF A SYSTEM
  - CAPABILITY TO BE IN LINE WITH SEC. SPECIFICATION/REQUIREMENTS
- MUST CHARACTERISTICS:
  - IMPARTIALITY → ACCREDITATION BODY → INDIPENDENT THIRD PARTIES FROM CLIENT
    - CERTIFICATION BODY
    - EVALUATOR (specialist that verify the product but don't release any certificate)
  - OBJECTIVITY → EVALUATION BASED ON EMPIRICAL EVIDENCE
  - REPEATABILITY → IF SAME EVALUATOR → REPEATS TEST UNDER SAME SEC. REQ. → RESULTS ARE SAME
  - REPRODUCIBILITY → OTHER EVALUATOR → REPEATS TEST UNDER SAME SEC. REQ. → RESULTS ARE SAME

- TSEC (TRUSTED COMPUTER SECURITY EVALUATION CRITERIA) → ISN'T A MODERN PRODUCT CERTIFICATION → BUT FIRST DOCUMENT FOR SW. CERTIFICATION
- MADE AVAILABLE BY NIST → INTRODUCED FIRST STANDARDIZED METHOD TO EVAL. & CLASSIFY SEC. LEVEL OF AN OPERATING SYSTEM
- BASED ON FUNDAMENTAL SEC. PRINCIPLES:
  - POLICY
  - ACCOUNTABILITY
  - ASSURANCE
- EVALUATION OF OPERATING SYSTEM → ATTRIBUTES TO 4 CLASSES:
  - MINIMAL PROTECTION
  - DISCRETIONARY PROTECTION
  - MANDATORY PROTECTION
  - VERIFIED PROTECTION

ITSEC IS EUROPEAN TSEC

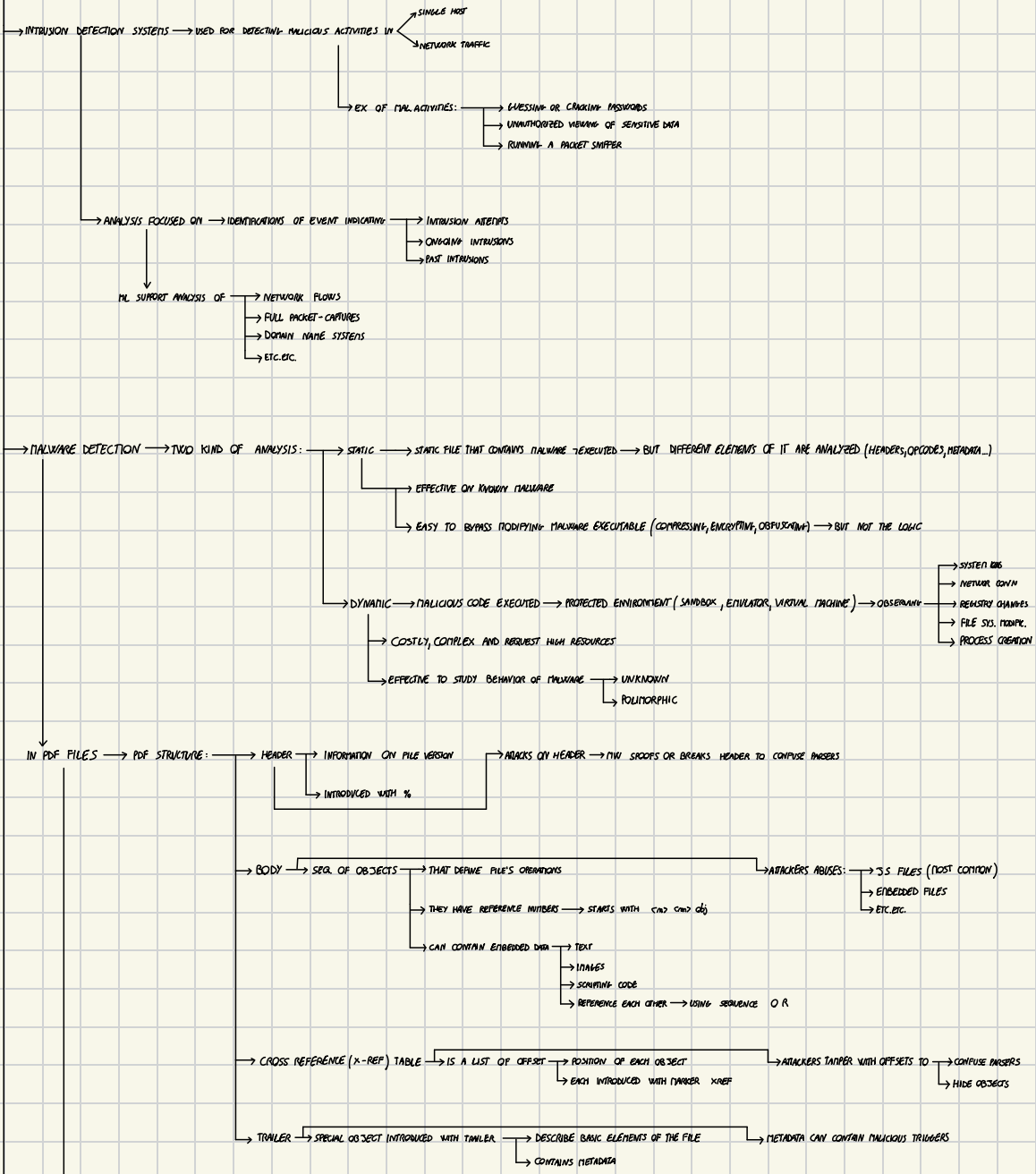
AFTERWARD TSEC/ITSEC ARE REPLACED BY COMMON CRITERIA (CC) → INTERNATIONAL STANDARD TO EVALUATE & CERTIFY SEC. OF IT PRODUCTS
- 18 AUTHORIZED MEMBERS TO RELEASE CERTIFICATIONS → ITALY PART OF IT WITH → ORGANISMO DI CERTIFICAZIONE DELLA SICUREZZA INFORMATICA (OCSI)

CC STRUCTURED AS:
- INTRODUCTION AND GENERAL MODEL → DEFINES BASIC PRINCIPLES
- SECURITY FUNCTIONAL REQUIREMENTS → A STANDARD TEMPLATE → DESCRIBE WHAT SEC. FUNCTIONS A PRODUCT PROVIDE AS:
  - AUTHENTICATION
  - AUDITING
  - ENCRYPTION
  - ACCESS CONTROL
  - DATA PROTECTION
- SECURITY ASSURANCE COMPONENTS → WHAT OF THE PRODUCT HAS TO BE TESTED AND VERIFIED
- FRAMEWORK FOR THE SPECIFICATION OF EVALUATION METHODS AND ACTIVITIES → HOW EVALUATORS SHOULD TEST
- PRE-DEFINED PACKAGES OF SECURITY REQUIREMENTS

CC DOCUMENTS:
- DESCRIBES:
  - WHICH PART OF PRODUCT ARE EVALUATED
  - WHAT SECURITY REQUIREMENTS MUST BE MET
  - LEVEL OF ASSURANCE REQUIRED
- ACTORS:
  - USER COMMUNITIES → (USERS WITH COMMON SECURITY NEEDS)
  - DEVELOPERS → (WHO DECLARE WHAT THE PRODUCT GIVES)
  - GOVERNMENTS OR LARGE CORPORATIONS → (WHO DEFINE MANDATORY REQUIREMENTS)

MACHINE LEARNING FOR COMPUTER SECURITY

- ML APPLICATION IN C.S CAUSED BY
  - RISING COMPLEXITY OF INFORMATION SYSTEM /\ INCREASED DATA FLOW
  - EVOLUTION OF DIGITAL THREATS
  - INCREASING DEPENDENCY OF SOCIETY ON IT SYSTEMS
- ML COULD SOLUTION FOR TASKS WHERE
  - UNKNOWN EXPLICIT ALGORITHM SOLUTION
  - POSSIBLE TO COLLECT LARGE AMOUNT OF TRAINING DATA
  - MANUALLY MANAGEMENT OF DATA VERY DIFFICULT
- EXAMPLES:
  - DETECTION OF
    - INTRUSIONS IN NETWORK
    - MALWARE
    - PHISHING
  - ANALYSIS OF
    - MALWARE
    - VULNERABILITIES
    - BINARY CODE
- CAPABILITIES OF ML
  - RECOGNITIONS OF HIDDEN, COMPLEX PATTERNS IN DATA
  - GENERALIZATIONS → CAN DETECT
    - ATTACKS NEVER SEEN
    - VARIANTS OF ALREADY KNOWN
- GOALS OF ML
  - ENABLE AUTOMATIC ANALYSIS OF LARGE AMOUNTS OF ATTACK'S DATA
  - DETECT ATTACKS THAT ARE INCREASING VARIABILITY /\ SOPHISTICATION
- ML APPROACHES IN COMPUTER SECURITY → FOUR TYPES OF TECHNIQUE
  - SUPERVISED LEARNING → TRAIN WITH LABELLED DATA → COSTLY
  - UNSUPERVISED LEARNING → TRAIN ON UNLABEL DATA
    - STANDALONE ATTACK DETECTION → BECAUSE IT RECOGNIZE PATTERNS → CLASSIFY
    - SUPPORTING TECHNIQUE
    - HARD TO EVALUATE CORRECTNESS WITHOUT LABELS
  - MISUSE BASED (SIGNATURE BASED) → ESTABLISHING DESCRIPTION OF KNOWN ATTACK MODELS → FLAG MALICIOUS IF MATCH WITH ANY
    - LOW FP → BUT EFFECTIVE ONLY WELL KNOWN THREATS
  - ANOMALY BASED → MODELS LEARN FROM "NORMAL BEHAVIOR" → FLAG ANOMALOUS EVERYTHING UNMATCH
    - POWERFUL DETECTING UNKNOWN ATTACKS → BUT
      - HARD DEFINE NORMAL
      - HIGH FP
- TYPICAL ML WORKFLOW
  - EVIDENCE A SEC. PROBLEM IS PRESENT
  - DATA COLLECTION (AND LABELLING)
  - SYSTEM DESIGN AND TRAINING
  - PERFORMANCE EVALUATION
  - DEPLOYMENT AND OPERATION
  - DELIVERY OF SECURITY SOLUTION
- PERFORMANCE EVALUATION → BASED ON:
  - EFFECTIVENESS → MEASURE FOR ITS EVAL → CONFUSION MATRIX → METRICS FROM IT
    - ACCURACY → $\frac{TP+TN}{ALL}$
    - PRECISION → $\frac{TP}{TP+FP}$
    - RECALL → $\frac{TP}{TP+FN}$
    - F-SCORE → $\frac{2}{\frac{1}{PRECISION}+\frac{1}{RECALL}}$
  - EFFICIENCY → COSTS AND USAGE OF RESOURCES
  - TRANSPARENCY → HOW UNDERSTANDABLE MODEL IS → BLACK BOXED MODEL MAKE IT HARD TO → JUSTIFY DECISIONS
    - DEBUG FP
  - CONTROLLABILITY → LEVEL OF CONFIDENCE OF AN ORG. IN DELEGATING SEC. DECISIONS TO AN ML SYSTEM
  - ROBUSTNESS → RESISTANCE OF THE MODEL TO → NOISE
    - EVASION ATTACKS → (MODIFY INPUTS TO TRICK THE ALREADY TRAINED MODEL)
      - RESULT IS CALLED ADVERSIAL EXAMPLE
    - DATA POISONING → MANIPULATING TRAINING DATA
- SPAM E-MAIL DETECTION/PHISHING: → LINEAR TEXT CLASSIFIER → WEIGH OF WORDS → CUMULATIVE SCORE → IF EXCEED A LIMIT → CLASSIFY SPAM / LEGITIMATE OTHERWISED


INTRUSION DETECTION SYSTEMS → USED FOR DETECTING MALICIOUS ACTIVITIES IN → SINGLE HOST / NETWORK TRAFFIC
EX. OF MAL. ACTIVITIES: → GUESSING OR CRACKING PASSWORDS / UNAUTHORIZED VIEWING OF SENSITIVE DATA / RUNNING A PACKET SNIFFER
ANALYSIS FOCUSED ON → IDENTIFICATIONS OF EVENT INDICATING → INTRUSION ATTEMPTS / ONGOING INTRUSIONS / PAST INTRUSIONS
ML SUPPORT ANALYSIS OF → NETWORK FLOWS / FULL PACKET-CAPTURES / DOMAIN NAME SYSTEMS / ETC.ETC.
MALWARE DETECTION → TWO KIND OF ANALYSIS: → STATIC → STATIC FILE THAT CONTAINS MALWARE ≠ EXECUTED → BUT DIFFERENT ELEMENTS OF IT ARE ANALYZED (HEADERS, OPCODES, METADATA...)
EFFECTIVE ON KNOWN MALWARE
EASY TO BYPASS MODIFYING MALWARE EXECUTABLE (COMPRESSING, ENCRYPTING, OBFUSCATING) → BUT NOT THE LOGIC
DYNAMIC → MALICIOUS CODE EXECUTED → PROTECTED ENVIRONMENT (SANDBOX, EMULATOR, VIRTUAL MACHINE) → OBSERVING → SYSTEM CALLS / NETWORK CONN / REGISTRY CHANGES / FILE SYS. MODIF. / PROCESS CREATION
COSTLY, COMPLEX AND REQUEST HIGH RESOURCES
EFFECTIVE TO STUDY BEHAVIOR OF MALWARE → UNKNOWN / POLIMORPHIC
IN PDF FILES → PDF STRUCTURE: → HEADER → INFORMATION ON FILE VERSION / INTRODUCED WITH %
ATTACKS ON HEADER → MW. SPOOFS OR BREAKS HEADER TO CONFUSE PARSERS
BODY → SEQ. OF OBJECTS → THAT DEFINE FILE'S OPERATIONS
THEY HAVE REFERENCE NUMBERS → STARTS WITH <num> <num> obj
CAN CONTAIN EMBEDDED DATA → TEXT / IMAGES / SCRIPTING CODE / REFERENCE EACH OTHER → USING SEQUENCE OF
ATTACKERS ABUSES: → JS FILES (MOST COMMON) / EMBEDDED FILES / ETC.ETC.
CROSS REFERENCE (X-REF) TABLE → IS A LIST OF OFFSET → POSITION OF EACH OBJECT / EACH INTRODUCED WITH MARKER xref
ATTACKERS TAMPER WITH OFFSETS TO → CONFUSE PARSERS / HIDE OBJECTS
TRAILER → SPECIAL OBJECT INTRODUCED WITH TRAILER → DESCRIBE BASIC ELEMENTS OF THE FILE / CONTAINS METADATA
METADATA CAN CONTAIN MALICIOUS TRIGGERS
PRE-PROCESSING THE FILE → TO DETECT → JS OR AS CODE / ANALYZE METADATA / VERIFYING INTEGRITY OF X-REF

→ LIMITATIONS OF ML FOR COMPUTER SECURITY → SOME EXAMPLES:

- → SPURIOUS CORRELATIONS → HAPPENS WHEN MODEL LEARNS PATTERNS THAT CORRELATE WRONGLY TO A LEABLE → EX: Long URL = MW
- → DATA SNOOPING → WHEN IN TRAINING SET THE MODEL SEES INFORMATION THAT WOULD BE AVAILABLE IN REAL-WORLD CONDITIONS:
  - EX: MALWARE 2015-2025 → DURING RANDOM SPLIT TRAINING 2024-2025, TEST 2019 → MODEL PERFECT IN TEST BECAUSE THEY ARE OLD VERSION
  - BUT IN PRODUCTION WHEN HE SEES A NEW VARIANT IT FAILS → SO IT MADE YOU THINK IT HAD A GOOD GENERALIZATION → BUT IT HASN'T
- → BASE RATE FALLACY → WHEN DATASET IS CLASS-IMBALANCED → ACCURACY IS MISLEADING → PREDICTING DOMINANT CLASS = HIGH ACCURACY
- → LABEL INACCURACY → WHEN LABELS ARE → WRONG / OUTDATED / INCONSISTENT / AMBIGUOUS

ADVERSIAL MACHINE LEARNING

→ CATEGORIZATION OF ATTACKS AGAINST MACHINE LEARNING → IN BASE OF COMPROMISING C.I.A. (CONFIDENTIALITY, INTEGRITY, AVAILABILITY) OF → TEST DATA / TRAINING DATA

→ ATTACKERS VS DEFENDERS → CALLED ARM RACE

→ COMMON WEAKNESS → ML MODELS LEARN THREAT/RISK MODEL → THAT MATCH HOW ATTACKERS BEHAVE IN REAL LIFE

EXAMPLE: SPAM FILTERING RACE → ATTACKERS EVOLVED AGAINST SPAM FILTER BASED ON KEYWORDS:

- → OBFUSCATION OF SUSPICIOUS WORD (FREE MONEY → FREE MONEY)
- → SPACE BETWEEN CHARACTERS
- → ADDING GOOD WORDS → TO KEEP DOWN THE SCORE
- → SPAM MESSAGES INTO ATTACHED IMAGES

→ DEFENDERS RESPOND WITH OCR (OPTICAL CHARACTER RECOGNITION) → ANALYSIS OF TEXT FROM ATTACHED IMAGES

WHAT IS IT? → SUBFIELD OF ML STUDIES

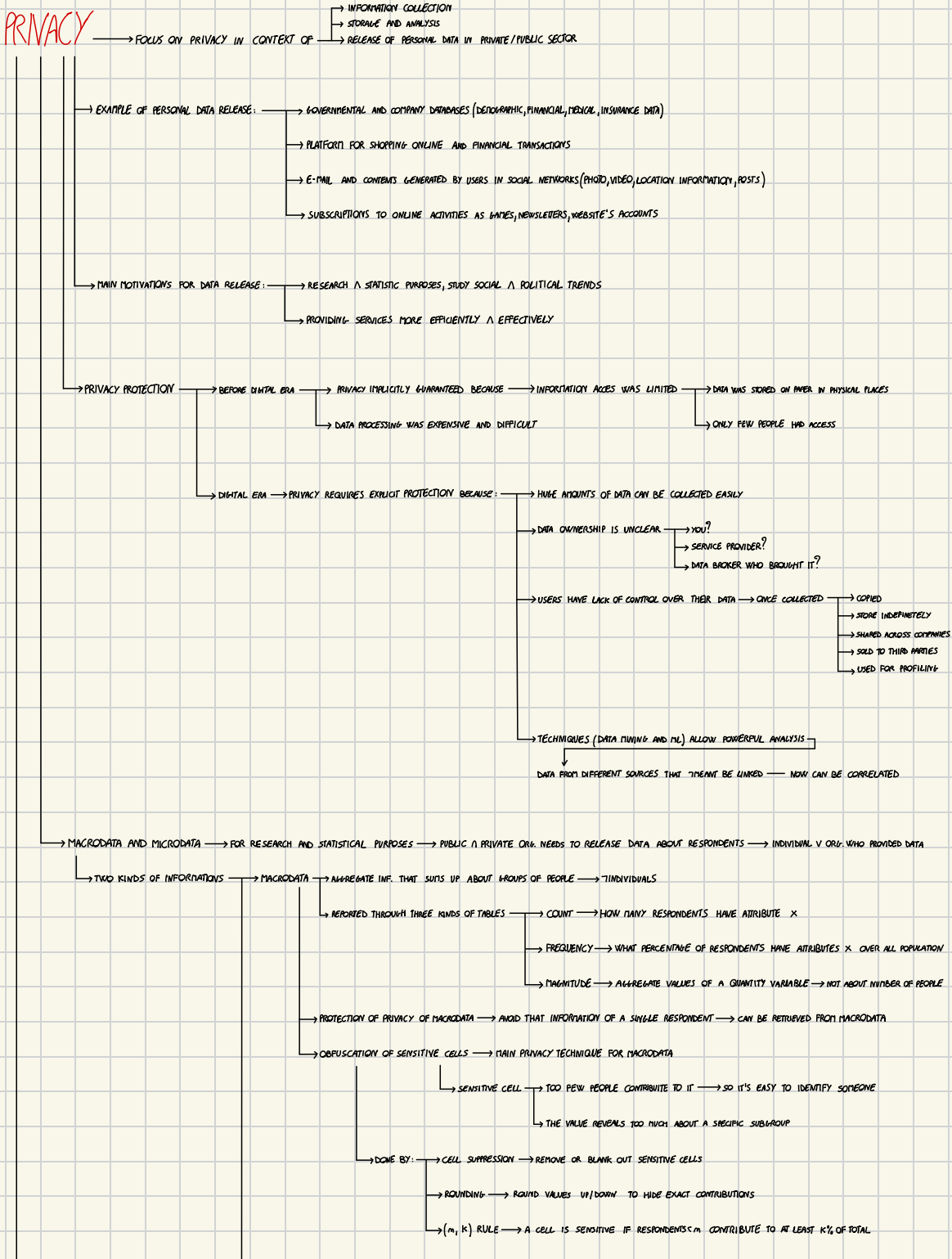
- → HOW ATTACKERS CAN MANIPULATE ML SYSTEMS
- → HOW TO MAKE ML MODELS SECURE BY DESIGN → MEANING SECURITY IS INCLUDE FROM THE BEGINNING OF THE DEVELOPMENT OF THE SYSTEM → "AFTER "BUILD MODEL AND THEN TRY TO DEFEND IT" BUT → U BUILD IT ALREADY KNOWING IT WILL BE ATTACKED

