



# 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

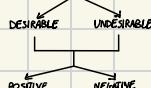
ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION) → NON GOVERNMENTAL → PUBLISHES INTERNATIONAL STANDARDS  
 ↗ ALL ASPECT OF TECHNOLOGY — IS A DOCUMENT — BEST PRACTICES ABOUT DOING SOMETHING (PRODUCTS, SERVICES OR PROCESSES)

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY) → GOVERNMENTAL ORGANIZATION → PART OF U.S. DEPARTMENT OF COMMERCE

→ DEFINITION RISK

ISO → VALID ANY ORG

RISK → MEASURE → DESCRIPTION OF EFFECT OF UNCERTAINTY ON OBJECTIVES



NIST → MEASURE OF RISK AND IMPACT ONLY → FOCUS INFORMATION SECURITY ASPECT

RISK MEASURE ENTITY THREATENED BY POTENTIAL EVENT

EXRESSED 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 PROTECTIVE ORGANIZATIONS → ALLOWS TO BALANCE ↗ OPERATIONAL AND ECONOMIC COSTS OF PROTECTIVE MEASURES

PROTECTION NEEDED

EACH ORG DECIDES WHETHER RISK ACCEPTABLE → BASED ON INFORMATION → AFTER DATA ANALYSIS

→ ISO 31000 STANDARD → COMPREHENSIVE APPROACH → MANAGE ANY KIND RISK → (7 SPECIFIC INF. SEC.)

→ APPLICATION CUSTOMIZED × ANY ORG ↗ CREATE VALUE INSIDE THE ORG.

PRINCIPLES → GOAL ↗ PROTECT VALUE

STRUCTURE → FRAMEWORK → GUIDE LINES HOW RISK IS MANAGED

↪ ITS EFFECTIVENESS DEPENDS ON GOVERNANCE & SUPERVISION

PROCESS → ITERATIVE PROCESS 3 PHASES :

→ RISK IDENTIFICATION → ANALYZE ↗ ASSETS  
 ↗ THREATS  
 ↗ OPPORTUNITIES

→ RISK ANALYSIS → EVALUATE ↗ CONSEQUENCES

→ RISK EVALUATION → DECIDE IF RISK BASED ON RISK'S LEVEL IS ACCEPTABLE OR NOT ↗ LIKELIHOOD RISK HAPPENS

→ 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 27005:2020

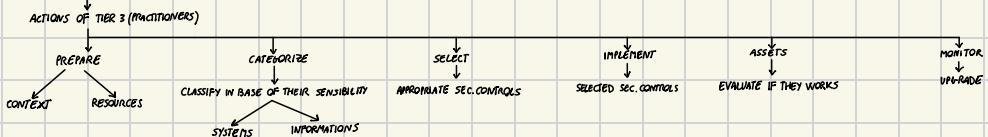
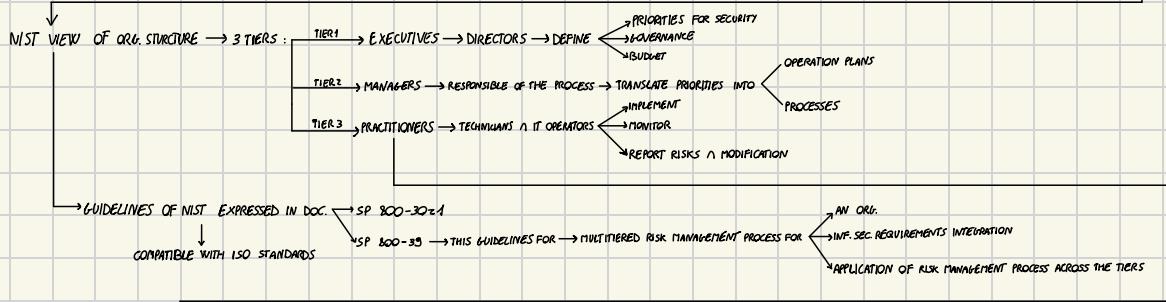
ISO STANDARD FOR INF. SEC., CYBER SEC., PRIVACY PROTECTION

GUIDE LINES FOR RISK MANAGEMENT IN INF. SEC.

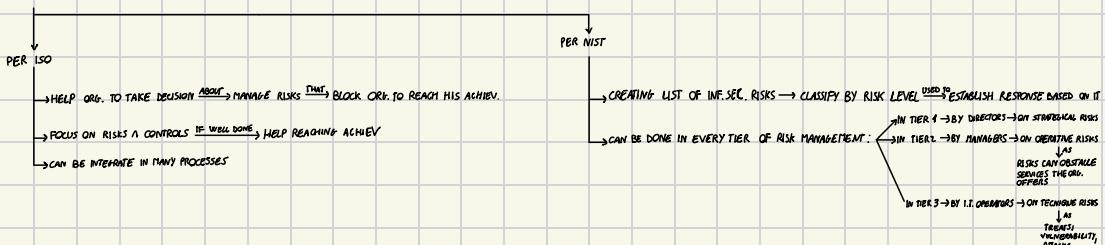
IT IDENTIFY 2 KIND OF INF. ASSETS:

PRIMARY/BUSINESS ASSETS  
 ↓  
 INF. V PROCESSES OF VALUE  
 (INTELLECTUAL PROPERTY)  
 FINANCIAL INF., INF. ABOUT CUSTOMERS...)

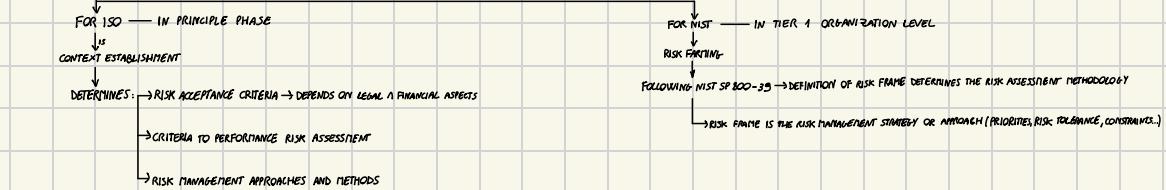
SUPPORTING ASSETS  
 ↓  
 COMPONENTS OF INF. SYS. ON WHICH  
 BUSINESS/PUBLIC ASSETS ARE  
 BASED (HARDWARE, SOFTWARE,  
 APPLICATION...)



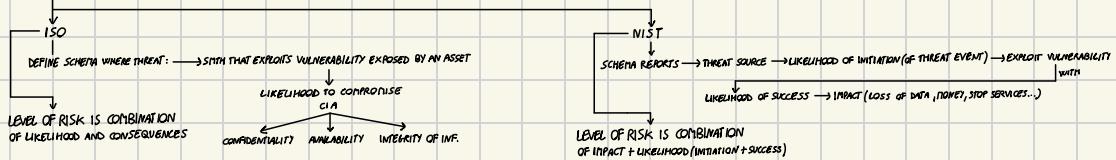
### GOAL OF RISK ASSESSMENT PROCESS:



