COM402

Spring 2017: Information Security and Privacy

[TOC]

Basic concept

- information sensitivity
  - context dependent : harmful for future
  - longevity dependent : ephemeral, active information, slowly changing, unchangeable

- threats : breaches, de-anonymisation. ransomware, phishing, by random people, crooks or state agency
- access control : who, what, how, when
- authentication : simple user and password, 2FA 2 factor authentication (token), device-centric, PKI public key infrastructure (certificat), PGP keys, ssh fingerprint, signal verification
- encryption : making darta unintelligible, non-private channels, who holds keys, keys lost/misplaces/forgotten, stolen laptop
- anonymization : scrub senstivite information, hide
- operational security : identifiy the risk, minizie it, prepare response
- compartementalization : limit damage, least-privilege, isolate zone

Common threats

- threats définition
  - ISO27005 : "A potential cause of an incident, that may result in harm of systems and organization."
  - NIST FIPS 200 : Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via

unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

- overview
  - physical
  - environmental : fire, water, pollution, earthquake, volcanic eruptions, cosmic radiation, war, riots
  - loss of essential service : electrical, air conditiong, telecommunication
  - technical failures
  - non-physical : social engineering, software vulnerabilities (0-day, buffer, injection, race, access control, leaks, IO, etc.), DDOS, malicious software (viruses, worms, trojans, rootkit, ransomware, backdoors (intent, conset, access))

- exploits : using something to one's own advantage, humans vulnerabilities, software bugs, system attacks
- cyber attacks lifecycle
  - preparation : define target, organize accomplices, builds tools, research target, prepare watering holes (trapes)
  - gain access : deployment, initial intrusion, privilege escalation
  - maintain access : strengthen foothold (rootkits), stealthy, internal reconnaissance, expand access
  - complete mission : exfiltrare data, damage target, other attacks
  - cover tracks : delete log files, modify logging, memory-only persistence

- commodity threats : non-targeted (shotgun approach), fully automated, short-term financial gains goal, considered low risk to attackers, starting point for sophisticated attacks, forms (computer worns, malicious ads, etc.)
- hacktivism : political motivated hacking or ararchic civil disobedience, forms (software PGP, website mirroring, website defacement, anonymous blogging, DDOS, etc.)
- advanced persistent threats : APTs
  - advanced : multi-steps attacks, full spectrum of intrusion, speciallized tools, multiple attack vector
  - persistent : low and slow approach, prioritize long-terme over short-term goal, continuous monitoring and interaction (max known length is 5 years)
  - threat : human coordinated attack, skilled/motivated/well-funded attacker with clear goal (espionage), no fire-and-forget approach as core component (fully automated)

- OWASP top 10 critical web application risk : injection, broken authentification and session management, cross-site scripting, insecure direct object references, security misconfiguration, sensitive data exposure, missing function level access control, cross-site request forgery, components with known vulnerabilities, unvalidated redirects and forwards

Crypto basics

- cryptography : toolbox for security mechanisms, secure data at rest and data in motion, not solution to all problems, not reliable unless used and implemented properly
- goal : confidentiality, integrity, authentication, accountability, availability, timestamping
- plaintext : m
- ciphertext : c
- symmetric : one private key, require keys securely exchanged
    - one-time pad : OTP $c = m \oplus key$, $m = c \oplus key$, key as long as plaintext, perfect secrecy but require truly uniform random values not used more than once - steam ciphers : $c = prg(key) \oplus m$ with pseudo-random generator, RC4 (HTTPS), CSS (DVD protection)
    - block ciphers : encrypt blocks of fixed size, AES, DES
    - electronic code book : ECB, bad, same plaintext encrypt to same ciphertext
    - cipher block chaining : CBC, good, next key is generated from previous ciphertext, use initilization vector (IV)

- hash : string any length to fixed length output in deterministic way, integrity, signin
    - property : one-way, collision-resistance (hash before getting a collision $2^{N/2}$), pseudo-randomness (indistinguishable from random oracle)

- data integrity : ensure not modification by unauthorized parties, MACs, $tag = S(key, m)$ can be verified $V(key, m, tag) = yes$

