**Human factor**: develop a mindset that recognize importance of user, work practice, organizational context

**HCI**: study of human interaction with digital tech, **includes creating effective interface and system to** meet people’s needs.

**Usability**: learnability(how ez first), memorability(how ez after break), efficiency(how quick), errors(how many, how quick recover, how severity), satisfaction(how pleasant)

Why **security** is important: human vulnerability, important for user, design fail in human factor

**Context**: a certain situation. Solution for one isn’t for another, solution not for one is not effective.

**Think like user**: understand domain, context of use, user knowledge, user experience, what to see

To **design test**: define what they need/want, need analysis of user goal

**Aesthetic**: may not be effective/efficient. Screen design is gud for aes/use but limited

**Mental model**: world view, current knowledge, detailed goals

**SSM:**  approach to solve problem involving soft system, start by identify **user needs, key factors, stackholders**. We consider **situation of concern, CATWOE(client, actor, transformation, worldview, owner, environmental constraint)** ,to get over challenge of **describing** and **understanding** problem.

**Soft system**: no clear defined solution, we don’t find for optimal solution, we find good enough solution created by iterative approach(create&test), introducing change will alter system.

**Concern for us**: phishing and social engineering, spoofing techniques to impersonate a trusted entity to conduct highly deceptive phishing attacks, by careful design and timing of a message, use people’s curious and interest.

**Penetration test, Security awareness training**, : learn which types of users pose the most risk for specific types of attacks while also identifying which employees require additional training. If people know what forms social engineering attacks are likely to take, they will be less likely to become victims.

**Spear phishing**: send a specially crafted email to very select individuals, by research targets, create customised email, for high value target.

**SSM2222**: concern, transformation(new system objective), stackholders’ worldview(mental model, what they think), context, environmental constraint.

**3 key methods for user need&pref**: study behaviour, what they say, trustworthy previous work

**Behaviour**: automated monitor- track behaviour, used for embedded training|ethnographic-observe in context and observer immerses themselves in small number ppl to get deep qualitied result,give richer data to auto monitor, works only if observers can present on time, need training|lab study- bring ppl into lab.

**Say**: in context-questionaire, out context-after lab, small group, hybrid

**Asking**: self awareness, self censorship, politeness, joke or lie

**high level user goals**: identify the goal based on all methods

**persona**: a representation of user group, need&expectation, how likely to use system, universal feature&functionality, real ppl with background, goal, value. Used as communication tool, discussion, design trade off. Do user need research, study similar&diff, identify group.

**Thinkaloud**: ask users do concrete task and record dont help unless they are unhappy. Need to consider representative. Record success, time, did, said. Tells mental model.

**Why important**: effective with learnability and error, inexpensive, why they feel hard, where they feel hard, how satisfied, effective for inexpert evaluators

**In the wild**: study of ppl daily live. Have many user, produce quantity result, easy to know what but hard to know why

**Qualitive and quantitive**: non-numbers and numbers.

**Link to mental model**: think aloud tells mental model, fix the system or fix the user(mental model)

**Prototype**: draft that allow u to explore idea and show intention behind feature or design concept. Do evaluation to inform next version(iterative)

**Lofi**: quick, many alternative, help communicate, willing to criticize, limit test possible

**Hifi:** actual working system, enable explore, costly, reluctance to change

**IA:** organization of information, match mental model, take account of user, context, domain. eg. Alphabedical, chronological, geographical, topical, task oriented, metaphor-driven, sitemap.

**Card sorting:** group cards. Open for creating own category, closed for pre-defined category.

**Mood board**: collect ideas useful, like comic, games, videos, to explore way to teach

**Screen design guidelines:** line length-ppl scanread cuz retina range is small, recommend 60 char&ppl may resize->responsive design. Fonts-> no more than 3, standard cuz more familiar, read faster. Use mixed case, line spacing, white space, text-background contrast, color blind, avoid blinking text-distract

**Ppl’s attribute**: mental&physical, which can be mostly similar or individual differ. And context which one ppl differ at different time.