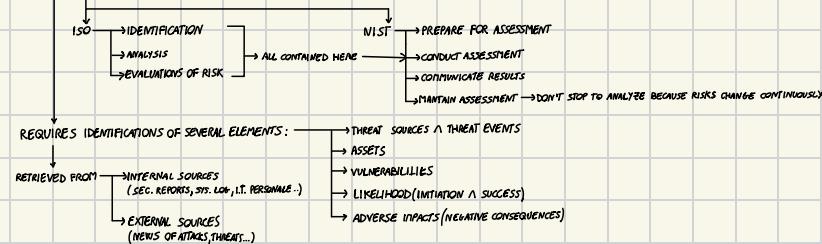
### RISK ASSESSMENT PRELIMINARY STEP



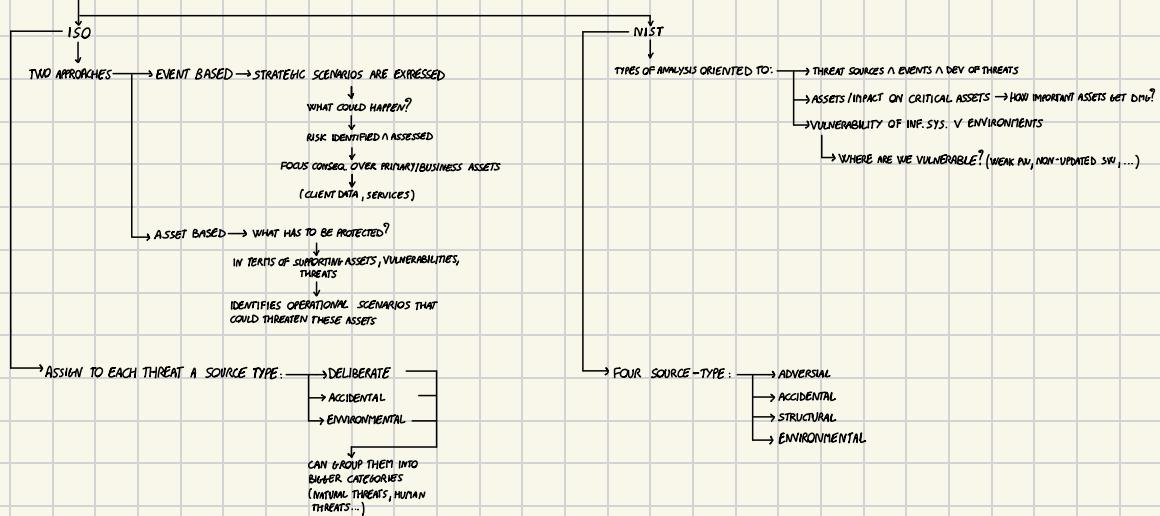
### RISK MODEL



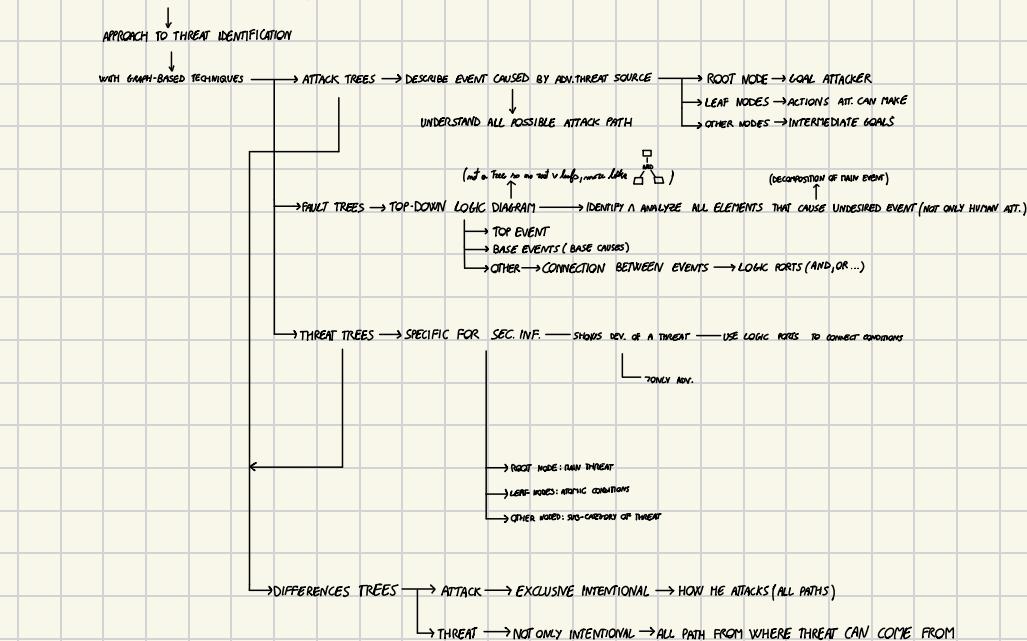
### RISK ASSESSMENT PROCESS



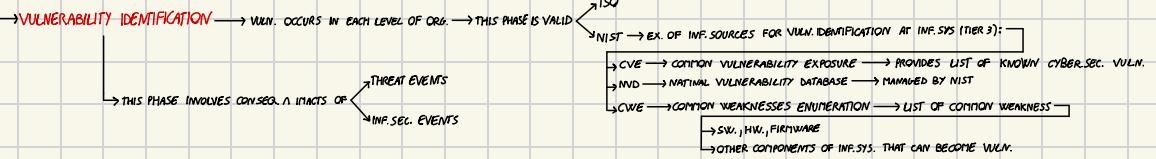
## RISK IDENTIFICATION

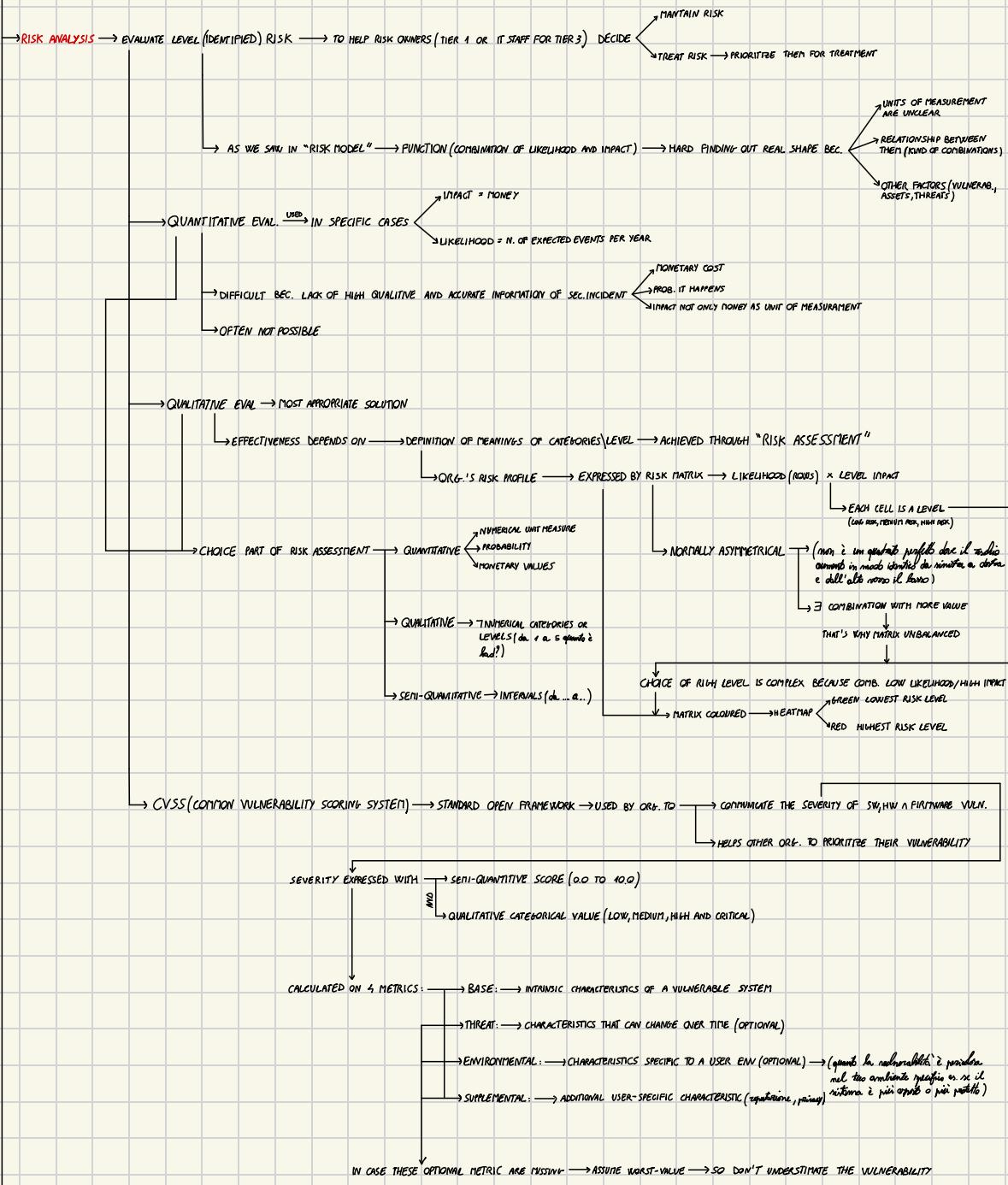


## THREAT IDENTIFICATION "THREAT MODELLING"

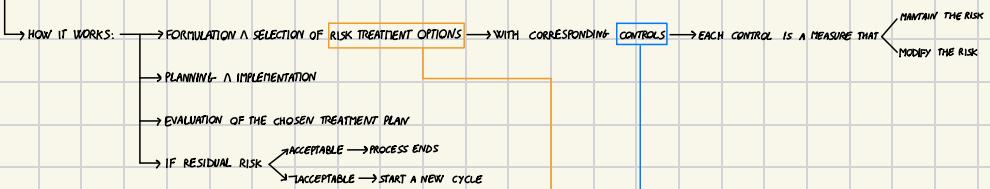


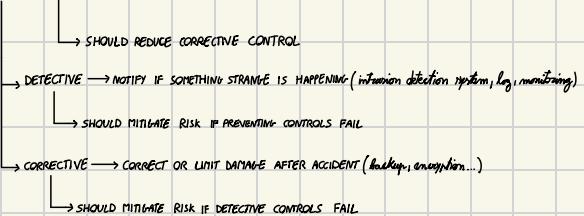
## VULNERABILITY IDENTIFICATION



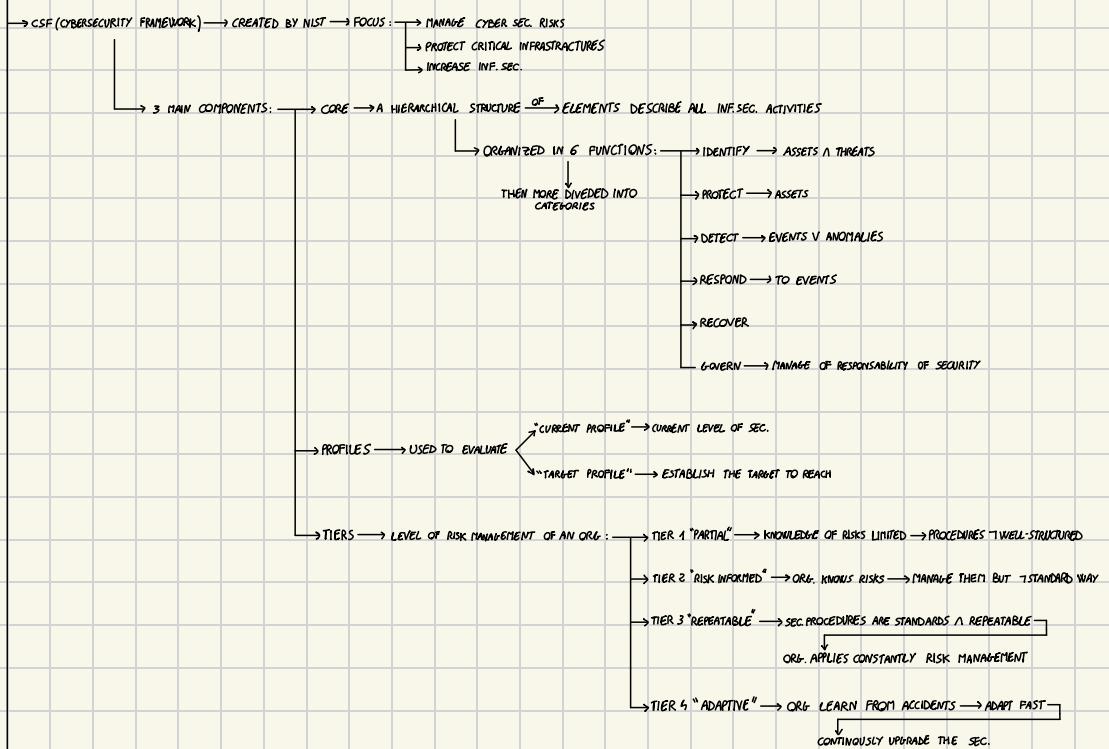


**RISK EVALUATION** → ONCE RISKS & RISK'S LEVEL ARE DETERMINED → GOAL IS DECIDE → ACCEPT RISK'S LEVELS

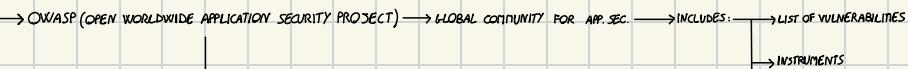
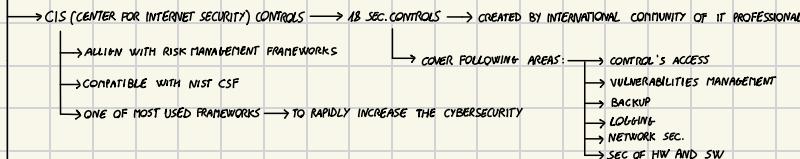


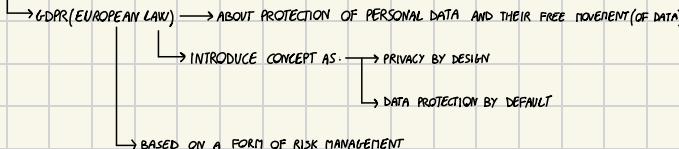
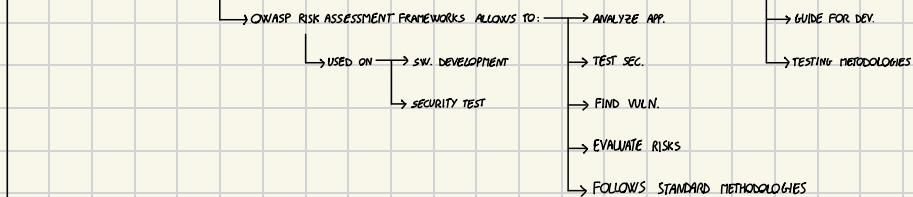


→ MANY FRAMEWORK → RELATED TO INF. SEC. → BASED ON A RISK MANAGEMENT APPROACH.

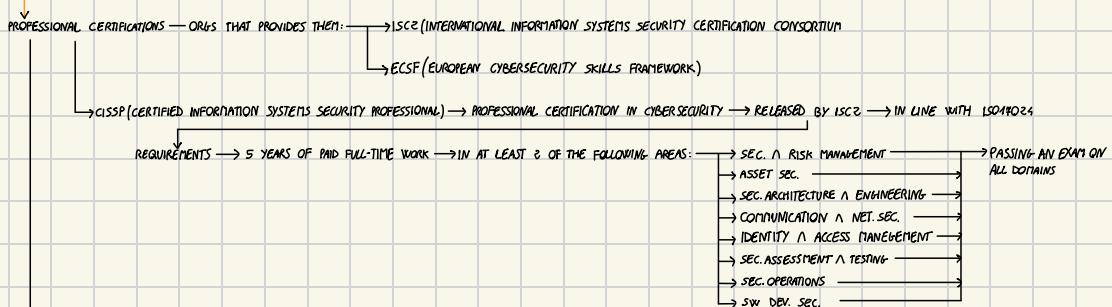
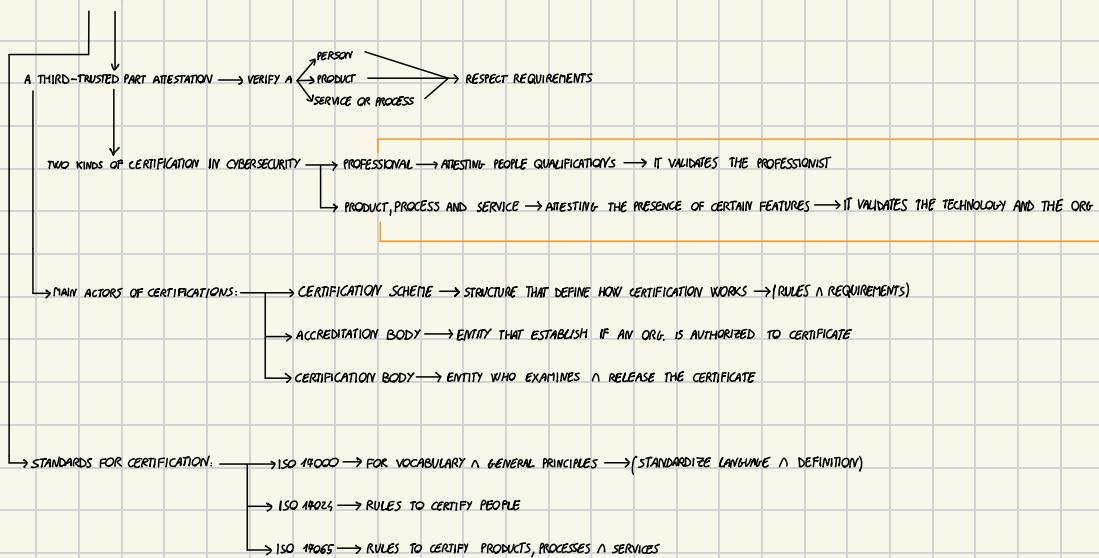


→ NATIONAL CYBERSECURITY FRAMEWORK (ITALY) → NATIONAL FRAMEWORK FOR CYBERSECURITY → BASED ON NIST CSF → ADAPTED TO ITALIAN CONTEXT

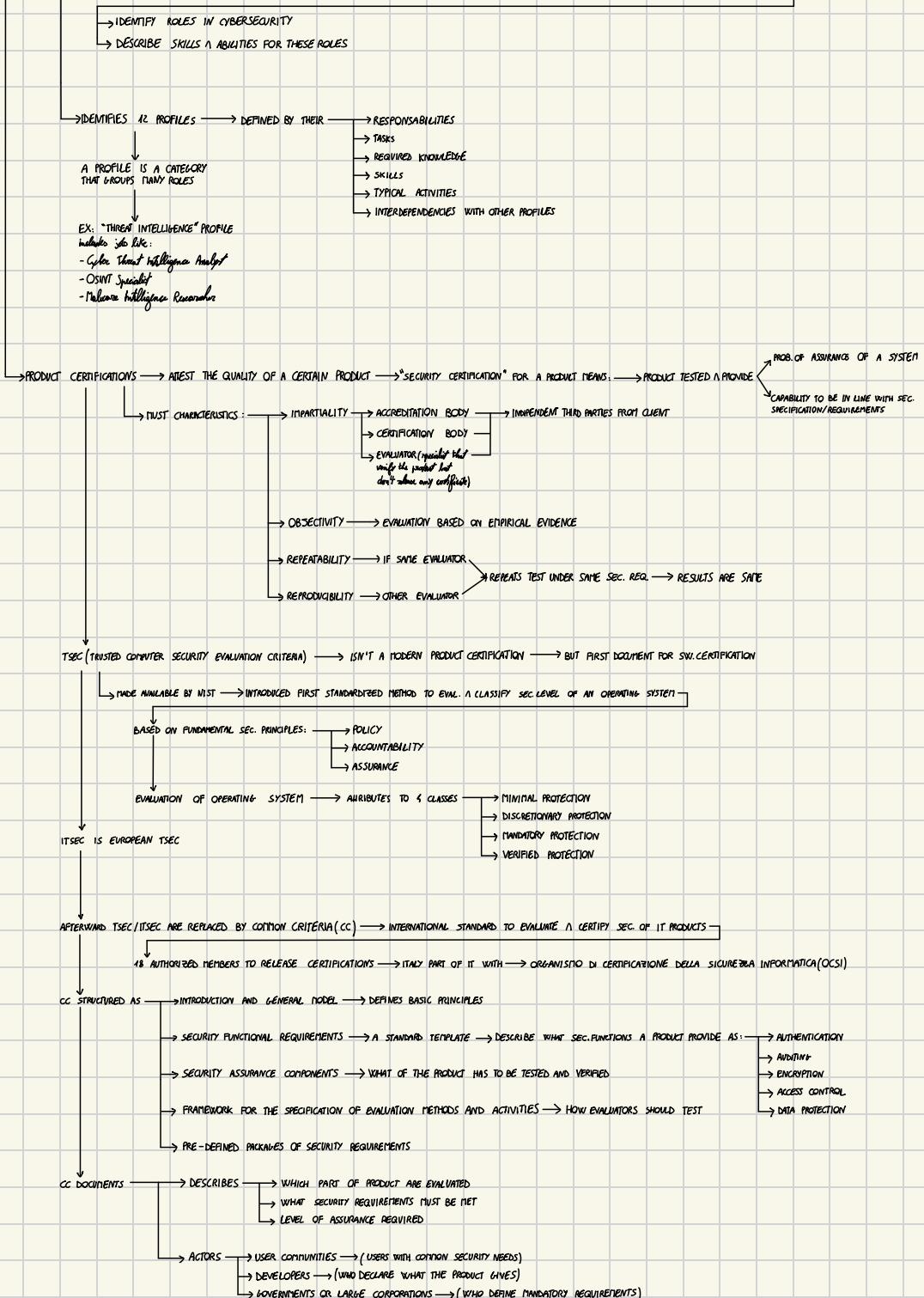




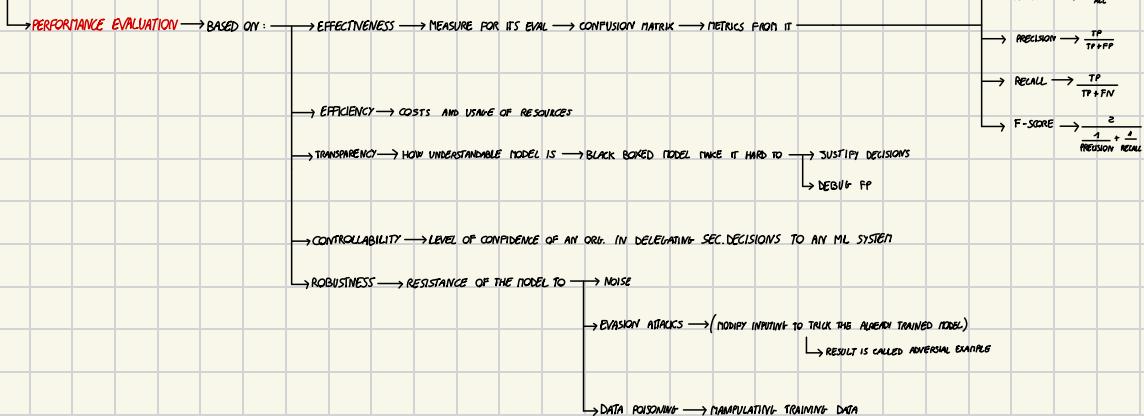
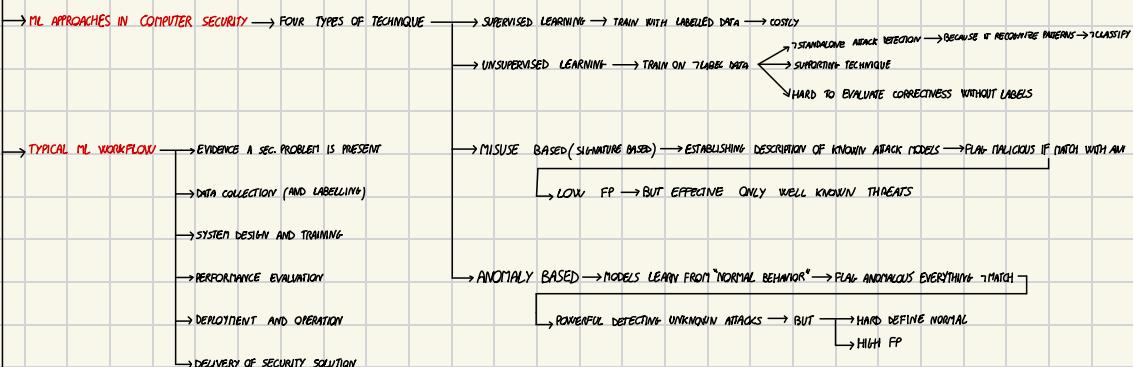
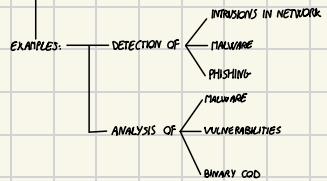
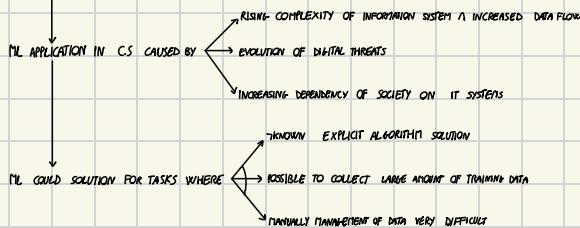
## CERTIFICATIONS



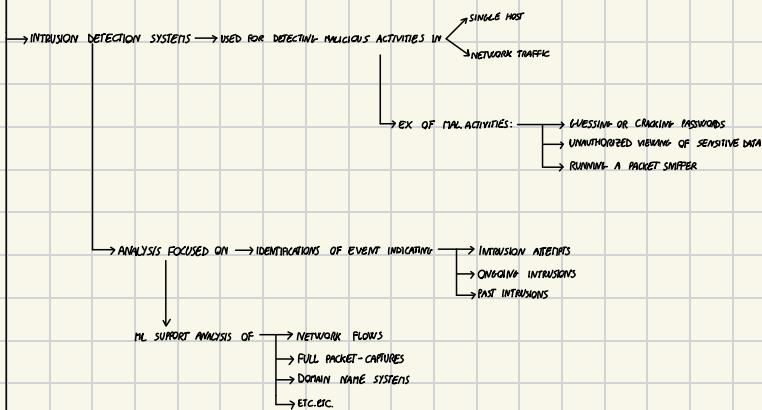
ECSF (EUROPEAN CYBERSECURITY SKILLS FRAMEWORK) → DOESN'T RELEASE CERTIFICATES → IT'S EUROPEAN STANDARD THAT HELPS TO



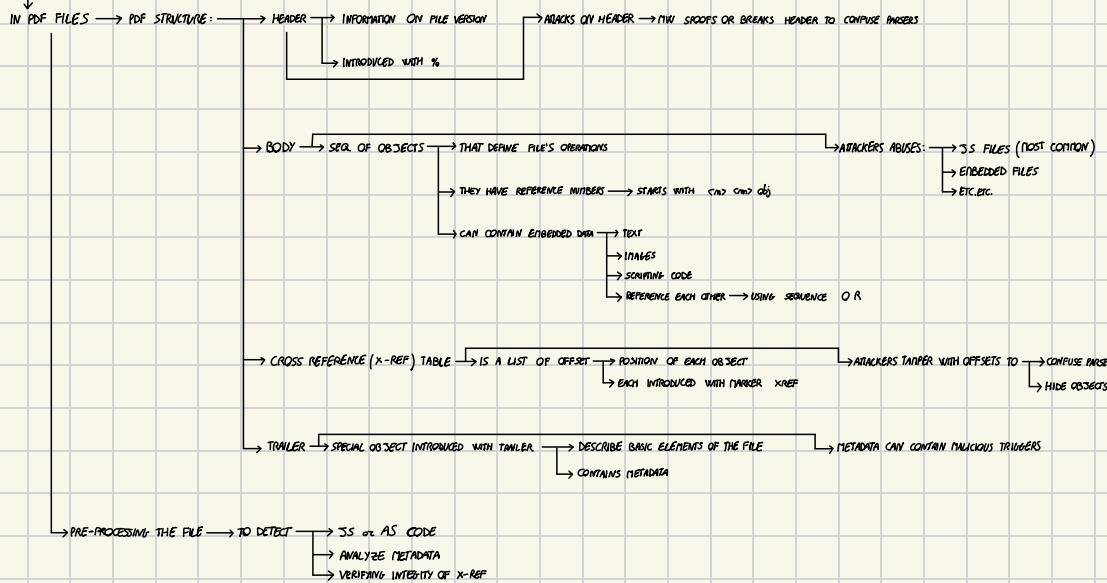
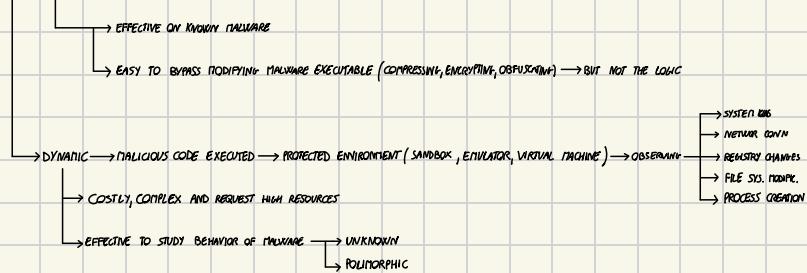
# MACHINE LEARNING FOR COMPUTER SECURITY