    - encrypt last block : CBC-MAC, last block of CBC encrypted + additional encryption step, banking system
    - hash message authentication code : HMAC, $key \oplus i_{pad} = i_{keypad}$, $key \oplus o_{pad} = o_{keypad}$, $hash(i_{keypad} message) = hash_1$, $hash(o_{keypad} hash_1) = hash_2 = hmac$TLS, IPsec

- authenticated encryption : AE, confidentiality and integrity, combine MAC and encryption (mac-than-encrypt (SSL), encrypt-and-mac (SSH), encrypt-then-mac (IPSec))
    - parameters : key, message (authenticated and encrypted), additional data A (only authenticated), nonce N (one-time initialisation), cipher, tag
    - offset codebook : OCB mode

- public key : public and private keys, digital signature, interactive key exchange over insecure channel, overhead compared to symmetric, relies on algebraic operations staying hard
    - RSA : hardness factorisation problem
    - pick large prime : p, q
    - compute : $n = pq$, $\phi_n = lcm(m - 1, n - 1)$

    - pick secret key : sk coprime with $m-1$ and $n-1$
    - compute public key : $pk = sk^{-1} \mod \phi_n$
    - encryption : $m^{pk} \mod n$
    - decryption : $c^{sk} \mod n$
    - elliptic curve cryptography : algebraic structure of elliptic curves over finite fields ($y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$), small key for equivalent security (256 bits ECC and 2048 bits RSA), faster, but some curves wakes
    - signature : public counterpart of MACs, certificated, authenticated email

- interactive key exchange
    - Diffie-Hellman : hardness of discrete logarithm problem, not hard in all groups, TLS
    - agree : finite group G with operator g
    - A picks : random a and send g^a
    - B picks : random b and send g^b
    - A compute : $s = (g^b)^a$
        - B compute : $s = (g^a)^b$

- key distribution : need either secret (private) or trusted (public) channel, organized into hierarchy or peer network
    - key distribution centers : KDC, shared secret keys through confidential tickets, require parties to have shared key with KDC
    - certification authorities : CA, provite trusted publics keys through signed certificated, require parties to have public keys of trusted CA

- public key infrastructure : PKI, set of roles, policies, procedures to create, manage, distriute, use, store and revoke digital certificates
    - certificate authority : CA, stores, issues ans signs
    - registration authority : RA, verifies
    - certificate policy : CP, defines purposes
    - methods
    - certificate authorities : CAs, trusted third party
    - web of trust : WOT, PGP, self-signed certificated
    - simple public-key infrastructure : SPKI, experimental, overcome complexities of CAs and WOT

- TLS : transport layer security / secure sockets layer
    - provide : secure connection, authentication, integrity, forward secrecy
    - attacks : downgrade attack, bugs in implementation (heartbleed), poodle, crime/breach (compression with TLS issue)

- HTTPS : HTTP with TLS, pre-installed list of trusted certificate authorities, major concern about mitm (man-in-the-middle) attacks over CA, HTTP strict transport security (HSTS) avoid protocol downgrade and cookie hijacking or ssl-stripping

Database security

- multitier architecture : presentation tier, logic/application tier, data tier
- threats : abused privileges, weak passwords, SQL injections, malware, poor auditing records, storage media exposure, dos
- access control : least privilege, OS security permissions, listening permission
    - discretionary access control : DAC, owner of object define subject that can access
    - role based access control : assign role to operations and objects to which operations need access, views (mysql)

- input validation and injection : sanitize user input using prepared statement
    - boolean injection : brute force
    - error leak information : user, hostname
    - out-of-band : database make query to specific website
    - time-based delay : guess value based on query time

- sensitive data : protect against weak password, hash, salt, avoid security by obscurity, dedicated password hash function (slow as bcrypt, memory hard as scrypt), hmac
    - brute-force : up to 1 trillion combination with AMD 7970 card in 2 minutes, heuristic (uppercase first letter, numbers at the end, only alphabetical, subsitution), rainbow tables (chain of hash reduce to plaintext, restart, different reduction function of each columns) - secrets keys : on another server, hardware security module (HSM), still can fail
    - randomness : need good pseudo random number generator
    - timing attack : constant time equaility check

