

Shrnutí hlavních bodů

1. **Organizace předmětu KKY/ITE** - Předmět má rozsah 2+2 hodiny týdně a je ohodnocen pěti kredity. Hlavní část hodnocení tvoří semestrální práce za 60 %, zbývajících 40 % připadá na zkouškový test a případnou ústní zkoušku. Pro splnění je nutné získat alespoň 70 %. Materiály a organizační informace se sdílejí prostřednictvím Google Classroom.
2. **Semestrální projekt** - Studenti pracují ve dvojicích na uceleném řešení, které propojuje Python, HTML, JavaScript, HTTP API, MQTT a fyzické IoT zařízení. Projekt navazuje na předmět KKY/APK, využívá spolupráci se společností AIMTEC a nabízí možnost zapojit CIV IoT Lab pro pájení, 3D tisk nebo výrobu dalších hardwarových částí. Důležitými termíny jsou zadání 19. října, kontrolní den 16. listopadu a závěrečné prezentace 14. prosince.
3. **Kvalita řešení a využití generativní AI** - Cílem není napsat co nejvíce vlastního kódu, ale vytvořit funkční, robustní a srozumitelnou architekturu s využitím vhodných existujících modulů. Generativní AI je povolena a doporučena nejen pro tvorbu kódu, ale také pro brainstorming, návrh architektury, hledání chyb, analýzu tracebacků, dokumentaci a testy. Každý tým musí použití AI a knihoven třetích stran transparentně popsat a při odevzdání dokázat vysvětlit architekturu, logiku i konkrétní kód.
4. **Internet jako propojení sítí** - Internet není jediná služba ani jedno zařízení, ale globální propojení mnoha sítí. Zahrnuje fyzickou infrastrukturu, přenosová média, síťové protokoly i aplikační služby, jako jsou web, e-mail, bankovníctví nebo streamování. Porozumění internetu proto vyžaduje sledovat vztah mezi jednotlivými vrstvami a důvody, proč jsou některé historické principy obtížně měnitelné.
5. **Kořeny decentralizované komunikace** - V 60. letech vznikla potřeba komunikační sítě odolné proti zničení centrálních telefonních ústředen. RAND v roce 1964 navrhla robustní, decentralizovanou síť, v níž jsou komunikační uzly rovnocenné a výpadek jednoho prvku nemusí přerušit celé spojení.
6. **Přepojování paketů** - Zpráva se rozdělí na menší pakety, z nichž každý obsahuje adresu cíle a může síť cestovat nezávisle. V cíli se pakety znovu složí do původní zprávy. Opakování adresy zvyšuje režii, ale současně umožňuje sdílet přenosové médium více uživateli a dynamicky volit náhradní trasu při výpadku.
7. **První experimentální síť a ARPANET** - V roce 1965 byly po telefonních linkách propojeny počítače TX-2, AN/FSQ-32 a počítač DEC rychlostí 1200 bitů za sekundu. Agentura ARPA, založená po startu Sputniku, následně financovala ARPANET. Jeho první čtyři uzly vznikly v roce 1969 na UCLA, SRI, UCSB a University of Utah. První pokus o vzdálené přihlášení přenesl pouze znaky „lo“, protože spojení před dokončením slova „login“ spadlo.
8. **Růst ARPANETu a oddělení MILNETu** - Síť rychle rostla z desítek na stovky uzlů a v roce 1973 získala i zámořská připojení. V roce 1983 byla vojenská část infrastruktury oddělena do sítě MILNET, zatímco akademická část pokračovala jako základ veřejného internetu. Kniha Kukaččí vejce od Cliffa Stolla ilustruje bezpečnostní problémy tehdejších propojených systémů.
9. **Přechod na TCP/IP a vývoj IP** - Původní protokol NCP byl 1. ledna 1983 nahrazen sadou TCP/IP. IPv4 se stal základem dnešního internetu, ale jeho omezený adresní prostor se postupně vyčerpal. IPv6 nabízí výrazně větší počet adres, avšak není jen prodlouženou adresou IPv4 - jde o odlišný protokol s vlastními mechanismy, který musí být samostatně spravován a zabezpečen.
10. **Historie e-mailu** - E-mail vznikl v roce 1965 jako zasílání zpráv mezi uživateli jednoho počítače. Ray Tomlinson rozšířil systém na komunikaci mezi počítači a použil znak @ k oddělení uživatelského jména od názvu hostitele. První síťový e-mail byl odeslán v roce

1971 a formát i přenos zpráv se v letech 1973 až 1977 standardizovaly prostřednictvím dokumentů RFC.