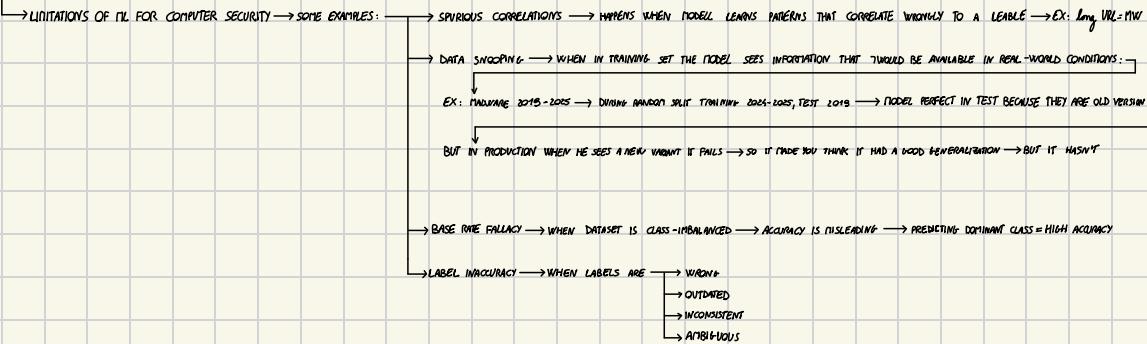


SPAM E-MAIL DETECTION/PHISHING: → LINEAR TEXT CLASSIFIER → WEIGH. OF WORDS → CUMULATIVE SCORE → IF EXCEED A UNIT → CLASSIFY SPAM → LEGITIMATE OTHERWISE

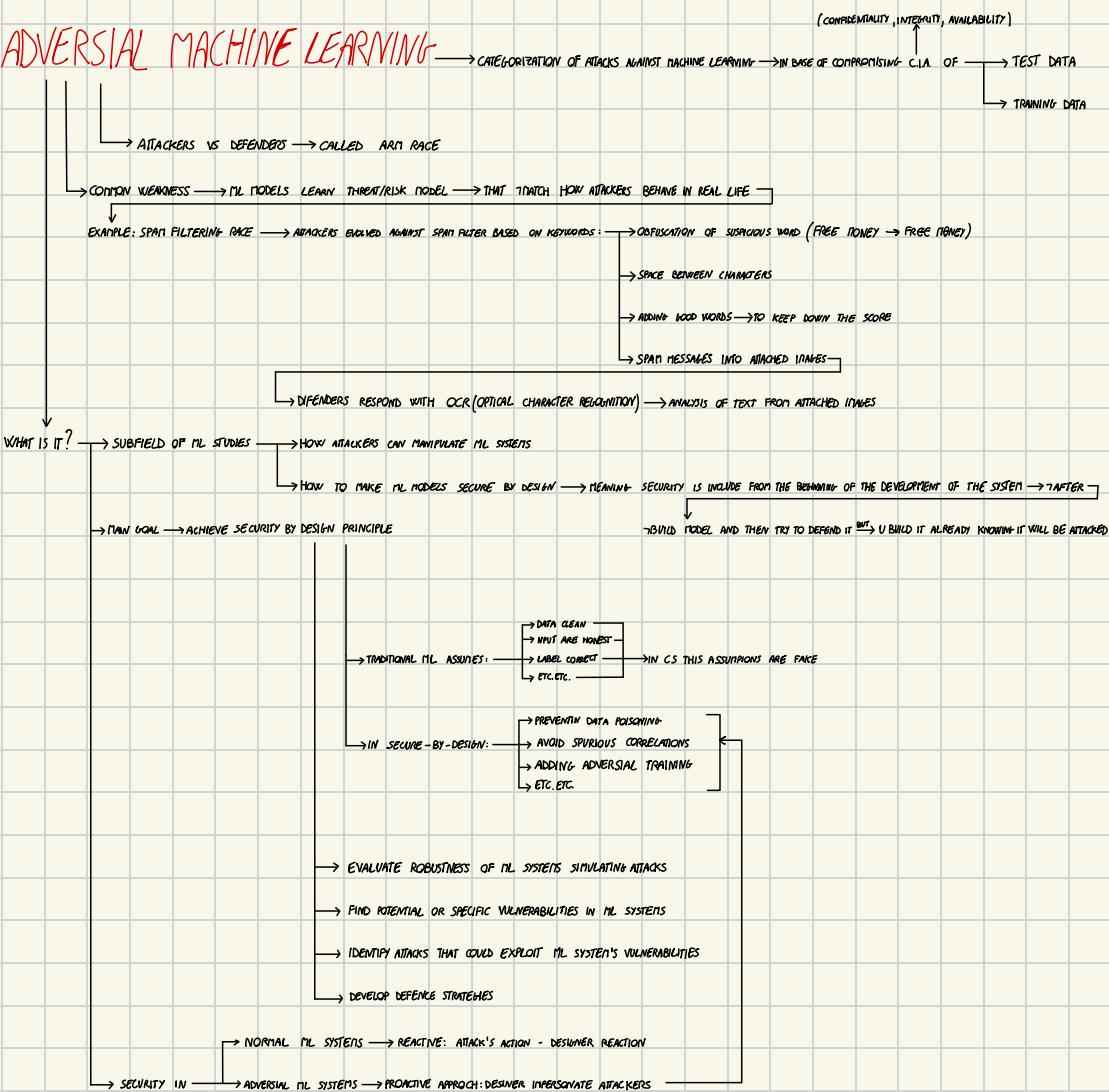


→ MALWARE DETECTION → TWO KIND OF ANALYSIS:





## ADVERSIAL MACHINE LEARNING



# 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 NAMES, NEWSLETTERS, WEBSITE'S ACCOUNTS

MAIN MOTIVATIONS FOR DATA RELEASE:

RESEARCH & STATISTIC PURPOSES, STUDY SOCIAL & POLITICAL TRENDS

PROVIDING SERVICES MORE EFFICIENTLY & EFFECTIVELY

PRIVACY PROTECTION

BECFORE DIGITAL ERA → PRIVACY IMPLICITLY GUARANTEED BECAUSE → INFORMATION ACES WAS LIMITED → DATA WAS STORED ON PAPER IN PHYSICAL PLACES

DATA PROCESSING WAS EXPENSIVE AND DIFFICULT

ONLY FEW PEOPLE HAD ACCESS

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 INDEFINITELY

SHARED ACROSS COMPANIES

SOLD TO THIRD PARTIES

USED FOR PROFILING

TECHNIQUES (DATA MINING AND ML) ALLOW POWERFUL ANALYSIS

DATA FROM DIFFERENT SOURCES THAT COULD NOT 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 INFORMATION

MACRODATA → AGGREGATE INF. THAT SUMS UP ABOUT GROUPS OF PEOPLE → 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

OBSCURATION OF SENSITIVE CELLS → MAIN PRIVACY TECHNIQUE FOR MACRODATA

SENSITIVE CELL → TOO FEW PEOPLE CONTRIBUTE TO IT → SO IT'S EASY TO IDENTIFY SOMEONE

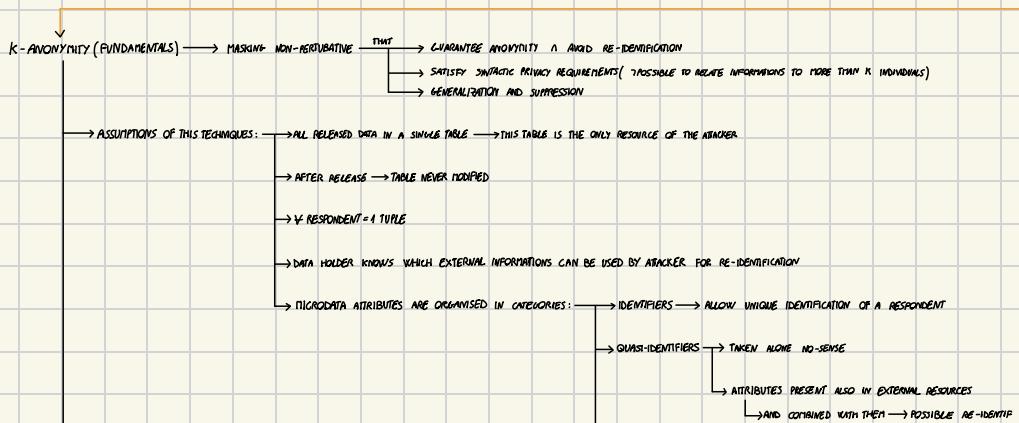
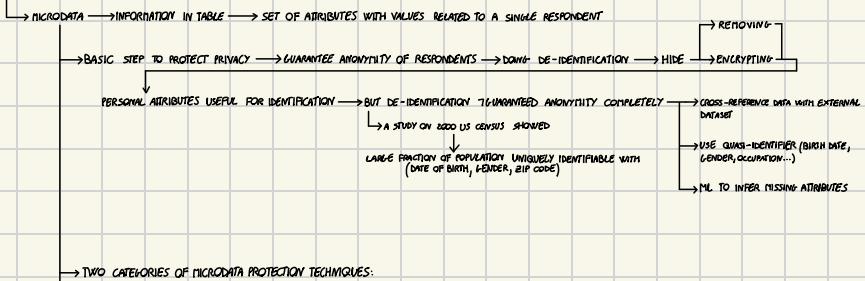
THE VALUE REVEALS TOO MUCH ABOUT A SPECIFIC SUBGROUP

DONE BY:

CELL SUPPRESSION → REMOVE OR BLANK OUT SENSITIVE CELLS

ROUNDING → ROUND VALUES UP/DOWN TO HIDE EXACT CONTRIBUTIONS

(m, k) RULE → A CELL IS SENSITIVE IF RESPONDENTS m CONTRIBUTE TO AT LEAST k% OF TOTAL



→ CONFIDENTIAL ATTRIBUTES → SENSITIVE INFORMATION  
 → CONFIDENTIAL ATTRIBUTES → SENSITIVE INFORMATION

K-ANONYMITY REQUIREMENTS → RELEASED INF. POSSIBLE RELATE TO LESS THAN K  
 → SAME COMBINATION OF QUASI-IDENTIFIER NOT APPEARS IN K DIFFERENT INDIVIDUALS → IN ORDER TO MAINTAIN THE REAL NATURE  
 → mattona caso che allora se il dataset di 10 righe, per ogni riga ci sono m ggrppi di righe uguali: ma i QUASI-IDENTIFIERS non stanno allora  
 due gruppi da 1 e uno da due. Se in quello K=3, il primo è il secondo gruppo resteranno le combinazioni univoci <math>2K</math>, ma il secondo  
 gruppo <math>2+1 = 3</math> righe → 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

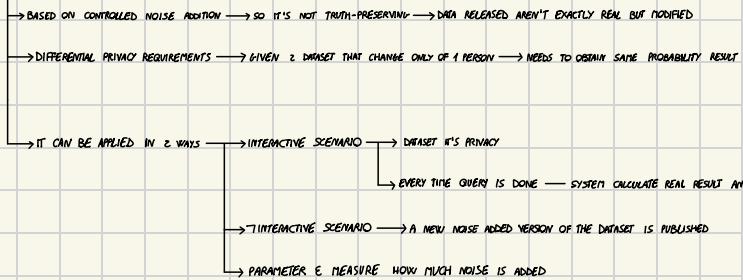
↓  
 ATTRIBUTE DISCLOSURE PROTECTION → K-ANONYMITY PROTECT IDENTITY OF RESPONDENTS → T(DISCLOSURE OF SENSITIVE INFORMATION)  
 → TWO ATTACKS CAN HAPPEN EVEN IF TABLE IS K-ANONYMOUS

HOMOGENEITY ATTACK → IF ALL ROWS WITH A COMBINATION OF ATTRIBUTES (QUASI-IDENTIFIER CLASS) HAVE SAME VALUE FOR SENSITIVE ATTRIBUTE
K-ANONYMITY IRELEVANT → EXAMPLE: even if we have K rows with same combination values, AGE-CAP-SEX-DISEASE, and DISEASE is sensitive, it doesn't matter if identity is protected if it doesn't matter because if anyone 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 SENSITIVE ATTRIBUTE → IS POSSIBLE TO REDUCE UNCERTAINTY
EXAMPLE: name, AGE-CAP-SEX-DISEASE but only one or two have the file instead of HIV and the attacker knows the victim hasn't been recorded in hospital, so attacker can say my victim is one of the two people with the file
THIS ATTACKS ASSUME ATTACKER KNOWS COMBINATION OF ATTRIBUTES THAT FORMS THE Q.I. CLASS AND ONLY ONE SENSITIVE ATTRIBUTE
I-DIVERSITY IS INTRODUCED TO SOLVE THIS PROBLEM → FOR EACH Q.I. CLASS NEEDS TO CONTAIN A NUMBER I OF DIFFERENT VALUES OF THE SENSITIVE ATTRIBUTE
K-ANONYMITY & I-DIVERSE TABLE STILL VULNERABLE TO ATTACKS THAT LEAD TO SENSITIVE ATTRIBUTE DISCLOSURE:
SKEWNESS (ASIMMETRIA) 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, another attacker disease where 3 different have disease, so even if it's not possible identify the real one, attacker knows for more a short disease
TO REDUCE EFFECTIVENESS 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

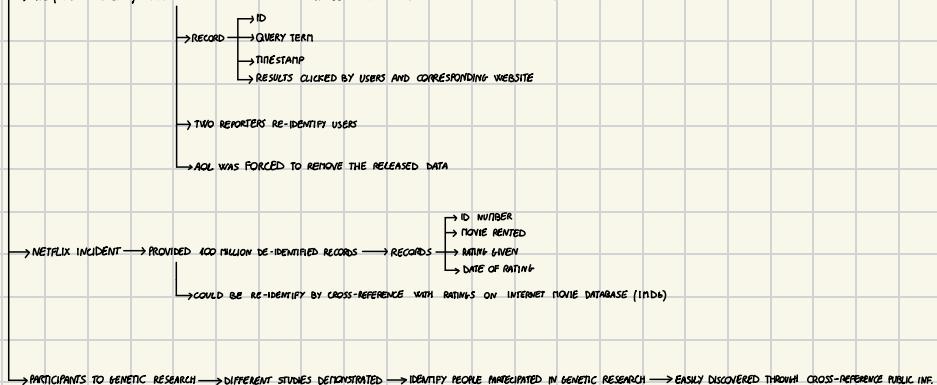
APPLICATION SCENARIOS → FOR K-ANONYMITY

- 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-ANONYMITY REQUIREMENTS CAN BE CUSTOMIZED

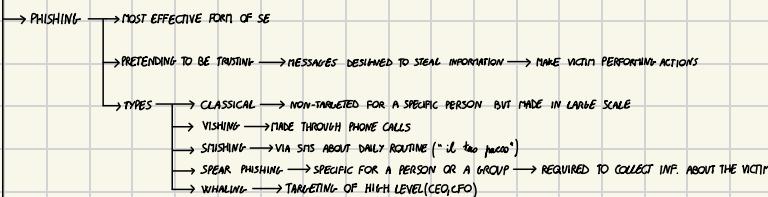
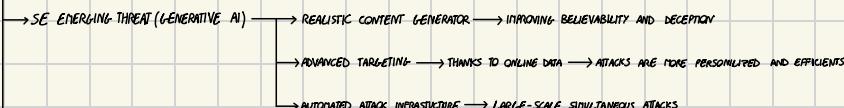
SEMANTIC APPROACHES → DIFFERENTIAL PRIVACY IS A TECHNIQUE → THAT AIMS TO PROTECT PRIVACY OF BOTH RESPONDENTS AND NON-RESPONDENTS → RESULTS OF ANALYSIS LET UNDERSTAND WHETHER U IN/OUT