**Physical**: perceive: see, hear, feel --- action: type, touch, speak

**Visual perception**: retina range, color sensitivity, color blindness-5%

**Cognitive bias**: ways human reasoning may not be rational.

**Google effect**- forget things easy to search on google

**Over confidence**- about performance, designers can be over confident about usability, think aloud can help them

**Stereotyping**: gud-> simplify complex stuff, reason based on incomplete evidence, make fast decisions. Interface designers/programmers may make many  assumptions about the users of their system. Do more user research and evaluate think aloud can help.

**Confirmation bia**s: ppl tend to believe what they already believe. it may be hard to change people’s belief, and in some case, even contradict evidence to their belief will help strengthen it. It will be hard for designers to give people information in some case, like when that information is contradicting to users’ mental model.

**Social desirability bias**: People tend to answer questions in a way that ensures the questioner will take a positive view of them. this makes it hard to observe/ask when they know they are being researched. Field trail will help.

**Problem ppl may meet:** information overload, world is confusing, we need to act quickly, we cant remember everything.

**How cog-bias help**: ppl don’t perceive everything, ppl search for meaning, ppl think quick, memory can make error

**Intuitive**: ez2learn,ez2remember,ez4errors,pleasant to use->ppl need background knowledge2use

**Usability for all**: focus on special need, but also include all requirement. Eg: physical, cognitive, social, cultural

**Week7 privacy**

**Privacy:** claim of individuals groups or institutions of **when, how, and to what extent** information about them is communicated to others he **balances** the desire for **privacy** with the desire for **disclosure and communication.**Have legislation controlling it,like personal data on computers

For below (a,b): x-axis: accuracy of personal information. Y-axis: amount of information

**Secrecy:**keep things hidden(1,1).**confidentiality**:keep someone else data hidden(2,1).**Availability**:oppose to secrecy.**Anonymity**:keep the identity of the person associated with the data secret(1,2).**privacy**:principles/rules to control availability of data. **Auditability**:able to keep a record of data made available. **Access control**:the rules for controlling privacy

**privacy involves a balance of secrecy and availability**

**ppl vary in privacy**:by their worldview, mental model and other factors. Diff privacy pref with diff ppl and diff things.ppl show similar comparative assessments for certain classes of personal data

**privacy paradox**: actual behavior is inconsistent with beliefs.eg. register without read terms.

**privacy by design**: methodology let privacy be built in architecture of information systems, business processes and networked infrastructure.aim to consider privacy before and through the initiatives that involve the collection and handling of personal information.

**Features**:Proactive not Reactive,Preventative not Remedial;Privacy as the Default Setting;Privacy Embedded into Design;Full Functionality-Positive‐Sum, not Zero‐Sum;End‐to‐End Security-Full Lifecycle Protection;Visibility and Transparency;Respect for User Privacy-Keep it User‐Centric

**right to be forgotten**: delist from search results articles relating to one’s past crimes.

**WEEK8 Security Mindset, Terminology, Threat Models**

**Security**: build and maintain systems that remain safe to use and dependable in the face of malice, error, and mischance.

**Mindset**:understand the big picture and specific detail.require:1.to think like the attack for what,how,why,and for money/fame.2.to think like user for get job done and low usability like complex warnings. Security is by design not afterwards.

**Map security space**: Policy: What supposed to achieve; Mechanisms:how to implement policy; Assurance: Amount of reliance placed on a control; Incentive: How to motivate those policy.

