

ДОМАЋИ РАД

Предмет:

Историја и филозофија рачунарства

Тема:

Савремена историја рачунарства: друштвене мреже, приватност, безбедносни изазови

Професор: Студент:

др Сташа Вујичић Станковић Андреа Ђукановић 105/2020

Београд 2024.

# Кратка историја рачунарства од појаве првих електронских рачунара

Електронски рачунари се користе од краја 1930-их до данас. Један од првих електронских рачунара ABC[[1]](#footnote-1) направили су 1939. године Џон Атанасов, математичар и физизичар и његов асистент на факултету, Клифорд Бери. Ова машина је прва користила бинарни бројевни систем и електричне кондензаторе за складиштење битова (систем који се у својим савременим варијантама користи и данас у оквиру такозване DRAM меморије) и није била програмабилна. Користила се за решавање система линеарних једначина.

Крајем Другог светског рата, у Енглеској, у истраживачком центру „Блечли парк“ (Bletchley Park) где је радио и Алан Тјуринг, конструисан је рачунар Колос (Colossus) намењен дешифровању немачких порука. Рачунар је омогућио разбијање немачке шифре засноване на машини Енигма, захваљујући чему су савезници били у стању да прате комуникацију немачке подморничке флоте, што је значајно утицало на исход Другог светског рата.

Најзад, у периоду између 1943. и 1946. године, конструисан је **први електронски рачунар опште намене** – ENIAC[[2]](#footnote-2). Конструисао га је тим универзитета у Пенсилванији на челу са Џоном Моклијем и Џејем Екертом, у сарадњи са америчком војском. Овај рачунар је имао 1700 вакуумских цеви, дужину од 30 метара и тежину од 30 тонa. Рачунске операције извршавао је хиљаду пута брже од електромеханичких машина које су се до тада користиле. Основна сврха ENIAC-а било је рачунање трајекторије пројектила. Било је могуће репрограмирати га за друге задатке, али је то захтевало интервенције на преклопницима и кабловима које су могле да трају данима.

Потпуна концептуална промена дошла је са појавом рачунара који програме на основу којих раде чувају у меморији заједно са подацима — **рачунара са сачуваним програмима** (stored program computers). За зачетника овакве архитектуре сматра се амерички математичар Џон Фон Нојман. У оквиру ових рачунара, постоји јасна подела на хардвер и софтвер. 1945. године уследио је први представник Фон-Нојманове архитектуре, рачунар EDVAC[[3]](#footnote-3) који је користио бинарни запис бројева и могао да складишти хиљаду 44-битних података. Основни елементи оваквих рачунара су процесор (који се састоји од аритметичко-логичке јединице, контролне јединице и регистара) и главна меморија, који су међусобно повезани. Остале компоненте рачунара (нпр. улазно-излазне јединице, спољашње меморије и сл.) се сматрају помоћним и повезују се на централни део рачунара који чине процесор и главна меморија.

Модерни програмабилни рачунари се, према технологији коју су користили, могу груписати у четири генерације засноване на Фон Нојмановој архитектури:

* Прва генерација рачунара (1940-их до средине 1950-их):
  + Користили вакуумске цеви за логичке и меморијске функције
  + Веома скупи, велики, и захтевали су много електричне енергије
  + Примери: EDSAC, MESM, EDVAC, UNIVAC
* Друга генерација рачунара (средина 1950-их до средине 1960-их):
  + Користили транзисторе уместо вакуумских цеви, што је довело до мање величине, ниже цене и веће поузданости
  + Развијена су магнетна језгра за главну меморију
  + Примери: IBM 1401 и IBM 7090
* Трећа генерација рачунара (средина 1960-их до средине 1970-их):
  + Користили интегрисане структуре које су укључивале више транзистора на једном чипу
  + Развој оперативних система и употреба виших програмских језика
  + Примери укључују IBM 360 и DEC PDP-11
* Четврта генерација рачунара (од средине 1970-их до данас):
  + Користили микропроцесоре који су довели до минијатуризације и популаризације личних рачунара
  + Развој рачунарских мрежа, интернета и мобилне технологије
  + Примери укључују IBM PC, Apple Macintosh и модерне PC, лаптоп и мобилне уређаје

Тржиштем данашњих рачунара доминирају рачунари засновани на PC архитектури и Apple Mac рачунари. Поред стоних (desktop) рачунара, популарни су и преносни (notebook или laptop) рачунари, а неизоставни су таблет уређаји и паметни телефони (smartphone).