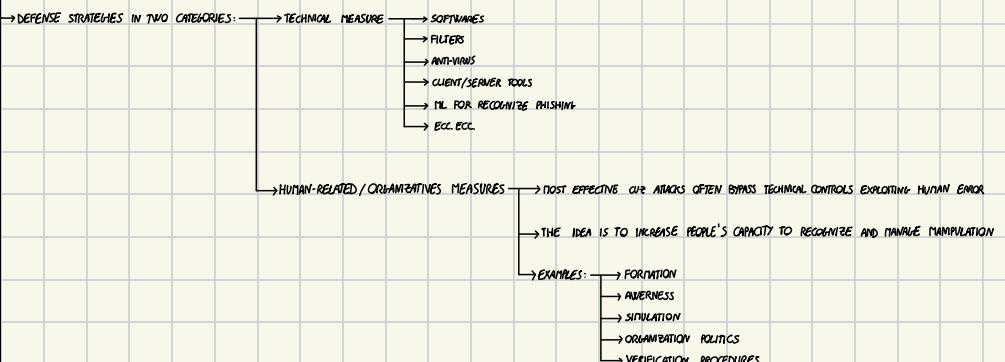
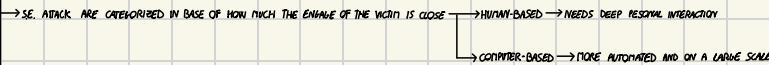
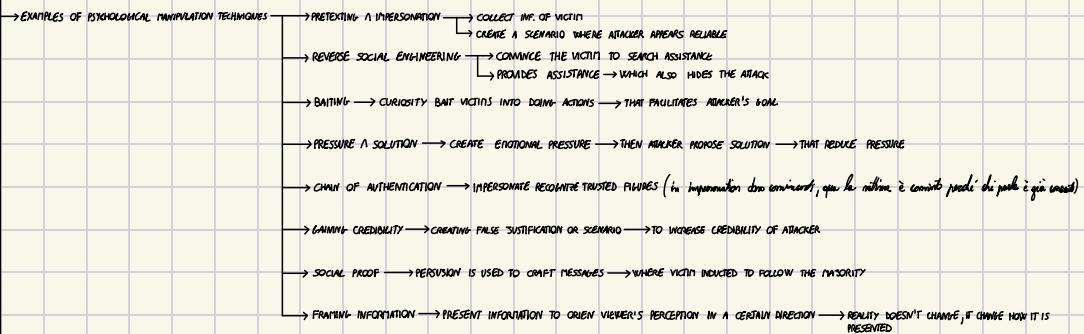
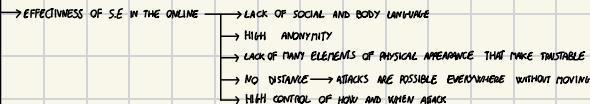
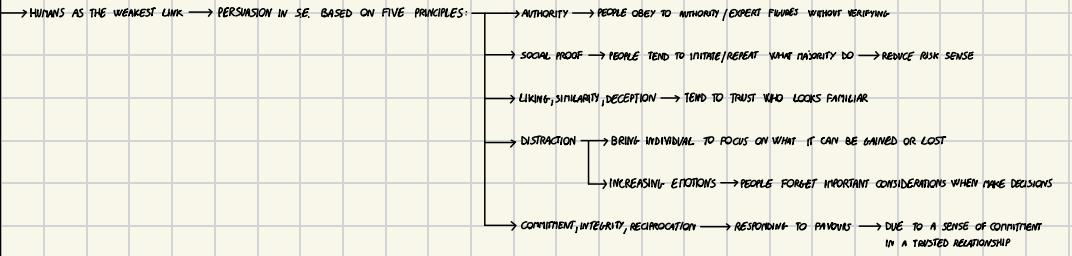


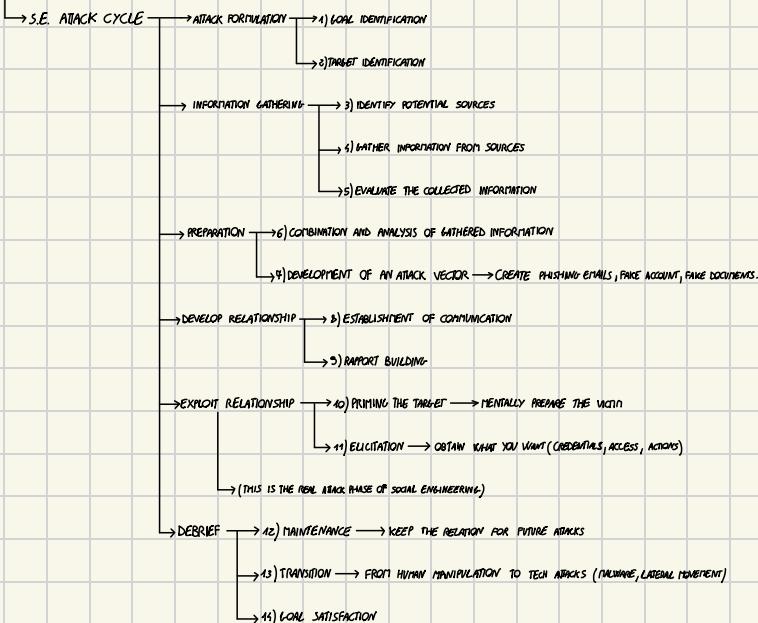
EXAMPLE OF PRIVACY VIOLATIONS:



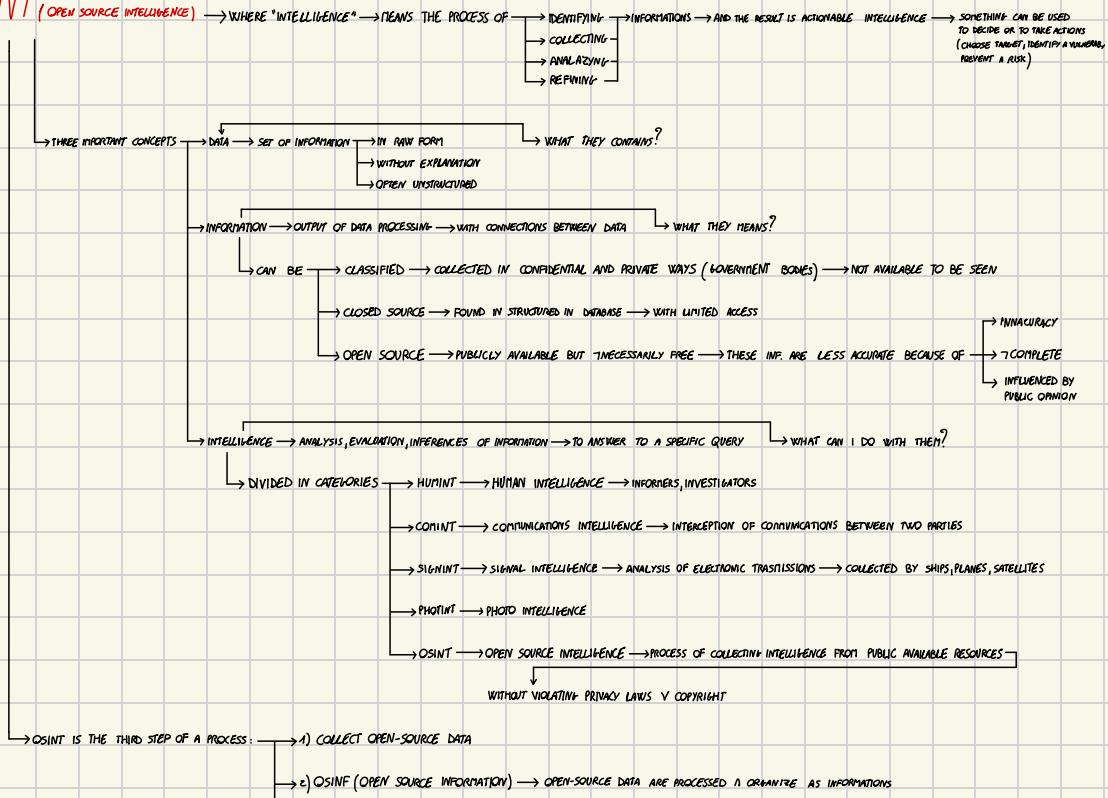
## SOCIAL ENGINEERING (SE)







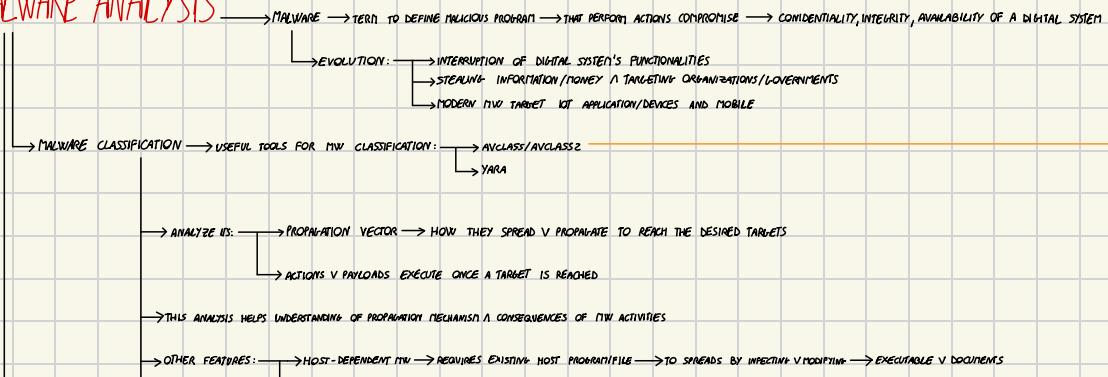
## OSINT (OPEN SOURCE INTELLIGENCE)

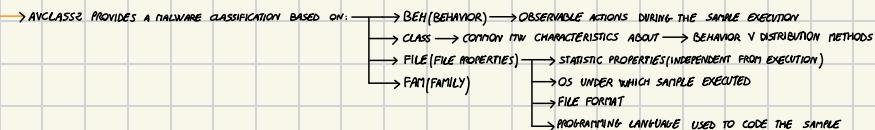
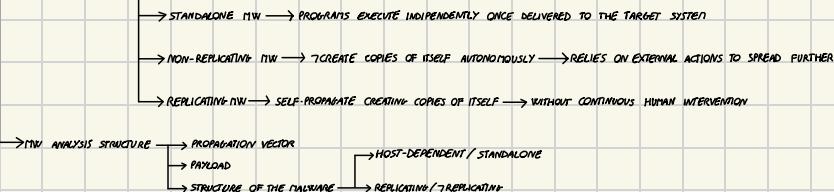


→ 3) OSINT → INTELLIGENCE DERIVED FROM OSINT → AS A RESULT OF EXPERT ANALYSIS

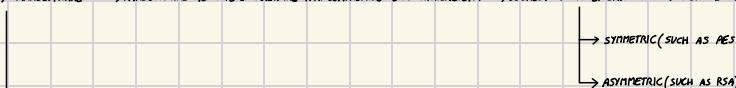


## MALWARE ANALYSIS

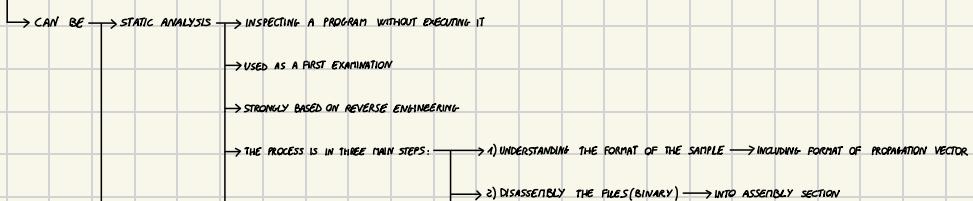
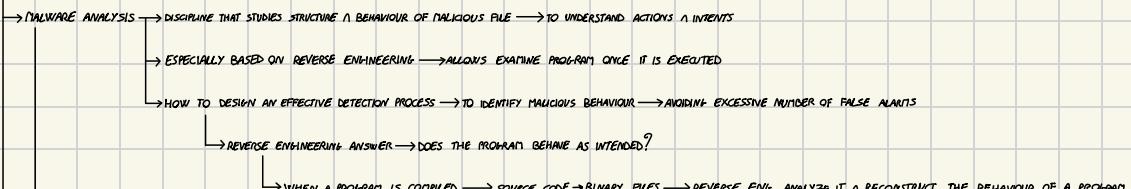
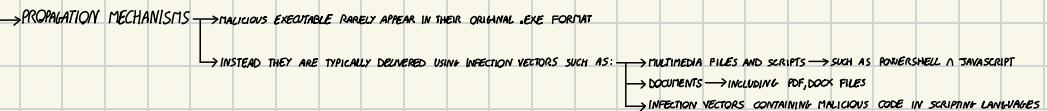




→ WANNACRY RANSOMWARE → RANSOMWARE IS A TYPE OF MULWARE THAT COMPROMISE DATA AVAILABILITY → USUALLY WITH ENCRYPTION → THEN ASK MONEY TO RESTORE THEM



- EVEN THOUGH MICROSOFT RELEASED A PATCH 2 MONTHS BEFORE WANNACRY HAPPENED → MANY USERS DIDN'T UPDATE → INFECTED 230K COMPUTERS IN 150 COUNTRIES
- CAUSED \$8 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



→ 3) DECOMPILE → TO OBTAIN AN EQUIVALENT REPRESENTATION OF THE ORIGINAL SOURCE CODE (HIGH LEVEL)

→ BY INTERPRETING ASSEMBLY INSTRUCTIONS

→ EXAMPLE: → PORTABLE EXECUTABLE (PE) FILES → .EXE V. DLL 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, .RODATA) → EXPRESSED AS A SEQUENCE OF BYTES

→ THESE BYTES CORRESPOND TO ASSEMBLY INSTRUCTIONS → THAT NEEDS DISASSEMBLED  
A THEN COMPILED

→ TYPES OF DISASSEMBLER: → LINEAR SWEEP DISASSEMBLER → DISASSEMBLE INSTRUCTIONS SEQUENTIALLY STARTING FROM A GIVEN ENTRY POINT (NO JUMP OR CALL)  
*(data X line)*

→ RECURSIVE TRAVERSAL DISASSEMBLER → DISASSEMBLE INSTRUCTIONS BY FOLLOWING SEMANTICS →

→ SUCH AS JUMPS AND BRANCHES → (function *func1* → 1-2-3-4-5-6-7-8-9-10-11)

→ DISASSEMBLERS: BINARY FILES → ASSEMBLY

→ DECOMPILE: ASSEMBLY/BINARY → SOURCE CODE (HIGH LEVEL CODE)

→ DISASSEMBLERS & DECOMPILE → CAN BE ELUDED WITH ANTI-REVERSE ENGINEERING TECHNIQUES → THAT CAUSE → INCREASE EFFORTS OF HUMAN DURING ANALYSIS

→ EXAMPLE: → PACKING → COMPRESSING & ENCODING INFORMATION

→ INFLATE → DECODE TOOLS → INCORRECT OUTPUTS

→ SO IT'S NOT STATISTICALLY VISIBLE

→ SO → ANALYZE WITHOUT EXECUTING THE PROGRAM

→ SEE REAL CODE OF THE MACHINE

→ U CAN SEE INSTRUCTIONS 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 ANTI-REVERSE ENG. TECH.

→ ONLINE SANDBOXES

→ IT IS DONE IN CONTROLLED ENVIRONMENTS → VIRTUALIZED ENVIRONMENTS

→ DEBUGGERS MONITOR PROGRAM EXECUTION AT → SOURCE LEVEL & ASSEMBLY LEVEL

→ MALWARE MIGHT IMPLEMENT ANTI-DEBUGGING TECHNIQUES → SINCE DEBUGGING REQUIRES ATTACHING A DEBUGGER TO A PROCESS

→ MALWARE PROGRAMS DETECT PRESENCE OF A DEBUGGER → AND ALTER THEIR BEHAVIOUR

*(most often used in malware analysis to mitigate or even exploit an infection strategy)*

→ 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

*(most often used in malware analysis to mitigate or even exploit an infection strategy)*

→ ADVANCED ANALYSIS TECHNIQUES

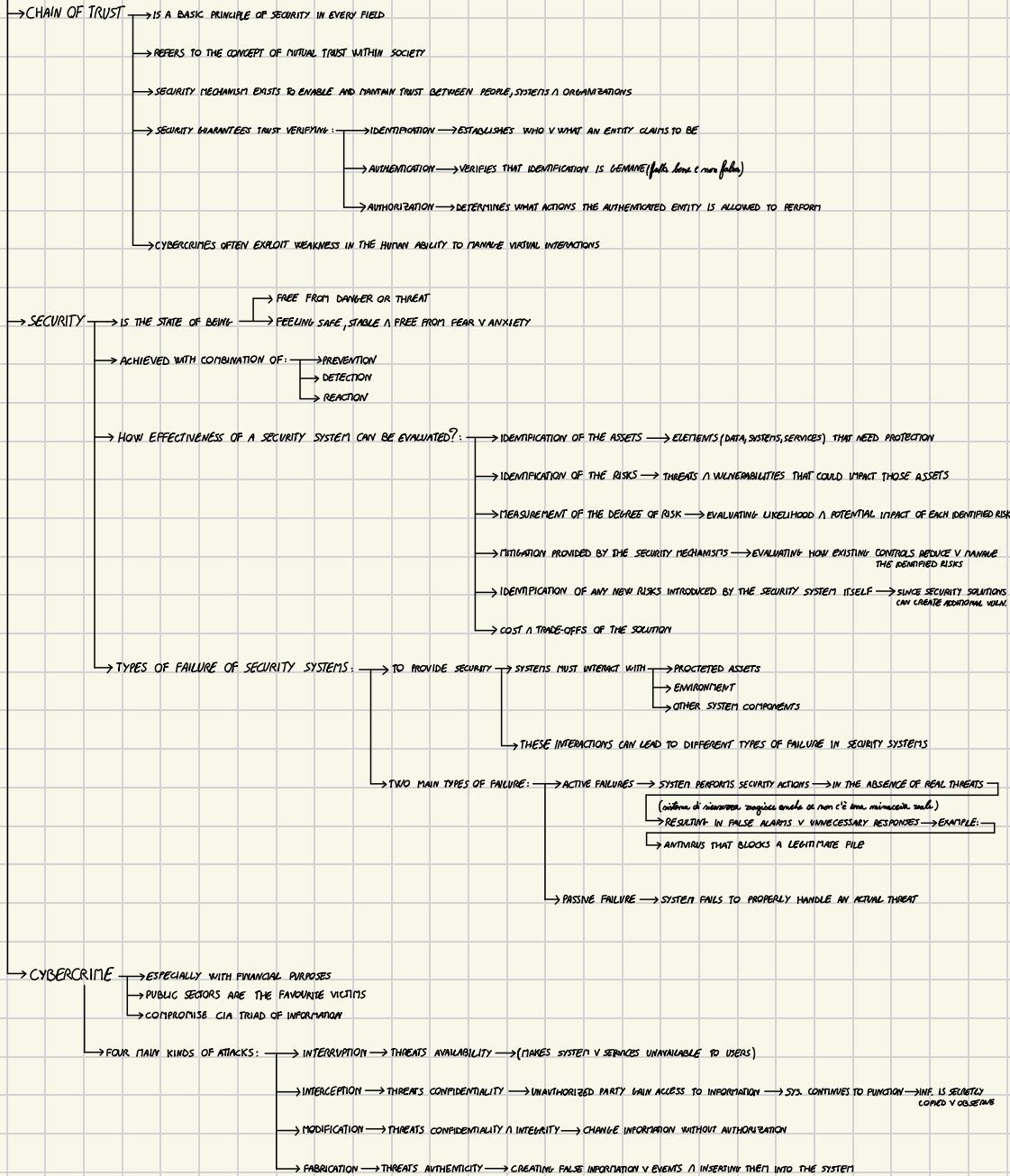
→ STATIC INSTRUMENTATION → APPLIED ON INJECTION VECTORS → SUCH AS COOLLOW → ANALYZE A NOOPY CODE WITHOUT EXECUTING IT