11. **Gopher** - Služba Gopher od roku 1991 umožňovala publikovat, vyhledávat a získávat dokumenty pomocí textových menu a pevné hierarchie. V českém internetu bylo v roce 1994 více serverů Gopher než WWW. Její rozvoj však omezily licenční poplatky, rigidní struktura a pozdější začlenění podpory Gopheru do webových prohlížečů.
12. **Vznik World Wide Webu** - Tim Berners-Lee a Robert Cailliau v CERNu navrhli systém, který propojuje libovolné dokumenty hypertextovými odkazy. Do konce roku 1990 vznikly klíčové součásti webu: HTTP 0.9, jazyk HTML, prohlížeč WorldWideWeb, serverový software httpd a první webový server info.cern.ch. WWW uspěl díky volné organizaci dokumentů, jednoduchému HTML, obrázkům a možnosti obsah nejen číst, ale také vytvářet.
13. **Cloud computing** - Cloud přesunul provoz hardwaru a softwaru od jednotlivých firem k poskytovatelům sdílené infrastruktury. Nabízí virtuální stroje, databáze, distribuovaná úložiště, výkonné výpočty, hostované aplikace a API pro automatizované řízení infrastruktury. Jeho přínosem je rychlý začátek, pružné škálování a možnost dosáhnout vyšší dostupnosti bez budování několika vlastních datacenter.
14. **Internet věcí** - IoT rozšiřuje internetové připojení na senzory, domácí spotřebiče, automobily, zemědělské stroje a další zařízení. Umožňuje komunikaci stroj-stroj a vznik chytrých farem, měst či budov, ale současně zvyšuje nároky na adresování, spolehlivost, zabezpečení, ochranu soukromí a fyzickou bezpečnost.
15. **Internet v běžném životě** - Internet propojuje streamování, sociální sítě, navigaci, komunikační platformy, fotografie, videa, bankovníctví a další služby. Digitální a fyzický svět se tím těsně propojují a výpadek nebo zneužití internetové služby může mít přímé společenské, ekonomické i bezpečnostní následky.
16. **Hrozby a sledování** - Mezi hlavní rizika patří kybernetické útoky, krádeže identity, ransomware, DDoS, útoky na energetiku a vodohospodářství, sledování uživatelů a cenzura. Digitální stopa vzniká kombinací údajů ze sociálních sítí, reklamních systémů, zařízení, vozidel a komunikačních služeb, takže bezpečnost nelze oddělit od ochrany soukromí.
17. **Šifrování a metadata** - Moderní internet směřuje k šifrování komunikace pomocí HTTPS, VPN a dalších technologií. Šifrování chrání obsah, ale obvykle neskryje všechna metadata, například kdo, kdy, jak dlouho a s jakou službou komunikuje. Tor zvyšuje anonymitu směrováním provozu přes více uzlů, ani ten však automaticky nezaručuje úplnou anonymitu uživatele.
18. **Současné trendy a agentní systémy** - LLM a agentní AI se zapojují do celého životního cyklu informačních systémů: od analýzy požadavků a návrhu přes tvorbu kódu, testů a dokumentace až po threat modeling, analýzu logů a třídění incidentů. Stejně schopnosti lze využít i k útoku. Novými riziky jsou zejména prompt injection, únik dat, nadměrná oprávnění, chybné použití nástrojů a ztráta přehledu nad činností autonomnějšího agenta.

Co nenajdete v prezentaci

1. **Interaktivní a zážitkové pojetí výuky** - Smyslem společných hodin není pouze zopakovat teorii dostupnou v online zdrojích, ale diskutovat praktické zkušenosti, provozní souvislosti a rozdíly mezi teorií a reálným vývojem. Studenti mají aktivně klást otázky a projít si celý proces vzniku systému od návrhu téměř po nasazení a prezentaci.