Области савременог рачунарства:

* Алгоритмика (процеси израчунавања и њихова сложеност);
* Структуре података (репрезентовање и обрада података);
* Програмски језици (дизајн и анализа својстава формалних језика за описивање алгоритама);
* Програмирање (процес записивања алгоритама у неком програмском језику);
* Софтверско инжењерство (процес дизајнирања, развоја и тестирања програма);
* Превођење програмских језика (ефикасно превођење виших програмских језика, обично на машински језик);
* Оперативни системи (системи за управљање рачунаром и програмима);
* Мрежно рачунарство (алгоритми и протоколи за комуникацију између рачунара);
* Примене (дизајн и развој софтвера за свакодневну употребу);
* Истраживање података (проналажење релевантних информација у великим скуповима података);
* Вештачка интелигенција (решавање проблема у којима се јавља комбинаторна експлозија);
* Роботика (алгоритми за контролу понашања робота);
* Рачунарска графика (анализа и синтеза слика и анимација);
* Криптографија (алгоритми за заштиту приватности података);
* Теоријско рачунарство (теоријске основе израчунавања, рачунарска математика, верификација софтвера, итд).

# Друштвене мреже

Друштвене мреже представљају онлајн заједнице људи који размењују поруке, деле информације и сарађују на заједничким активностима. Чланови креирају и одржавају личне профиле које повезују са профилима других чланова. Настала мрежа „пријатеља“ или „контаката“ који деле сличне интересе, пословне циљеве или академске курсеве заменила је за многе људе, посебно младе, старе концепте заједнице. У почетку, друштвене мреже су омогућавале пријатељима да коментаришу профиле једни другима, шаљу приватне поруке унутар мреже и разгледају мрежу пријатеља видљивих на профилу осталих чланова. Касније је омогућено члановима да унапреде своје профиле разним мултимедијалним садржајем.

Прве онлајн друштвене мреже настале су чим је технологија могла да их подржи. Електронска пошта и програми за четовање су се појавили почетком 1970-их, али праве заједнице су настале тек стварањем Јузнета (USENET) 1979. године. Јузнет је почео као систем за обавештавање између Дјук универзитета и Универзитета Северне Каролине, али се брзо проширио на друге америчке универзитете и владине агенције. Омогућио је корисницима да објављују и примају поруке у оквиру тематских области (newsgroups). Заједно са њим и други форуми за дискусије омогућили су људима да комуницирају у онлајн друштвеним мрежама, али сваки од њих је био суштински засебан систем. Са појавом Мозаик (Mosaic) веб прегледача 1993. године, ти системи су спојени са лаким графичким интерфејсом за коришћење.

Прве компаније које су креирале друштвене мреже базиране на веб технологији биле су Classmates.com и SixDegrees.com. Classmates.com, основан 1995. године, користио је агресивну кампању појављивања „pop-up“ прозора како би привукли веб сурфере на свој сајт. Базирао је своју друштвену мрежу на постојећим везама између чланова средњошколских и факултетских генерација, војних одељења и радних места. SixDegrees.com био је **прва права друштвена мрежа**. Покренут је 1997. године са већином функција које ће касније карактерисати такве сајтове: чланови су могли да креирају профиле, имају пријатеље и контактирају једни друге путем приватног система порука на сајту. SixDegrees.com тврдио је да је до 2000. године привукао више од три милиона корисника, али није успео да те бројке претвори у приход и пропао је заједно са многим другим dot-com фирмама у том периоду.

Други су брзо препознали потенцијал оваквих сајтова, па је настао Фендстер (Friendster) 2002. године са почетним циљем да конкурише популарним сајтовима за упознавање који су захтевали плаћање чланарине као што је Match.com. Међутим, убрзо је доживео велику популарност. Ипак, сервери сајта нису могли да издрже изненадни пораст саобраћаја, па је често долазило до прекида у раду. Члановима додатно није одговарало што је сајт почео масовно да затвара лажне профиле (као на пример профил за Исуса Христа или ликове из серија).

Због свега наведеног Френдстер је убрзо заменио МајСпејс (MySpace) настао 2003. године. Док је први, као сајт за упознавање, првобитно привлачио старију публику, други је активно циљао младе људе. Брзо је постао место где се рок бендови повезују са фановима и премијерно представљају нову музику. За разлику од Френдстерa, МајСпејс је имао инфраструктуру која је подржавала његов експлозивни раст, па су се чланови придруживали у милионима. *News Corporation Ltd.* (компанија за управљање медијима основана од стране аустралијског предузетника Руперта Мурдока) га је купио 2005. године, а велика популарност сајта довела је до проблема због правних органа који су били забринути за безбедност огромне популације малолетника.