→ DYNAMIC INSTRUMENTATION → MONITORING DURING PROGRAM EXECUTION

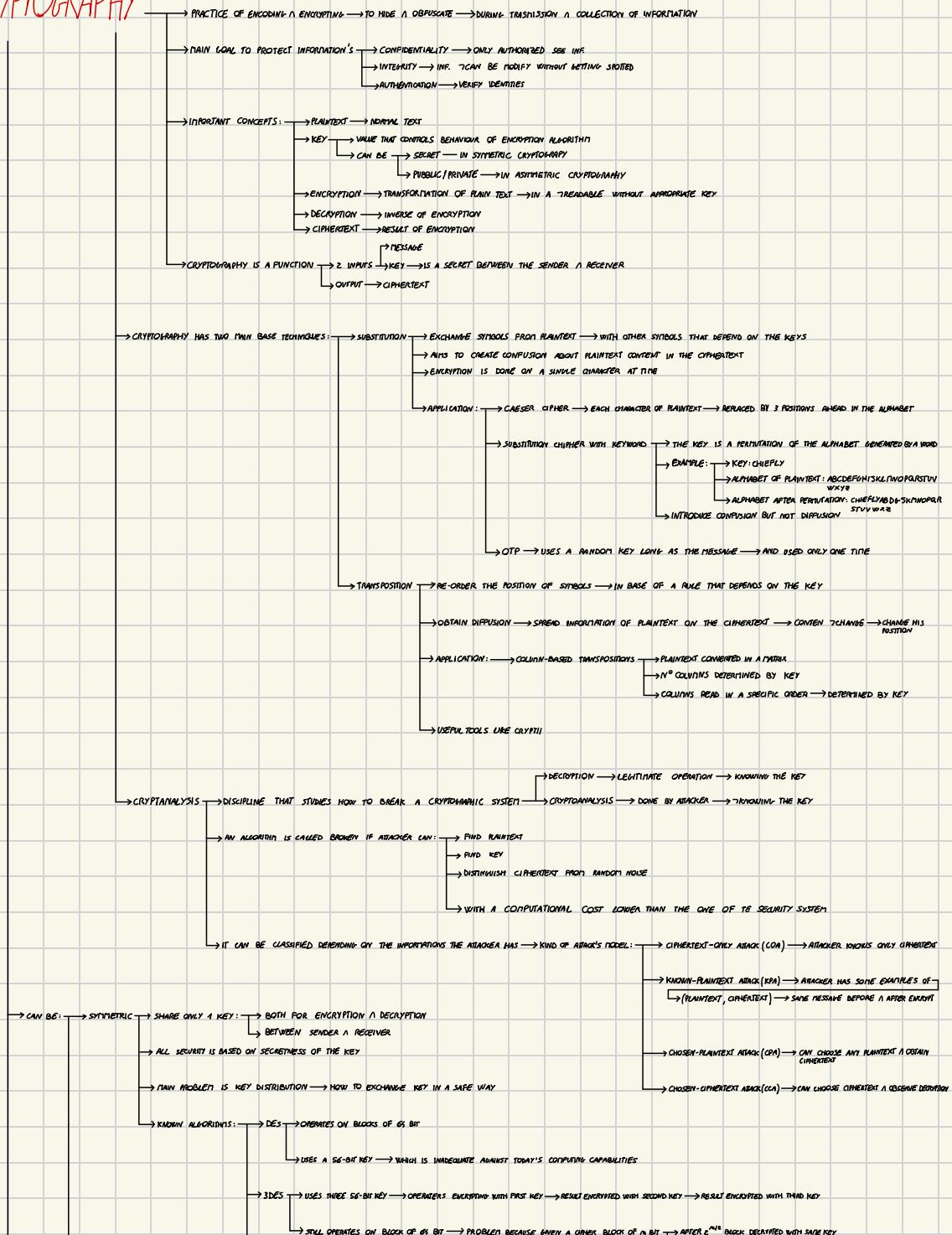
→ SYMBOLIC EXECUTION → TREAT INPUTS AS SYMBOLIC VALUES → TO EXPLORE DIFFERENT EXECUTION PATHS → WITHOUT TESTING ALL POSSIBLE INPUTS EXPLICITY

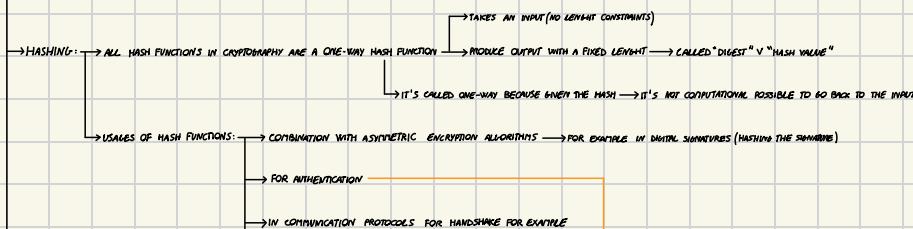
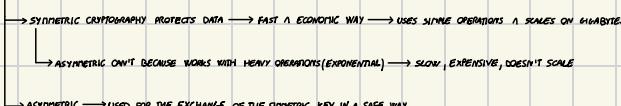
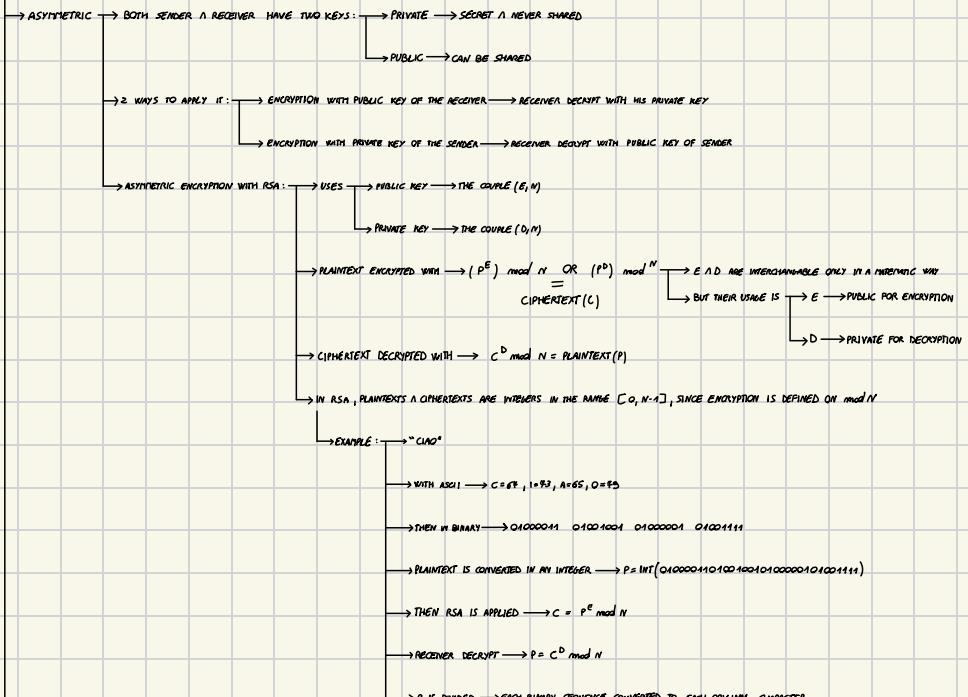
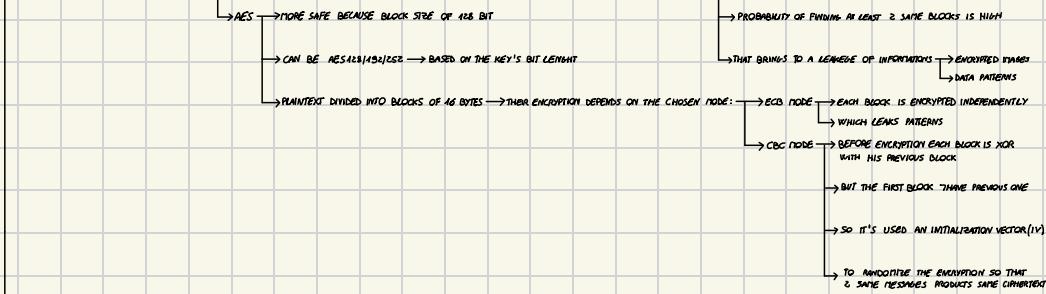
→ EMULATION → REPLICATING SPECIFIC HW/V SW ENVIRONMENTS ON DIFFERENT PLATFORMS → THAT IMITATES THE ORIGINAL TARGET SYSTEM → *(taking it possible to analyse malwares behaviour without running it directly on real hardware)*

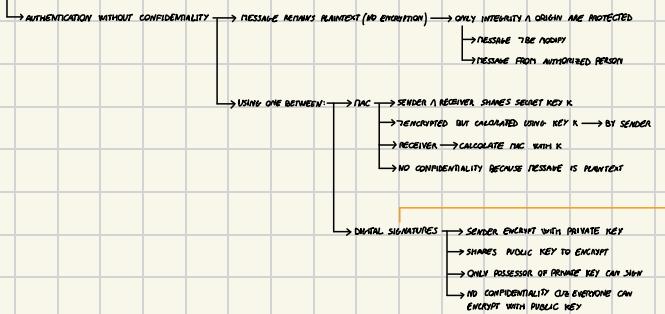
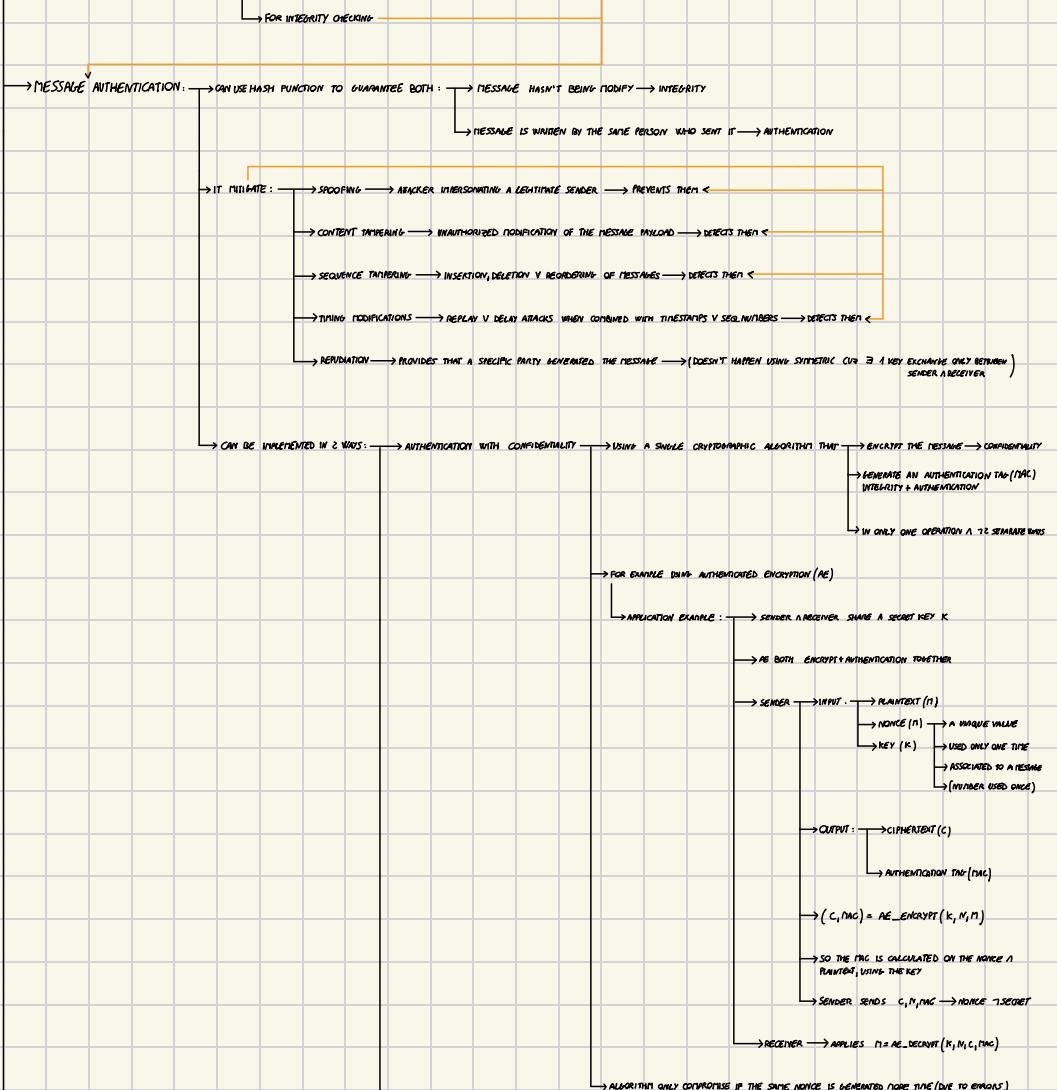
# SECURITY AND CYBERSECURITY



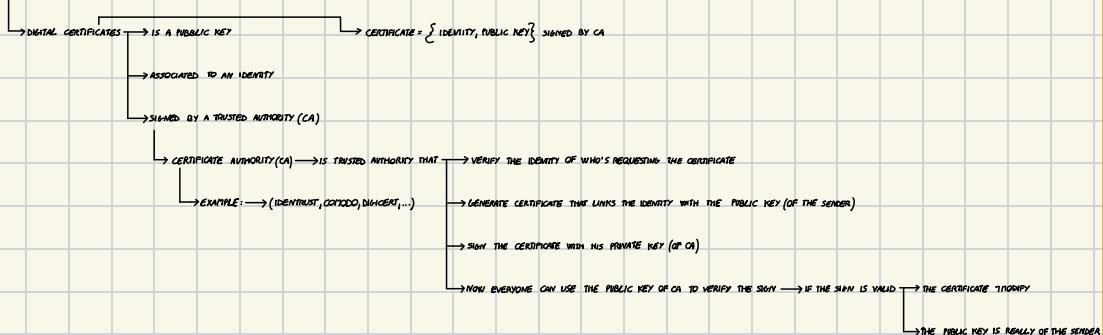
# CRYPTOGRAPHY







→ WHEN YOU RECEIVE A PUBLIC KEY? → WHO IS IT? HOW DO YOU KNOW IT'S NOT OF AN ATTACKER?