2. **Propojení projektu s kyberbezpečností** - Aplikace vytvořená v KKY/ITE bude provozována na virtuálním stroji, zatímco v navazujícím předmětu se studenti věnují jeho nastavení, nasazení a zabezpečení. Obě části tak společně pokrývají softwarový vývoj i ochranu výsledného systému.
3. **Praktický pracovní postup s agentní AI** - Doporučený postup nezačíná okamžitým generováním kódu. Nejprve je vhodné s agentem rozpracovat požadavky, varianty architektury a specifikaci, nechat návrh kritizovat, připravit jednotkové, integrační i akceptační testy a teprve poté přejít k implementaci. Agent má fungovat také jako nezávislý partner pro revizi, nikoli jako nekontrolovaný autor výsledku.
4. **Význam čtení a vysvětlování kódu** - S rostoucí schopností nástrojů kód vytvářet se zvyšuje význam schopnosti cizí kód přečíst, vysvětlit jeho chování, rozpoznat architektonické vztahy a bezpečně jej upravit. Tato dovednost zůstává důležitá i při zkoušce a při obhajobě semestrální práce.
5. **Odhalování skrytých chyb v dlouhodobě udržovaném softwaru** - Na příkladu staršího systému zaznělo, že agent dokázal navrhnout opravu vzácné souběžné chyby a současně odhalil záměnu sekund a milisekund, kvůli níž se úklidová operace spouštěla tisíckrát častěji. Přínos AI tak může spočívat i v procházení historického kódu a hledání problémů mimo původní zadání.
6. **Důsledky nedostatku IPv4 adres** - Uživatel bez veřejné IPv4 adresy nemůže jednoduše přijímat přímá spojení a komunikace dvou takových sítí často vyžaduje veřejně dostupného prostředníka. Tím se oslabuje původní princip přímé komunikace každého s každým. Při souběžném provozu IPv4 a IPv6 je navíc nutné samostatně nastavit zabezpečení obou protokolů, jinak může služba zůstat dostupná nechráněnou cestou.
7. **Dnešní vnitřní podoba e-mailu** - Původní jednoduchá zpráva s několika hlavičkami a textovým tělem se rozrostla o kódování národních znaků, alternativní HTML část a ochranné mechanismy. SPF určuje, které servery smějí odesílat poštu za danou doménu, a DKIM umožňuje ověřovat digitální podpis zprávy. Správná správa poštovního serveru je proto výrazně složitější než původní návrh.
8. **Ekonomika vzniku veřejného cloudu** - Amazon potřeboval velkou výpočetní kapacitu během předvánoční špičky a po zbytek roku měl část infrastruktury nevyužitou. Nabídnutí této kapacity a interních nástrojů dalším zákazníkům pomohlo vytvořit model veřejného cloudu. Ve větším měřítku může být i drahá cloudová služba levnější než vlastní redundantní datacentra, protože zahrnuje konektivitu, migraci služeb, úložiště i fyzickou obsluhu.
9. **Mesh síť Zigbee v chytré domácnosti** - Zařízení Zigbee nemusí mít přímý dosah k jednomu centrálnímu bodu, protože si zprávy mohou předávat přes více uzlů. Pro pokrytí budovy může být tato síťová topologie vhodnější než připojení každého zařízení přímo k Wi-Fi.
10. **Bezpečnost připojených vozidel a strojů** - Připojené automobily kombinují kamery, polohová data, další senzory a internetovou konektivitu, a mohou se tak stát sondou v citlivém prostředí. U autonomních nebo dálkově spravovaných zemědělských strojů se digitální útok může projevit také fyzickým pohybem či škodou. Posuzovat je proto nutné jako kybernetický i fyzický bezpečnostní problém.
11. **Pseudonymita a dlouhodobá dohledatelnost** - Tor ani kryptoměny samy o sobě nezaručují úplnou anonymitu. Záznamy síťového nebo transakčního provozu lze uchovávat, později spojovat s dalšími důkazy a zpětně přiřadit ke konkrétní osobě. Rozhodující není jen skrytí identity v jednom okamžiku, ale také stopy vznikající v delším čase.
12. **Proč se internet od počátku nešifroval** - Rané sítě tvořilo malé množství vzájemně se znajících institucí a šifrování bylo výpočetně nákladné. Návrháři proto obtížně předvíдали

přechod od desítek důvěryhodných systémů ke globální infrastruktuře se stovkami milionů zařízení. Dodatečné zavádění bezpečnosti je dnes obtížné právě kvůli této historické architektuře.