→ MAIN GOAL → ACHIEVE SECURITY BY DESIGN PRINCIPLE

- → TRADITIONAL ML ASSUMES: → DATA CLEAN / INPUT ARE HONEST / LABEL CORRECT / ETC.ETC. → IN C.S THIS ASSUMPTIONS ARE FAKE
- → IN SECURE-BY-DESIGN: → PREVENTIN DATA POISONING / AVOID SPURIOUS CORRELATIONS / ADDING ADVERSIAL TRAINING / ETC.ETC.
- → EVALUATE ROBUSTNESS OF ML SYSTEMS SIMULATING ATTACKS
- → FIND POTENTIAL OR SPECIFIC VULNERABILITIES IN ML SYSTEMS
- → IDENTIFY ATTACKS THAT COULD EXPLOIT ML SYSTEM'S VULNERABILITIES
- → DEVELOP DEFENCE STRATEGIES

→ SECURITY IN

- → NORMAL ML SYSTEMS → REACTIVE: ATTACK'S ACTION - DESIGNER REACTION
- → ADVERSIAL ML SYSTEMS → PROACTIVE APPROCH: DESIGNER IMPERSONATE ATTACKERS


PRIVACY
FOCUS ON PRIVACY IN CONTEXT OF
INFORMATION COLLECTION
STORAGE AND ANALYSIS
RELEASE OF PERSONAL DATA IN PRIVATE/PUBLIC SECTOR
EXAMPLE OF PERSONAL DATA RELEASE:
GOVERNMENTAL AND COMPANY DATABASES (DEMOGRAPHIC, FINANCIAL, MEDICAL, INSURANCE DATA)
PLATFORM FOR SHOPPING ONLINE AND FINANCIAL TRANSACTIONS
E-MAIL AND CONTENTS GENERATED BY USERS IN SOCIAL NETWORKS (PHOTO, VIDEO, LOCATION INFORMATION, POSTS)
SUBSCRIPTIONS TO ONLINE ACTIVITIES AS DATES, NEWSLETTERS, WEBSITE'S ACCOUNTS
MAIN MOTIVATIONS FOR DATA RELEASE:
RESEARCH & STATISTIC PURPOSES, STUDY SOCIAL & POLITICAL TRENDS
PROVIDING SERVICES MORE EFFICIENTLY & EFFECTIVELY
PRIVACY PROTECTION
BEFORE DIGITAL ERA
PRIVACY IMPLICITLY GUARANTEED BECAUSE
INFORMATION ACCES WAS LIMITED
DATA WAS STORED ON PAPER IN PHYSICAL PLACES
ONLY FEW PEOPLE HAD ACCESS
DATA PROCESSING WAS EXPENSIVE AND DIFFICULT
DIGITAL ERA
PRIVACY REQUIRES EXPLICIT PROTECTION BECAUSE:
HUGE AMOUNTS OF DATA CAN BE COLLECTED EASILY
DATA OWNERSHIP IS UNCLEAR
YOU?
SERVICE PROVIDER?
DATA BROKER WHO BROUGHT IT?
USERS HAVE LACK OF CONTROL OVER THEIR DATA
ONCE COLLECTED
COPIED
STORE INDEFINETELY
SHARED ACROSS COMPANIES
SOLD TO THIRD PARTIES
USED FOR PROFILING
TECHNIQUES (DATA MINING AND ML) ALLOW POWERFUL ANALYSIS
DATA FROM DIFFERENT SOURCES THAT MEANT BE LINKED
NOW CAN BE CORRELATED
MACRODATA AND MICRODATA
FOR RESEARCH AND STATISTICAL PURPOSES
PUBLIC & PRIVATE ORG. NEEDS TO RELEASE DATA ABOUT RESPONDENTS
INDIVIDUAL V ORG: WHO PROVIDED DATA
TWO KINDS OF INFORMATIONS
MACRODATA
AGGREGATE INF. THAT SUMS UP ABOUT GROUPS OF PEOPLE
NOT INDIVIDUALS
REPORTED THROUGH THREE KINDS OF TABLES
COUNT
HOW MANY RESPONDENTS HAVE ATTRIBUTE X
FREQUENCY
WHAT PERCENTAGE OF RESPONDENTS HAVE ATTRIBUTES X OVER ALL POPULATION
MAGNITUDE
AGGREGATE VALUES OF A QUANTITY VARIABLE
NOT ABOUT NUMBER OF PEOPLE
PROTECTION OF PRIVACY OF MACRODATA
AVOID THAT INFORMATION OF A SINGLE RESPONDENT
CAN BE RETRIEVED FROM MACRODATA
OBFUSCATION OF SENSITIVE CELLS
MAIN PRIVACY TECHNIQUE FOR MACRODATA
SENSITIVE CELL
TOO FEW PEOPLE CONTRIBUTE TO IT
SO IT'S EASY TO IDENTIFY SOMEONE
THE VALUE REVEALS TOO MUCH ABOUT A SPECIFIC SUBGROUP
DONE BY:
CELL SUPPRESSION
REMOVE OR BLANK OUT SENSITIVE CELLS
ROUNDING
ROUND VALUES UP/DOWN TO HIDE EXACT CONTRIBUTIONS
(n, k) RULE
A CELL IS SENSITIVE IF RESPONDENTS ≤ n CONTRIBUTE TO AT LEAST k% OF TOTAL

- MICRODATA → INFORMATION IN TABLE → SET OF ATTRIBUTES WITH VALUES RELATED TO A SINGLE RESPONDENT
  - BASIC STEP TO PROTECT PRIVACY → GUARANTEE ANONYMITY OF RESPONDENTS → DOING DE-IDENTIFICATION → HIDE → REMOVING / ENCRYPTING
    - PERSONAL ATTRIBUTES USEFUL FOR IDENTIFICATION → BUT DE-IDENTIFICATION ¬GUARANTEED ANONYMITY COMPLETELY
      - A STUDY ON 2000 US CENSUS SHOWED → LARGE FRACTION OF POPULATION UNIQUELY IDENTIFIABLE WITH (DATE OF BIRTH, GENDER, ZIP CODE)
      - → CROSS-REFERENCE DATA WITH EXTERNAL DATASET
      - → USE QUASI-IDENTIFIER (BIRTH DATE, GENDER, OCCUPATION...)
      - → ML TO INFER MISSING ATTRIBUTES
  - TWO CATEGORIES OF MICRODATA PROTECTION TECHNIQUES:
    - SYNTACTIC → GOAL IS PROTECT PRIVACY OF RESPONDENTS ONLY → PRIVACY LEVEL BASED ON K-ANONYMITY: → EACH DATA MUST CORRELATED TO AT LEAST K INDIVIDUALS SO ¬POSSIBLE UNDERSTAND SPECIFIC USER BELONGS TO
      - MASKING TECHNIQUES → ORIGINAL DATA ARE MODELLED MAINTAINING VALIDITY OF STATISTICAL ANALYSIS
        - PERTURBATIVE → MODIFY DATA KEEPING SAME STATISTICS
          - NOISE ADDITION: 1-2-3 AVG ≅ 2 → 1.2-1.9-3.2 AVG ≅ 2
          - SWAPPING VALUES: 1-2-3 → 3-1-2
          - MICROAGGREGATION: 1-2-3 AVG = 2 → 2-2-2 AVG = 2
        - NON PERTURBATIVE → REMOVE OR GENERALIZE
          - CELL SUPPRESSION: AVG SALARY: 150k → AVG SALARY: SUPPRESSED → VALUE ¬CHANGE AND ¬PUBLISHED
          - GENERALIZATION: AVG SALARY: 150k → AVG SALARY: 100k-200k
      - IN GENERAL SYNTHETIC DATA TECHNIQUES → GENERATE ARTIFICIAL DATAS THAT IMITATES THE REAL ONES (KEEP SAME STATISTICS)
        - FULLY SYNTHETIC → EVERY RECORD IS ARTIFICIAL → DISTRIBUTIONS STAY ALMOST THE SAME
        - PARTIALLY SYNTHETIC DATA → ONLY SENSITIVE COLUMNS ARE ARTIFICIAL
    - SEMANTIC → GOAL IS PROTECT PRIVACY OF
      - RESPONDENTS
      - NON-RESPONDENTS → (è importante perché magari un attacker vuole capire se tu sei presente nel dataset: se analisi è identica con o senza di lui allora non c'è altrimenti c'è)
      - DIFFERENTIAL PRIVACY: → ANALYSIS OUTPUT SHOULD BE INSENSITIVE → CANNOT DISTINGUISH IF AN INDIVIDUAL PRESENT OR NOT IN DATASET:
        - IF I'M PART OF DATASET → RESULT
        - IF ¬PART OF DATASET → ≅RESULT
  - STARTING FROM A DATASET "T" OF MICRODATA → APPLYING MICRODATA PROTECTION TECHNIQUES PRODUCE NEW DATASET T_0 WITH 2 REQUIREMENTS
    - ENOUGH MODIFIED/PROTECTED TO ¬RE-IDENTIFY
    - KEEP ALMOST SAME STATISTICS OF ORIGINAL DATASET "T"

- K-ANONYMITY (FUNDAMENTALS) → MASKING NON-PERTUBATIVE THAT
  - GUARANTEE ANONYMITY ∧ AVOID RE-IDENTIFICATION
  - SATISFY SYNTACTIC PRIVACY REQUIREMENTS (¬POSSIBLE TO RELATE INFORMATIONS TO MORE THAN K INDIVIDUALS)
  - GENERALIZATION AND SUPPRESSION
  - ASSUMPTIONS OF THIS TECHNIQUES:
    - ALL RELEASED DATA IN A SINGLE TABLE → THIS TABLE IS THE ONLY RESOURCE OF THE ATTACKER
    - AFTER RELEASE → TABLE NEVER MODIFIED
    - ∀ RESPONDENT = 1 TUPLE
    - DATA HOLDER KNOWS WHICH EXTERNAL INFORMATIONS CAN BE USED BY ATTACKER FOR RE-IDENTIFICATION
    - MICRODATA ATTRIBUTES ARE ORGANISED IN CATEGORIES:
      - IDENTIFIERS → ALLOW UNIQUE IDENTIFICATION OF A RESPONDENT
      - QUASI-IDENTIFIERS
        - TAKEN ALONE NO-SENSE
        - ATTRIBUTES PRESENT ALSO IN EXTERNAL RESOURCES
          - AND COMBINED WITH THEM → POSSIBLE RE-IDENTIF

→ CONFIDENTIAL ATTRIBUTES ⟶ SENSITIVE INFORMATION

→ ¬ CONFIDENTIAL ATTRIBUTES ⟶ ¬ SENSITIVE INFORMATION

K-ANONYMITY REQUIREMENTS ⟶ RELEASED INF. ¬POSSIBLE RELATE TO LESS THAN K

→ SAME COMBINATION OF QUASI-IDENTIFIER MUST APPEARS IN K DIFFERENT INDIVIDUALS ⟶ IN ORDER TO ¬KNOW THE REAL MATCH

→ multiforme caso che abbiamo un dataset di 10 righe. Per ogni riga esiste un gruppo di righe uguali sui QUASI-IDENTIFIERS per esempio abbiamo due gruppi da 4 e uno da due. Se io voglio K=4 il primo e il secondo gruppo soddisfano la condizione cardinalità ≥ k, ma il secondo gruppo 2 2 4 no. In questo caso ⟶ MICRODATA TABLE ¬SATISFY K-ANONYMITY REQ. ⟶ IF SO GENERALISATION V SUPPRESSION ARE NECESSARY

→ BOTH CAUSE INF.LOSS BUT IT'S A COMPROMISE ⟶ IDEAL GOAL COMPUTE MICRODATA TABLE FOR DESIRED K WITH MINIMAL LOSS OF INFORMATION

ATTRIBUTE DISCLOSURE PROTECTION — K-ANONYMITY PROTECT IDENTITY OF RESPONDENTS — ¬(RISERVATEZZA) ¬ DISCLOSURE OF SENSITIVE INFORMATION — TWO ATTACKS CAN HAPPEN EVEN IF TABLE IS K-ANONYMOUS

→ HOMOGEINITY ATTACK — IF ALL ROWS WITH A COMBINATION OF ATTRIBUTES (QUASI-IDENTIFIER CLASS) — HAVE SAME VALUE FOR SENSITIVE ATTRIBUTE

↓ K-ANONYMITY IRRELEVANT — EXAMPLE: even if we have K rows with same combination values, AGE-CAP-SEX-DISEASE, and DISEASE is sensitive, it don't matter if identity is protected it don't matter because if everyone has DISEASE: HIV, even if i don't know which exactly is my victim, i know it has HIV

→ EXTERNAL KNOWLEDGE ATTACK — ATTACKERS HAVE MORE INFORMATION ON THE VICTIM — AND GIVEN THE VALUE OF A SENSITIV ATTRIBUTE — IS POSSIBLE TO REDUCE UNCERTAINTY

→ EXAMPLE: name AGE-CAP-SEX-DISEASE but only one or two have the flu instead of HIV and the attacker knows the victim hasn't been recovered in hospital, he attacker can say victim is one of the two people with the flu

→ THIS ATTACKS ASSUME ATTACKER KNOWS COMBINATION OF ATTRIBUTES THAT FORMS THE Q.I. CLASS AND 1 ONLY ONE SENSITIVE ATTRIBUTE

→ l-DIVERSITY IS INTRODUCED TO SOLVE THIS PROBLEM — FOR EACH Q.I. CLASS NEEDS TO CONTAIN A NUMBER l OF DIFFENT VALUE OF THE SENSITIVE ATTRIBUTE

→ k-ANONYMOUS ∧ l-DIVERSE TABLE STILL VULNERABLE TO ATTACKS THAT LEAD TO SENSITIVE ATTRIBUTE DISCLOSURE:

→ SKEWNESS (ASSIMETRIA) ATTACKS: IF DISTRIBUTION OF SENSITIVE DATA IS UNBALANCED IT CAN REVEAL PERCENTAGES — WHICH ALSO IS A VIOLATION OF PRIVACY

→ SIMILARITY ATTACKS: WHEN VALUES ARE SEMANTICALLY SIMILAR — EXAMPLE: we have 3 rows, sensitive attribute DISEASE shows 3 different heart diseases, so even if it's not possible identify the real one, attacker knows for sure a heart disease.

→ TO REDUCE EFFECTIVNESS OF BOTH ATTACKS — t-CLOSENESS: — DISTRIBUTION IN A Q.I. CLASS — SIMILAR TO THE GLOBAL DISTRIBUTION OF THE WHOLE TABLE

→ VALUE OF t IS THE DEGREE OF ATTRIBUTE DISCLOSURE PROTECTION

APPLICATION SCENARIOS — FOR K-ANONYMITY

→ LOCATION-BASED SERVICES — POSITION IS BOTH A Q.I. AND A SENSITIVE DATA — NEEDS PROTECTION

→ MOVEMENTS DATA — TRAJECTORY CAN BE SENSITIVE

→ SOCIAL NETWORKS ANALYSIS

→ CONTACT TRACING — IDENTIFY CONTACT AT RISK WITHOUT REVEALING IDENTITY — BUT IF ATTACKERS KNOWS WHERE/WHEN OR HOW MANY CONTACT VICTIM HAD — K-ANON USELESS

→ FOR EACH SCENARIO — k-ANONIMITY REQUIREMENTS CAN BE CUSTOMIZED

SEMANTIC APPROACHES ⟶ DIFFERENTIAL PRIVACY IS A TECHNIQUE ⟶ THAT AIMS TO PROTECT PRIVACY OF BOTH RESPONDENTS AND ¬RESPONDENTS ⟶ RESULTS OF ANALYSIS ¬LET UNDERSTAND WHETHER U IN/OUT

- BASED ON CONTROLLED NOISE ADDITION → SO IT'S NOT TRUTH-PRESERVING → DATA RELEASED AREN'T EXACTLY REAL BUT MODIFIED
- DIFFERENTIAL PRIVACY REQUIREMENTS → GIVEN 2 DATASET THAT CHANGE ONLY OF 1 PERSON → NEEDS TO OBTAIN SAME PROBABILITY RESULT
- IT CAN BE APPLIED IN 2 WAYS → INTERACTIVE SCENARIO → DATASET W'S PRIVACY
  - EVERY TIME QUERY IS DONE — SYSTEM CALCULATE REAL RESULT AND THEN ADD NOISE
  - NON-INTERACTIVE SCENARIO → A NEW NOISE ADDED VERSION OF THE DATASET IS PUBLISHED
  - PARAMETER ε MEASURE HOW MUCH NOISE IS ADDED

- EXAMPLE OF PRIVACY VIOLATIONS:
  - AOL (AMERICA ONLINE) → RELEASED 20 MILLION RECORDS OF 650K USERS OF IT'S SEARCH ENGINE → FOR RESEARCH PURPOSE
    - RECORD → ID, QUERY TERM, TIMESTAMP, RESULTS CLICKED BY USERS AND CORRESPONDING WEBSITE
    - TWO REPORTERS RE-IDENTIFY USERS
    - AOL WAS FORCED TO REMOVE THE RELEASED DATA
  - NETFLIX INCIDENT → PROVIDED 100 MILLION DE-IDENTIFIED RECORDS → RECORDS → ID NUMBER, MOVIE RENTED, RATING GIVEN, DATE OF RATING
    - COULD BE RE-IDENTIFY BY CROSS-REFERENCE WITH RATINGS ON INTERNET MOVIE DATABASE (IMDb)
  - PARTICIPANTS TO GENETIC RESEARCH → DIFFERENT STUDIES DEMONSTRATED → IDENTIFY PEOPLE PARTECIPATED IN GENETIC RESEARCH → EASILY DISCOVERED THROUGH CROSS-REFERENCE PUBLIC INF.

SOCIAL ENGINEERING (SE)

→ ALL TECHNIQUES THAT TRICKS PEOPLE WITH PSYCHOLOGICAL MANIPULATION → TO DO → ACTIONS, DIVULGATE SENSITIVE/CONFIDENTIAL INF.