→ RANDOM NUMBER ARE ESSENTIALS FOR SAFETY BECAUSE THEY ARE USED FOR:



→ 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 SINCE THEY ARE PREDICTABLE  
UNPREDICTABILITY → EACH NUMBER IS STATISTICALLY INDEPENDENT → IT'S A SECURITY PROPERTY → PREDICTABLE BY AN ATTACKER

→ HOWEVER ALGORITHMS ARE DETERMINISTIC:



→ 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 (TRNGs) → USED FOR GENERATE TRULY RANDOM NUMBER

→ RELY ON PROCESSES THAT FOLLOW PHYSICAL RULES → SUCH AS RADIATIVE DECAY, THERMAL NOISE, ... → THESE PHENOMENA ARE:  
DETERMINISTIC  
INREPRODUCIBLE  
PREDICTABLE

→ PROPERTIES OF DIGITAL SIGNATURE: (Definition)  
UNFORGEABLE → INTEGRITY PROPERTY → MUST ASSURE THAT NO ONE OTHER THAN THE SIGNER CAN PRODUCE THE SIGNATURE WITHOUT THE SIGNER'S PRIVATE KEY

→ AUTHENTIC → IDENTITY PROPERTY → MUST ASSURE THE RECEIVER CAN VERIFY THAT SIGNATURE REALLY WAS FROM THE SIGNER

→ NOT ALTERABLE → DISDISPENSABLE PROPERTY → NO ONE (INCLUDING SIGNER & RECEIVER) CAN MODIFY THE SIGNATURE WITHOUT THE TAMPERING BEING EVIDENT → PROTECTS INTEGRITY

→ NOT REUSABLE → DISDISPENSABLE 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 COMES FROM SOMEONE

→ DIGITAL CERTIFICATE → SIGNED BY CA → ON A PUBLIC KEY → GUARANTEE THAT A PUBLIC KEY BELONGS TO SOMEONE

→ PROCESS:

→ DOCUMENT IS SIGNED WITH AN HASH

→ THIS HASH IS SIGNED WITH SENDER'S PRIVATE KEY

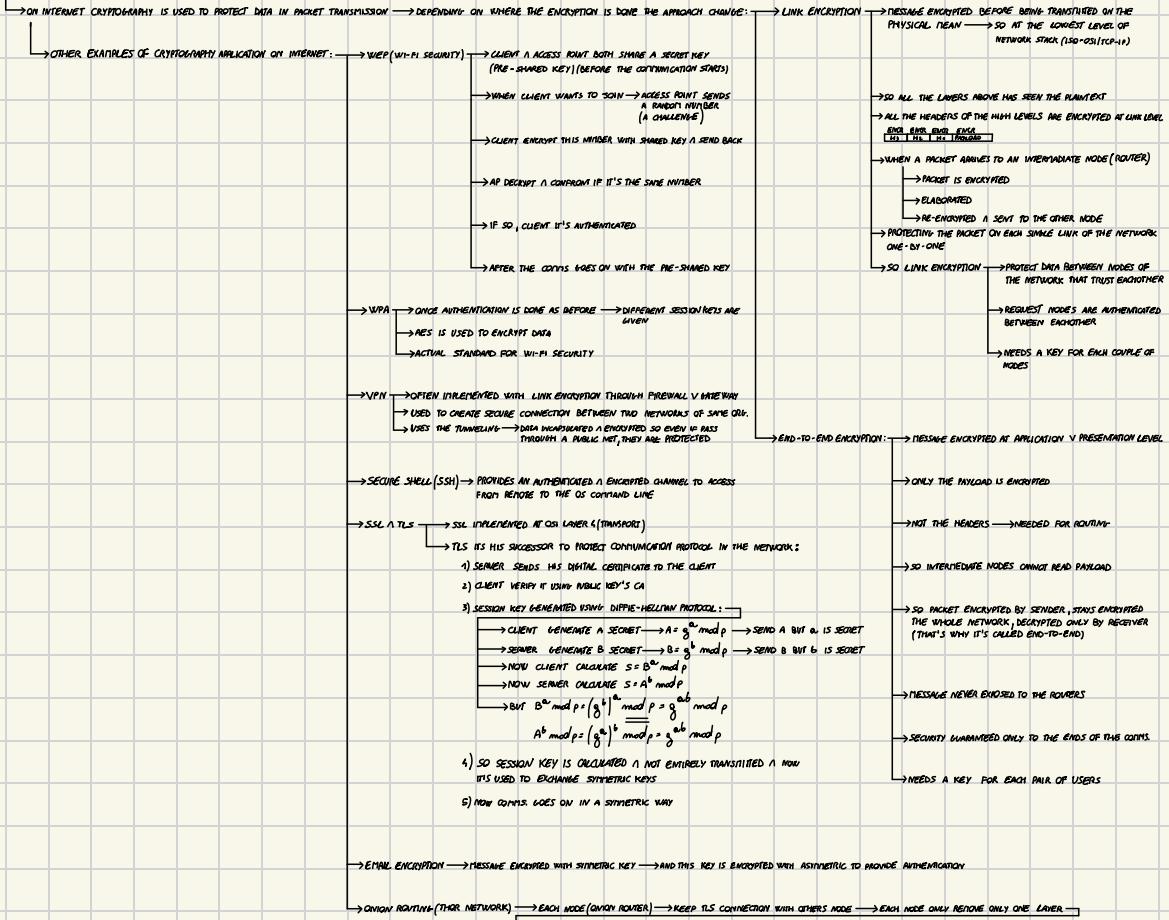
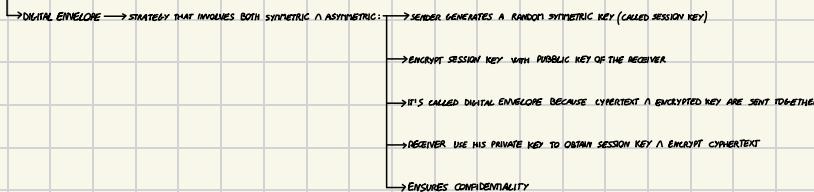
→ ATTACHED AT THE DOCUMENT. THE DIGITAL CERTIFICATE (FOR THE PUBLIC KEY)

→ THEN VERIFY THE PUBLIC KEY IN THE CERTIFICATE (WITH THE PUBLIC KEY OF CA)

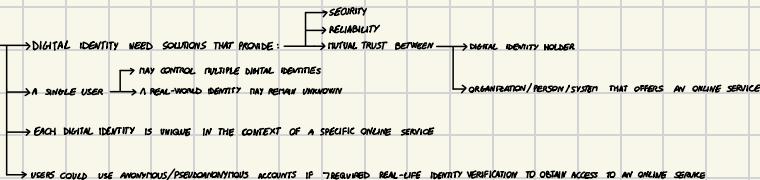
→ VERIFY THE HASH WITH THE PUBLIC KEY

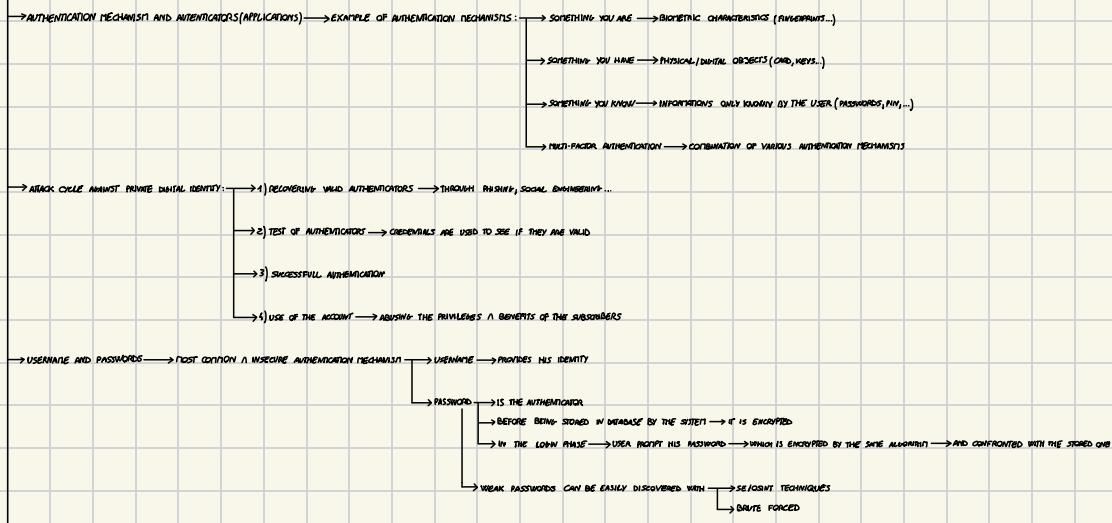
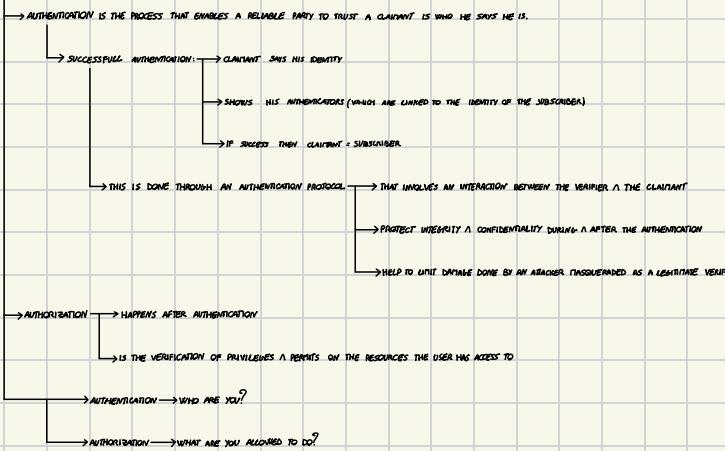
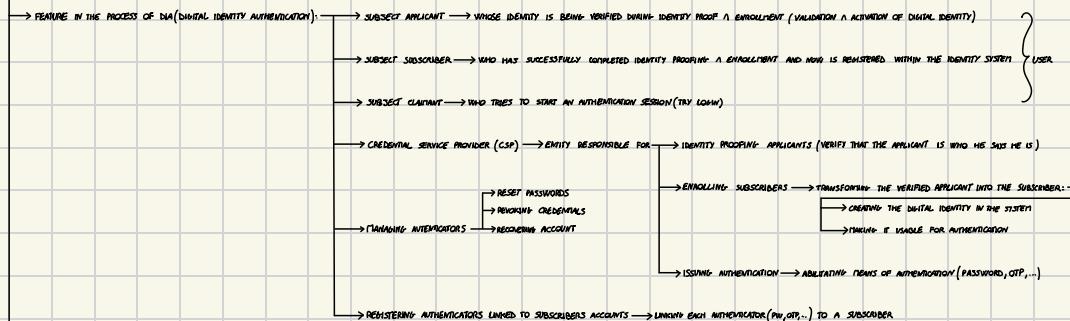
→ THE RECEIVER CALCULATE THE HASH (HASH FUNCTIONS ARE PUBLIC) → TO VERIFY DOCUMENT MODIFIED

→ DIGITAL SIGNATURES GUARANTEE AUTHENTICITY OF SIGNER & INTEGRITY OF DATA



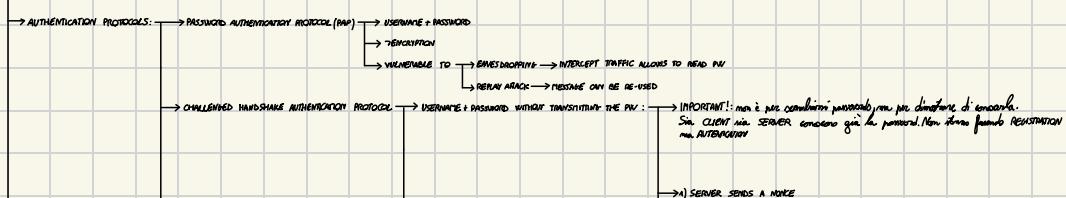
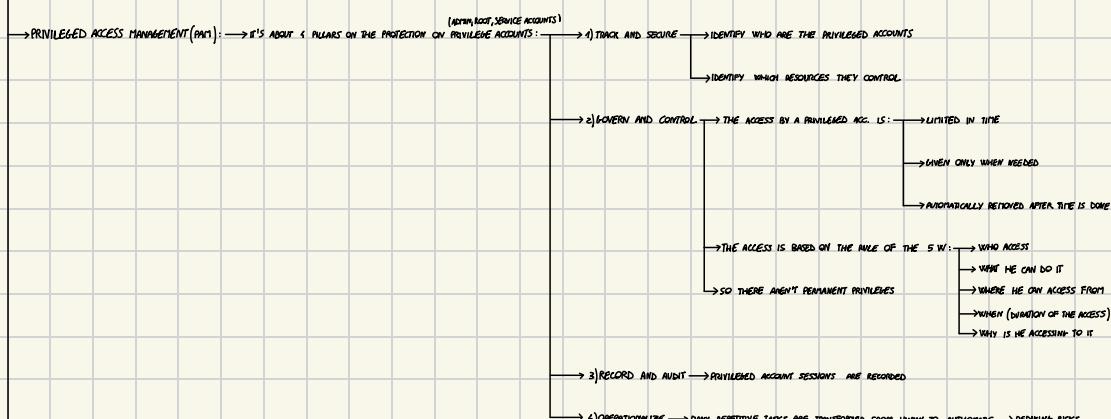
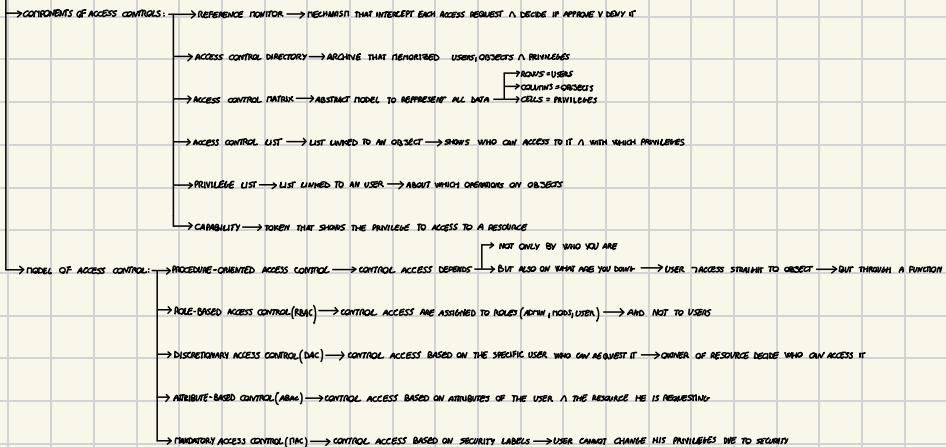
## AUTHENTICATION

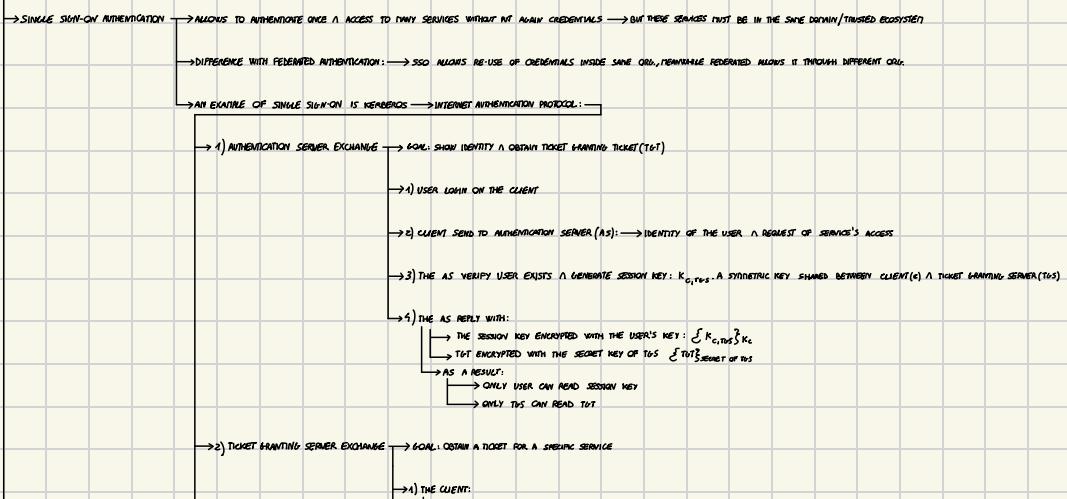
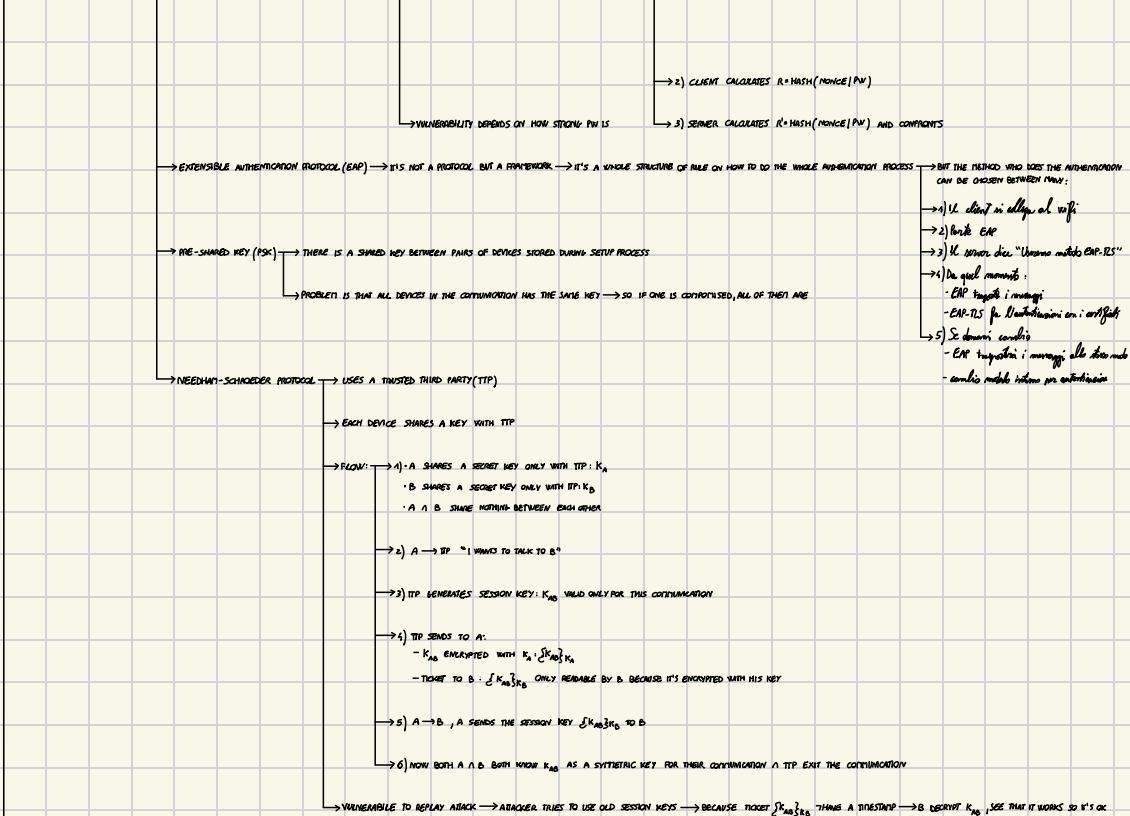


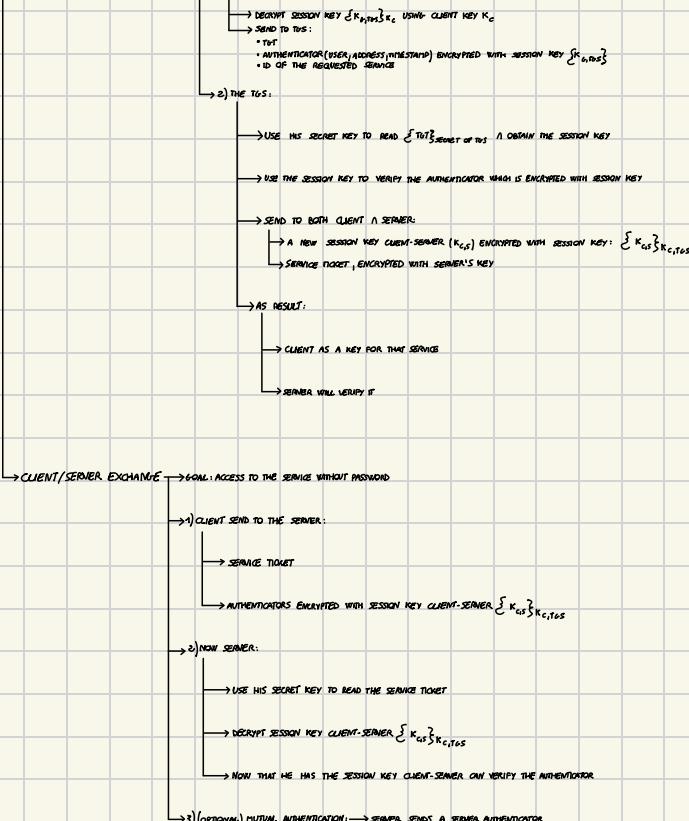


→ APPLY THE PRINCIPLE OF "LEAST PRIVILEGE" → EACH USER HAS ONLY THE ESSENTIALS

→ VERIFY THE USAGE OF THE RESOURCES → USE THE RESOURCE IS ACCORDINGLY IN THE WAY EXPECTED BY THE POLICY







→ 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 API)

→ FAST IDENTITY ONLINE (FIDO) → IS AN OPEN INDUSTRY ASSOCIATION THAT: → PROMOTES THE DEVELOPMENTS OF STANDARDS FOR AUTHENTICATION

→ IT IS ALSO A STANDARD → ELIMINATE & REDUCE THE USE OF PASSWORDS, DEVELOPING TECHNICAL SPECIFICATIONS

→ FIDO2 → IS A (PROTOCOL) INOPEN STANDARD FOR POWER-LESS AUTHENTICATION:

→ WHY IS IT MORE SECURE?