- confinement : only authentifcated servers can acces, host least privilege, physical security (datacenters, corruptions, coercions)
- encryption
    - data in motion : can be intercepted (mitm, etc.), use certificate
    - data at rest : read the disk, full-disk encryption, application level encryption, database level encryption (5% overhead in mariadb, fine-grained)

- data inference : through aggreation of forbidden access
- encrypted database processing : homomorphic encryption to allow operation to run over encrypted data, private information retrievaé (database do not knowns which data retrieved), privacy conscious data sharing

Personally identifiable information

- PII : any information about individual maintained by an agency

    - including : any information that can be used to distinguish or trace identity (name, social security number, date, place of birth, mother's maiden name, biometric recors etc.) and any information linkable (medical, educational financial, employement information, etc.)
    - danger : embarrasing, disadvantage (medical, financial), location, allergies, drone attacks, medical implants, deanomyization
    - co-location : with someone that is located, face-recognition, ip-address, available wlan or gsm network

- confidentiality impacts levels : potential harm that could result to individual
    - factors : identifiability, quantity, sensitivity, context of use
    - low : limited adverse effect, minor financial loss
    - moderate : serious adverse effect, significant degradation
    - high : severe adverse effect, serious threatening

- management concepts
    - pre-collection : what and why data collected, inteded use, shared with whom, how secured
    - operating phase : protective measure (encryption separation), de-identify or anonymize data, don't exchange unnecessary data, generalizing date (discretize), suppressing, add noise, swap (for statistics)
    - incident response : preparation (report, processus, informed, backup), detection, analysis, containment, eradication, recovery, post-incident activity (improve)

- legislation : apply if the processor or subject based in
    - CH : regulated acts on data (collection, storage, use, revision, disclosure, archiving, destruction), private company not force to publish (but public yes)
    - Europe : opt-in instead of opt-out for usage, breaches must be reported within 72 hours, right to be forgotten, responsability and accountability, proction directive (notice, purpose, consent, security, disclosure, acces, accountability)

User management

- access control
    - level : network, within enterprise, operating system, application itself
    - role-based : RBAC, a role can contain multiple permissions, easy to manage and give an explanantion, difficult to define granularity and fuzzyness
    - discretionary : DAC, owner specifies policies to access what owned, flexible, intuitive but rely on owner judgement, vulnerable to trojans
    - access control list : ACL, by resources, revocation changes objects, new accesses require update, difficult to delegate, unix
    - access rights : capability, by users, no instant revocation

    - mandatory : MAC, security labels over subjects and objects (unclassified, confidential, secret, top secret), modified by trusted admin, immutable during execution, linux security modules (LSM, SELinux), implemented using reference monitor with policy store, very restrictive

- authentication : procedure by which an entity establishes claimed relationship property to another entity
    - habits : low entropy, similar passwords, predictable place for non-alpha or uppercase, physical write down

- kerberos : authentication server T keys in exchange of password, ticket-granting server G issues ticket with keys, then request service with keys and tickets, distributed, limited period of validity, mutual authentication, requires clock synchronization, replay cannot be avoided, first password is a weak spot
- multi-factor authentication : separate pieces of information to authenticate, two of knowledge/biometrics/possession
    - one time password : hash chains, avoid eavesdrop
    - client stores : x
    - server stores : $t = H^n(x)$
    - servers sends : n
    - client computes : $y = H^{n-1}(x)$
    - servers check : $H(y) == t$ and decremente n
    - biometrics : behavioral (speech, keystroke), physiological (iris, face), registration (creation, storage), authentication (acquisition, comparison), can change depeding on environment or age
    - errors : higher sensitvity is always the best, crosover error rate is best between false accept rate (FAR) and false reject rate (FRR)

- ldap : standard for accessing corporate repository for commonly used information, TLS, certificate, tcp/ip, model object (users, groups) and attributes
- user training : carefull password management, software updates, antivirus, policies, avoid random devices connection, phishing warnings