- THEY EXPLOIT HUMAN TENDENCY TO → TRUST AUTHORITIES, TRUST URGENT MESSAGES, ACT INSTICTIVELY IN STRESS
- BECAUSE THE WEAKEST LINK ISN'T THE SISTEM → BUT PEOPLE

- SE EMERGING THREAT (GENERATIVE AI) → REALISTIC CONTENT GENERATOR → IMPROVING BELIEVABILITY AND DECEPTION
  - ADVANCED TARGETING → THANKS TO ONLINE DATA → ATTACKS ARE MORE PERSONALIZED AND EFFICIENTS
  - AUTOMATED ATTACK INFRASTUCTURE → LARGE-SCALE SIMULTANEOUS ATTACKS

- PHISHING → MOST EFFECTIVE FORM OF SE
  - PRETENDING TO BE TRUSTING → MESSAGES DESIGNED TO STEAL INFORMATION → MAKE VICTIM PERFORMING ACTIONS
  - TYPES → CLASSICAL → NON-TARGETED FOR A SPECIFIC PERSON BUT MADE IN LARGE SCALE
    - VISHING → MADE THROUGH PHONE CALLS
    - SMISHING → VIA SMS ABOUT DAILY ROUTINE ("il tuo pacco")
    - SPEAR PHISHING → SPECIFIC FOR A PERSON OR A GROUP → REQUIRED TO COLLECT INF. ABOUT THE VICTIM
    - WHALING → TARGETING OF HIGH LEVEL (CEO, CFO)

- HUMANS AS THE WEAKEST LINK → PERSUASION IN S.E. BASED ON FIVE PRINCIPLES:
  - AUTHORITY → PEOPLE OBEY TO AUTHORITY / EXPERT FIGURES WITHOUT VERIFYING
  - SOCIAL PROOF → PEOPLE TEND TO IMITATE / REPEAT WHAT MAJORITY DO → REDUCE RISK SENSE
  - LIKING, SIMILARITY, DECEPTION → TEND TO TRUST WHO LOOKS FAMILIAR
  - DISTRACTION
    - → BRING INDIVIDUAL TO FOCUS ON WHAT IT CAN BE GAINED OR LOST
    - → INCREASING EMOTIONS → PEOPLE FORGET IMPORTANT CONSIDERATIONS WHEN MAKE DECISIONS
  - COMMITMENT, INTEGRITY, RECIPROCATION → RESPONDING TO FAVOURS → DUE TO A SENSE OF COMMITMENT IN A TRUSTED RELATIONSHIP

- EFFECTIVNESS OF S.E IN THE ONLINE
  - LACK OF SOCIAL AND BODY LANGUAGE
  - HIGH ANONYMITY
  - LACK OF MANY ELEMENTS OF PHYSICAL APPEARANCE THAT MAKE TRUSTABLE
  - NO DISTANCE → ATTACKS ARE POSSIBLE EVERYWHERE WITHOUT MOVING
  - HIGH CONTROL OF HOW AND WHEN ATTACK

- EXAMPLES OF PSYCHOLOGICAL MANIPULATION TECHNIQUES
  - PRETEXTING ∧ IMPERSONATION
    - → COLLECT INF. OF VICTIM
    - → CREATE A SCENARIO WHERE ATTACKER APPEARS RELIABLE
  - REVERSE SOCIAL ENGINEERING
    - → CONVINCE THE VICTIM TO SEARCH ASSISTANCE
    - → PROVIDES ASSISTANCE → WHICH ALSO HIDES THE ATTACK
  - BAITING → CURIOSITY BAIT VICTIMS INTO DOING ACTIONS → THAT FACILITATES ATTACKER'S GOAL
  - PRESSURE ∧ SOLUTION → CREATE EMOTIONAL PRESSURE → THEN ATTACKER PROPOSE SOLUTION → THAT REDUCE PRESSURE
  - CHAIN OF AUTHENTICATION → IMPERSONATE RECOGNIZE TRUSTED FIGURES (in impersonation devo convincerli, qua la vittima è convinta perché chi parla è già conosciuto)
  - GAINING CREDIBILITY → CREATING FALSE JUSTIFICATION OR SCENARIO → TO INCREASE CREDIBILITY OF ATTACKER
  - SOCIAL PROOF → PERSUSION IS USED TO CRAFT MESSAGES → WHERE VICTIM INDUCTED TO FOLLOW THE MAJORITY
  - FRAMING INFORMATION → PRESENT INFORMATION TO ORIEN VIEWER'S PERCEPTION IN A CERTAIN DIRECTION → REALITY DOESN'T CHANGE, IT CHANGE HOW IT IS PRESENTED

- S.E. ATTACK ARE CATEGORIZED IN BASE OF HOW MUCH THE ENGAGE OF THE VICTIM IS CLOSE
  - HUMAN-BASED → NEEDS DEEP PESONAL INTERACTION
  - COMPUTER-BASED → MORE AUTOMATED AND ON A LARGE SCALE

- S.E. IS JUST THE THIRD STEP OF AN ATTACK
  - 1) OSINT → RESOURCES ABOUT THE VICTIM ARE GATHERED
  - 2) SELECTION OF THE TARGET
  - 3) S.E. CAMPAIGN → TECHNIQUES ARE APPLIED
  - 4) AD-HOC TECHNOLOGICAL ATTACKS → DUE TO ACCESS TO ASSETS AND SENSITIVE DATA ARE RETRIEVED
  - (steps 1–4) → THIS IS CALLED **ATTACK VECTOR**

- DEFENSE STRATEGIES IN TWO CATEGORIES:
  - TECHNICAL MEASURE
    - SOFTWARES
    - FILTERS
    - ANTI-VIRUS
    - CLIENT/SERVER TOOLS
    - ML FOR RECOGNIZE PHISHING
    - ECC. ECC.
  - HUMAN-RELATED / ORGANIZATIVES MEASURES
    - → MOST EFFECTIVE CUZ ATTACKS OFTEN BYPASS TECHNICAL CONTROLS EXPLOITING HUMAN ERROR
    - → THE IDEA IS TO INCREASE PEOPLE'S CAPACITY TO RECOGNIZE AND MANAGE MANIPULATION
    - → EXAMPLES:
      - FORMATION
      - AWERNESS
      - SIMULATION
      - ORGANIZATION POLITICS
      - VERIFICATION PROCEDURES

- S.E. ATTACK CYCLE
  - ATTACK FORMULATION
    - 1) GOAL IDENTIFICATION
    - 2) TARGET IDENTIFICATION
  - INFORMATION GATHERING
    - 3) IDENTIFY POTENTIAL SOURCES
    - 4) GATHER INFORMATION FROM SOURCES
    - 5) EVALUATE THE COLLECTED INFORMATION
  - PREPARATION
    - 6) COMBINATION AND ANALYSIS OF GATHERED INFORMATION
    - 7) DEVELOPMENT OF AN ATTACK VECTOR → CREATE PHISHING EMAILS, FAKE ACCOUNT, FAKE DOCUMENTS...
  - DEVELOP RELATIONSHIP
    - 8) ESTABLISHMENT OF COMMUNICATION
    - 9) RAPPORT BUILDING
  - EXPLOIT RELATIONSHIP
    - 10) PRIMING THE TARGET → MENTALLY PREPARE THE VICTIM
    - 11) ELICITATION → OBTAIN WHAT YOU WANT (CREDENTIALS, ACCESS, ACTIONS)
    - (THIS IS THE REAL ATTACK PHASE OF SOCIAL ENGINEERING)
  - DEBRIEF
    - 12) MAINTENANCE → KEEP THE RELATION FOR FUTURE ATTACKS
    - 13) TRANSITION → FROM HUMAN MANIPULATION TO TECH ATTACKS (MALWARE, LATERAL MOVEMENT)
    - 14) GOAL SATISFACTION

OSINT (OPEN SOURCE INTELLIGENCE)

- WHERE "INTELLIGENCE" → MEANS THE PROCESS OF
  - IDENTIFYING
  - COLLECTING
  - ANALAZYING
  - REFINING
  - → INFORMATIONS → AND THE RESULT IS ACTIONABLE INTELLIGENCE → SOMETHING CAN BE USED TO DECIDE OR TO TAKE ACTIONS (CHOOSE TARGET, IDENTIFY A VULNERAB, PREVENT A RISK)

- THREE IMPORTANT CONCEPTS
  - DATA → SET OF INFORMATION → IN RAW FORM → WHAT THEY CONTAINS?
    - WITHOUT EXPLANATION
    - OPAEN UNSTRUCTURED
  - INFORMATION → OUTPUT OF DATA PROCESSING → WITH CONNECTIONS BETWEEN DATA → WHAT THEY MEANS?
    - CAN BE
      - CLASSIFIED → COLLECTED IN CONFIDENTIAL AND PRIVATE WAYS (GOVERNMENT BODIES) → NOT AVAILABLE TO BE SEEN
      - CLOSED SOURCE → FOUND IN STRUCTURED IN DATABASE → WITH LIMITED ACCESS
      - OPEN SOURCE → PUBLICLY AVAILABLE BUT ¬NECESSARILY FREE → THESE INF. ARE LESS ACCURATE BECAUSE OF
        - ¬INACCURACY
        - ¬COMPLETE
        - INFLUENCED BY PUBLIC OPINION
  - INTELLIGENCE → ANALYSIS, EVALUATION, INFERENCES OF INFORMATION → TO ANSWER TO A SPECIFIC QUERY → WHAT CAN I DO WITH THEM?
    - DIVIDED IN CATEGORIES
      - HUMINT → HUMAN INTELLIGENCE → INFORMERS, INVESTIGATORS
      - COMINT → COMMUNICATIONS INTELLIGENCE → INTERCEPTION OF COMMUNICATIONS BETWEEN TWO PARTIES
      - SIGINT → SIGNAL INTELLIGENCE → ANALYSIS OF ELECTRONIC TRASMISSIONS → COLLECTED BY SHIPS, PLANES, SATELLITES
      - PHOTINT → PHOTO INTELLIGENCE
      - OSINT → OPEN SOURCE INTELLIGENCE → PROCESS OF COLLECTING INTELLIGENCE FROM PUBLIC AVAILABLE RESOURCES
        - WITHOUT VIOLATING PRIVACY LAWS V COPYRIGHT

- OSINT IS THE THIRD STEP OF A PROCESS:
  - 1) COLLECT OPEN-SOURCE DATA
  - 2) OSINF (OPEN SOURCE INFORMATION) → OPEN-SOURCE DATA ARE PROCESSED ∧ ORGANIZE AS INFORMATIONS

3) OSINT → INTELLIGENCE DERIVED FROM OSINF → AS A RESULT OF EXPERT ANALYSIS

→ WHO USES OSINT? → BY →
- NATIONAL SECURITY
- NON-GOVERNMENTAL ORGANIZATION (NATO)
- ACADEMIC RESEARCH
- INVESTIVE JOURNALISM
- PRIVATE INDIVIDUALS
- TRACK PEOPLE V FIND MISSING PEOPLE

→ IN CYBERSECURITY CONTEXT BOTH FOR ATTACKING Λ DEFENSE

→ USING OSINT FOR INVESTIGATIONS CAN REVEAL INFORMATION NOT EXPICITLY MADE PUBLICLY AVAILABLE → PUTTING PRIVACY AT RISK → SUCH AS →
- POLITICAL INCLINATION
- RELIGIOUS BEEFS
- SEXUAL ORIENTATION

→ OSINT IS LEGAL ONLY IF IT DOESN'T VIOLATE →
- RULE OF ACCESS → OF THE PLATFORMS
- AUTHENTICATIONS
- SERVICE'S TERM

→ EXAMPLES:
- ¬ CREATE FAKE ACCOUNTS IF SOCIALS DOESN'T ALLOW IT
- ¬ ACCESS PRIVATE INFORMATIONS EVADING LOGIN CONTROL
- ¬ VIOLATE RESTRICTIONS BASED ON IP, GEOLOCALIZATION, PRIVACY SETTINGS

→ OSINT CAN BE →
- PASSIVE → ¬ INTERACT WITH THE TARGET → COLLECT INF WITHOUT BEING NOTICED → LOW RISK OF ATTRIBUTION
- ACTIVE → INTERACT →
  - DIRECTLY (MESSAGES...)
  - INDIRECTLY (VISUALIZATIONS...)

→ OSINT OPERATIONS → CAN BE ATTRIBUTED TO SOMEONE → BECAUSE THEY LEAVE FOOTPRINT →
- LOG RECORDS
- METADATAS
- COOKIES
- PLUG-INS

→ THAT MAY ALLOWS → TARGETS TO DETECT THEY ARE THE SUBJECT Λ ADAPT COUNTERMEASURES

→ SO IT'S IMPORTANT TO AVOID THAT OSINT ACTIVITIES CAN BE LINKED TO THE INVESTIGATOR

→ LIST OF SERVICES TO FIND RESOURCES:
- WEB SEARCH ENGINE
- SOCIAL NETWORK
- E-MAIL ADDRESS SEARCH ENGINE
- USERNAME SEARCH ENGINE
- IP ADDRESS / DOMAIN SEARCH ENGINE

→ USE OF SOME OF THEM IS ENOUGH FOR A BASIC SEARCH

→ COMPLEX INVESTIGATIONS REQUIRES MANY SERVICES COMBINING OUTCOMES → WITH AUTOMATIC TOOLS FOR A STRUCTURE WORKFLOW

→ OSINT FRAMEWORK → IT'S A ORGANIZED REPOSITORY THAT COLLECT OSINT RESOURCES FOR CYBERSECURITY

→ OPSEC (OPERATIONAL SECURITY) → IT'S THE PROCESS WHERE AN ORGANIZATION: →
- IDENTIFY WHICH OF THEIR PUBLIC INFORMATION INCLUDING INF THEY ¬ REALIZE WAS PUBLIC → CAN BE EXPLOITED BY ATTACKER
- RISKS RELATED TO THOSE INFORMATIONS
- DEPLOY COUNTERMEASURES TO LIMIT THE EXPOSURE

→ IT'S A FORM OF AUTO-OSINT

MALWARE ANALYSIS

→ MALWARE → TERM TO DEFINE MALICIOUS PROGRAM → THAT PERFORM ACTIONS COMPROMISE → CONFIDENTIALITY, INTEGRITY, AVAILABILITY OF A DIGITAL SYSTEM

→ EVOLUTION: →
- INTERRUPTION OF DIGITAL SYSTEM'S FUNCTIONALITIES
- STEALING INFORMATION / MONEY Λ TARGETING ORGANIZATIONS / GOVERNMENTS
- MODERN MW TARGET IOT APPLICATION / DEVICES AND MOBILE

→ MALWARE CLASSIFICATION → USEFUL TOOLS FOR MW CLASSIFICATION: →
- AVCLASS / AVCLASS2
- YARA

→ ANALYZE ITS: →
- PROPAGATION VECTOR → HOW THEY SPREAD V PROPAGATE TO REACH THE DESIRED TARGETS
- ACTIONS V PAYLOADS EXECUTE ONCE A TARGET IS REACHED

→ THIS ANALYSIS HELPS UNDERSTANDING OF PROPAGATION MECHANISM Λ CONSEQUENCES OF MW ACTIVITIES

→ OTHER FEATURES: → HOST-DEPENDENT MW → REQUIRES EXISTING HOST PROGRAM/FILE → TO SPREADS BY INFECTING V MODIFYING → EXECUTABLE V DOCUMENTS

- STANDALONE MW → PROGRAMS EXECUTE INDIPENDENTLY ONCE DELIVERED TO THE TARGET SYSTEM
- NON-REPLICATING MW → ¬CREATE COPIES OF ITSELF AUTONOMOUSLY → RELIES ON EXTERNAL ACTIONS TO SPREAD FURTHER
- REPLICATING MW → SELF-PROPAGATE CREATING COPIES OF ITSELF → WITHOUT CONTINUOUS HUMAN INTERVENTION

MW ANALYSIS STRUCTURE
- PROPAGATION VECTOR
- PAYLOAD
- STRUCTURE OF THE MALWARE
  - HOST-DEPENDENT / STANDALONE
  - REPLICATING / ¬REPLICATING

AVCLASS2 PROVIDES A MALWARE CLASSIFICATION BASED ON:
- BEH (BEHAVIOR) → OBSERVABLE ACTIONS DURING THE SAMPLE EXECUTION
- CLASS → COMMON MW CHARACTERISTICS ABOUT → BEHAVIOR V DISTRIBUTION METHODS
- FILE (FILE PROPERTIES)
  - STATISTIC PROPERTIES (INDEPENDENT FROM EXECUTION)
  - OS UNDER WHICH SAMPLE EXECUTED
  - FILE FORMAT
  - PROGRAMMING LANGUAGE USED TO CODE THE SAMPLE
- FAM (FAMILY)

WANNACRY RANSOMWARE → RANSOMWARE IS TYPE OF MALWARE THAT COMPROMISE DATA AVAILABILITY → USUALLY WITH ENCRYPTION → THEN ASK MONEY TO RESTORE THEM
- SYMMETRIC (SUCH AS AES)
- ASYMMETRIC (SUCH AS RSA)

- EMERGED IN 2017 → SPREAD BY EXPLOITING ETERNALBLUE VULNERABILITY → A SMB WINDOW'S PROTOCOL
  - REPLICATING AUTONOMOUSLY
- EVEN THOUGH MICROSOFT RELEASED A PATCH 2 MONTHS BEFORE WANNACRY HAPPENED → MANY USERS DIDN'T UPDATE → INFECTED 230K COMPUTERS IN 130 COUNTRIES
- CAUSED 4$ BILLION DAMAGE
- IT STOPPED SPREADING AFTER A HARD-CODED DOMAIN NAME WAS RESOLVED ACTING LIKE A "KILL SWITCH" → SO IT WASN'T COMPLETELY UNCONTROLLABLE
- MANY GOVERNMENTS LINKED WANNACRY TO NORTH KOREA

PROPAGATION MECHANISMS → MALICIOUS EXECUTABLE RARELY APPEAR IN THEIR ORIGINAL .EXE FORMAT
- INSTEAD THEY ARE TYPICALLY DELIVERED USING INFECTION VECTORS SUCH AS:
  - MULTIMEDIA FILES AND SCRIPTS → SUCH AS POWERSHELL ∧ JAVASCRIPT
  - DOCUMENTS → INCLUDING PDF, DOCX FILES
  - INFECTION VECTORS CONTAINING MALICIOUS CODE IN SCRIPTING LANGUAGES

MALWARE ANALYSIS → DISCIPLINE THAT STUDIES STRUCTURE ∧ BEHAVIOUR OF MALICIOUS FILE → TO UNDERSTAND ACTIONS ∧ INTENTS
- ESPECIALLY BASED ON REVERSE ENGINEERING → ALLOWS EXAMINE PROGRAM ONCE IT IS EXECUTED
- HOW TO DESIGN AN EFFECTIVE DETECTION PROCESS → TO IDENTIFY MALICIOUS BEHAVIOUR → AVOIDING EXCESSIVE NUMBER OF FALSE ALARMS
  - REVERSE ENGINEERING ANSWER → DOES THE PROGRAM BEHAVE AS INTENDED?
    - WHEN A PROGRAM IS COMPILED → SOURCE CODE → BINARY FILES → REVERSE ENG. ANALYZE IT ∧ RECONSTRUCT THE BEHAVIOUR OF A PROGRAM

CAN BE → STATIC ANALYSIS
- INSPECTING A PROGRAM WITHOUT EXECUTING IT
- USED AS A FIRST EXAMINATION
- STRONGLY BASED ON REVERSE ENGINEERING
- THE PROCESS IS IN THREE MAIN STEPS:
  - 1) UNDERSTANDING THE FORMAT OF THE SAMPLE → INCLUDING FORMAT OF PROPAGATION VECTOR
  - 2) DISASSEMBLY THE FILES (BINARY) → INTO ASSEMBLY SECTION

- 3) DECOMPILATION → TO OBTAIN AN EQUIVALENT REPRESENTATION OF THE ORIGINAL SOURCE CODE (HIGH LEVEL)
  - → BY INTERPRETING ASSEMBLY INSTRUCTIONS

- → EXAMPLE: → PORTABLE EXECUTABLE (PE) FILES → .EXE V .DDL FORMATS
  - → STRUCTURE INTO SEVERAL COMPONENTS INCLUDING:
    - → DOS HEADER AND STUB
    - → SECTION TABLE → DESCRIBES LOCATION OF DATA SECTIONS → WHICH CONTAIN ACTUAL DATA
    - → SECTIONS THAT CONTAINS THE CODE (.TEXT, .DATA, .RDATA) → EXPRESSED AS A SEQUENCE BYTES
      - → THESE BYTES CORRESPOND TO ASSEMBLY INSTRUCTIONS → THAT NEEDS DISASSEMBLE ∧ THEN COMPILED

- → TYPES OF DISASSEMBLER: → LINEAR SWEEP DISASSEMBLER → DISASSEMBLE INSTRUCTIONS SEQUENTIALLY STARTING FROM A GIVEN ENTRY POINT (NO JUMP, una linea dopo l'altra)
  - → RECURSIVE TRAVERSAL DISASSEMBLER → DISASSEMBLE INSTRUCTIONS BY FOLLOWING SEMANTICS
    - → SUCH AS JUMPS AND BRANCHES → (traducendo linea 1-2-3-44-55-56-4-5-6-7-80-81)

- → DISASSEMBLERS: BINARY FILES → ASSEMBLY

- → DECOMPILERS: ASSEMBLY/BINARY → SOURCE CODE (HIGH LEVEL CODE)

- → DISASSEMBLERS ∧ DECOMPILERS → CAN BE ELUDED WITH ANTI-REVERSE ENGINEERING TECHNIQUES → THAT CAUSE
  - → INCREASE EFFORTS OF HUMAN DURING ANALYSIS
  - → MAKING GENERATE TOOLS INCORRECT OUTPUTS
  - → EXAMPLE: → PACKING
    - → COMPRESSING V ENCODING INFORMATION
    - → SO IT'S NOT STATISTICALLY VISIBLE
      - → SO ¬ANALYZE WITHOUT EXECUTING THE PROGRAM
      - → ¬SEE REAL CODE OF THE MALWARE
      - → V CAN SEE ISTRUCTIONS WITHOUT LOGIC SENSE