→ ANTI-PHISHING → A FALSE SITE MAY TRICK THE USER THAT INPUTS HIS PASSWORD  
BUT SINCE PRIVATE KEY IS UNIQUE FOR DEVICE/SERVICE/ACCOUNT  
THE DEVICE CAN SEE THAT THE DOMAIN OF FALSE SITE REGISTERED AS  
A FIDO SITE SUPPORTED A 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, TORMORISE SECURITY OF OTHERS

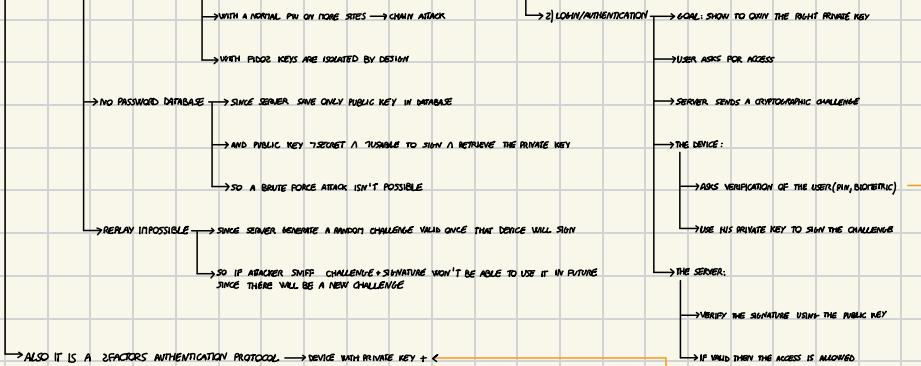
→ 1) REGISTRATION → GOAL: LINK A DEVICE TO MY ACCOUNT THAT WANTS TO USE A SERVICE

→ USER STARTS THE REGISTRATION TO A SERVICE THAT SUPPORTS FIDO PROTOCOL

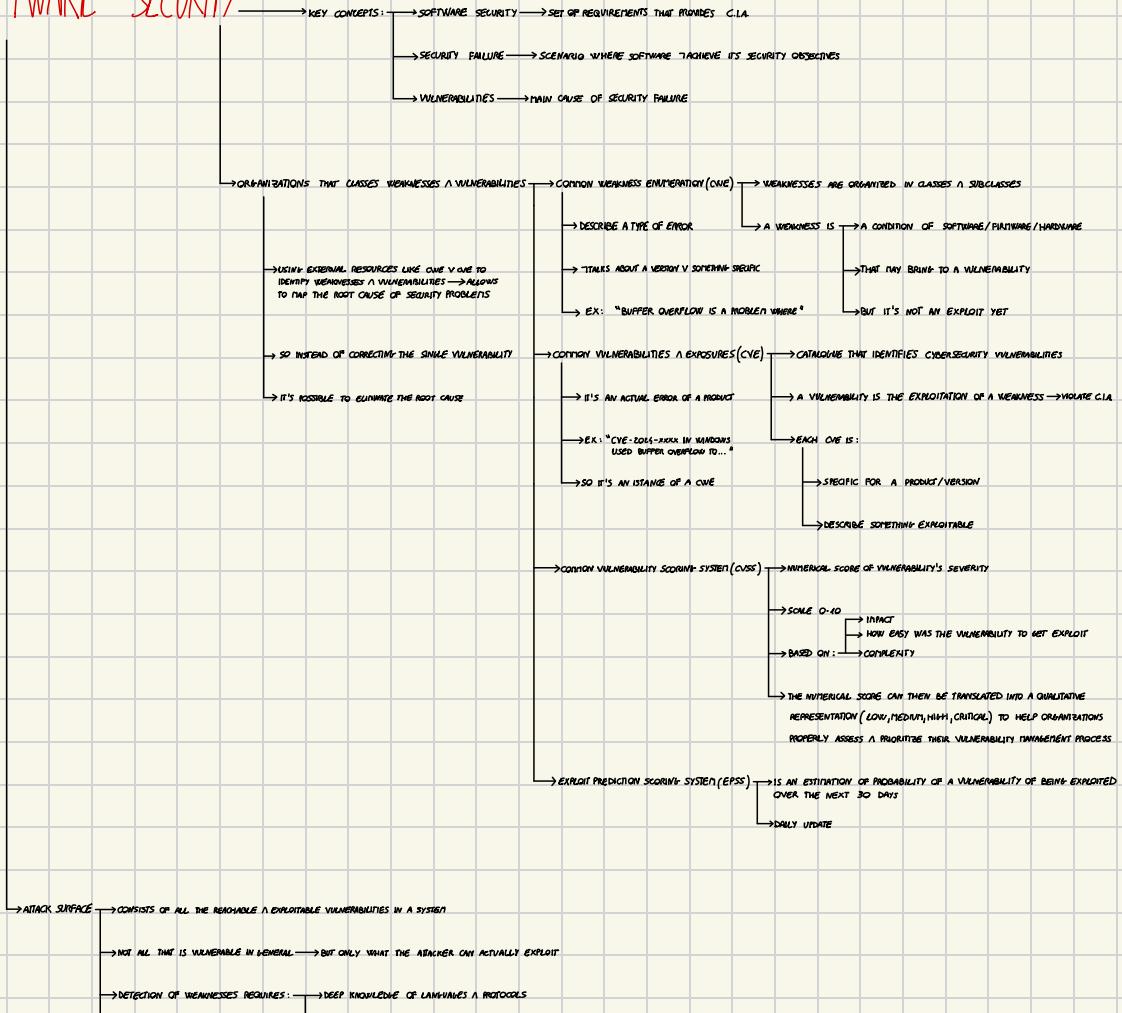
→ SERVER ASK THE DEVICE TO GENERATE:

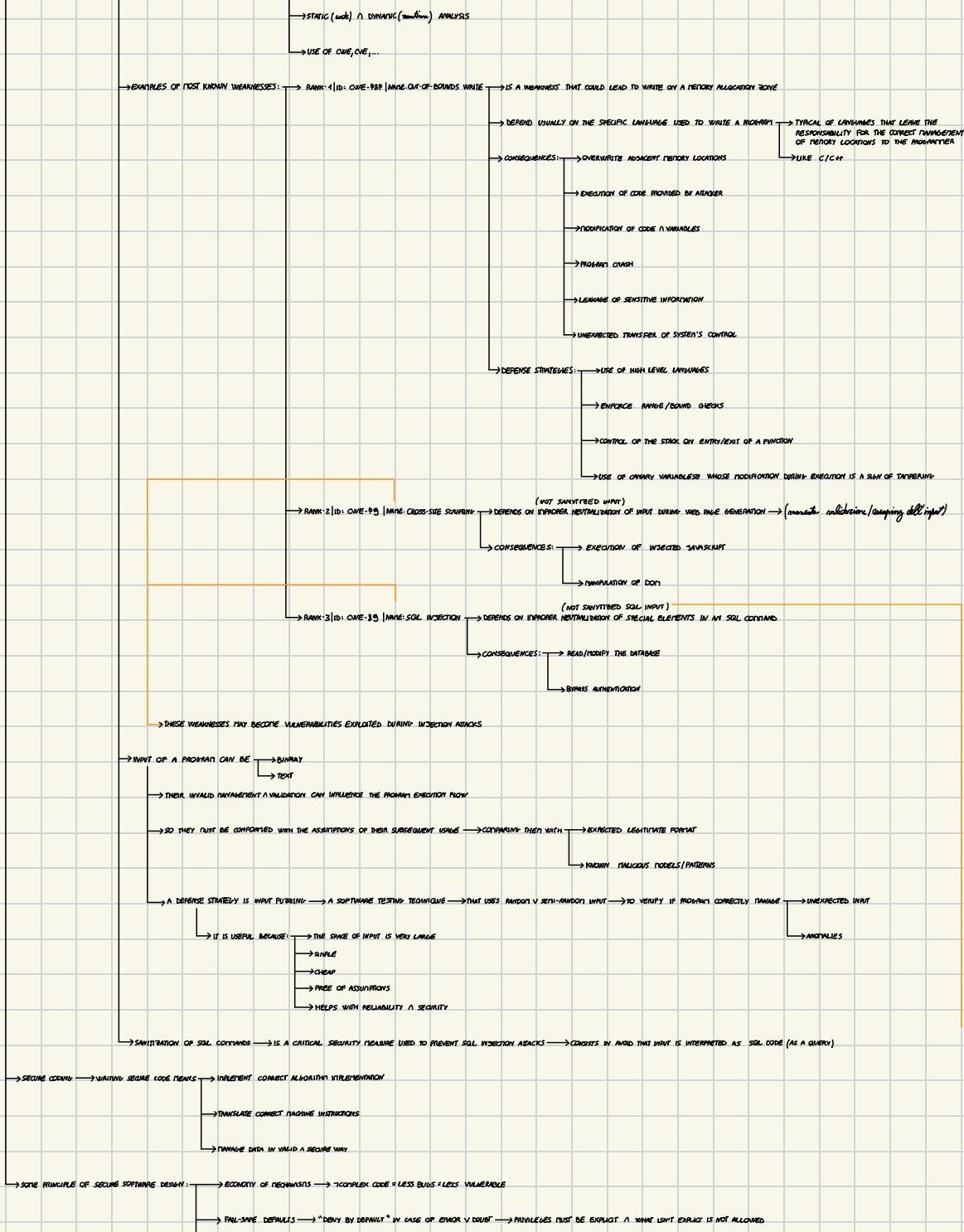
→ PRIVATE KEY → THAT MUST STAY ON THE DEVICE  
IT'S UNIQUE FOR THE COMBINATION OF DEVICE/SERVICE/ACCOUNT

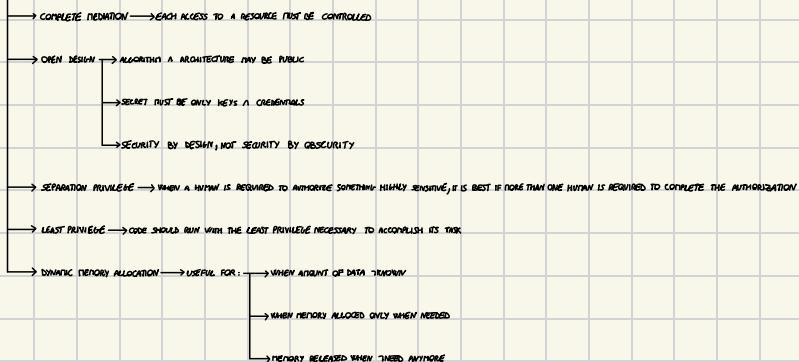
→ PUBLIC KEY → NEEDS TO BE SENT TO THE SERVER  
ASSOCIATED TO THE ACCOUNT  
SAVED ON THE DATABASE



## SOFTWARE SECURITY







## OS SECURITY



→ 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

→ TRUST BE: → UNTRUSTED → (ROT)

→ UNTRUSTED → FROM NORMAL OS

→ PRIVILEGED → LESS CODE = LESS BUGS

→ P.S. STARTS THE SECURE BOOT → WHICH CRYPTOGRAPHICALLY VERIFIES: → FIRMWARE → CODE THAT STARTS HARDWARE BEFORE A UNDER OS

→ OS

→ NEXT COMPONENTS

→ OS COMPONENTS IN TEE ARCHITECTURE: → ROOT OF TRUST

→ TRUSTED OS → INITIAL OS OF TEE

→ TRUSTED KERNEL → MANAGE → SCHEDULING

→ ISOLATION

→ RESOURCES

→ TRUSTED CORE FRAMEWORK → PROVIDES OS SERVICES FOR TRUSTED APPLICATIONS → EXPOSES SAFE API FOR SENSITIVE OPERATIONS & CRYPTOGRAPHY & KEYS MANAGEMENT

→ TRUSTED DEVICE DRIVERS → PROVIDES A COMMUNICATION'S INTERFACE WITH TRUSTED PERIPHERALS

→ TEE COMMUNICATION AGENT → IS THE TEE'S SIDE COMMUNICATION COMPONENT → WORKS ALONG WITH REE COMMUNICATION AGENT

→ REE & TEE COMMUNICATE THROUGH A DEFINED A PROTECTED INTERFACE → TEE CLIENT API → A COMMUNICATION CHANNEL DESIGN TO: → TRANSMIT DATA FROM REE TO TEE (& VICEVERSA) SECURELY

→ REE DYNAMIC GENERIC OPERATIONS & TRANSIENTS OF THE SYSTEM

→ PREVENT UNAUTHORIZED ACCESS BY THE REE TO THE TEE

→ WHEN AN OPERATION IS CRITICAL → THE REE SENDS A REQUEST TO THE TEE → AND EXECUTE IT IN A SAFE WAY

→ LIMIT INTERACTIONS ONLY TO A NECESSARY REQUEST → (CRYPTOGRAPHIC V AUTHENTICATION OPERATIONS)

→ SO REE USE SERVICES OF TEE → WITHOUT VIOLATING ISOLATION & CONFIDENTIALITY → RECEIVING ONLY THE FINAL RESULT OF REQUESTED CREATION

→ THREATS AND MITIGATION IN OS → A CRITICAL THREAT IS WHEN A SYSTEM IS COMPROMISED IN PHASE OF

→ INSTALLATION

→ DEPLOYMENT

→ IF AN OS STAYS 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 DESIGNED TO REACH SOME GOALS:

→ ASSESS RISKS AND PLAN SYSTEM DEFENCE

→ ANALYSIS OF THREATS } → BEFORE INSTALLATION

→ CRITICAL ASSETS

→ ATTACK SURFACE

→ 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 (PROTOCOL...)