Network security practices

- organizational network security practices : break network into functional zone
    - access control lists : ACLs, manage zone to zone permissions in routers or firewalls, prevent all-at-once compromise, hard to manage
    - demilitarized zone : DMZ, local network facing outside (e.g. for web, mail, dns, ftp), single or dual firewall
    - virtual local area networks : VLANs, networkong partitioning at layer 2 (data link), network visibility

    - MAC flooding : switch routing table overflow, sends spoofed MAC addresss to fill, watch arp broadcast
    - hopping : see traffic from other vlan
        - switch spoofing : emulate config message from legitimate switch
        - double tagging : embed hidden 802.1Q tag inside another as most switch perform on single level, solve by ensuring port separation between user and switches
    - active directory : AD, windows domain networks, domain controller (DC) authenticate and authorizes
    - secure communication : TLS, IPSec

- virtual private network : VPN, extension of private network over public one, network layer (IPSec via tunnel) or link layer (L2TP via virtual link-layer, do not provide confidentiality, relies on encryption)
    - local area network : LAN, interconnect VPN services at multiple geographic areas
    - dial-up services : access intranet from remote location
    - extranet services : combine local area and dial-up

- securing network perimeter : hide internal network, prevent employers to access malicious websites
    - firewalls : only authorized traffic passes
    - packet filters : examine datagram (ip, addresss, transport, ports, TCP flags), can be spoofed
    - stateful packet filters : track connection state, block not standard behaviour (sequence), no udp support
    - application gateway : proxy, inspect packet data, slower
    - intrusion detection systems : IDS, deep packet inspection for all application, generate alert, intrusion prevention system (IPS) filters sucj traffic out, false issues
    - signature-based : predetermined attacks pattern, can be DDOS, require knowledge of signature
    - anomaly-based : profile traffic, look for statistically unusual packet streams

- logging : identifying incidents, monitor violation, non-repudiation, include (failures, authorization decision, errors, higher-risk functionality), exclude (tokens, illegal user info)
- backup : full, incremental (change since any previous), differential (change since previous full), 3-2-1 rule, 3 copies of data, stored on 2 different media, 1 copies must be stored offsite, encryption

Security/privacy policy

- information security policy : incentives, responsibility/liability, market-driven, product

cost, free but data selling business model, lemon market (buyers less information lead to sellers reduce quality), no security competition (avoid general mistrust)
    - alternative approchaces : standardized algo, independent evaluation authorities, profession licensing (doctors title like), liability for failures
    - standards : US NIST (national institute of standards and technology) for DES, AES, SHA, voluntarily or mandatory uses

- crypto wars : privacy versus governments, balance rights of individual info against security needs, fight backdoors (security weakness), misused, need legal request
- data protection laws : company use click-wrap (all we can do, cannot be sued), regardless of what click-wrap say users can sue for violation
    - EU : directives (implemented by each member), regulation (directly applied to each member), general data protection regulation (GPPR, data collection reported, mandatory privacy impact assessment, breach reported in 72 hours, keep only for usage, right to be forgotten, extends liability beyond data controllers and processors)
    - US : depend on type or data usage

- privacy, speech, anonymity, accountability : free speechs (marginalized groups), trolling (revenge porn), doxing (broadcasting senstive personal data), tor, fake news, sponsored trolling, truth, bans

Anonymization

- anonymization : technology that converts clear text data into a non-human-readable and irreversible form, enables the transfer of information across a boundary
- motivation : bug report, humanitarian data, meta-data
- naive anonymization : unlinking users from attributes, obfuscate identities/attributes (can be correlated)/aggregation (limited)
- k-anonymity : attributes suppressed/generalized until each user identical with at least k-1 other users
- differential privacy : $Pr(Q(D) = R)Pr(Q(D_{\pm i}) = R) < e^{\epsilon}$ with R public results, private data $|D_{\pm i} - D| \leq 1, R \in Range(Q)$ and ϵ privacy budget (amount of information you release), ensure minimal evidence of individual participation, protect PII to chosen level ϵ, machine learning (introduce some error to the model, model diffcult to reverse)
- confidentiality using encrypt : database, leave information intact for indexing, range queries, clustering, keyword search, general computation
    - property-preserving encryption : property function $P(m_1, \ldots, m_k) = 0, 1$, oder preserving encryption OPE vs deterministic encryption DET
    - scheme : every row/column intersection encrypted RND (max security), DET (deterministic), OPE, HOM (homomorphic encryption), JOIN, SEARCH (per-word