Důležité pojmy

- **Agentní AI** - Systém využívající model k plánování a provádění více krokových úloh, často s přístupem k souborům, nástrojům nebo externím službám.
- **API (Application Programming Interface)** - Rozhraní, přes které spolu softwarové systémy nebo jejich části programově komunikují.
- **ARPA/DARPA** - Americká agentura podporující pokročilý výzkum, která financovala vznik ARPANETu; dnešní název DARPA zdůrazňuje obranné zaměření.
- **ARPANET** - Raná paketová síť spuštěná v roce 1969, která propojila výzkumné instituce a stala se technologickým základem internetu.
- **AWS (Amazon Web Services)** - Veřejná cloudová platforma nabízející výpočetní výkon, úložiště, databáze a další infrastrukturní služby.
- **Cloud computing** - Poskytování výpočetních prostředků a softwarových služeb na vyžádání ze sdílené vzdálené infrastruktury.
- **DDoS (Distributed Denial of Service)** - Distribuovaný útok, který zahlcuje službu provozem z mnoha zdrojů a omezuje její dostupnost.
- **DKIM (DomainKeys Identified Mail)** - Mechanismus digitálního podepisování e-mailů, který pomáhá ověřit původ zprávy a neporušenost jejího obsahu.
- **E-mail** - Síťová služba pro asynchronní výměnu zpráv, jejíž adresa tradičně spojuje uživatelské jméno a doménu znakem @.
- **Gopher** - Předchůdce webu založený na textových menu a hierarchické organizaci dokumentů.
- **HTML (HyperText Markup Language)** - Značkovací jazyk popisující strukturu a obsah webových dokumentů.
- **HTTP/HTTPS** - Protokol pro přenos webového obsahu a jeho šifrovaná varianta chráněná pomocí TLS.
- **IoT (Internet of Things)** - Internet věcí, tedy síť senzorů, spotřebičů, strojů a dalších fyzických zařízení schopných komunikovat a sdílet data.
- **IPv4** - Čtvrtá verze internetového protokolu s omezeným adresním prostorem, která je stále nejrozšířenějším základem internetové komunikace.
- **IPv6** - Novější internetový protokol s výrazně větším adresním prostorem a vlastní sadou síťových mechanismů.
- **LLM (Large Language Model)** - Velký jazykový model schopný pracovat s přirozeným jazykem a podporovat analýzu, návrh, programování i další úlohy.
- **Metadata** - Údaje o komunikaci, například čas, účastníci, cílová služba nebo objem přenesených dat, nikoli samotný obsah zprávy.
- **MILNET** - Vojenská síť oddělená od ARPANETu v roce 1983.
- **MQTT (Message Queuing Telemetry Transport)** - Lehký komunikační protokol založený na publikování a odběru zpráv, často používaný v IoT.

- **NCP (Network Control Program)** - Původní komunikační protokol ARPANETu, který byl v roce 1983 nahrazen TCP/IP.
- **Paket** - Samostatně přenášený blok dat obsahující užitečný obsah i řídicí informace, například cílovou adresu.
- **Přepojování paketů** - Princip, při němž se zprávy dělí na pakety putující sítí nezávisle a skládají se až v cíli.
- **Prompt injection** - Útok nebo nežádoucí instrukce, které se snaží změnit chování AI systému a přimět jej k obcházení pravidel či zneužití nástrojů.
- **RAND Corporation** - Výzkumná organizace, která v 60. letech rozpracovala návrh decentralizované komunikační sítě odolné proti výpadkům.
- **Ransomware** - Škodlivý software nebo útok, který omezuje přístup k datům či systémům a požaduje výkupné.
- **RFC (Request for Comments)** - Publikovaný technický dokument používaný k návrhu a standardizaci internetových protokolů a formátů.
- **Robustnost** - Schopnost systému zachovat správnou funkci nebo se zotavit i při výpadku, chybě či neočekávaném zatížení.
- **SPF (Sender Policy Framework)** - E-mailový mechanismus určující, které servery jsou oprávněny odesílat poštu jménem konkrétní domény.
- **TCP/IP** - Rodina protokolů, která od roku 1983 tvoří základ komunikace v internetu.
- **Tor** - Síť směřující provoz přes více uzlů s cílem omezit možnost spojit uživatele s cílem jeho komunikace.
- **VPN (Virtual Private Network)** - Šifrované virtuální spojení, které chrání provoz mezi zařízením a vzdáleným bodem sítě.
- **World Wide Web (WWW)** - Hypertextový informační systém využívající prohlížeče, webové servery, HTML, URL a protokol HTTP.
- **Zigbee** - Bezdrátový protokol s nízkou spotřebou, který podporuje mesh síť a používá se například v chytrých domácnostech.