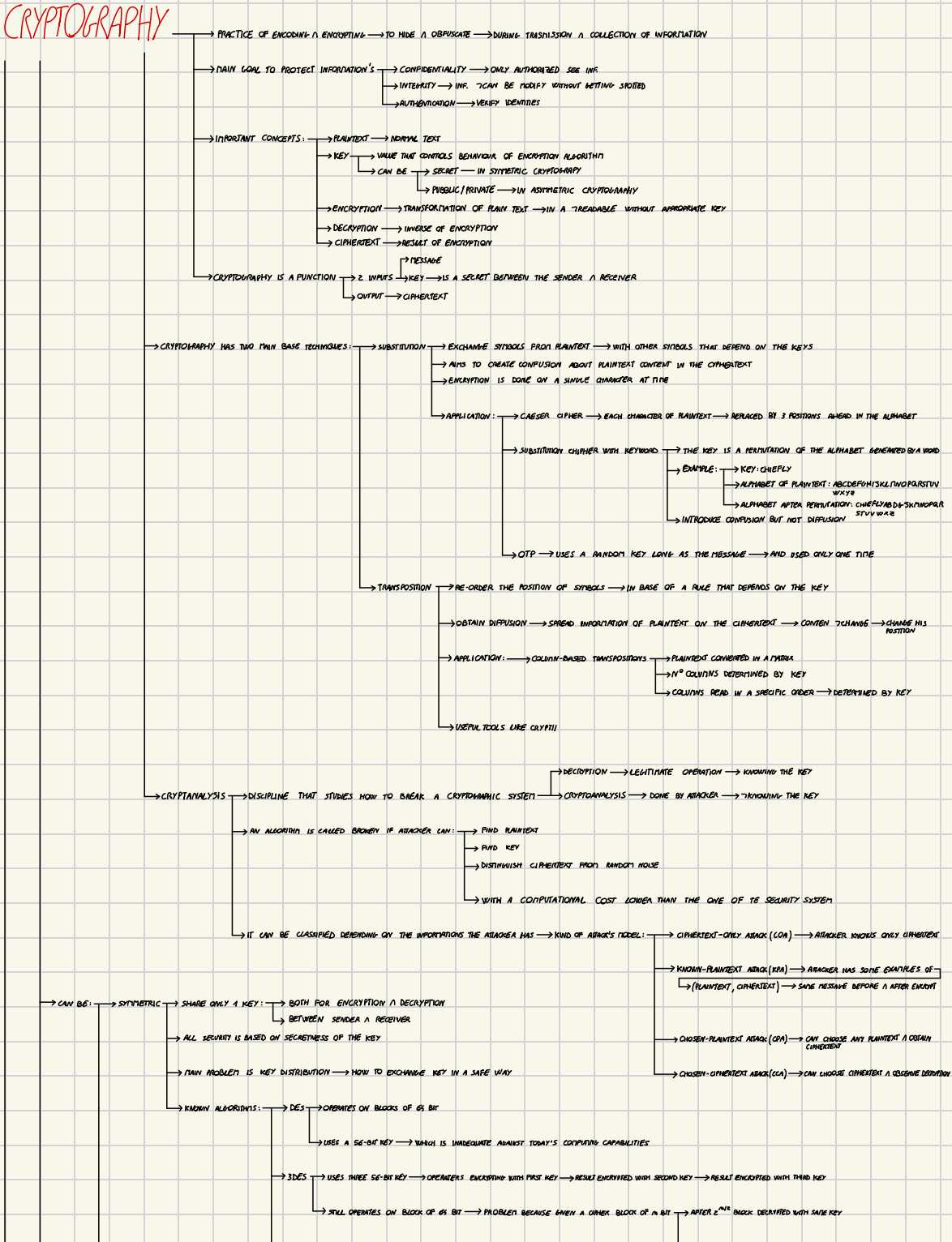
- → DYNAMIC ANALYSIS
  - → BASED ON EXECUTION OF MALICIOUS CODE — IN A CONTROLLED ENVIRONMENT
  - → MONITOR WHAT THE PROCESSOR EXECUTES — AND WHAT IS STORED IN MEMORY
  - → EXECUTION CAN BE PAUSED V BLOCKED TO FOCUS ANALYSIS ON A SPECIFIC PROCESSOR STATE — USEFUL FOR OBSERVING THE EVOLUTION OF THE VARIABLES
  - → DYNAMIC ANALYSIS → EFFECT AGAINST MANY ANT-REVERSE ENG. TECH.
  - → IT IS DONE IN CONTROLLED ENVIRONMENTS
    - → ONLINE SANBOXES
    - → VIRTUALIZED ENVIRONMENTS
  - → DEBUGGERS MONITOR PROGRAM EXECUTION AT → SOURCE LEVEL ∧ ASSEMBLY LEVEL
  - → MALWARE MIGHT IMPLEMENTS ANTI-DEBUGGING TECHNIQUES
    - → SINCE DEBUGGING REQUIRES ATTACHING A DEBUGGER TO A PROCESS
    - → MALICIOUS PROGRAMS DETECT PRESENCE OF A DEBUGGER → AND ALTER THEIR BEHAVIOUR

- → MALWARE TO ACHIEVE THEIR GOALS:
  - → MUST BE INSTALLED ON A COMPUTER DEVICE
  - → MUST BEHAVE LIKE A LEGITIMATE PROGRAM
  - → MUST GET ACCESS TO COMPUTER RESOURCES (FILES, MEMORY, LIBRARIES, ETC...)
  - → OPEN COMMUNICATION CHANNELS

- → ADVANCED ANALYSIS TECHNIQUES
  - → STATIC INSTRUMENTATION → APPLIED ON INFECTION VECTORS (i mezzi attraverso cui il malware viene trasmesso e riesce a raggiungere ed essere eseguito su un sistema bersaglio) → SUCH AS OBLIVION → ANALYZE ∧ MODIFY CODE WITHOUT EXECUTING IT
  - → DYNAMIC INSTRUMENTATION → MONITORING DURING PROGRAM EXECUTION
  - → SYMBOLIC EXECUTION → TREAT INPUTS AS SYMBOLS R.T.H. VALUES → TO EXPLORE DIFFERENT EXECUTION PATHS → WITHOUT TESTING ALL POSSIBLE INPUTS EXPLICITY
  - → EMULATION → REPLICATING SPECIFIC HW V SW ENVIRONMENTS ON DIFFERENT PLATFORMS → THAT MIMICS THE ORIGINAL TARGET SYSTEM → MAKING IT POSSIBLE TO ANALYZE MALWARE BEHAVIOUR WITHOUT RUNNING IT DIRECTLY ON REAL HARDWARE

SECURITY AND CYBERSECURITY

- CHAIN OF TRUST
  - IS A BASIC PRINCIPLE OF SECURITY IN EVERY FIELD
  - REFERS TO THE CONCEPT OF MUTUAL TRUST WITHIN SOCIETY
  - SECURITY MECHANISMS EXISTS TO ENABLE AND MAINTAIN TRUST BETWEEN PEOPLE, SYSTEMS & ORGANIZATIONS
  - SECURITY GUARANTEES TRUST VERIFYING:
    - IDENTIFICATION → ESTABLISHES WHO V WHAT AN ENTITY CLAIMS TO BE
    - AUTHENTICATION → VERIFIES THAT IDENTIFICATION IS GENUINE (fatto bene e non falso)
    - AUTHORIZATION → DETERMINES WHAT ACTIONS THE AUTHENTICATED ENTITY IS ALLOWED TO PERFORM
  - CYBERCRIMES OFTEN EXPLOIT WEAKNESS IN THE HUMAN ABILITY TO MANAGE VIRTUAL INTERACTIONS
- SECURITY
  - IS THE STATE OF BEING:
    - FREE FROM DANGER OR THREAT
    - FEELING SAFE, STABLE & FREE FROM FEAR V ANXIETY
  - ACHIEVED WITH COMBINATION OF:
    - PREVENTION
    - DETECTION
    - REACTION
  - HOW EFFECTIVENESS OF A SECURITY SYSTEM CAN BE EVALUATED?:
    - IDENTIFICATION OF THE ASSETS → ELEMENTS (DATA, SYSTEMS, SERVICES) THAT NEED PROTECTION
    - IDENTIFICATION OF THE RISKS → THREATS & VULNERABILITIES THAT COULD IMPACT THOSE ASSETS
    - MEASUREMENT OF THE DEGREE OF RISK → EVALUATING LIKELIHOOD & POTENTIAL IMPACT OF EACH IDENTIFIED RISK
    - MITIGATION PROVIDED BY THE SECURITY MECHANISMS → EVALUATING HOW EXISTING CONTROLS REDUCE V MANAGE THE IDENTIFIED RISKS
    - IDENTIFICATION OF ANY NEW RISKS INTRODUCED BY THE SECURITY SYSTEM ITSELF → SINCE SECURITY SOLUTIONS CAN CREATE ADDITIONAL VULN.
    - COST & TRADE-OFFS OF THE SOLUTION
  - TYPES OF FAILURE OF SECURITY SYSTEMS:
    - TO PROVIDE SECURITY → SYSTEMS MUST INTERACT WITH
      - PROCTETED ASSETS
      - ENVIRONMENT
      - OTHER SYSTEM COMPONENTS
    - THESE INTERACTIONS CAN LEAD TO DIFFERENT TYPES OF FAILURE IN SECURITY SYSTEMS
    - TWO MAIN TYPES OF FAILURE:
      - ACTIVE FAILURES → SYSTEM PERFORMS SECURITY ACTIONS → IN THE ABSENCE OF REAL THREATS (sistema di sicurezza reagisce anche se non c'è una minaccia reale)
        - RESULTING IN FALSE ALARMS V UNNECESSARY RESPONSES → EXAMPLE:
          - ANTIVIRUS THAT BLOCKS A LEGITIMATE FILE
      - PASSIVE FAILURE → SYSTEM FAILS TO PROPERLY HANDLE AN ACTUAL THREAT
- CYBERCRIME
  - ESPECIALLY WITH FINANCIAL PURPOSES
  - PUBLIC SECTORS ARE THE FAVOURITE VICTIMS
  - COMPROMISE CIA TRIAD OF INFORMATION
  - FOUR MAIN KINDS OF ATTACKS:
    - INTERRUPTION → THREATS AVAILABILITY → (MAKES SYSTEM V SERVICES UNAVAILABLE TO USERS)
    - INTERCEPTION → THREATS CONFIDENTIALITY → UNAUTHORIZED PARTY GAIN ACCESS TO INFORMATION → SYS. CONTINUES TO FUNCTION → INF. IS SECRETLY COPIED V OBSERVED
    - MODIFICATION → THREATS CONFIDENTIALITY & INTEGRITY → CHANGE INFORMATION WITHOUT AUTHORIZATION
    - FABRICATION → THREATS AUTHENTICITY → CREATING FALSE INFORMATION V EVENTS & INSERTING THEM INTO THE SYSTEM

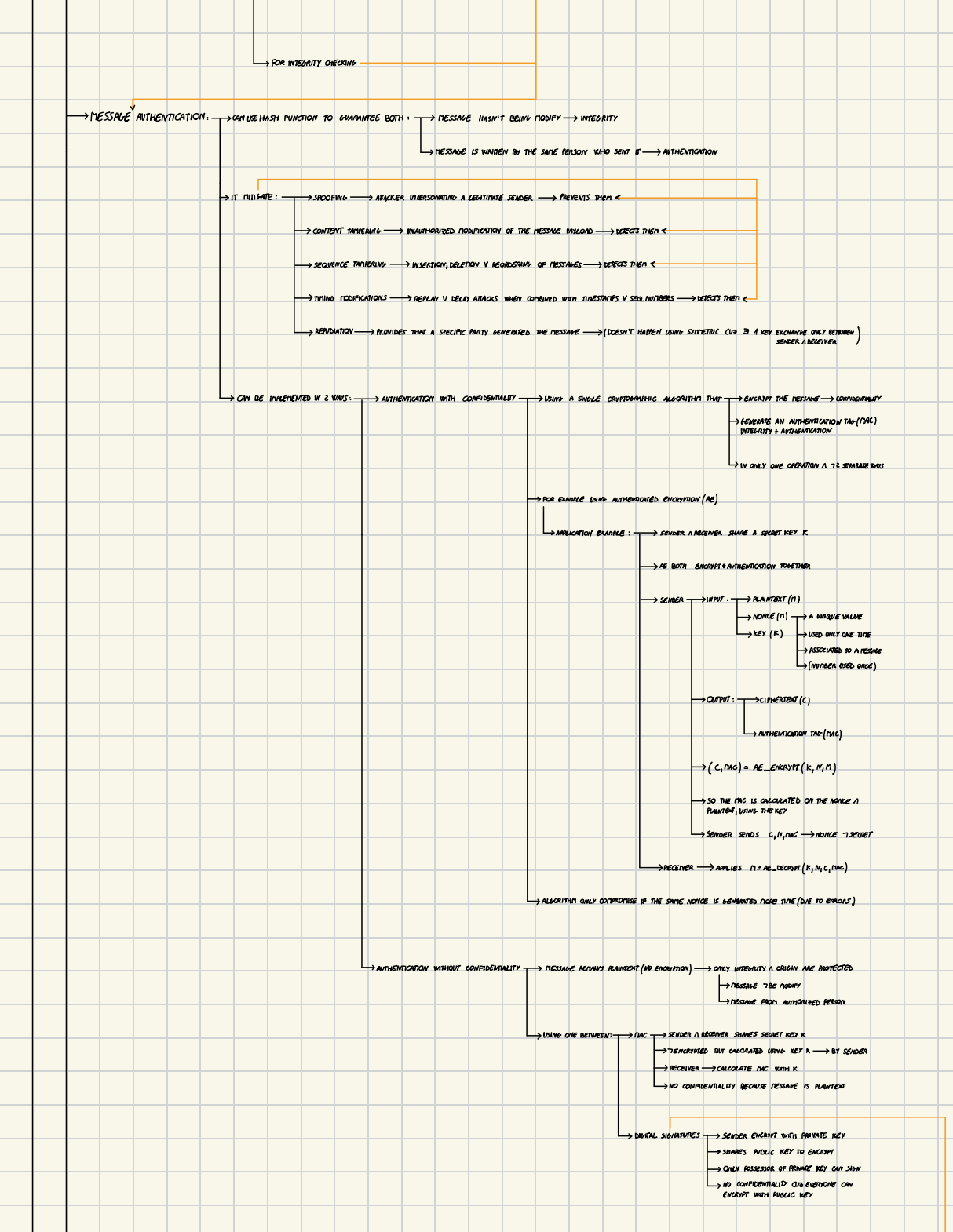

CRYPTOGRAPHY
PRACTICE OF ENCODING / ENCRYPTING → TO HIDE / OBFUSCATE → DURING TRASMISSION / COLLECTION OF INFORMATION
MAIN GOAL TO PROTECT INFORMATION'S
CONFIDENTIALITY → ONLY AUTHORIZED SEE INF.
INTEGRITY → INF. CAN BE MODIFY WITHOUT BEEING SPOTTED
AUTHENTICATION → VERIFY IDENTITIES
IMPORTANT CONCEPTS:
PLAINTEXT → NORMAL TEXT
KEY → VALUE THAT CONTROLS BEHAVIOUR OF ENCRYPTION ALGORITHM
CAN BE → SECRET → IN SYMMETRIC CRYPTOGRAPHY
PUBBLIC / PRIVATE → IN ASYMMETRIC CRYPTOGRAPHY
ENCRYPTION → TRANSFORMATION OF PLAIN TEXT → IN A "READABLE" WITHOUT APPROPRIATE KEY
DECRYPTION → INVERSE OF ENCRYPTION
CIPHERTEXT → RESULT OF ENCRYPTION
CRYPTOGRAPHY IS A FUNCTION → 2 INPUTS → MESSAGE
KEY → IS A SECRET BETWEEN THE SENDER / RECEIVER
OUTPUT → CIPHERTEXT
CRYPTOGRAPHY HAS TWO MAIN BASE TECHNIQUES:
SUBSTITUTION → EXCHANGE SYMBOLS FROM PLAINTEXT → WITH OTHER SYMBOLS THAT DEPEND ON THE KEYS
AIMS TO CREATE CONFUSION ABOUT PLAINTEXT CONTENT IN THE CIPHERTEXT
ENCRYPTION IS DONE ON A SINGLE CHARACTER AT TIME
APPLICATION: → CAESER CIPHER → EACH CHARACTER OF PLAINTEXT → REPLACED BY 3 POSITIONS AHEAD IN THE ALPHABET
SUBSTITUTION CHIPHER WITH KEYWORD → THE KEY IS A PERMUTATION OF THE ALPHABET GENERATED BY A WORD
EXAMPLE: → KEY: CHIEFLY
ALPHABET OF PLAINTEXT: ABCDEFGHISKLMNOPQRSTUVWXYZ
ALPHABET AFTER PERMUTATION: CHIEFLYABDGKMNOPQRSTUVWXZ
INTRODUCE CONFUSION BUT NOT DIFFUSION
OTP → USES A RANDOM KEY LONG AS THE MESSAGE → AND USED ONLY ONE TIME
TRANSPOSITION → RE-ORDER THE POSITION OF SYMBOLS → IN BASE OF A RULE THAT DEPENDS ON THE KEY
OBTAIN DIFFUSION → SPREAD INFORMATION OF PLAINTEXT ON THE CIPHERTEXT → CONTEN 7CHANGE → CHANGE HIS POSITION
APPLICATION: → COLUMN-BASED TRANSPOSITIONS → PLAINTEXT CONVERTED IN A MATRIX
N° COLUMNS DETERMINED BY KEY
COLUMNS READ IN A SPECIFIC ORDER → DETERMINED BY KEY
USEFUL TOOLS LIKE CRYPTII
CRYPTANALYSIS → DISCIPLINE THAT STUDIES HOW TO BREAK A CRYPTOGRAPHIC SYSTEM → DECRYPTION → LEGITIMATE OPERATION → KNOWING THE KEY
CRYPTOANALYSIS → DONE BY ATTACKER → "KNOWING THE KEY
AN ALGORITHM IS CALLED BROKEN IF ATTACKER CAN: → FIND PLAINTEXT
FIND KEY
DISTINGUISH CIPHERTEXT FROM RANDOM NOISE
WITH A COMPUTATIONAL COST LOWER THAN THE ONE OF TE SECURITY SYSTEM
IT CAN BE CLASSIFIED DEPENDING ON THE INFORMATIONS THE ATTACKER HAS → KIND OF ATTACK'S MODEL: → CIPHERTEXT-ONLY ATTACK (COA) → ATTACKER KNOWS ONLY CIPHERTEXT
KNOWN-PLAINTEXT ATTACK (KPA) → ATTACKER HAS SOME EXAMPLES OF
(PLAINTEXT, CIPHERTEXT) → SAME MESSAVE BEFORE / AFTER ENCRYPT
CHOSEN-PLAINTEXT ATTACK (CPA) → CAN CHOOSE ANY PLAINTEXT / OBTAIN CIPHERTEXT
CHOSEN-CIPHERTEXT ATTACK (CCA) → CAN CHOOSE CIPHERTEXT / OBSERVE DECRYPTION
CAN BE: → SYMMETRIC → SHARE ONLY A KEY: → BOTH FOR ENCRYPTION / DECRYPTION
BETWEEN SENDER / RECEIVER
ALL SECURITY IS BASED ON SECRETNESS OF THE KEY
MAIN PROBLEM IS KEY DISTRIBUTION → HOW TO EXCHANGE KEY IN A SAFE WAY
KNOWN ALGORITHMS: → DES → OPERATES ON BLOCKS OF 64 BIT
USES A 56-BIT KEY → WHICH IS INADEQUATE AGAINST TODAY'S COMPUTING CAPABILITIES
3DES → USES THREE 56-BIT KEY → OPERATES ENCRYPTING WITH FIRST KEY → RESULT ENCRYPTED WITH SECOND KEY → RESULT ENCRYPTED WITH THIRD KEY
STILL OPERATES ON BLOCK OF 64 BIT → PROBLEM BECAUSE GIVEN A CIPHER BLOCK OF n BIT → AFTER $2^{n/2}$ BLOCK DECRYPTED WITH SAME KEY

- AES
  - MORE SAFE BECAUSE BLOCK SIZE OF 128 BIT
  - CAN BE AES128/192/256 → BASED ON THE KEY'S BIT LENGHT
  - PLAINTEXT DIVIDED INTO BLOCKS OF 16 BYTES → THEN ENCRYPTION DEPENDS ON THE CHOSEN MODE:
    - ECB MODE
      - EACH BLOCK IS ENCRYPTED INDEPENDENTLY
      - WHICH LEAKS PATTERNS
    - CBC MODE
      - BEFORE ENCRYPTION EACH BLOCK IS XOR WITH HIS PREVIOUS BLOCK
      - BUT THE FIRST BLOCK "HAVE PREVIOUS ONE
      - SO IT'S USED AN INITIALIZATION VECTOR (IV)
      - TO RANDOMIZE THE ENCRYPTION SO THAT 2 SAME MESSAGES PRODUCES SAME CIPHERTEXT
    - PROBABILITY OF FINDING AT LEAST 2 SAME BLOCKS IS HIGH
    - THAT BRINGS TO A LEAKAGE OF INFORMATIONS
      - ENCRYPTED IMAGES
      - DATA PATTERNS

- ASYMMETRIC
  - BOTH SENDER & RECEIVER HAVE TWO KEYS:
    - PRIVATE → SECRET & NEVER SHARED
    - PUBLIC → CAN BE SHARED
  - 2 WAYS TO APPLY IT:
    - ENCRYPTION WITH PUBLIC KEY OF THE RECEIVER → RECEIVER DECRYPT WITH HIS PRIVATE KEY
    - ENCRYPTION WITH PRIVATE KEY OF THE SENDER → RECEIVER DECRYPT WITH PUBLIC KEY OF SENDER
  - ASYMMETRIC ENCRYPTION WITH RSA:
    - USES
      - PUBLIC KEY → THE COUPLE (E, N)
      - PRIVATE KEY → THE COUPLE (D, N)
    - PLAINTEXT ENCRYPTED WITH → $(P^E) \bmod N$ OR $(P^D) \bmod N$ = CIPHERTEXT (C)
      - E & D ARE INTERCHANGABLE ONLY IN A MATHEMATIC WAY
      - BUT THEIR USAGE IS
        - E → PUBLIC FOR ENCRYPTION
        - D → PRIVATE FOR DECRYPTION
    - CIPHERTEXT DECRYPTED WITH → $C^D \bmod N = \text{PLAINTEXT}(P)$
    - IN RSA, PLAINTEXTS & CIPHERTEXTS ARE INTEGERS IN THE RANGE $[0, N-1]$, SINCE ENCRYPTION IS DEFINED ON $\bmod N$
      - EXAMPLE:
        - "CIAO"
        - WITH ASCII → C = 67, I = 73, A = 65, O = 79
        - THEN IN BINARY → 01000011 01001001 01000001 01001111
        - PLAINTEXT IS CONVERTED IN AN INTEGER → P = INT(01000011010010010100000101001111)
        - THEN RSA IS APPLIED → $C = P^E \bmod N$
        - RECEIVER DECRYPT → $P = C^D \bmod N$
        - P IS DIVIDED → EACH BINARY SEQUENCE CONVERTED TO EACH ORIGINAL CHARACTER