**Systems:ppl** use **technology**(software, hardware) to perform **activities**.security is keep work gud

**Ppl**:security depend on behaviours.ppl are not machines, not rational.ppls differ in many ways.

**Risk management**:quantity\*chance;human is bad on this;fear, uncertainty, doubt->cloud thinking

**Adages**:hide don’t make things safe,only frustrate attker.assume he can find,never rely on hide.

**Def in depth**:only raise cose/time for attker,avoid eggshell model->one ctrl fail->not full sys fail

**Vulnerability**:Weakness in system at implementation level;known or unknown;eg.buffer overflow

**Flaws**: Weakness in the system at design level; cannot always be addressed after sell product.

**Threat**:diff meaning depend on context;all high-level environmental factors a system expose to.

**Attack**: Activity that intends to cause harm to the system;can happen even no vulnerability.

**Controls**: A measure to defend the system by avoiding risk or attack, detecting it, or mitigating it;can be Preventive, Detective,corrective;can be technical, but may not Physical, Operational, Regulatory.

**Trust**:trusted system will operate as intended. trusted component if its failure would compromise the system's security. trustworthy component if we can safely assume that it is not going to fail

**Confidentiality**: the obligation to protect secrecy;is a security goal.

**Integrity**: be able to verify that information has not been(illegaly)altered

**Auditability**:find out what happened(who did);legal requirement may exist;useful after failure.

**Availability**: provide service for the intended users;require: process&acceptable time.

**Anonymity**: do things without being identified;may conflict with other aspects;perfect anonymity is impossible

**Non-repudiation**:identity/action/belonging is not able to be challenged/disguised.

**Trade-off**: control has costs as well as benefits;both harder for attkers&users.

**Threat modelling**:context matters,eg:what’s protecting?who’s attacking?how long?attacker’s motivation,organisation;social engi can be used to breach from human side.

**Week9 Operational Security and Authentication**

**Operational security**: defend against attacks against procedures and processes, not technology;asymmetrical, no tech required;bypass tech defense,attack psychological weakness that are normally beneficial in a social context, by social engineering.

**critical information**: your own intentions and capabilities that enemy need to act against you

**Analyze threat**: Systematic analysis potential opponents:who, motivation and goals, capabilities, determination.

**Analyze weaknesses**: assume the opponent's role and think like them: Which parts of your own organization show weakness? Which practices could be exploited? What equipment do you use could potentially harbour a weakness?

**Assess risks**: Assign a risk level to each identified weakness;help decide investment.

**Apply countermeasure**: prioritize the risks; mitigation plan:tech&non-tech measures; security is process, not state(threat&countermeasure change);business consideration.

**Pretext**:pretend to be someone else;policy against:call back.

**Phishing**: policy:disallow email for high value transaction.

**Baiting**: Tricking someone into accepting/using a malicious gift.policy:education,security culture.

**Tailgating**:walk behind authorised ppl to restricted area. Only in physical space;policy:guard.

**Quidproquo**: promise of a benefit in exchange for some information;defense: ensuring critical information flows are need to know rather than need to withhold.

**AAA (Triple-A)**: Authentication, authorization, accounting

**Authentication**: "what you know, what you possess, what you are"

**Week10 Software security**

**Memory**: **Stack**: local variables, function return addresses;**Heap**: dynamically allocated memory; **Global**: global variables; **Code**: program instructions;

**buffer overflow**: program defect triggered by crafted input, Overrun the part of a data structure with data that will cause execution of malicious code.**steps**: Find the overflow, Change the control flow(memory loc), Insert foreign program, Execute program.

**Atker**: Need binary machine instructions to overwrite stack; Code must have absolute entry address; once found successful attack vector , it can be reused.

**Defer**: Understand how memory is accessed; check validate inputs&sanity check

**Heap overflow**: memory pointer was changed, could overwrite files.

**Time of check&time of use**:atker change status of file between system check the file and open it.

**Def methods**:use safe version of program language;static code check(no run);dynamic code check(run);unit test;no-exec mem area;aslr(random mem);stack canaries(place value in stack and check periodically);shadow stack(use copy of stack);fuzzing(random input test);

**Online context**:information belong to a session,including cookies, javascripts, data, plugin, etc.

**Malware**:virus: Attach to programs or data , get loaded into memory,replicate and infect other programs;worm: Spreads stand-alone copies of itself via a network; trojan: Disguise as a useful software; keyloggers:record keyboard input; backdoor:debug admin features;

**Def principle**: user:never work at higher privilege;developer:check input, test, clear memory, failsafe default;operator:avoid monoculture, config manage(update).