→ ASSURE APPROPRIATE PROCESSES ARE USED TO MAINTAIN SECURITY → AS } → PATCH MANAGEMENT

→ MONITORING

→ LOGGING & AUDITING

→ FLOW OF PLANNIFICATION:

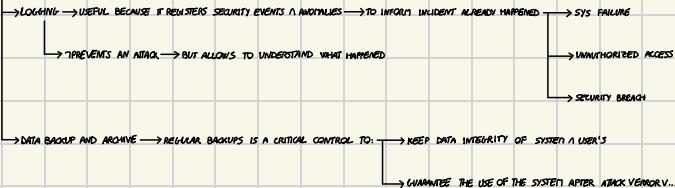
→ 1) SECURITY OF DATA, INFORMATION & APPLICATIONS → INSTALLATION OF NECESSARY FEATURES

→ 2) ASSESSMENT & IDENTIFICATION OF PRIVILEGES → LEAST PRIVILEGE

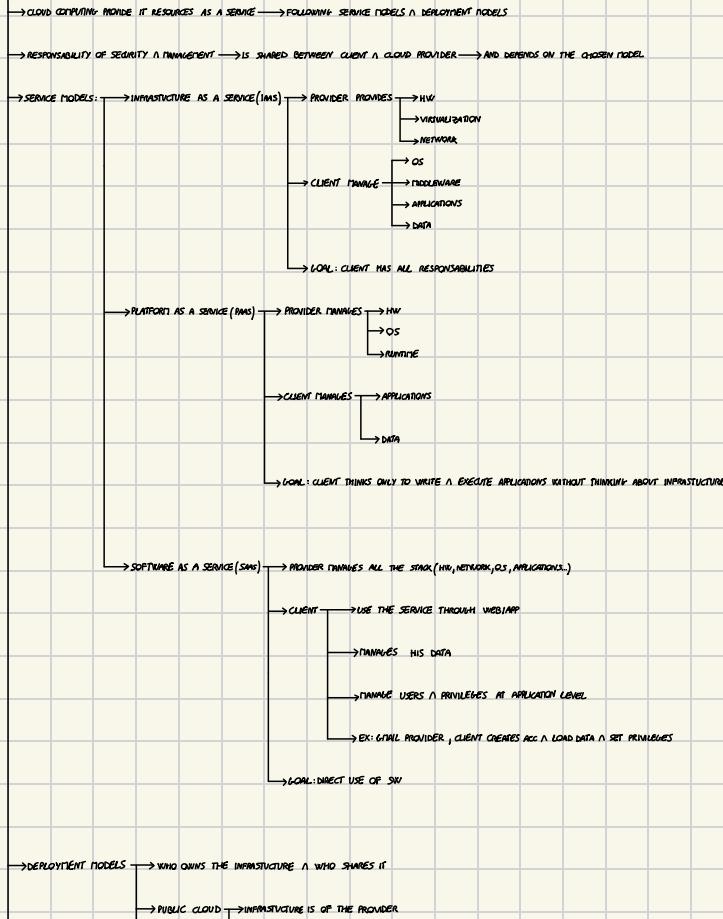
→ 3) METHODS FOR AUTHENTICATION OF AUTHORIZED USERS

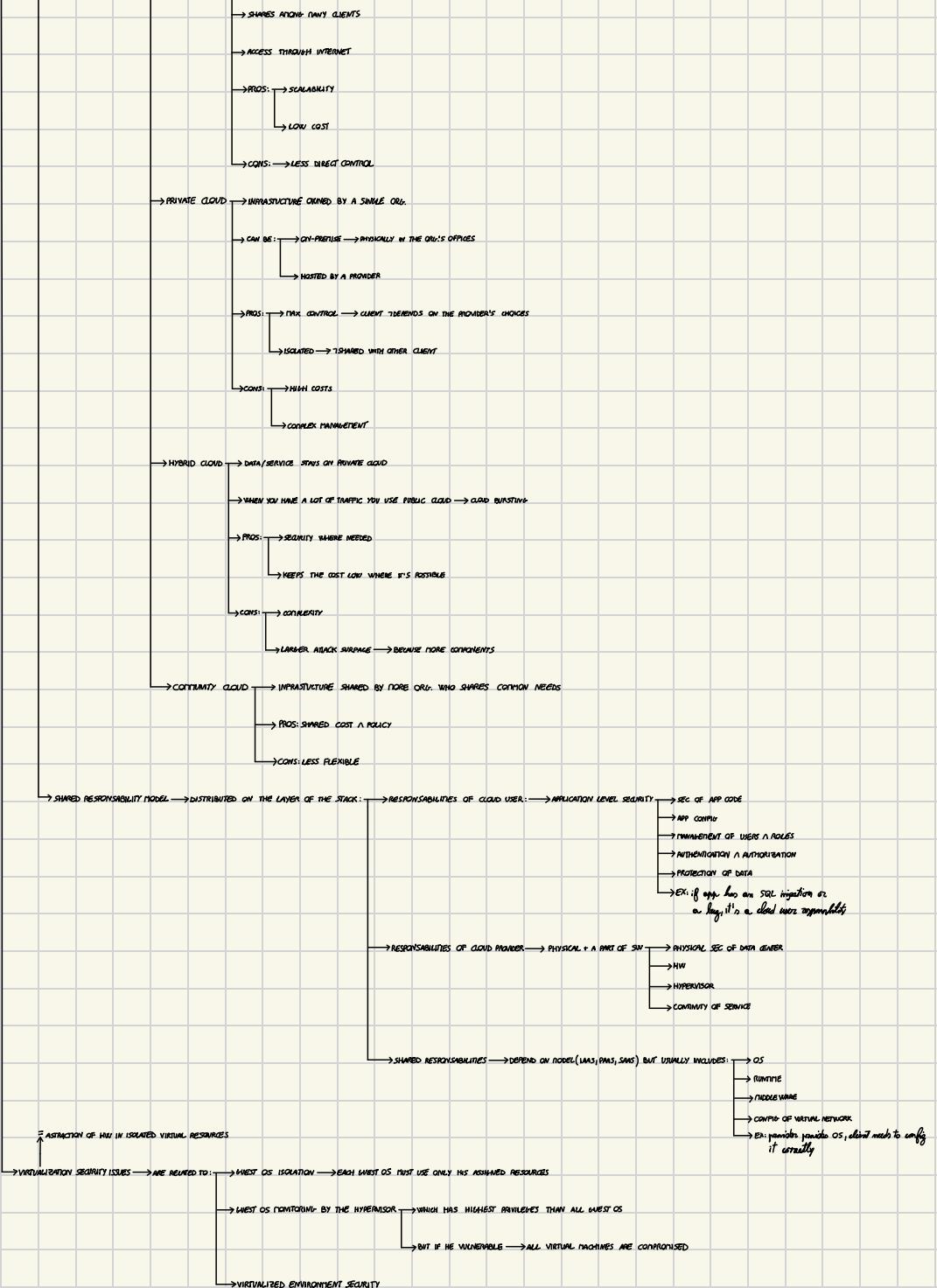
→ 4) METHODS FOR ACCESSING DATA → NOT ALL AUTHORIZED USERS SHOULD SEE ALL

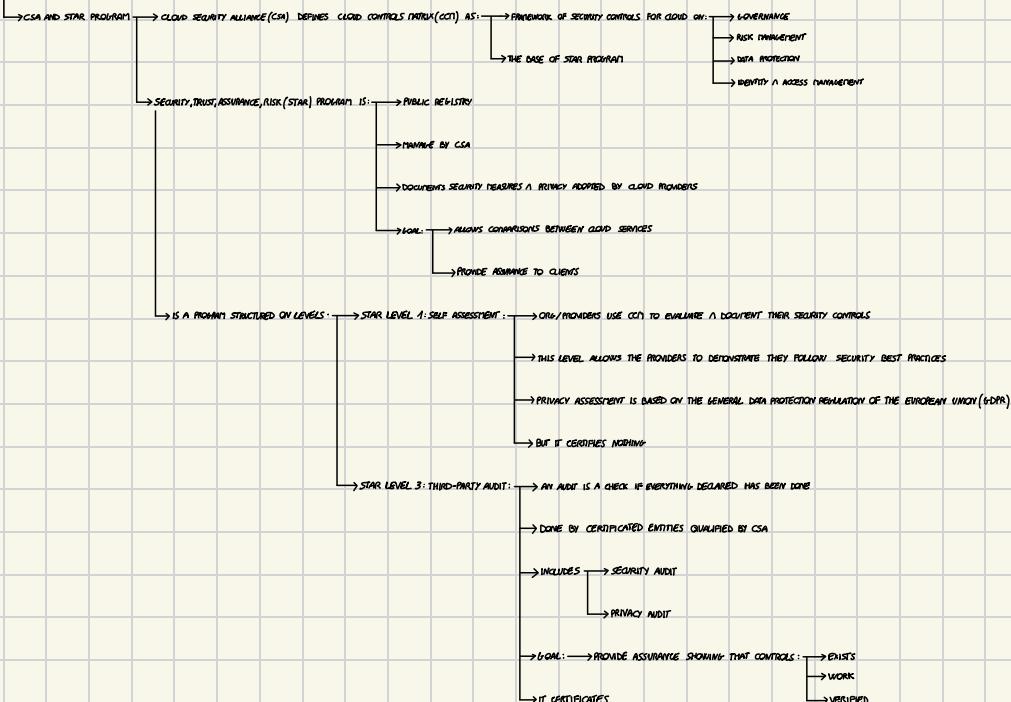
- 5) INTERACTIONS BETWEEN THE SYSTEM & EXTERNAL RESOURCES → ANALYSIS OF COMM. WITH EXTERNAL NETWORKS / API / THIRD PARTIES → UNINTENDED INTERACTIONS
- 6) SYSTEM MANAGEMENT: WHO & HOW
- 7) ADDITIONAL SECURITY MEASURES → [FIREWALL, ANTIVIRUS, DETECTION SYS] → THESE DOESN'T SUBSTITUTE SECURE BY DESIGN



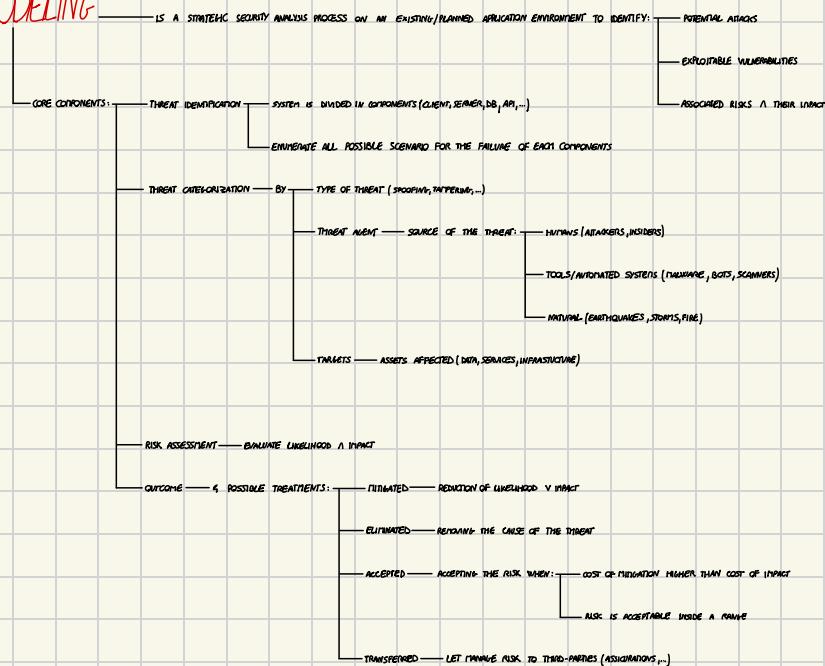
## CLOUD AND IoT SECURITY

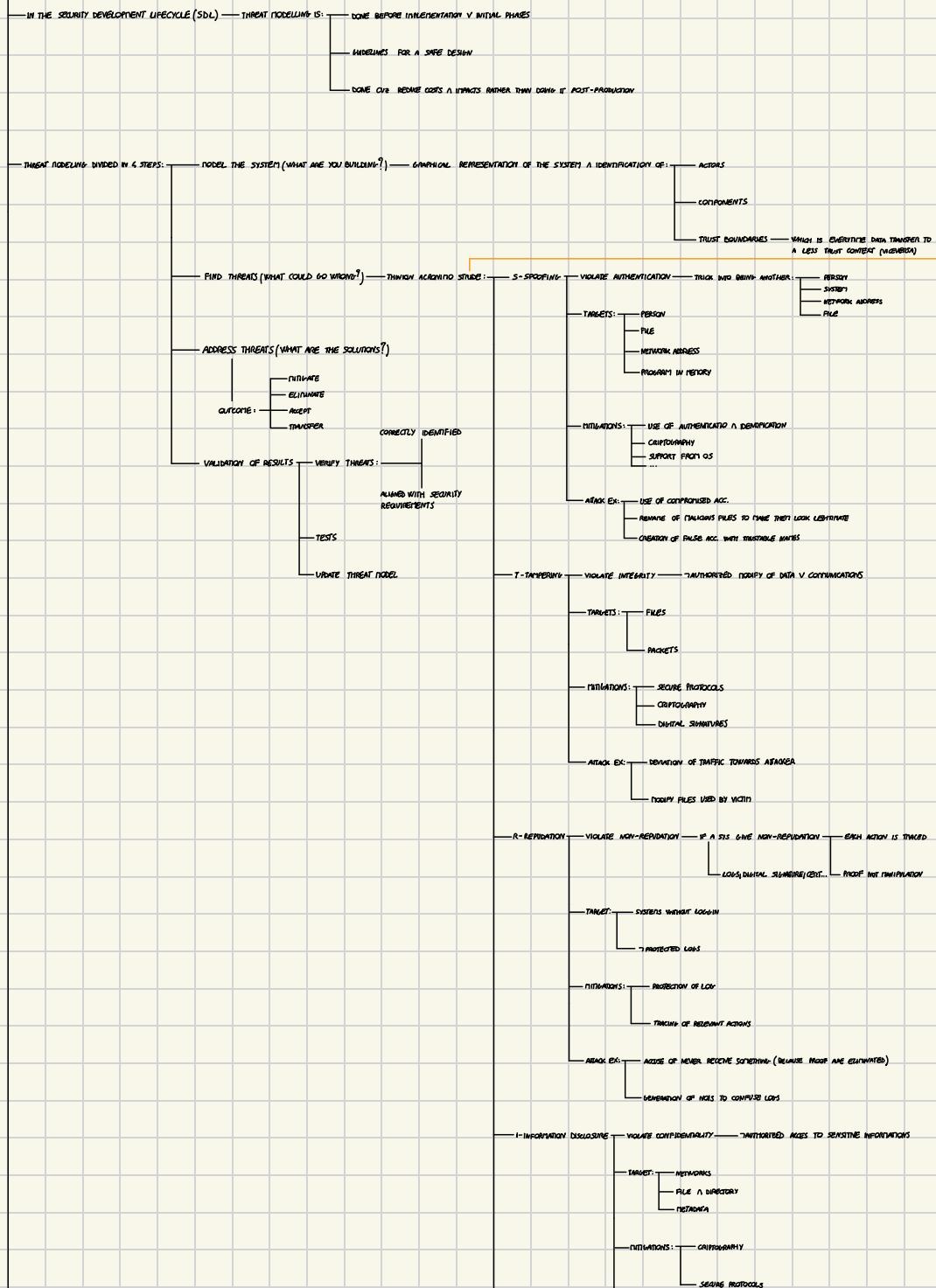






## THREAT MODELING





ATTACK EX: EXTRACTION OF SECRETS FROM ERROR MESSAGES

RETRIEVE CRYPTOGRAPHIC KEYS FROM MEMORY

TRAFFIC ANALYSIS

OBERVE DNS TO KNOW WHO TALKS TO WHO

D-DENIAL OF SERVICE VIOLATE AVAILABILITY INTERRUPT SERVICES V. CORRUDE PERFORMANCES

TARGET: APPLICATION  
SYSTEM  
NETWORK

MITIGATIONS: ACCESS CONTROL

CLOUD & SCALABILITY MECHANISMS

ATTACK EX: FLLOODING ATTACK

EXCESSIVE CONSUMPTION OF NETWORK BANDWIDTH

E-ELEVATION OF PRIVILEGE VIOLATE AUTHORIZATION LOW MIGHT PRIVILEGES THAN YOU SHOULD

TARGET: CODE  
MEMORY

MITIGATIONS: HIGH LEVEL LANGUAGE  
SEGREGATION BETWEEN CODE & DATA  
SANDBOXING

ATTACK EX: EXECUTION OF OPERATION RESERVED FOR PRIVILEGED USER

INPUTS INCORRECTLY MANAGE

THREAT MODELING 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 A BY WHO?

ASSETS  
ATTACKERS  
VULNERABILITIES

SOFTWARE IS MODELED USING DIAGRAMS STARTING FROM THREAT ASSESSMENT

DATA FLOW DIAGRAM (DFD) — A DFD SHOWS HOW DATA MOVES THROUGH A SYSTEM IT IS THE PRIMARY DIAGRAM USED IN THREAT MODELING

WHICH COMPONENT PROCESS THEM

WHERE TRUST BOUNDARIES ARE CROSSED

GOALS: VISUALIZE DATA FLOWS

EXPOSE ASSET SHAPES

MAKE TRUST BOUNDARIES EXPLICIT

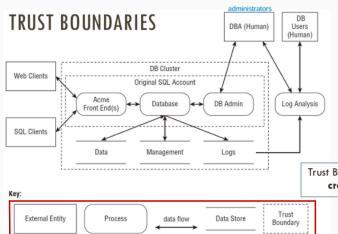
DEFINE ELEMENTS WHERE IT'S POSSIBLE TO APPLY STRIDE

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 ACTUALLY OBSERVED ATTACKS
- MANY ATTACK LIBRARIES:
  - CAPER BY NISTRE — LIST OF ATTACK MATRIX (EXECUTION OF AN ATTACK)
  - ATTACK BY NISTRE — TACTICS & TECHNIQUES USED BY ATTACKERS
  - OWASP — MOST COMMON ATTACKS ON WEB APP

— SCORING SYSTEM THAT EVALUATE AN ALREADY KNOWN THREAT.

- DREAD MODEL
- RISK = NOVEL BASED THREAT MODELING — USEFUL TO FIND THREATS — BUT INHIBITING THEM — EACH THREAT EVALUATED ON 5 DIMENSIONS — WITH A SCORE 1-3 — FINAL SCORE = D \* A \* R \* E \* D
  - D - DAMAGE POTENTIAL
  - R - REPRODUCIBILITY — HOW EASY TO REPRODUCE ATTACK
  - E - EXCLOUTABILITY — HOW HARD TO EXCLOUT 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 MODELING FRAMEWORK DOES COMPLETE ANALYSIS:

- DEFINITION OF BUSINESS ASSETS
- DEFINITION OF ARCHITECTURE, COMPONENTS, FLOW DIAGRAMS
- THREAT INTELLIGENCE — COLLECT INF. ON ATTACKERS, MOTIVATIONS, TECHNIQUES...
- VULNERABILITY ANALYSIS — ATTACK SURFACE
- ATTACK SIMULATION
- RISK & IMPACT — ANALYSIS OF POSSIBLE DNG
- MITIGATION — COMPREHENSIVE MEASURES & 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