- SYMMETRIC CRYPTOGRAPHY PROTECTS DATA → FAST & ECONOMIC WAY → USES SIMPLE OPERATIONS & SCALES ON GIGABYTES
  - ASYMMETRIC CAN'T BECAUSE WORKS WITH HEAVY OPERATIONS (EXPONENTIAL) → SLOW, EXPENSIVE, DOESN'T SCALE
- ASYMMETRIC → USED FOR THE EXCHANGE OF THE SIMMETRIC KEY IN A SAFE WAY

- HASHING:
  - ALL HASH FUNCTIONS IN CRYPTOGRAPHY ARE A ONE-WAY HASH FUNCTION
    - TAKES AN INPUT (NO LENGHT CONSTRAINTS)
    - PRODUCE OUTPUT WITH A FIXED LENGHT → CALLED "DIGEST" V "HASH VALUE"
    - IT'S CALLED ONE-WAY BECAUSE GIVEN THE HASH → IT'S NOT COMPUTATIONAL POSSIBLE TO GO BACK TO THE INPUT
  - USAGES OF HASH FUNCTIONS:
    - COMBINATION WITH ASYMMETRIC ENCRYPTION ALGORITHMS → FOR EXAMPLE IN DIGITAL SIGNATURES (HASHING THE SIGNATURE)
    - FOR AUTHENTICATION
    - IN COMMUNICATION PROTOCOLS FOR HANDSHAKE FOR EXAMPLE


FOR INTEGRITY CHECKING
MESSAGE AUTHENTICATION :
CAN USE HASH FUNCTION TO GUARANTEE BOTH :
MESSAGE HASN'T BEING MODIFY → INTEGRITY
MESSAGE IS WRITTEN BY THE SAME PERSON WHO SENT IT → AUTHENTICATION
IT MITIGATE :
SPOOFING → ATTACKER IMPERSONATING A LEGITIMATE SENDER → PREVENTS THEM
CONTENT TAMPERING → UNAUTHORIZED MODIFICATION OF THE MESSAGE PAYLOAD → DETECTS THEM
SEQUENCE TAMPERING → INSERTION, DELETION V REORDERING OF MESSAGES → DETECTS THEM
TIMING MODIFICATIONS → REPLAY V DELAY ATTACKS WHEN COMBINED WITH TIMESTAMPS V SEQ. NUMBERS → DETECTS THEM
REPUDIATION → PROVIDES THAT A SPECIFIC PARTY GENERATED THE MESSAGE → (DOESN'T HAPPEN USING SYMMETRIC CIF. ∃ A KEY EXCHANGE ONLY BETWEEN SENDER & RECEIVER)
CAN BE IMPLEMENTED IN 2 WAYS :
AUTHENTICATION WITH CONFIDENTIALITY
USING A SINGLE CRYPTOGRAPHIC ALGORITHM THAT
ENCRYPT THE MESSAGE → CONFIDENTIALITY
GENERATE AN AUTHENTICATION TAG (MAC) INTEGRITY & AUTHENTICATION
IN ONLY ONE OPERATION ∧ ¬2 SEPARATE WAYS
FOR EXAMPLE USING AUTHENTICATED ENCRYPTION (AE)
APPLICATION EXAMPLE :
SENDER ∧ RECEIVER SHARE A SECRET KEY K
AE BOTH ENCRYPT & AUTHENTICATION TOGETHER
SENDER
INPUT :
PLAINTEXT (M)
NONCE (N)
A UNIQUE VALUE
USED ONLY ONE TIME
ASSOCIATED TO A MESSAGE
(NUMBER USED ONCE)
KEY (K)
OUTPUT :
CIPHERTEXT (C)
AUTHENTICATION TAG (TAG)
(C, TAG) = AE_ENCRYPT (K, N, M)
SO THE TAG IS CALCULATED ON THE NONCE ∧ PLAINTEXT, USING THE KEY
SENDER SENDS C, N, TAG → NONCE ¬SECRET
RECEIVER → APPLIES M = AE_DECRYPT (K, N, C, TAG)
ALGORITHM ONLY COMPROMISE IF THE SAME NONCE IS GENERATED MORE TIME (DUE TO ERRORS)
AUTHENTICATION WITHOUT CONFIDENTIALITY
MESSAGE REMAIN'S PLAINTEXT (NO ENCRYPTION) → ONLY INTEGRITY ∧ ORIGIN ARE PROTECTED
¬MESSAGE ¬BE MODIFY
MESSAGE FROM AUTHORIZED PERSON
USING ONE BETWEEN:
MAC
SENDER ∧ RECEIVER SHARES SECRET KEY K
¬ENCRYPTED BUT CALCULATED USING KEY K → BY SENDER
RECEIVER → CALCULATE MAC WITH K
NO CONFIDENTIALITY BECAUSE MESSAGE IS PLAINTEXT
DIGITAL SIGNATURES
SENDER ENCRYPT WITH PRIVATE KEY
SHARES PUBLIC KEY TO ENCRYPT
ONLY POSSESSOR OF PRIVATE KEY CAN SIGN
NO CONFIDENTIALITY CUZ EVERYONE CAN ENCRYPT WITH PUBLIC KEY

- WHEN YOU RECEIVE A PUBLIC KEY? → WHOM IS IT? HOW DO YOU KNOW IT'S NOT OF AN ATTACKER?
  - DIGITAL CERTIFICATES → IS A PUBLIC KEY
    - → ASSOCIATED TO AN IDENTITY
    - → SIGNED BY A TRUSTED AUTHORITY (CA)
      - CERTIFICATE AUTHORITY (CA) → IS TRUSTED AUTHORITY THAT
        - → VERIFY THE IDENTITY OF WHO'S REQUESTING THE CERTIFICATE
        - → GENERATE CERTIFICATE THAT LINKS THE IDENTITY WITH THE PUBLIC KEY (OF THE SENDER)
        - → SIGN THE CERTIFICATE WITH HIS PRIVATE KEY (OF CA)
        - → NOW EVERYONE CAN USE THE PUBLIC KEY OF CA TO VERIFY THE SIGN → IF THE SIGN IS VALID → THE CERTIFICATE "TRUMPS"
          - → THE PUBLIC KEY IS REALLY OF THE SENDER
      - EXAMPLE: → (IDENTRUST, COMODO, DIGICERT, ...)
  - CERTIFICATE = { IDENTITY, PUBLIC KEY } SIGNED BY CA

- RANDOM NUMBER → ARE ESSENTIALS FOR SAFETY BECAUSE THEY ARE USED FOR:
  - → GENERATE CRYPTOGRAPHIC KEYS
  - → NONCE ∧ IV
  - → HANDSHAKE
  - → THEY HAVE TWO REQUIREMENTS:
    - RANDOMNESS → THE NUMBER SHOULD BE UNIFORMLY DISTRIBUTED → MEANING EACH POSSIBLE OUTCOME OCCURS WITH APPROXIMATELY EQUAL PROBABILITY
    - → THEY SHOULD BE INDEPENDENT → IT'S A STATISTICAL PROPERTY → NUMBERS LOOK RANDOM → BUT MAYBE THEY ARE PREDICTABLE
    - UNPREDICTABILITY → EACH NUMBER IS STATISTICALLY INDEPENDENT → IT'S A SECURITY PROPERTY → "PREDICTABLE BY AN ATTACKER
  - → HOWEVER ALGORITHM ARE DETERMINISTIC:
    - → EXECUTE FIXED INSTRUCTIONS
    - → SAME INPUT PRODUCES SAME OUTPUT
    - → SO NUMBERS GENERATED ARE PSEUDORANDOM → THAT APPEAR RANDOM BECAUSE SATISFY STATISTICAL TEST FOR RANDOMNESS → BUT CAN BE PREDICTED IF SEED ∧ ALGORITHM ARE KNOWN
  - → TRUE RANDOM NUMBER GENERATORS (TRNG's)
    - → USED FOR GENERATE TRULY RANDOM NUMBER
    - → RELY ON PROCESSES THAT "FOLLOW MATH RULES → SUCH AS RADIOACTIVE DECAY, THERMAL NOISE, ... → THESE PHENOMENONS ARE:
      - → "DETERMINISTIC
      - → "REPRODUCIBLE
      - → "PREDICTABLE
    - → MODERN PROCESSOR OFTEN INTEGRATE TRNG's

- PROPERTIES OF DIGITAL SIGNATURE:
  - UNFORGEABLE → ("Obligatoria.") MANDATORY PROPERTY → MUST ASSURE THAT NO ONE OTHER THAN THE SIGNER CAN PRODUCE THE SIGNATURE WITHOUT THE SIGNER'S PRIVATE KEY
  - → AUTHENTIC → MANDATORY PROPERTY → MUST ASSURE THE RECEIVER CAN VERIFY THAT SIGNATURE REALLY WAS FROM THE SIGNER
  - → NOT ALTERABLE → DESIRABLE PROPERTY → NO ONE (INCLUDING SIGNER ∧ RECEIVER) CAN MODIFY THE SIGNATURE ∨ MESSAGE WITHOUT THE TAMPERING BEING EVIDENT → PROTECTS INTEGRITY
  - → NOT REUSABLE → DESIRABLE PROPERTY → ANY ATTEMPT TO REUSE A PREVIOUS SIGNATURE WILL BE DETECTED BY RECEIVER → PROTECT FROM REPLAY

- → DIGITAL SIGNATURE & DIGITAL CERTIFICATE
  - DIGITAL SIGNATURE → ON A MESSAGE → GUARANTEE THAT A MESSAGE COME FROM SOMEONE
  - → DIGITAL CERTIFICATE → SIGN BY CA → ON A PUBLIC KEY → GUARANTEE THAT A PUBLIC KEY BELONGS TO SOMEONE

- → PROCESS:
  - → DOCUMENT IS SIGNED WITH AN HASH
  - → THEN HASH IS SIGNED WITH SENDER'S PRIVATE KEY
  - → ATTACHED AT THE DOCUMENT THE DIGITAL CERTIFICATE (FOR THE PUBLIC KEY)
  - → THEN VERIFY THE PUBLIC KEY IN THE CERTIFICATE (USING THE PUBLIC KEY OF CA)
  - → VERIFY THE HASH WITH THE PUBLIC KEY
  - → THE RECEIVER CALCULATE THE HASH (HASH FUNCTIONS ARE PUBLIC) → TO VERIFY DOCUMENT "MODIFIED

- → DIGITAL SIGNATURES GUARANTEE AUTHENTICITY OF SIGNERS ∧ INTEGRITY OF DATA

- DIGITAL ENVELOPE → STRATEGY THAT INVOLVES BOTH SYMMETRIC ∧ ASYMMETRIC:
  - → SENDER GENERATES A RANDOM SYMMETRIC KEY (CALLED SESSION KEY)
  - → ENCRYPT SESSION KEY WITH PUBBLIC KEY OF THE RECEIVER
  - → IT'S CALLED DIGITAL ENVELOPE BECAUSE CYPERTEXT ∧ ENCRYPTED KEY ARE SENT TOGETHER
  - → RECEIVER USE HIS PRIVATE KEY TO OBTAIN SESSION KEY ∧ ENCRYPT CYPHERTEXT
  - → ENSURES CONFIDENTIALITY

- ON INTERNET CRYPTOGRAPHY IS USED TO PROTECT DATA IN PACKET TRANSMISSION → DEPENDING ON WHERE THE ENCRYPTION IS DONE THE APPROACH CHANGE:
  - → LINK ENCRYPTION
    - → MESSAGE ENCRYPTED BEFORE BEING TRANSMITTED ON THE PHYSICAL MEAN → SO AT THE LOWEST LEVEL OF NETWORK STACK (1.50-OSI/TCP-IP)
    - → SO ALL THE LAYERS ABOVE HAS SEEN THE PLAINTEXT
    - → ALL THE HEADERS OF THE HIGH LEVELS ARE ENCRYPTED AT LINK LEVEL

ENCR	ENCR	ENCR	ENCR
H3	H4	H5	PAYLOAD

    - → WHEN A PACKET ARRIVES TO AN INTERMEDIATE NODE (ROUTER)
      - → PACKET IS ENCRYPTED
      - → ELABORATED
      - → RE-ENCRYPTED ∧ SENT TO THE OTHER NODE
    - → PROTECTING THE PACKET ON EACH SINGLE LINK OF THE NETWORK ONE-BY-ONE
    - → SO LINK ENCRYPTION
      - → PROTECT DATA BETWEEN NODES OF THE NETWORK THAT TRUST EACHOTHER
      - → REQUEST NODES ARE AUTHENTICATED BETWEEN EACHOTHER
      - → NEEDS A KEY FOR EACH COUPLE OF NODES
  - → END-TO-END ENCRYPTION:
    - → MESSAGE ENCRYPTED AT APPLICATION ∨ PRESENTATION LEVEL
    - → ONLY THE PAYLOAD IS ENCRYPTED
    - → NOT THE HEADERS → NEEDED FOR ROUTING
    - → SO INTERMEDIATE NODES CANNOT READ PAYLOAD
    - → SO PACKET ENCRYPTED BY SENDER, STAYS ENCRYPTED THE WHOLE NETWORK, DECRYPTED ONLY BY RECEIVER (THAT'S WHY IT'S CALLED END-TO-END)
    - → MESSAGE NEVER EXPOSED TO THE ROUTERS
    - → SECURITY GUARANTEED ONLY TO THE ENDS OF THE COMMS.
    - → NEEDS A KEY FOR EACH PAIR OF USERS

- OTHER EXAMPLES OF CRYPTOGRAPHY APPLICATION ON INTERNET:
  - → WEP (WI-FI SECURITY)
    - → CLIENT ∧ ACCESS POINT BOTH SHARE A SECRET KEY (PRE-SHARED KEY) (BEFORE THE COMMUNICATION STARTS)
    - → WHEN CLIENT WANTS TO JOIN → ACCESS POINT SENDS A RANDOM NUMBER (A CHALLENGE)
    - → CLIENT ENCRYPT THIS NUMBER WITH SHARED KEY ∧ SEND BACK
    - → AP DECRYPT ∧ CONFROM IF IT'S THE SAME NUMBER
    - → IF SO, CLIENT IS AUTHENTICATED
    - → AFTER THE COMMS GOES ON WITH THE PRE-SHARED KEY
  - → WPA
    - → ONCE AUTHENTICATION IS DONE AS BEFORE → DIFFERENT SESSION KEYS ARE GIVEN
    - → AES IS USED TO ENCRYPT DATA
    - → ACTUAL STANDARD FOR WI-FI SECURITY
  - → VPN
    - → OFTEN IMPLEMENTED WITH LINK ENCRYPTION THROUGH FIREWALL ∨ GATEWAY
    - → USED TO CREATE SECURE CONNECTION BETWEEN TWO NETWORKS OF SAME ORG.
    - → USES THE TUNNELING → DATA INCAPSULATED ∧ ENCRYPTED SO EVEN IF PASS THROUGH A PUBLIC NET, THEY ARE PROTECTED
  - → SECURE SHELL (SSH) → PROVIDES AN AUTHENTICATED ∧ ENCRYPTED CHANNEL TO ACCESS FROM REMOTE TO THE OS COMMAND LINE
  - → SSL ∧ TLS
    - → SSL IMPLEMENTED AT OSI LAYER 4 (TRANSPORT)
    - → TLS IS HIS SUCCESSOR TO PROTECT COMMUNICATION PROTOCOL IN THE NETWORK:
      1) SERVER SENDS HIS DIGITAL CERTIFICATE TO THE CLIENT
      2) CLIENT VERIFY IT USING PUBLIC KEY'S CA
      3) SESSION KEY GENERATED USING: DIFFIE-HELLMAN PROTOCOL:
         - → CLIENT GENERATE A SECRET → $A = g^a \bmod p$ → SEND A BUT a IS SECRET
         - → SERVER GENERATE B SECRET → $B = g^b \bmod p$ → SEND B BUT b IS SECRET
         - → NOW CLIENT CALCULATE $S = B^a \bmod p$
         - → NOW SERVER CALCULATE $S = A^b \bmod p$
         - → BUT $B^a \bmod p = (g^b)^a \bmod p = g^{ab} \bmod p$

           $A^b \bmod p = (g^a)^b \bmod p = g^{ab} \bmod p$
      4) SO SESSION KEY IS CALCULATED ∧ NOT ENTIRELY TRANSMITTED ∧ NOW IT'S USED TO EXCHANGE SYMMETRIC KEYS
      5) NOW COMMS. GOES ON IN A SYMMETRIC WAY
  - → EMAIL ENCRYPTION → MESSAGE ENCRYPTED WITH SYMMETRIC KEY → AND THIS KEY IS ENCRYPTED WITH ASYMMETRIC TO PROVIDE AUTHENTICATION
  - → ONION ROUTING (TOR NETWORK) → EACH NODE (ONION ROUTER) → KEEP TLS CONNECTION WITH OTHERS NODE → EACH NODE ONLY REMOVE ONLY ONE LAYER
    - → THE RECEIVER CANNOT KNOW WHO STARTED THE COMMUNICATION
    - → NO ONE NODE KNOWS THE WHOLE PATH
    - → GUARANTEE ANONIMITY

AUTHENTICATION

- DIGITAL IDENTITY NEED SOLUTIONS THAT PROVIDE: → SECURITY, RELIABILITY, MUTUAL TRUST BETWEEN
  - → DIGITAL IDENTITY HOLDER
  - → ORGANIZATION / PERSON / SYSTEM THAT OFFERS AN ONLINE SERVICE
- A SINGLE USER
  - → MAY CONTROL MULTIPLE DIGITAL IDENTITIES
  - ∧ REAL-WORLD IDENTITY MAY REMAIN UNKNOWN
- EACH DIGITAL IDENTITY IS UNIQUE IN THE CONTEXT OF A SPECIFIC ONLINE SERVICE
- USERS COULD USE ANONYMOUS/PSEUDONYMOUS ACCOUNTS IF "REQUIRED REAL-LIFE IDENTITY VERIFICATION TO OBTAIN ACCESS TO AN ONLINE SERVICE

- FEATURE IN THE PROCESS OF IAA (DIGITAL IDENTITY AUTHENTICATION):
  - SUBJECT APPLICANT → WHOSE IDENTITY IS BEING VERIFIED DURING IDENTITY PROOF & ENROLLMENT (VALIDATION & ACTIVATION OF DIGITAL IDENTITY)
  - SUBJECT SUBSCRIBER → WHO HAS SUCCESSFULLY COMPLETED IDENTITY PROOFING & ENROLLMENT AND NOW IS REGISTERED WITHIN THE IDENTITY SYSTEM
  - SUBJECT CLAIMANT → WHO TRIES TO START AN AUTHENTICATION SESSION (TRY LOGIN)

  } USER

  - CREDENTIAL SERVICE PROVIDER (CSP) → ENTITY RESPONSIBLE FOR:
    - IDENTITY PROOFING APPLICANTS (VERIFY THAT THE APPLICANT IS WHO HE SAYS HE IS)
    - ENROLLING SUBSCRIBERS → TRANSFORMING THE VERIFIED APPLICANT INTO THE SUBSCRIBER:
      - CREATING THE DIGITAL IDENTITY IN THE SYSTEM
      - MAKING IT USABLE FOR AUTHENTICATION
    - ISSUING AUTHENTICATION → ABILITATING MEANS OF AUTHENTICATION (PASSWORD, OTP, ...)
    - MANAGING AUTHENTICATORS:
      - RESET PASSWORDS
      - REVOKING CREDENTIALS
      - RECOVERING ACCOUNT
  - REGISTERING AUTHENTICATORS LINKED TO SUBSCRIBERS ACCOUNTS → LINKING EACH AUTHENTICATOR (PIN, OTP, ...) TO A SUBSCRIBER

- AUTHENTICATION IS THE PROCESS THAT ENABLES A RELIABLE PARTY TO TRUST A CLAIMANT IS WHO HE SAYS HE IS.
  - SUCCESSFULL AUTHENTICATION:
    - CLAIMANT SAYS HIS IDENTITY
    - SHOWS HIS AUTHENTICATORS (WHICH ARE LINKED TO THE IDENTITY OF THE SUBSCRIBER)
    - IF SUCCESS THEN CLAIMANT = SUBSCRIBER
  - THIS IS DONE THROUGH AN AUTHENTICATION PROTOCOL → THAT INVOLVES AN INTERACTION BETWEEN THE VERIFIER & THE CLAIMANT
    - PROTECT INTEGRITY & CONFIDENTIALITY DURING & AFTER THE AUTHENTICATION
    - HELP TO LIMIT DAMAGE DONE BY AN ATTACKER MASQUERADED AS A LEGITIMATE VERIFIER
- AUTHORIZATION → HAPPENS AFTER AUTHENTICATION
  - IS THE VERIFICATION OF PRIVILEGES & PERMITS ON THE RESOURCES THE USER HAS ACCESS TO
- AUTHENTICATION → WHO ARE YOU?
- AUTHORIZATION → WHAT ARE YOU ALLOWED TO DO?