padded)
    - attacks : frequency analysis, sorting attack, cumulative attack
    - building on property-revealing encryption : BoPET, encrypt data before uploading, not restricted to 1 bit
    - multi-key searchable encryption : MKSE, no server access but can search/compare
    - threat model : snapshot passive (onetime server snapshot), persistent passive (record operation), active (misbehave to collude with users)

Machine learning

- dark sides : algo bias, reinforce discrimination, treat decision carefully
- attacking : identify feature space with high error, non-linear non-convex optimization
    - attack surface : manipulate collection of data, rig processing, corrupt model, tamper output
    - adversarial capabilities : training data, influence, logic corruption, blackbox, whitebox
    - adversarial goals : confidentiality, privacy, integrity, availability (prevent good result), fooling AI, fraud, crashing vehicule
    - integrity : $b \leq e/(1+e)$ with b fraction of data modified, $1-e$ targeted learning accuracy
    - membership inference : prediction leak information of training data, overfit, classification problem (ML against ML)

- defending : generate adversarial samples, defensive distillation (train 2 models, one only for decision), difficult theory, mostly static not adaptive

Secure multi-party computation SMC

- multiparty computation : SMC, distributed computing tasks in secure manner, run data mining algorithm on union of parties databases without allowing any party to view another individual's private data, e-voting, auctions
- requirements
    - privacy : no party learn anything more than prescived output
    - correctness
    - independence of inputs : corrupted parties choose inputs independently of honest parties
    - guaranteed output delivery : corrupted parties not able to prevent honest parties to receive
    - fairness : corrupted parties receive their ouputs iff honest parties also receive their outputs

- security definition : protocol said to be secure if no adversary can do more harm in real execution than execution within ideal world with globally third party trusted
- adversarial power : strategey (static/adaptive), behaviour (semi-honest/malicious), complexity (polynomial-time/unbounded)
- feasibility : m number of parties, t bound on number of corrupted parties
    - $t < m/3$: achieve for any function
    - $t < m/2$: achieve for any function assuming all parties have broadcast channel
    - $t \geq m/2$: without fairness and guaranteed output delivery assuming broadcast channel access
- preliminaries : assumptions (static corruption, no honest majority, polynomial-time adversary), security parameter n (length key)
    - negligible function : $\mu(\cdot)$ if for every positive polynomial there exists an interger N s.t. for all $n \geq N$ it holds $\mu(n) < 1/p(n)$
    - computationally indistinguishable : $X \equiv^c Y$ for distribution ensemble $X = \{X(n,a)\}$ and $Y = \{Y(n,a)\}$ for $a \in \{0,1\}^*$ if for every non-uniform polynomial-time distinguisher D $|Pr(D(X(n,a)) = 1) - Pr(D(Y(n,a)) = 1)| < \mu(n)$, no algo can tell them apart
- semi-honest : adversary controls one parties statically and follows protocol exactly
    - secure if exist probabilistic algorithm S_1 and S_2 s.t. for every $x, y \in \{0,1\}^*$ where $|x| = |y|$ we have $\{(S_1(1^n, x, f_1(x,y)), f(x,y))\}_n \equiv^c \{view_1^\pi(n,x,y), output^\pi(n,x,y)\}_n$
- oblivious transfer : $((x_0, x_1), \sigma) \mapsto (\lambda, x_\sigma)$, party 2 receive x_σ but learn nothing about other string, party 1 not learn anything about σ, compute by private protocol π
    - receiver : generate two random public keys, P_σ with decryption key known, $P_{(1-\sigma)}$ without decryption key known, send both to sender
    - sender : encrypt x_0 with P_0, encrypt x_1 with P_1, send back result
    - receiver : can only decrypt x_σ
    - must ensure receiver choose appropriately his public keys
    - efficient OT : generator of group of order n
    - $\sigma = 0 : \gamma = (g^a, g^b, g^{ab}, g^c)$
    - $\sigma = 1 : \gamma = (g^a, g^b, g^c, g^{ab})$
    - sender : receive x, y, z_0, z_1, choose random u_0, u_1, v_0, v_1 and computes $w_0 = x^{u_0} g^{v_0}$, $w_1 = x^{u_1} g^{v_1}$, $k_0 = (z_0)^{u_0} y^{v_0}$, $k_1 = (z_1)^{u_1} y^{v_1}$, compute $c_0 = m_0 k_0$ and $c1 = m_1 k_1$
    - receiver : $k_\sigma = (w_\sigma)^b$, $m_\sigma = c_\sigma (k_\sigma)^{-1}$
    - Diffie-Hellman : tuple indistinguishable
- view : $view_i^\pi(n,x,y)$ view of i party during execution π