Страх од онлајн предатора мало је утицао на број чланова (који је достигао 70 милиона активних месечних корисника у 2007. години), али је отворио врата другим друштвеним мрежама. 2004. године Марк Закерберг, Едуард Саверин, Дастин Московиц и Крис Хјуз на Харварду оснивају Фејсбук (Facebook), који је првобитно био академски оријентисана алтернатива МајСпејсу, али је 2006. пружио могућнст свим старосним групама преко 13 година и превазишао МајСпејс као најпопуларнију друштвену мрежу 2008.

Тренутно, најпопуларније друштвене мреже у свету су Фејсбук, Инстаграм (Instagram), Икс (X, бивше Twitter), ЛинкдИн (LinkedIn), Јутјуб (YouTube), Снепчет (Snapchat) и Тик-ток (TikTok). Фејсбук је и даље најпосећенија мрежа са преко три милијарде корисника. *Meta Platforms*, компанија која је његов власник, такође поседује Инстаграм, Воцап (WhatsApp) и Фејсбук Месинџер (Facebook Messenger). Тик-ток, који је постао глобални хит последњих година, посебно је популаран међу младима. ЛинкдИн је остао водећа мрежа за професионалне контакте, са преко 675 милиона корисника широм света.

Друштвене мреже су постале кључне тачке за дигитални маркетинг и оглашавање, привлачећи пажњу како корисника тако и маркетиншких стручњака. Већ дуго представљају витални део свакодневног живота милијарди људи широм света, мењајући начин комуникације, забаве и пословања. Забринутост у вези са могућим негативним ефектима друштвених мрежа такође расте у складу са развојем технологије. На пример, неки стручњаци сматрају да оне подстичу дехуманизацију која се дешава када се комуницира преко екрана на рачунарима и мобилним уређајима. Истраживања такође указују на јаку повезаност између велике употребе друштвених мрежа и повећане депресије, анксиозности, самоће, тенденција ка самоубилачким понашањима и осећаја неприпадности.

# Приватност и безбедност на друштвеним мрежама

Популарност друштвених мрежа поред свих предности, ствара велики ризик за њихове кориснике. Велика количина личних података које корисници деле чини их метама за разне нападе. Нападачи могу добити осетљиве личне податке и могу их злоупотребити на много начина. Овакви напади укључују спам, злонамерни софтвер и крађу идентитета. Осим тога, они могу пронаћи друге значајне податке, као што су информације о банковним рачунима што може довести до значајних последица. Добро осмишљен напад може угрозити чак и велика предузећа.

На многим друштвеним мрежама, као што је Фејсбук, преовладавају мултимедијални садржаји који се производе и деле. Сваких 60 секунди се постави преко 240.000 фотографија. Просечна стопа гледања и дељења видеа на Фејсбуку повећава се из дана у дан. Због великог обима мултимедијалних података, безбедносни ризици такође се повећавају. Корисници могу да деле злонамерне информације на друштвеним мрежама тако што ће их сакрити унутар мултимедијалних садржаја. Поред тога, овако нападач може лако пронаћи осетљиве информације, као што су идентитет и локација.

У 2005. години, Мајспејс је напао вирус „Samy worm”, који се преносио веома брзо. Није крао личне податке корисника, али је имао опасан ефекат на општу безбедност ове мреже. Носио је садржај који би на профилу жртве приказао поруку „but most of all, samy is my hero“ и послао захтев за пријатељство Семију. Када би други корисник отворио тај профил, садржај би се копирао и поставио на њихов профил, настављајући ширење вируса. Мајспејс је од тада појачао безбедност свог сајта. У априлу 2009. године, (тадашњи) Твитер је напао вирус „Mikeyy“, који такође није крао личне информације корисника, већ је заменио њихове податке са неким неупотребљивим подацима. У мају 2009. године, Фејсбук је напао вирус „Koobface“, који је крао осетљиве податке, као што је лозинка. Чак је и сам извршни директор Фејсбука, Марк Закерберг, био жртва хакерског напада 2015. године, када је нападач користио његову ЛинкдИн лозинку "dadada" како би приступио налозима на Пинтрасту (Pinterest) и (тадашњем) Твитеру.

Са порастом напада, многи стручњаци су предложили различита решења како би заштитили кориснике друштвених мрежа од претњи изазваних мултимедијалним подацима, као што су увођење дигиталних водених жигова (watermarking) и стеганализа (steganalysis). Детекција спама и детекција фишинга (phishing) користе се за ублажавање традиционалних претњи. Међутим, многа уграђена сигурносна решења, као што су механизми аутентификације и поставке приватности, као и комерцијална решења, као што су надгледање малолетника (minor monitor) и апликације за друштвену заштиту (social protection applications), такође служе као заштита од оба типа претњи на друштвеним мрежама.