- AUTHENTICATION MECHANISM AND AUTENTICATORS (APPLICATIONS) → EXAMPLE OF AUTHENTICATION MECHANISMS:
  - SOMETHING YOU ARE → BIOMETRIC CHARACTERISTICS (FINGERPRINTS...)
  - SOMETHING YOU HAVE → PHYSICAL/DIGITAL OBJECTS (CARD, KEYS...)
  - SOMETHING YOU KNOW → INFORMATIONS ONLY KNOWN BY THE USER (PASSWORDS, PIN, ...)
  - MULTI-FACTOR AUTHENTICATION → COMBINATION OF VARIOUS AUTHENTICATION MECHANISMS

- ATTACK CYCLE AGAINST PRIVATE DIGITAL IDENTITY:
  1) RECOVERING VALID AUTHENTICATORS → THROUGH PHISHING, SOCIAL ENGINEERING ...
  2) TEST OF AUTHENTICATORS → CREDENTIALS ARE USED TO SEE IF THEY ARE VALID
  3) SUCCESSFULL AUTHENTICATION
  4) USE OF THE ACCOUNT → ABUSING THE PRIVILEGES & BENEFITS OF THE SUBSCRIBERS

- USERNAME AND PASSWORDS → MOST COMMON & INSECURE AUTHENTICATION MECHANISM
  - USERNAME → PROVIDES HIS IDENTITY
  - PASSWORD → IS THE AUTHENTICATOR
    - BEFORE BEING STORED IN DATABASE BY THE SYSTEM → IT IS ENCRYPTED
    - IN THE LOGIN PHASE → USER PROMPT HIS PASSWORD → WHICH IS ENCRYPTED BY THE SAME ALGORITHM → AND CONFRONTED WITH THE STORED ONE
    - WEAK PASSWORDS CAN BE EASILY DISCOVERED WITH → SELFOSINT TECHNIQUES
      - BRUTE FORCED

- ACCESS CONTROL AND SECURITY → NIST SP 800-171 PROVIDES ACCESS CONTROL SECURITY & ACCOUNT MANAGEMENT REQUIREMENTS → MAIN GOALS: → VERIFY EACH ACCESS TO THE RESOURCES

- → APPLY THE PRINCIPLE OF "LEAST PRIVILAGE" → EACH USER HAS ONLY THE ESSENTIALS
- → VERIFY THE USAGE OF THE RESOURCES → USE THE RESOURCE IS ACCEPTABLE IN THE WAY EXPECTED BY THE POLICY

- → COMPONENTS OF ACCESS CONTROLS:
  - → REFERENCE MONITOR → MECHANISM THAT INTERCEPT EACH ACCESS REQUEST ∧ DECIDE IF APPROVE ∨ DENY IT
  - → ACCESS CONTROL DIRECTORY → ARCHIVE THAT MEMORIZED USERS, OBJECTS ∧ PRIVILEGES
  - → ACCESS CONTROL MATRIX → ABSTRACT MODEL TO REPRESENT ALL DATA →
    - ROWS = USERS
    - COLUMNS = OBJECTS
    - CELLS = PRIVILEGES
  - → ACCESS CONTROL LIST → LIST LINKED TO AN OBJECT → SHOWS WHO CAN ACCESS TO IT ∧ WITH WHICH PRIVILEGES
  - → PRIVILEGE LIST → LIST LINKED TO AN USER → ABOUT WHICH OPERATIONS ON OBJECTS
  - → CAPABILITY → TOKEN THAT SHOWS THE PRIVILEGE TO ACCESS TO A RESOURCE
- → MODEL OF ACCESS CONTROL:
  - → PROCEDURE-ORIENTED ACCESS CONTROL → CONTROL ACCESS DEPENDS →
    - NOT ONLY BY WHO YOU ARE
    - BUT ALSO ON WHAT ARE YOU DOING → USER ¬ACCESS STRAIGHT TO OBJECT → BUT THROUGH A FUNCTION
  - → ROLE-BASED ACCESS CONTROL (RBAC) → CONTROL ACCESS ARE ASSIGNED TO ROLES (ADMIN, MODS, USER) → AND NOT TO USERS
  - → DISCRETIONARY ACCESS CONTROL (DAC) → CONTROL ACCESS BASED ON THE SPECIFIC USER WHO CAN REQUEST IT → OWNER OF RESOURCE DECIDE WHO CAN ACCESS IT
  - → ATTRIBUTE-BASED CONTROL (ABAC) → CONTROL ACCESS BASED ON ATTRIBUTES OF THE USER ∧ THE RESOURCE HE IS REQUESTING
  - → MANDATORY ACCESS CONTROL (MAC) → CONTROL ACCESS BASED ON SECURITY LABELS → USER CANNOT CHANGE HIS PRIVILEGES DUE TO SECURITY

→ SCHEME OF SERVICE:
- → SUBJECT → ENTITY WHO REQUESTS ACCESS TO A RESOURCE
- → OBJECT → ACCESSABLE RESOURCE WHICH ACCESS HAPPENS IN A CONTROLLED WAY
- → ACCESS RIGHT → HOW SUBJECT INTERACT WITH AN OBJECT

→ PRIVILEGED ACCESS MANAGEMENT (PAM): → IT'S ABOUT 4 PILLARS ON THE PROTECTION ON PRIVILEGE ACCOUNTS (ADMIN, ROOT, SERVICE ACCOUNTS):
- → 1) TRACK AND SECURE →
  - IDENTIFY WHO ARE THE PRIVILEGED ACCOUNTS
  - IDENTIFY WHICH RESOURCES THEY CONTROL
- → 2) GOVERN AND CONTROL →
  - THE ACCESS BY A PRIVILEGED ACC. IS:
    - → LIMITED IN TIME
    - → GIVEN ONLY WHEN NEEDED
    - → AUTOMATICALLY REMOVED AFTER TIME IS DONE
  - → THE ACCESS IS BASED ON THE RULE OF THE 5 W:
    - → WHO ACCESS
    - → WHAT HE CAN DO IT
    - → WHERE HE CAN ACCESS FROM
    - → WHEN (DURATION OF THE ACCESS)
    - → WHY IS HE ACCESSING TO IT
  - → SO THERE AREN'T PERMANENT PRIVILEGES
- → 3) RECORD AND AUDIT → PRIVILEGED ACCOUNT SESSIONS ARE RECORDED
- → 4) OPERATIONALIZE → MANY REPETITIVE TASKS ARE TRANSFORMED FROM HUMAN TO AUTHOMATIC → REDUCING RISKS

→ AUTHENTICATION PROTOCOLS:
- → PASSWORD AUTHENTICATION PROTOCOL (PAP) →
  - → USERNAME + PASSWORD
  - → ¬ENCRYPTION
  - → VULNERABLE TO →
    - → EAVESDROPPING → INTERCEPT TRAFFIC ALLOWS TO READ PW
    - → REPLAY ATTACK → MESSAGE CAN BE RE-USED
- → CHALLENGED HANDSHAKE AUTHENTICATION PROTOCOL → USERNAME + PASSWORD WITHOUT TRANSMITTING THE PW:
  - → IMPORTANT!: non è per scambiarsi password, ma per dimostrare di conoscerla. Sia CLIENT sia SERVER conoscono già la password. Non stanno facendo REGISTRATION ma AUTENTICATION
  - → 1) SERVER SENDS A NONCE

- → 2) CLIENT CALCULATES R = HASH(NONCE | PW)
- → 3) SERVER CALCULATES R' = HASH(NONCE | PW) AND CONFRONTS
- → VULNERABILITY DEPENDS ON HOW STRONG PW IS

→ EXTENSIBLE AUTHENTICATION PROTOCOL (EAP) → IT'S NOT A PROTOCOL BUT A FRAMEWORK → IT'S A WHOLE STRUCTURE OF RULE ON HOW TO DO THE WHOLE AUTHENTICATION PROCESS → BUT THE METHOD WHO USES THE AUTHENTICATION CAN BE CHOSEN BETWEEN MANY:
- → 1) Il client invia all'ap. al volo
- → 2) Parla EAP
- → 3) Il server dice: "Usiamo metodo EAP-TLS"
- → 4) Da quel momento:
  - EAP trasporta i messaggi
  - EAP-TLS fa l'autenticazione con i certificati
- → 5) Se domani cambio
  - EAP trasporta i messaggi allo stesso modo
  - cambio metodo interno per autenticarsi

→ PRE-SHARED KEY (PSK) → THERE IS A SHARED KEY BETWEEN PAIRS OF DEVICES STORED DURING SETUP PROCESS
- → PROBLEM IS THAT ALL DEVICES IN THE COMMUNICATION HAS THE SAME KEY → SO IF ONE IS COMPROMISED, ALL OF THEM ARE

→ NEEDHAM-SCHROEDER PROTOCOL → USES A TRUSTED THIRD PARTY (TTP)
- → EACH DEVICE SHARES A KEY WITH TTP
- → FLOW:
  - → 1) • A SHARES A SECRET KEY ONLY WITH TTP: K_A
    • B SHARES A SECRET KEY ONLY WITH TTP: K_B
    • A & B SHARE NONCES BETWEEN EACH OTHER
  - → 2) A → TTP "I WANT TO TALK TO B"
  - → 3) TTP GENERATES SESSION KEY: K_{AB} VALID ONLY FOR THIS COMMUNICATION
  - → 4) TTP SENDS TO A:
    - K_{AB} ENCRYPTED WITH K_A: $\{K_{AB}\}_{K_A}$
    - TICKET TO B: $\{K_{AB}\}_{K_B}$ ONLY READABLE BY B. BECAUSE IT'S ENCRYPTED WITH HIS KEY
  - → 5) A → B, A SENDS THE SESSION KEY $\{K_{AB}\}_{K_B}$ TO B
  - → 6) NOW BOTH A & B BOTH KNOW K_{AB} AS A SYMMETRIC KEY FOR THEIR COMMUNICATION & TTP EXIT THE COMMUNICATION
- → VULNERABLE TO REPLAY ATTACK → ATTACKER TRIES TO USE OLD SESSION KEYS → BECAUSE TICKET $\{K_{AB}\}_{K_B}$ → HAVE A TIMESTAMP → B DECRYPT K_{AB}, SEE THAT IT WORKS SO IT'S OK

→ FEDERATED AUTHENTICATION → IT ALLOWS A USER TO:
- → TO AUTHENTICATE ONLY ONE TIME
- → WITH AN IDENTITY PROVIDER (IDP) THAT CHECK CREDENTIALS
- → USE SERVICES OF MANY ORGANIZATIONS THAT TRUST THE IDP

→ SINGLE SIGN-ON AUTHENTICATION → ALLOWS TO AUTHENTICATE ONCE & ACCESS TO MANY SERVICES WITHOUT PUT AGAIN CREDENTIALS → BUT THESE SERVICES MUST BE IN THE SAME DOMAIN/TRUSTED ECOSYSTEM
- → DIFFERENCE WITH FEDERATED AUTHENTICATION: → SSO ALLOWS RE-USE OF CREDENTIALS INSIDE SAME ORG., FEDERATED ALLOWS IT THROUGH DIFFERENT ORG.
- → AN EXAMPLE OF SINGLE SIGN-ON IS KERBEROS → INTERNET AUTHENTICATION PROTOCOL:
  - → 1) AUTHENTICATION SERVER EXCHANGE → GOAL: SHOW IDENTITY & OBTAIN TICKET GRANTING TICKET (TGT)
    - → 1) USER LOGIN ON THE CLIENT
    - → 2) CLIENT SEND TO AUTHENTICATION SERVER (AS): → IDENTITY OF THE USER & REQUEST OF SERVICE'S ACCESS
    - → 3) THE AS VERIFY USER EXISTS & GENERATE SESSION KEY: $K_{C,TGS}$ - A SYMMETRIC KEY SHARED BETWEEN CLIENT (C) & TICKET GRANTING SERVER (TGS)
    - → 4) THE AS REPLY WITH:
      - → THE SESSION KEY ENCRYPTED WITH THE USER'S KEY: $\{K_{C,TGS}\}_{K_C}$
      - → TGT ENCRYPTED WITH THE SECRET KEY OF TGS $\{TGT\}_{SECRET\ OF\ TGS}$
      - → AS A RESULT:
        - → ONLY USER CAN READ SESSION KEY
        - → ONLY TGS CAN READ TGT
  - → 2) TICKET GRANTING SERVER EXCHANGE → GOAL: OBTAIN A TICKET FOR A SPECIFIC SERVICE
    - → 1) THE CLIENT:

- DECRYPT SESSION KEY $\{K_{c,tgs}\}_{K_c}$ USING CLIENT KEY K_c
- SEND TO TGS:
  - TGT
  - AUTHENTICATOR (USER, ADDRESS, TIMESTAMP) ENCRYPTED WITH SESSION KEY $\{K_{c,tgs}\}$
  - ID OF THE REQUESTED SERVICE

2) THE TGS:

- USE HIS SECRET KEY TO READ $\{TGT\}_{SECRET\ OF\ TGS}$ & OBTAIN THE SESSION KEY
- USE THE SESSION KEY TO VERIFY THE AUTHENTICATOR WHICH IS ENCRYPTED WITH SESSION KEY
- SEND TO BOTH CLIENT & SERVER:
  - A NEW SESSION KEY CLIENT-SERVER ($K_{c,s}$) ENCRYPTED WITH SESSION KEY: $\{K_{c,s}\}_{K_{c,TGS}}$
  - SERVICE TICKET, ENCRYPTED WITH SERVER'S KEY
- AS RESULT:
  - CLIENT AS A KEY FOR THAT SERVICE
  - SERVER WILL VERIFY IT

CLIENT/SERVER EXCHANGE

- GOAL: ACCESS TO THE SERVICE WITHOUT PASSWORD

1) CLIENT SEND TO THE SERVER:

- SERVICE TICKET
- AUTHENTICATORS ENCRYPTED WITH SESSION KEY CLIENT-SERVER $\{K_{c,s}\}_{K_{c,TGS}}$

2) NOW SERVER:

- USE HIS SECRET KEY TO READ THE SERVICE TICKET
- DECRYPT SESSION KEY CLIENT-SERVER $\{K_{c,s}\}_{K_{c,TGS}}$
- NOW THAT HE HAS THE SESSION KEY CLIENT-SERVER CAN VERIFY THE AUTHENTICATOR

3) (OPTIONAL) MUTUAL AUTHENTICATION: → SERVER SENDS A SERVER AUTHENTICATOR

OAUTH

- IS AN AUTHORIZATION STANDARD → NOT AUTHENTICATION
- ALLOWS A THIRD-PARTIES APPLICATION:
  - TO ACCESS TO RESOURCES/API WITH USER CONSENT AS IF IT WAS THE USER
  - WITHOUT KNOWING ITS PASSWORD
- EXAMPLE: → OAUTH IS CALLED WHEN FACEBOOK ASKS A USER IF A NEW APPLICATION CAN HAVE ACCESS TO HIS PHOTOS (WITHOUT SHARING PW)

FAST IDENTITY ONLINE (FIDO)

- IS AN OPEN INDUSTRY ASSOCIATION THAT:
  - PROMOTES THE DEVELOPMENTS OF STANDARDS FOR AUTHENTICATION
  - ELIMINATE V REDUCE THE USE OF PASSWORDS DEVELOPING TECHNICAL SPECIFICATIONS
- IT IS ALSO A STANDARD

FIDO2 → IS A (PROTOCOL) MODERN STANDARD FOR PASSWORD-LESS AUTHENTICATION:

WHY IS IT MORE SECURE?

ANTI-PHISHING:

- A FALSE SITE CAN TRICK THE USER THAT INTS HIS PASSWORD
- BUT SINCE PRIVATE KEY IS UNIQUE FOR DOMAIN / DEVICE/SERVICE/ACCOUNT
- THE DEVICE CAN SEE THAT THE DOMAIN OF FAKE SITE ≠ REGISTERED AS A FIDO2 SITE SUPPORTER & HIS KEY ≠ REGISTERED

NO CREDENTIAL REUSE:

- SINCE EACH SERVICE HAS A DIFFERENT KEY
- AND SINCE EACH ACCOUNT HAS A DIFFERENT KEY
- THE BREACH OF A SERVICE ≠ COMPROMISE SECURITY OF OTHERS

1) REGISTRATION

- GOAL: LINK A DEVICE TO AN ACCOUNT THAT WANTS TO USE A SERVICE
- USER STARTS THE REGISTRATION TO A SERVICE THAT SUPPORTS FIDO2 PROTOCOL
- SERVER ASK THE DEVICE TO GENERATE:
  - PRIVATE KEY → THAT MUST STAY ON THE DEVICE
    - IT'S UNIQUE FOR THE COMBINATION OF DEVICE/SERVICE/ACCOUNT
  - PUBLIC KEY → NEEDS TO BE SENT TO THE SERVER
    - ASSOCIATED TO THE ACCOUNT
    - SAVED ON THE DATABASE

- WITH A NORMAL PIN ON MORE SITES → CHAIN ATTACK
- WITH PUDC KEYS ARE ISOLATED BY DESIGN

- NO PASSWORD DATABASE → SINCE SERVER SAVE ONLY PUBLIC KEY IN DATABASE
  - AND PUBLIC KEY ↗SECAST Λ ↗USABLE TO SIGN Λ RETRIEVE THE PRIVATE KEY
  - SO A BRUTE FORCE ATTACK ISN'T POSSIBLE
- REPLAY IMPOSSIBLE → SINCE SERVER GENERATE A RANDOM CHALLENGE VALID ONCE THAT DEVICE WILL SIGN
  - SO IF ATTACKER SNIFF CHALLENGE + SIGNATURE WON'T BE ABLE TO USE IT IN FUTURE SINCE THERE WILL BE A NEW CHALLENGE

- ALSO IT IS A 2FACTORS AUTHENTICATION PROTOCOL → DEVICE WITH PRIVATE KEY + <

2) LOGIN/AUTHENTICATION → GOAL: SHOW TO OWN THE RIGHT PRIVATE KEY

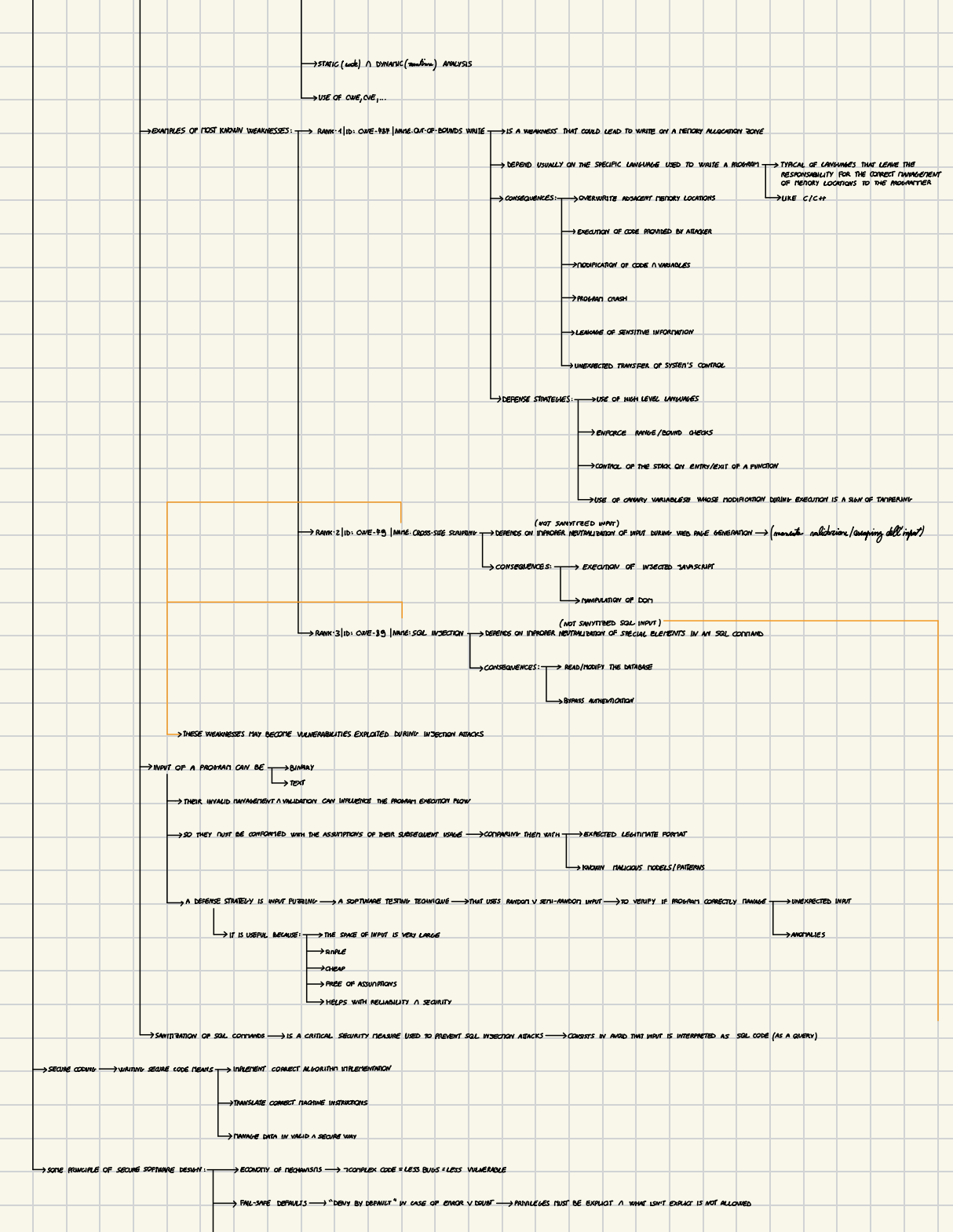
- USER ASKS FOR ACCESS
- SERVER SENDS A CRYPTOGRAPHIC CHALLENGE
- THE DEVICE:
  - ASKS VERIFICATION OF THE USER (PIN, BIOMETRIC)
  - USE HIS PRIVATE KEY TO SIGN THE CHALLENGE
- THE SERVER:
  - VERIFY THE SIGNATURE USING THE PUBLIC KEY
  - IF VALID THEN THE ACCESS IS ALLOWED