**Week11 cyptography**

**Defination**:convert data to hide original content and prevent modify it

**Goal&purpose**:confidentiality:protect from interception, ensure confidential if intercepted; integrity:detect whether be tampered with; authenticity:ensure know who is sender, non-repudiation.

**Cryptosystem**: cryptographic algorithms needed to encrypt and decrypt; have: Plaintext space, Ciphertext space, Key space, Encryption function/s, Decryption function/s

**Symmetric cryptsys**: use shared key ;Confusion: Ensuring the key does not relate in a simple way to the ciphertext. Each character should rely on several parts of the key; Diffusion: Changing a single part of the plaintext results in many intractable changes to the ciphertext. EG: one time pad, DES, AES; block mode: break msg into blocks; streaming cipher;one bit at a time, key never reused.

**Asymmetric Cryptography**: public encrypt key, secret decrypt key;EG: PKI, Digital Signatures, Certificates

Attack: brute force obtain key, attack implement,

**WEEK12 network**

**Motivation**: Mobile networks changed dramatically the way we live and we depend on it heavily.

network security analysis: evaluates the potential risk of the threats to the entities using a network, and estimates the resources needed to perform known attacks

**Cryptographic protocols**: series of steps and message exchanges between multiple entities in order to achieve a specific security objective; **Confidentiality**: symmetric + asymmetric encryption ciphers; **Identity authentication**: signatures; **Message authenticatio**n: signatures or MACs; **Message integrity**: MACs

**Transport Layer Security (TLS)**：the most popular security protocol on the Internet

**Denial of Service attacks**：Disruption, Degradation, Data breach, Control;**technique**: Resource destruction, Resource depletion.

**Defence**: **against penetration**: system administration, Firewall;**Implementation defences**: Code reviews, testing,DoS-aware design; **against resource depletion**: Rate Control, Authentication of clients; Ingress filtering at ISPs, Egress filtering

**Firewall can**: enforce a security policy, log Internet activity efficiently, block unwanted traffic if the traffic can be characterized, limit exposure to security problems.

**Firewall cant**: against malicious insiders, against connections that don’t go through it, against completely new threats, fully protect against viruses,, cryptographic operations, set itself up correctly

**WEEK13 MANAGEMENT**

**What’s in policy**: Audiences- examine the security policy, Purpose- related to the overall goal, Assets-hardware&software&information, Nature of the protection-who&what can do, Responsibility-who do what

**Good policy**: Coverage(all scenario), Durability(withstand time change), Realism(reasonable cost&tech), Clarity(clear language)

**Policy**: High-level, expressed in business terms, Set by senior management, publicly available, change only rarely

**Procedure**: Concrete and detailed, expressed in technical terms, Set by middle managers and technical staff Specific to particular classes of employees, change with technology, in line with policy

**Risk analysis**: Identify the assets-> Identify the vulnerabilities and threats-> Give values to key parameters for each risk(impact\*probability)

**advantage risk analysis**: Value of varied participants, in advance, discussions give useful knowledge, tradeoffs can lead to better decisions, strengthen the political case for security investments

**disadvantage risk analysis:** False sense of precision, Time consuming, Results may get obsolete

**Operational planning**: Determine steps, Estimate time, Allocate people, Check on progress, Modify plans if too slow

**Review cycle**: Security policy and procedure should be reviewed regularly to Make sure that they are still appropriate

**Reflection**: Cost&benefit trade off, IT Security should fit into general management framework, Policy should drive procedures, Don’t confuse documented procedures with actual practices

**Ethics goal**: recognize ethical tensions in security topics, justify your decision

**Ethical reasoning**: **Teleological**: based on consequences of the decision, **Deontological**: providing general guidance on duties, and how to weigh up conflicting duties