- malicious model : refuse to participate, substitute local input, abort the protocol
- covert adversary : willing to cheat iff not caught, add ϵ factor as probability of cheat detected
- garbled circuits : and/or gates with k=128 bits, result replaced by garbled values, semi-honest, issue with malicious (modify circuit, generate lots of shared circuits looks for likelyhood of modification), cut-and choose protocol (require at least 160 circuits for securit of 2^{-40})
- more : oblivious RAM, blind signature, anonymous credentials, searchable encrypt, zero-knowledge proofs
- private information retrieval : PIR protect user queries

Fault tolerance & blockchain

- redundancy and fault-tolerance : denial not a strategy
  - coding : DRAM ECC (single-bit errors, detect double), raid5 (symmetric parity), raid6 (galois-field), forward error correction (FEC, correct link error), cyclic redundancy check (CRC, detect link error), tcp checksum
  - data replication
  - n-modular programming : run on different implementation, tandom NONSTOP (redundant hardward, process pairs, fast detction, fail-fast, fast recovery)
  - software replication
  - recovery time objective : RTO
  - fault : underlying defect
  - failure : not producing desired result
  - level : ideal, defective, faulty, erroneous, malfunctioning, degraded, failed

- high availability and data consistency : system guarantees a response even during network partitions
  - CAP theorem : consistency, availability, partition tolerance
  - weak consistency : high available, low-latency, no coordination
  - strong consistency : safety first, halts on partition, need consensus, atomic

- consensus : validity, agreement (no two correct decision different), termination (eventually all decide), integrity (no double decision)
  - byzantines : some nodes might be malicious, N processes, f failure
  - fundamentally need : $N = 3f + 1$ (can be $N = 2f + 1$ under trusted hardware, synchronicity and other assumption)
  - no consensus : $f \geq N/3$

- bitcoin & blockchains : leader election, nonce, unstable concensus, risk or wait (confirmation takes 10 minutes, risky real-time), honest majority as fraction of hashpower, incentives for following the protocol, no need to output final decision

(stabilizing consensus), strategic mining

- smarts contracts : user-defined programs running on top of blockchain
  - ethereum : trusted for correctness, availability but not privacy
  - basic : transaction contans code as data, contract have account balance and persistent storage file, submit transaction to blockchain to interact with contact, validity
  - dao : bug

Side channel attacks

- side channel : the system device itself not input/output pair
- timing attacks : statistically model, keystrocke, evict cached data, defend by guaranting the time (avoid branch, introduce random delay)
- power analsis : leak keys, differential power analysis DPA, observe, guess and try, defend by introducing noise, include hardware in crypto
- electromagnetics : works through wall, detect operations
- acoustic cryptanalysis : sounds of voltage regulator
- fault attacks : change voltage, tamper clock
- row hammer : access modify contents nearyby memory rows
- optical covert channel : exfiltrate data from air gapped computers, drive LEDs blink frequency