SOFTWARE SECURITY

- KEY CONCEPTS:
  - SOFTWARE SECURITY → SET OF REQUIREMENTS THAT PROVIDES C.I.A.
  - SECURITY FAILURE → SCENARIO WHERE SOFTWARE ↗ACHIEVE ITS SECURITY OBJECTIVES
  - VULNERABILITIES → MAIN CAUSE OF SECURITY FAILURE

- ORGANIZATIONS THAT CLASSES WEAKNESSES Λ VULNERABILITIES
  - USING EXTERNAL RESOURCES LIKE CWE V CVE TO IDENTIFY WEAKNESSES Λ VULNERABILITIES → ALLOWS TO MAP THE ROOT CAUSE OF SECURITY PROBLEMS
  - SO INSTEAD OF CORRECTING THE SINGLE VULNERABILITY
  - IT'S POSSIBLE TO ELIMINATE THE ROOT CAUSE
  - COMMON WEAKNESS ENUMERATION (CWE) → WEAKNESSES ARE ORGANIZED IN CLASSES Λ SUBCLASSES
    - DESCRIBE A TYPE OF ERROR
    - "TALKS ABOUT A VERSION V SOMETHING SPECIFIC
    - EX: "BUFFER OVERFLOW IS A PROBLEM WHERE"
    - A WEAKNESS IS → A CONDITION OF SOFTWARE/FIRMWARE/HARDWARE
      - THAT MAY BRING TO A VULNERABILITY
      - BUT IT'S NOT AN EXPLOIT YET
  - COMMON VULNERABILITIES Λ EXPOSURES (CVE) → CATALOGUE THAT IDENTIFIES CYBERSECURITY VULNERABILITIES
    - IT'S AN ACTUAL ERROR OF A PRODUCT
    - EX: "CVE-2016-XXXX IN WINDOWS USED BUFFER OVERFLOW TO..."
    - SO IT'S AN ISTANCE OF A CWE
    - A VULNERABILITY IS THE EXPLOITATION OF A WEAKNESS → VIOLATE C.I.A.
    - EACH CVE IS:
      - SPECIFIC FOR A PRODUCT/VERSION
      - DESCRIBE SOMETHING EXPLOITABLE
  - COMMON VULNERABILITY SCORING SYSTEM (CVSS) → NUMERICAL SCORE OF VULNERABILITY'S SEVERITY
    - SCALE 0-10
    - BASED ON:
      - IMPACT
      - HOW EASY WAS THE VULNERABILITY TO GET EXPLOIT
      - COMPLEXITY
    - THE NUMERICAL SCORE CAN THEN BE TRANSLATED INTO A QUALITATIVE REPRESENTATION (LOW, MEDIUM, HIGH, CRITICAL) TO HELP ORGANIZATIONS PROPERLY ASSESS Λ PRIORITIZE THEIR VULNERABILITY MANAGEMENT PROCESS
  - EXPLOIT PREDICTION SCORING SYSTEM (EPSS) → IS AN ESTIMATION OF PROBABILITY OF A VULNERABILITY OF BEING EXPLOITED OVER THE NEXT 30 DAYS
    - DAILY UPDATE

- ATTACK SURFACE → CONSISTS OF ALL THE REACHABLE Λ EXPLOITABLE VULNERABILITIES IN A SYSTEM
  - NOT ALL THAT IS VULNERABLE IN GENERAL → BUT ONLY WHAT THE ATTACKER CAN ACTUALLY EXPLOIT
  - DETECTION OF WEAKNESSES REQUIRES: → DEEP KNOWLEDGE OF LANGUAGES Λ PROTOCOLS


STATIC (code) ∧ DYNAMIC (runtime) ANALYSIS
USE OF CWE_i, CWE_j, ...
EXAMPLES OF MOST KNOWN WEAKNESSES:
RANK: 1 | ID: CWE-787 | NAME: OUT-OF-BOUNDS WRITE
IS A WEAKNESS THAT COULD LEAD TO WRITE ON A MEMORY ALLOCATION ZONE
DEPEND USUALLY ON THE SPECIFIC LANGUAGE USED TO WRITE A PROGRAM
TYPICAL OF LANGUAGES THAT LEAVE THE RESPONSABILITY FOR THE CORRECT MANAGEMENT OF MEMORY LOCATIONS TO THE PROGRAMMER
LIKE C/C++
CONSEQUENCES:
OVERWRITE ADJACENT MEMORY LOCATIONS
EXECUTION OF CODE PROVIDED BY ATTACKER
MODIFICATION OF CODE ∧ VARIABLES
PROGRAM CRASH
LEAKAGE OF SENSITIVE INFORMATION
UNEXPECTED TRANSFER OF SYSTEM'S CONTROL
DEFENSE STRATEGIES:
USE OF HIGH LEVEL LANGUAGES
ENFORCE RANGE/BOUND CHECKS
CONTROL OF THE STACK ON ENTRY/EXIT OF A FUNCTION
USE OF CANARY VARIABLES!! WHOSE MODIFICATION DURING EXECUTION IS A SIGN OF TAMPERING
RANK: 2 | ID: CWE-79 | NAME: CROSS-SITE SCRIPTING
(NOT SANYTIZED INPUT)
DEPENDS ON IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION
(example: malicious/escaping data input)
CONSEQUENCES:
EXECUTION OF INJECTED JAVASCRIPT
MANIPULATION OF DOM
RANK: 3 | ID: CWE-89 | NAME: SQL INJECTION
(NOT SANYTIZED SQL INPUT)
DEPENDS ON IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS IN AN SQL COMMAND
CONSEQUENCES:
READ/MODIFY THE DATABASE
BYPASS AUTHENTICATION
THESE WEAKNESSES MAY BECOME VULNERABILITIES EXPLOITED DURING INJECTION ATTACKS
INPUT OF A PROGRAM CAN BE
BINARY
TEXT
THEIR INVALID MANAGEMENT ∧ VALIDATION CAN INFLUENCE THE PROGRAM EXECUTION FLOW
SO THEY MUST BE CONFORMED WITH THE ASSUMPTIONS OF THEIR SUBSEQUENT USAGE
COMPARING THEM WITH
EXPECTED LEGITIMATE FORMAT
KNOWN MALICIOUS MODELS/PATTERNS
A DEFENSE STRATEGY IS INPUT FUZZING
A SOFTWARE TESTING TECHNIQUE
THAT USES RANDOM V SEMI-RANDOM INPUT
TO VERIFY IF PROGRAM CORRECTLY MANAGE
UNEXPECTED INPUT
ANOMALIES
IT IS USEFUL BECAUSE:
THE SPACE OF INPUT IS VERY LARGE
SIMPLE
CHEAP
FREE OF ASSUNTIONS
HELPS WITH RELIABILITY ∧ SECURITY
SANITIZATION OF SQL COMMANDS
IS A CRITICAL SECURITY MEASURE USED TO PREVENT SQL INJECTION ATTACKS
CONSISTS IN AVOID THAT INPUT IS INTERPRETED AS SQL CODE (AS A QUERY)
SECURE CODING
WRITING SECURE CODE MEANS
IMPLEMENT CORRECT ALGORITHM IMPLEMENTATION
TRANSLATE CORRECT MACHINE INSTRUCTIONS
MANAGE DATA IN VALID ∧ SECURE WAY
SOME PRINCIPLE OF SECURE SOFTWARE DESIGN:
ECONOMY OF MECHANISMS
"COMPLEX CODE = LESS BUGS = LESS VULNERABLE
FAIL-SAFE DEFAULTS
"DENY BY DEFAULT" IN CASE OF ERROR V DOUBT
PRIVILEGES MUST BE EXPLICIT ∧ WHAT ISN'T EXPLICIT IS NOT ALLOWED

- COMPLETE MEDIATION → EACH ACCESS TO A RESOURCE MUST BE CONTROLLED
- OPEN DESIGN → ALGORITHM & ARCHITECTURE MAY BE PUBLIC
  - SECRET MUST BE ONLY KEYS & CREDENTIALS
  - SECURITY BY DESIGN, NOT SECURITY BY OBSCURITY
- SEPARATION PRIVILEGE → WHEN A HUMAN IS REQUIRED TO AUTHORIZE SOMETHING HIGHLY SENSITIVE, IT IS BEST IF MORE THAN ONE HUMAN IS REQUIRED TO COMPLETE THE AUTHORIZATION
- LEAST PRIVILEGE → CODE SHOULD RUN WITH THE LEAST PRIVILEGE NECESSARY TO ACCOMPLISH ITS TASK
- DYNAMIC MEMORY ALLOCATION → USEFUL FOR:
  - WHEN AMOUNT OF DATA UNKNOWN
  - WHEN MEMORY ALLOCED ONLY WHEN NEEDED
  - MEMORY RELEASED WHEN UNEED ANYMORE

OS SECURITY

- AN OPERATING SYSTEM (OS):
  - MANAGES ACCESSES & AUTHORIZATIONS
  - PLANS & EXECUTES PROCESSES
  - MANAGES RESOURCES SHARED AMONG THE PROCESSES EXECUTED IN SAME ENVIRONMENT
  - GRANTS ISOLATION OF PROCESSES & EXECUTION ENVIRONMENT
  - SEPARATE CONTROL PLANE (DECISIONS, POLICY) & DATA PLANE (DATA)
- THE SIMPLEST WAY TO COMPROMISE THE SYSTEM IS TO INSERT:
  - MALICIOUS DRIVERS
  - KERNEL MODULES
  - UNTRUSTED EXTENSIONS
  - TO HOLD THE CONTROL OVER THE TIME AN ATTACKER MAY INJECT THE SYSTEM'S BOOT PROCESS → SO THAT MALICIOUS CODE LOADS BEFORE THE OS → DIFFICULT TO DETECT & REMOVE
- ATTACKERS OFTEN EXPLOIT VULNERABILITIES AS:
  - MEMORY ERRORS → (BUFFER OVERFLOWS)
  - LACK OF INPUT VALIDATION → AT KERNEL V DRIVER LEVEL
  - CONCURRENCY BUGS → (RACE CONDITION)
  - DOUBLE FETCH → (SAME VARIABLE READ 2 TIMES BUT WITH DIFFERENT VALUES)

- GLOBALPLATFORM → IS AN INITIATIVE OF DIFFERENT COMPANIES THAT AIMS TO DEVELOP STANDARD TECHNOLOGIES → FOR MANAGEMENT OF INNOVATIVE SERVICES & DEVICES PROTECTED BY THE PRINCIPLE OF SECURE BY DESIGN
- RICH EXECUTION ENVIRONMENT (REE) → UNTRUSTED EXECUTION ENVIRONMENT OF A SYSTEM → IT'S THE NORMAL ENV WHER OS & NORMAL APPLICATION ARE EXECUTED
- TRUSTED EXECUTION ENVIRONMENT (TEE) → IT'S AN EXECUTION ENVIRONMENT ISOLATED & VERIFIED INSIDE A SYS → FOR THE EXECUTION OF SENSITIVE OPERATIONS → EVEN WHEN THE REE IS COMPROMISED
  - CONFORM WITH GLOBALPLATFORM'S PRINCIPLES → TEE PROTECTION PROFILE DESCRIBE WHAT A TEE SHOULD GUARANTEE → NOT TALK ABOUT HOW IMPLEMENTS IT
  - TEE PROTECTION PROFILE ESTABLISHES A TEE SHOULD HAVE:
    - AUTHENTICITY → ONLY AUTHENTICATED CODE CAN BE EXECUTED ON TEE
    - INTEGRITY → CODE, DATA, STATE → ALL PROTECTED BY UNAUTHORIZED CHANGES → BY ISOLATION, CRYPTOGRAPHY, SECURE BOOT
    - DATA CONFIDENTIALITY → DATA & CRYPTOGRAPHIC KEYS → REMAIN SECRET EVEN IF REE IS COMPROMISED
    - TRUSTED APPLICATION'S (TA) CODE CONFIDENTIALITY → CODE OF TA NOT READABLE FROM OUTSIDE
    - SECURITY → MUST RESIST AGAINST KNOWN → SOFTWARE & HARDWARE ATTACKS
    - DEBUG & TRACE PROTECTION → IF UNAUTHORIZED THEY ARE BLOCKED

- THE TRUSTED OPERATIVE SYSTEM OF TEE STARTS FROM A ROOT OF TRUST (RoT) → WHICH IS THE FIRST COMPONENT THAT THE SYSTEM TRUST TO START THE SECURITY CHAIN
  - MUST BE:
    - IMMUTABLE → (ROM)
    - ISOLATED → FROM NORMAL OS
    - MINIMAL → LESS CODE = LESS BUGS
  - RoT STARTS THE SECURE BOOT → WHICH CRYPTOGRAPHICALLY VERIFIES:
    - FIRMWARE → CODE THAT STARTS HARDWARE BEFORE & UNDER OS
    - OS
    - NEXT COMPONENTS

- OS COMPONENTS INSIDE TEE ARCHITECTURE:
  - ROOT OF TRUST
  - TRUSTED OS → MINIMAL OS OF TEE
  - TRUSTED KERNEL → MANAGE
    - SCHEDULING
    - ISOLATION
    - RESOURCES
  - TRUSTED CORE FRAMEWORK → PROVIDES OS SERVICES FOR TRUSTED APPLICATIONS → EXPOSES SAFE APIs FOR SENSITIVE OPERATIONS & CRYPTOGRAPHY & KEYS MANAGEMENT
  - TRUSTED DEVICE DRIVERS → PROVIDES A COMMUNICATION'S INTERFACE WITH TRUSTED PERIPHERICALS
  - TEE COMMUNICATION AGENT → IS THE TEE' SIDE COMMUNICATION COMPONENT → WORKS ALONG WITH REE COMMUNICATION AGENT

- REE & TEE COMMUNICATE THROUGH A DEFINED & PROTECTED INTERFACE → TEE CLIENT API → A COMMUNICATION CHANNEL DESIGN TO:
  - TRANSMIT DATA FROM REE TO TEE (& VICEVERSA) SECURELY
  - PREVENT UNAUTHORIZED ACCESS BY THE REE TO THE TEE
  - LIMIT INTERACTIONS ONLY TO A NECESSARY REQUEST → (CRYPTOGRAPHIC V AUTHENTICATION OPERATIONS)
- REE MANAGE GENERIC OPERATIONS & INSENSITIVE OF THE SYSTEM
- WHEN AN OPERATION IS CRITIC → THE REE SENDS A REQUEST TO THE TEE → AND ELABORATE IT IN A SAFE WAY
- SO REE USE SERVICES OF TEE → WITHOUT VIOLATING ISOLATION & CONFIDENTIALITY → RECEIVING ONLY THE FINAL RESULT OF REQUESTED OPERATION

- THREATS AND MITIGATION IN OS → A CRITIC THREAT IS WHEN A SYSTEM IS COMPROMISED IN PHASE OF
  - INSTALLATION
  - DEPLOYMENT
- IF AN OS STARTS COMPROMISED → ALL ABOVE LEVELS INHERITATE THE COMPROMISE
- THAT'S WHY BUILDING A SYSTEM ISN'T AN ISOLATE ACTION → BUT A SAFETY PLAN PROCESS
- THE PLAN IS DESIGN TO REACH SOME GOALS: → ASSESS RISKS AND PLAN SYSTEM DEPLOYMENT → (BEFORE INSTALLATION)
  - ANALYSIS OF THREATS
  - CRITIC ASSETS
  - ATTACK SURFACES
  - ACCEPTABLE LEVEL OF RISK
  - → SECURE THE UNDERLYING OPERATING SYSTEM AND THEN THE KEY APPLICATIONS
  - → ASSURE CRITICAL CONTENT IS SECURED
  - → ASSURE APPROPRIATE NETWORK PROTECTION MECHANISMS ARE USED → REDUCE NETWORK'S ATTACK SURFACE (FIREWALL...)
  - → ASSURE APPROPRIATE PROCESSES ARE USED TO MAINTAIN SECURITY → AS
    - PATCH MANAGEMENT
    - MONITORING
    - LOGGING & AUDITING
- FLOW OF PLANIFICATION:
  - 1) SECURITY OF DATA, INFORMATION & APPLICATIONS → INSTALLATION OF NECESSARY FEATURES
  - 2) ASSESSMENT & IDENTIFICATION OF PRIVILEGES → LEAST PRIVILEGE
  - 3) METHODS FOR AUTHENTICATION OF AUTHORIZED USERS
  - 4) METHODS FOR ACCESSING DATA → NOT ALL AUTHORIZED USERS SHOULD SEE ALL

- 5) INTERACTIONS BETWEEN THE SYSTEM ∧ EXTERNAL RESOURCES → ANALYSIS OF CONNS WITH EXTERNAL NETWORKS ∧ API ∧ THIRD PARTIES → LIMITING INTERACTIONS
- 6) SYSTEM MANAGEMENT: WHO ∧ HOW
- 7) ADDITIONAL SECURITY MEASURES → (FIREWALL, ANTIVIRUS, DETECTION SYS) → THESE DOESN'T SUBSTITUTE SECURE BY DESIGN

- LOGGING → USEFUL BECAUSE IT REGISTERS SECURITY EVENTS ∧ ANOMALIES → TO INFORM INCIDENT ALREADY HAPPENED
  - SYS FAILURE
  - UNAUTHORIZED ACCESS
  - SECURITY BREACH
  - PREVENTS AN ATTACK → BUT ALLOWS TO UNDERSTAND WHAT HAPPENED
- DATA BACKUP AND ARCHIVE → REGULAR BACKUPS IS A CRITICAL CONTROL TO:
  - KEEP DATA INTEGRITY OF SYSTEM ∧ USER'S
  - GUARANTEE THE USE OF THE SYSTEM AFTER ATTACK VECTOR V...