Безбедносне претње на мрежама можемо класификовати на следећи начин:

* **Претња од мултимедијалног садржаја**
  + Изложеност мултимедијалном садржају
  + Заједничко власништво
  + Манипулација мултимедијалног садржаја
  + Стеганографија (корисници могу да деле злонамерне информације скривене у мултимедијалном садржају, као што су слике)
  + Метаподаци (мултимедијални садржаји су као метаподаци јер могу открити друге важне податке као што су ЈМБГ и локација)
  + Дељење веза ка мултимедијалном садржају
  + „Outsourcing“ и транспарентност дата центара (мултимедијални подаци који се чувају на мрежама нису енкриптовани, што омогућава злонамерним корисницима да приступе подацима без ауторизације)
  + Видео позиви
  + Таговање (означавање)
  + Недозвољено дељење података
* **Традиционалне претње**
  + Фишинг (phishing)
  + Малвер
  + Лажни профил
  + Спам
  + Кликџекинг (нападачи сакривају злонамерне апликације иза корисничких интерфејса или дугмића како би кликове корисника злоупотребили их у своје циљеве)
  + Откривање идентитета
  + Лажно представљање
* **Социјалне претње**
  + Онлајн злостављање и манипулација (децом)
  + Злоупотреба података унутар компанија
  + Ухођење на интернету

Постоје разни начини за решавање оваквих проблема:

1. Увођење дигиталних водених жигова (watermarking): метода у којој се подаци уграђују у медијски садржај како би се доказало власништво над тим садржајем.
2. Заједничко власништво (co-ownership): омогућава више корисника да примене своја подешавања приватности на заједничке видео записе и слике.
3. Стеганализа (steganalysis): механизам за откривање злонамерних информација унутар мултимедијалних података.
4. Дигитално заборављање (digital oblivion): постављање временског ограничења на дигиталне податке како би се спречило приступање тим подацима након истека времена.
5. Енкрипција складиштења (storage encryption): омогућава корисницима ефикасно чување и повратак података без излагања тих података услугама трећих страна
6. Уклањање метаподатака и њихова заштита
7. Детекција злонамерног софтвера
8. Детекција лажних профила
9. Детекција фишинга
10. Детекција спамера: издвајање скупа карактеристика којима разликујемо спам кориснике од легитимних корисника.
11. Комерцијална решења: различити производи развијени од стране безбедносних компанија за заштиту корисника (Diego Casorran, Net Nanny, McAfee, Kaspersky...)
12. Уграђена решења за безбедност: подешавања приватности корисника, механизми ауторизације, пријава злоупотребљеног садржаја.
13. Препознавање лажних профила: развој функције која аутоматски открива клониране профиле на основу препозавања ликова и обавештава кориснике о њима

Друштвене мреже омогућиле су нам начин комуникације који је некад био незамислив. Повезаност са породицом и пријатељима широм света, брз приступ информацијама, могућност другачијег образовања, политички активизам, лакша потрага за послом и сл, отварају нове могућности у животу и раду. Ово представља не само технолошки напредак, већ и средство за подизање свести, учешће у заједници и лични развој. Међутим, важно је препознати и управљати потенцијалним изазовима које оваква повезаност може донети и користити ове алате на етичан и одговоран начин. Са порастом корисника друштвених мрежа свих узраста, порастао је и број оних који би то да злоупотребе. Безбедност на друштвеним мрежама представља значајан изазов у савременом друштву. Као што је поменуто, напади полазе од безазлених спам порука или лажних профила, до озбиљних проблема попут циљаног таргетирања деце и младих у злонамерне сврхе. Образовање и ширење свести о безбедности на интернету од изузетног су значаја у заштити корисника од потенцијалних опасности које могу настати на друштвеним мрежама.

# ЛИТЕРАТУРА

1. *др Филип Марић, др Предраг Јаничић: Прогрмирање 1*, Математички факултет Универзитета у Београду, 2024
2. www.britannica.com
3. Social network security: Issues, challenges, threats, and solutions - *Shailendra Rathore, Pradip Kumar Sharma, Vincenzo Loia, Young-Sik Jeong, Jong Hyuk Park: Information Sciences*, 2017

1. Atanasoff-Berry Computer [↑](#footnote-ref-1)
2. Electronic Numerical Integrator and Calculator [↑](#footnote-ref-2)
3. Electronic Discrete Variable Automatic Computer [↑](#footnote-ref-3)