CLOUD AND IOT SECURITY

- CLOUD COMPUTING: PROVIDE IT RESOURCES AS A SERVICE → FOLLOWING SERVICE MODELS ∧ DEPLOYMENT MODELS
- RESPONSABILITY OF SECURITY ∧ MANAGEMENT → IS SHARED BETWEEN CLIENT ∧ CLOUD PROVIDER → AND DEPENDS ON THE CHOSEN MODEL
- SERVICE MODELS:
  - INFRASTUCTURE AS A SERVICE (IAAS)
    - PROVIDER PROVIDES
      - HW
      - VIRTUALIZATION
      - NETWORK
    - CLIENT MANAGE
      - OS
      - MIDDLEWARE
      - APPLICATIONS
      - DATA
    - GOAL: CLIENT HAS ALL RESPONSABILITIES
  - PLATFORM AS A SERVICE (PAAS)
    - PROVIDER MANAGES
      - HW
      - OS
      - RUNTIME
    - CLIENT MANAGES
      - APPLICATIONS
      - DATA
    - GOAL: CLIENT THINKS ONLY TO WRITE ∧ EXECUTE APPLICATIONS WITHOUT THINKING ABOUT INFRASTUCTURE
  - SOFTWARE AS A SERVICE (SAAS)
    - PROVIDER MANAGES ALL THE STACK (HW, NETWORK, OS, APPLICATIONS..)
    - CLIENT
      - USE THE SERVICE THROUGH WEB/APP
      - MANAGES HIS DATA
      - MANAGE USERS ∧ PRIVILEGES AT APPLICATION LEVEL
      - EX: GMAIL PROVIDER, CLIENT CREATES ACC ∧ LOAD DATA ∧ SET PRIVILEGES
    - GOAL: DIRECT USE OF SW
- DEPLOYMENT MODELS → WHO OWNS THE INFRASTUCTURE ∧ WHO SHARES IT
  - PUBLIC CLOUD → INFRASTUCTURE IS OF THE PROVIDER

- SHARES AMONG MANY CLIENTS
- ACCESS THROUGH INTERNET
- PROS:
  - SCALABILITY
  - LOW COST
- CONS:
  - LESS DIRECT CONTROL

- PRIVATE CLOUD
  - INFRASTUCTURE OWNED BY A SINGLE ORG.
  - CAN BE:
    - ON-PREMISE → PHYSICALLY IN THE ORG.'S OFFICES
    - HOSTED BY A PROVIDER
  - PROS:
    - MAX. CONTROL → CLIENT DEPENDS ON THE PROVIDER'S CHOICES
    - ISOLATED → ISHARED WITH OTHER CLIENT
  - CONS:
    - HIGH COSTS
    - COMPLEX MANAGEMENT

- HYBRID CLOUD
  - DATA/SERVICE STAYS ON PRIVATE CLOUD
  - WHEN YOU HAVE A LOT OF TRAFFIC YOU USE PUBLIC CLOUD → CLOUD BURSTING
  - PROS:
    - SECURITY WHERE NEEDED
    - KEEPS THE COST LOW WHERE IT'S POSSIBLE
  - CONS:
    - COMPLEXITY
    - LARGER ATTACK SURFACE → BECAUSE MORE COMPONENTS

- COMMUNITY CLOUD
  - INFRASTUCTURE SHARED BY MORE ORG. WHO SHARES COMMON NEEDS
  - PROS: SHARED COST & POLICY
  - CONS: LESS FLEXIBLE

- SHARED RESPONSABILITY MODEL → DISTRIBUTED ON THE LAYER OF THE STACK:
  - RESPONSABILITIES OF CLOUD USER: → APPLICATION LEVEL SECURITY
    - SEC. OF APP CODE
    - APP CONFIG
    - MANAGEMENT OF USERS & ROLES
    - AUTHENTICATION & AUTHORIZATION
    - PROTECTION OF DATA
    - EX: if app. has an SQL injection or an bug, it's a cloud user responsibility
  - RESPONSABILITIES OF CLOUD PROVIDER → PHYSICAL + A PART OF SW
    - PHYSICAL SEC OF DATA CENTER
    - HW
    - HYPERVISOR
    - CONTINUITY OF SERVICE
  - SHARED RESPONSABILITIES → DEPEND ON MODEL (IAAS, PAAS, SAAS) BUT USUALLY INCLUDES:
    - OS
    - RUNTIME
    - MIDDLEWARE
    - CONFIG OF VIRTUAL NETWORK
    - EX: provider provide OS, client needs to config it correctly

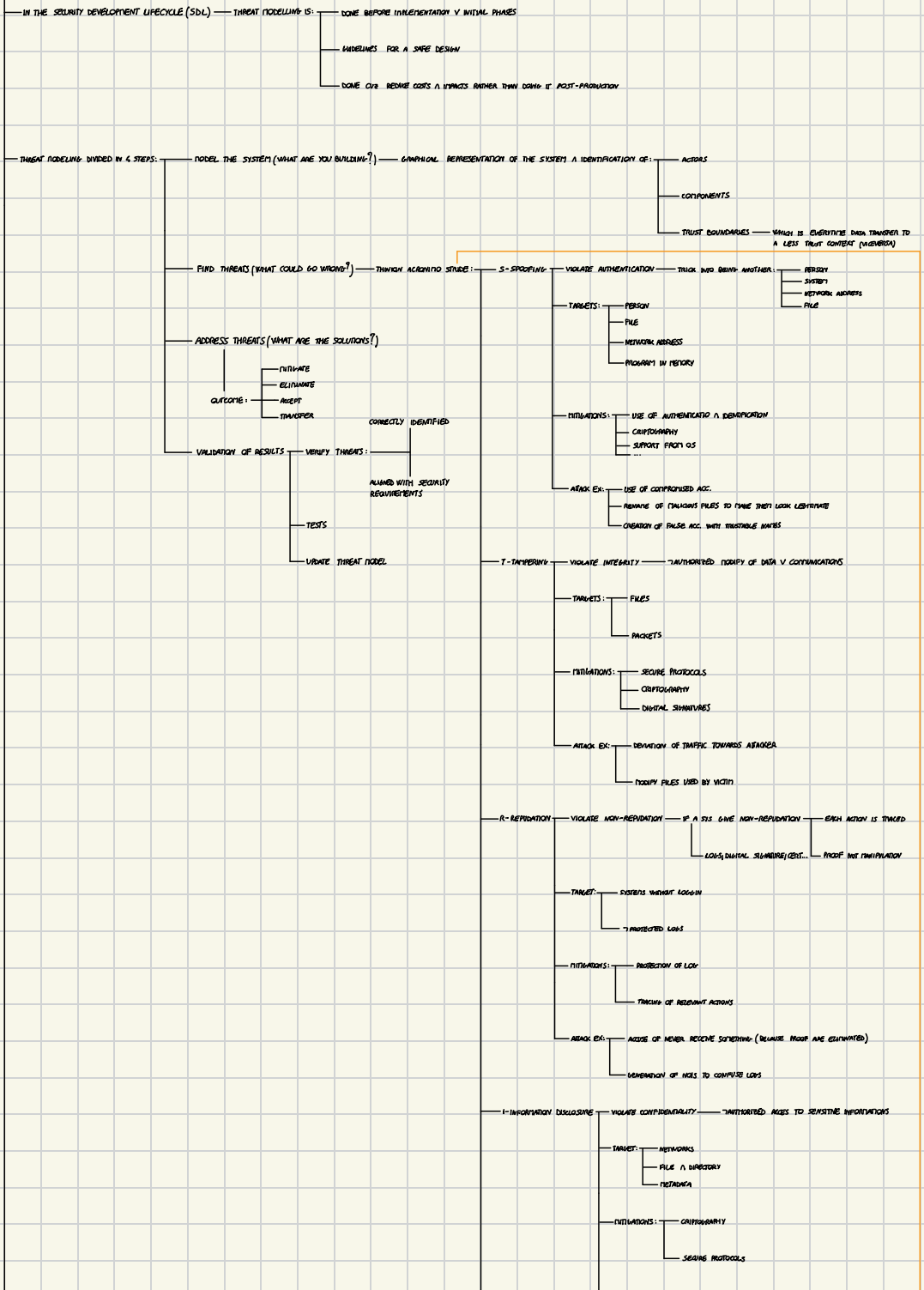
- VIRTUALIZATION SECURITY ISSUES → ARE RELATED TO:
  - GUEST OS ISOLATION → EACH GUEST OS MUST USE ONLY HIS ASSIGNED RESOURCES
  - GUEST OS MONITORING BY THE HYPERVISOR → WHICH HAS HIGHEST PRIVILEGES THAN ALL GUEST OS
    - BUT IF HE VULNERABLE → ALL VIRTUAL MACHINES ARE COMPROMISED
  - VIRTUALIZED ENVIRONMENT SECURITY

= ASTRACTION OF HW IN ISOLATED VIRTUAL RESOURCES

- CSA AND STAR PROGRAM
  - CLOUD SECURITY ALLIANCE (CSA) DEFINES CLOUD CONTROLS MATRIX (CCM) AS:
    - FRAMEWORK OF SECURITY CONTROLS FOR CLOUD ON:
      - GOVERNANCE
      - RISK MANAGEMENT
      - DATA PROTECTION
      - IDENTITY & ACCESS MANAGEMENT
    - THE BASE OF STAR PROGRAM
  - SECURITY, TRUST, ASSURANCE, RISK (STAR) PROGRAM IS:
    - PUBLIC REGISTRY
      - MANAGE BY CSA
      - DOCUMENTS SECURITY MEASURES & PRIVACY ADOPTED BY CLOUD PROVIDERS
      - GOAL:
        - ALLOWS COMPARISONS BETWEEN CLOUD SERVICES
        - PROVIDE ASSURANCE TO CLIENTS
  - IS A PROGRAM STRUCTURED ON LEVELS:
    - STAR LEVEL 1: SELF ASSESSMENT:
      - CSPs/PROVIDERS USE CCM TO EVALUATE & DOCUMENT THEIR SECURITY CONTROLS
      - THIS LEVEL ALLOWS THE PROVIDERS TO DEMONSTRATE THEY FOLLOW SECURITY BEST PRACTICES
      - PRIVACY ASSESSMENT IS BASED ON THE GENERAL DATA PROTECTION REGULATION OF THE EUROPEAN UNION (GDPR)
      - BUT IT CERTIFIES NOTHING
    - STAR LEVEL 3: THIRD-PARTY AUDIT:
      - AN AUDIT IS A CHECK IF EVERYTHING DECLARED HAS BEEN DONE
      - DONE BY CERTIFICATED ENTITIES QUALIFIED BY CSA
      - INCLUDES
        - SECURITY AUDIT
        - PRIVACY AUDIT
      - GOAL:
        - PROVIDE ASSURANCE SHOWING THAT CONTROLS:
          - EXISTS
          - WORK
          - VERIFIED
      - IT CERTIFICATES

THREAT MODELING

- IS A STRATEGIC SECURITY ANALYSIS PROCESS ON AN EXISTING/PLANNED APPLICATION ENVIRONMENT TO IDENTIFY:
  - POTENTIAL ATTACKS
  - EXPLOITABLE VULNERABILITIES
  - ASSOCIATED RISKS & THEIR IMPACT
- CORE COMPONENTS:
  - THREAT IDENTIFICATION
    - SYSTEM IS DIVIDED IN COMPONENTS (CLIENT, SERVER, DB, API, ...)
    - ENUMERATE ALL POSSIBLE SCENARIO FOR THE FAILURE OF EACH COMPONENTS
  - THREAT CATEGORIZATION BY
    - TYPE OF THREAT (SPOOFING, TAMPERING, ...)
    - THREAT AGENT — SOURCE OF THE THREAT:
      - HUMANS (ATTACKERS, INSIDERS)
      - TOOLS/AUTOMATED SYSTEMS (MALWARE, BOTS, SCANNERS)
      - NATURAL (EARTHQUAKES, STORMS, FIRE)
    - TARGETS — ASSETS AFFECTED (DATA, SERVICES, INFRASTRUCTURE)
  - RISK ASSESSMENT — EVALUATE LIKELIHOOD & IMPACT
  - OUTCOME — 4 POSSIBLE TREATMENTS:
    - MITIGATED — REDUCTION OF LIKELIHOOD & IMPACT
    - ELIMINATED — REMOVAL THE CAUSE OF THE THREAT
    - ACCEPTED — ACCEPTING THE RISK WHEN:
      - COST OF MITIGATION HIGHER THAN COST OF IMPACT
      - RISK IS ACCEPTABLE INSIDE A RANGE
    - TRANSFERRED — LET MANAGE RISK TO THIRD-PARTIES (ASSICURATIONS, ...)


IN THE SECURITY DEVELOPMENT LIFECYCLE (SDL)
THREAT MODELLING IS:
DONE BEFORE IMPLEMENTATION V INITIAL PHASES
GUIDELINES FOR A SAFE DESIGN
DONE C'è BISOGNO COSTI A IMPACTS RATHER THAN DOING IT POST-PRODUCTION
THREAT MODELING DIVIDED IN 4 STEPS:
MODEL THE SYSTEM (WHAT ARE YOU BUILDING?)
GRAPHICAL REPRESENTATION OF THE SYSTEM A IDENTIFICATION OF:
ACTORS
COMPONENTS
TRUST BOUNDARIES
WHICH IS EVERYTIME DATA TRANSFER TO A LESS TRUST CONTEXT (VICEVERSA)
FIND THREATS (WHAT COULD GO WRONG?)
THEMON ACRONIMO STRIDE:
S-SPOOFING
VIOLATE AUTHENTICATION
TRICK WHO BEING ANOTHER:
PERSON
SYSTEM
NETWORK ADDRESS
FILE
TARGETS:
PERSON
FILE
NETWORK ADDRESS
PROGRAM IN MEMORY
MITIGATIONS:
USE OF AUTHENTICATIO A IDENTIFICATION
CRIPTOGRAPHY
SUPPORT FROM OS
...
ATTACK EX:
USE OF COMPROMISED ACC.
RENAME OF MALICIOUS FILES TO MAKE THEM LOOK LEGITIMATE
CREATION OF FALSE ACC. WITH MISTAKABLE NAMES
T-TAMPERING
VIOLATE INTEGRITY
=AUTHORIZED MODIFY OF DATA V COMMUNICATIONS
TARGETS:
FILES
PACKETS
MITIGATIONS:
SECURE PROTOCOLS
CRIPTOGRAPHY
DIGITAL SIGNATURES
ATTACK EX:
DEVIATION OF TRAFFIC TOWARDS ATTACKER
MODIFY FILES USED BY VICTIM
R-REPUDIATION
VIOLATE NON-REPUDIATION
IF A SYS GIVE NON-REPUDIATION
EACH ACTION IS TRACED
LOGS, DIGITAL SIGNATURE, CERT...
PROOF NOT MANIPULATION
TARGET:
SYSTEMS WITHOUT LOGGIN
=PROTECTED LOGS
MITIGATIONS:
PROTECTION OF LOG
TRACING OF RELEVANT ACTIONS
ATTACK EX:
ACCUSE OF NEVER RECEIVE SOMETHING (BECAUSE PROOF ARE ELIMINATED)
GENERATION OF LOGS TO CONFUSE LOGS
I-INFORMATION DISCLOSURE
VIOLATE CONFIDENTIALITY
=AUTHORIZED ACCES TO SENSITIVE INFORMATIONS
TARGET:
NETWORKS
FILE A DIRECTORY
METADATA
MITIGATIONS:
CRIPTOGRAPHY
SECURE PROTOCOLS
ADDRESS THREATS (WHAT ARE THE SOLUTIONS?)
OUTCOME:
MITIGATE
ELIMINATE
ACCEPT
TRANSFER
VALIDATION OF RESULTS
VERIFY THREATS:
CORRECTLY IDENTIFIED
ALIGNED WITH SECURITY REQUIREMENTS
TESTS
UPDATE THREAT MODEL

- ATTACK EX:
  - EXTRACTION OF SECRETS FROM ERROR MESSAGES
  - RETRIEVE CRYPTOGRAPHIC KEYS FROM MEMORY
  - TRAFFIC ANALYSIS
  - OBSERVE DNS TO KNOW WHO TALKS TO WHO
- D-DENIAL OF SERVICE — VIOLATE AVAILABILITY — INTERRUPT SERVICE V. DOWNGRADE PERFORMANCES
  - TARGET:
    - APPLICATION
    - SYSTEM
    - NETWORK
  - MITIGATIONS:
    - ACCESS CONTROL
    - CLOUD N SCALABILITY MECHANISMS
  - ATTACK EX:
    - FLOODING ATTACK
    - EXCESSIVE CONSUME OF NETWORK BANDWIDTH
- E-ELEVATION OF PRIVILEGE — VIOLATE AUTHORIZATION — GAIN HIGHER PRIVILEGES THAN YOU SHOULD
  - TARGET:
    - CODE
    - MEMORY
  - MITIGATIONS:
    - HIGH LEVEL LANGUAGE
    - SEPARATION BETWEEN CODE N DATA
    - SANDBOXING
  - ATTACK EX:
    - EXECUTION OF OPERATION RESERVED FOR PRIVILEGED USER
    - INPUTS INCORRECTLY HANDLE

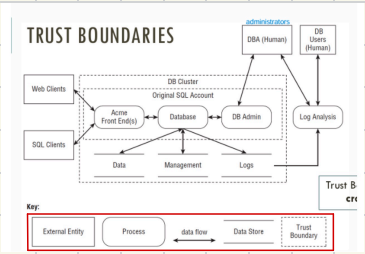
- THREAT MODELLING PROCESS HAVE 2 APPROACHES:
  - SECURITY-CENTRIC CONCENTRATES ON — WHERE CAN THE SYSTEM BREAK
    - TECHNICAL WEAKNESSES
    - PROTOCOLS
    - CONFIGURATIONS
  - RISK-BASED CONCENTRATES ON — WHAT'S IMPORTANT TO PROTECT N BY WHO?
    - ASSETS
    - ATTACKERS
    - IMPACT

- SOFTWARE IS MODELLED USING DIAGRAMS STARTING FROM TRUST BOUNDARIES
  - DATA FLOW DIAGRAM (DFD) — A DFD
    - SHOWS HOW DATA MOVES THROUGH A SYSTEM
    - WHICH COMPONENT PROCESS THEM
    - WHERE TRUST BOUNDARIES ARE CROSSED
    - GOALS:
      - VISUALISE DATA FLOWS
      - EXPOSE ATTACK SURFACES
      - MAKE TRUST BOUNDARIES EXPLICIT
      - DEFINE ELEMENTS WHERE IT'S POSSIBLE TO APPLY STRIDE
    - IT IS THE PRIMARY DIAGRAM USED IN THREAT MODELLING
  - HOW TO BUILD A DFD:

ELEMENT	APPEARANCE	MEANING	EXAMPLES
Process	Rounded rectangle, circle, or concentric circles	Any running code	Code written in C, C#, Python, or PHP
Data flow	Arrow	Communication between processes, or between processes and data stores	Network connections, HTTP, RPC, LPC
Data store	Two parallel lines with a label between them	Things that store data	Files, databases, the Windows Registry, shared memory segments
External entity	Rectangle with sharp corners	People, or code outside your control	Your customer, Microsoft.com

— THEY ARE OUTSIDE THE TRUST BOUNDARY — WHICH IS DOTTED LINE

- EXAMPLE:



- ONCE ELEMENTS ARE IDENTIFIED IT'S POSSIBLE TO APPLY STRIDE
- BUT STRIDE DON'T LIST SPECIFIC ATTACKS — BUT ONLY CATEGORIES
- TRANSITION FROM "TYPE OF THREAT" TO "REAL ATTACK" — DONE USING ATTACK LIBRARIES — THAT COLLECT ALREADY OBSERVED ATTACKS
- MAIN ATTACK LIBRARIES:
  - CAPEC BY MITRE — LIST OF ATTACK PATTERN (EXECUTION OF AN ATTACK)
  - ATT&CK BY MITRE — TACTICS & TECHNIQUES USED BY ATTACKERS
  - OWASP — MOST COMMON ATTACKS ON WEB APP

- SCORING SYSTEM THAT EVALUATE AN ALREADY KNOWN THREAT
- DREAD MODEL — RISK-MODEL BASED THREAT MODELLING — USEFUL TO FIND THREATS — BUT PRIORITIZE THEM — EACH THREAT EVALUATED ON 5 DIMENSIONS — WITH A SCORE 1-3 — FINAL SCORE = D+R+E+A+D
  - D - DAMAGE POTENTIAL
  - R - REPRODUCIBILITY — HOW EASY TO REPRODUCE ATTACK
  - E - EXPLOITABILITY — HOW HARD TO EXPLOIT THE VULNERABILITY
  - A - AFFECTED USERS — HOW MANY
  - D - DISCOVERABILITY — HOW EASY TO DISCOVER THE VULN
- PROCESS FOR ATTACK SIMULATION AND THREAT ANALYSIS (PASTA) MODEL — THREAT MODELLING FRAMEWORK DOES COMPLETE ANALYSIS:
  - DEFINITION OF BUSINESS ASSETS
  - DEFINITION OF ARCHITECTURE, COMPONENTS, TRUST BOUNDARIES
  - THREAT INTELLIGENCE — COLLECT INFO ON ATTACKER, MOTIVATIONS, TECHNIQUES...
  - VULNERABILITY ANALYSIS — ATTACK SURFACE
  - ATTACK SIMULATION
  - RISK & IMPACT — ANALYSIS OF POSSIBLE DMG
  - MITIGATION — COUNTERMEASURES & ACCEPTANCE OF RISK

THREAT INTELLIGENCE

- SECURITY INFORMATION & EVENT MANAGEMENT (SIEM) — IS A COLLECTIVE SYSTEM — FOR CORRELATION & ANALYSIS — OF SECURITY EVENTS
  - TRANSFORM RAW DATA — INTO USEFUL INFORMATION TO IDENTIFY REAL THREATS — PUT TOGETHER LOGS & EVENTS FROM — FIREWALLS | SERVER | DB | APP | ...
    - WITHOUT SIEM THEY ARE SPARSE DATA — SIEM HELPS TO HAVE A UNIFIED VISION OF THEM — TO CREATE ATTACK PATTERN — THANKS TO MACHINE LEARNING