Паметне куће: Колико су безбедни Ваши подаци?

Семинарски рад у оквиру курса
Рачунарство и друштво
Математички факултет

Тамара Ђукић
tamarazdjukic@gmail.com

24. мај 2022.

Абстракт

Брз технолошки напредак, све већа дигитализација и све већи токови података. Идеја о повезаној „паметној“ кући је све више актуелнија и примамљивија него икада. Али шта тачно значи паметна кућа? Где леже корени ове технологије? Које су користи и ризици? Како ће изгледати паметна кућа у будућности? На нека од ових питања ћемо одговорити у наставку текста.

Садржај

1 Увод

Паметне куће се дефинишу као куће у којима су присутни паметни уређаји. То могу бити апарати за кафу, усисивачи или дигитални асистенти који се активирају гласом [1]. Паметни уређаји се рекламирају потрошачима због своје погодности [2]. Они су дизајнирани да буду једноставни за употребу [3].
Уређаји у паметној кући су међусобно повезани и може им се приступити преко једне централне тачке - паметног телефона, таблета, лаптопа, итд. Преко система који је инсталиран на централном уређају, корисник може да креира временске распореде када ће се нешто обавити. Паметни уређаји долазе са вештинама самоучења како би могли да науче распореде власника куће и по потреби врше прилагођавања.

Слика 1: Приказ паметне куће

Због недавног напретка технологије, све је више савета о дигиталној безбедности и о томе како остати безбедан на интернету. Да би се овај савет проширио на све слојеве друштва, он није намењен само деци, већ и одраслима. Технологија се стално развија и мења, па се као резултат тога, дигиталне безбедносне претње могу јавити много брже него што су појединци раније били навикнути када је у питању лична безбедност. Како ове претње нису физичке, постоји ризик да буду схваћене мање озбиљно. Такође може доћи до неспоразума о томе шта је тачно претња. То је делимично зато што појединци могу пренети менталне моделе физичке сигурности на дигиталну сигурност, што их доводи до погрешних очекивања о природи и последицама претњи са којима се могу суочити.

Међутим, важно је дигиталну сигурност схватити једнако озбиљно као и физичку. Ово је посебно важно у контексту паметне куће. Постоје два примарна проблема при увођењу паметних уређаја у дом:

- Паметни уређај је безбедан, али није сигуран - уређај има неефикасну безбедност, на пример уређај се може лако хаковати
- Паметни уређај је сигуран, али корисници немају контролу над подацима - корисницима се манипулише како би произвођачима

омогућили приступ више података него што заиста су желели да поделе

2 Паметни уређај је безбедан, али није сигуран

У случајевима када обезбеђена заштита није довољна, долази до проблема јер постоји разлика између менталних модела корисника и дизајнера уређаја. Корисници могу да верују овим уређајима зато што верују компанији која их производи, дизајнеру уређаја или зато што нису свесни који подаци могу бити прикупљени. Ово се често компликује чињеницом да многи корисници претпостављају да су приватност и безбедност синоними. Пошто подаци могу бити шифровани и безбедни од хакера, корисници могу претпоставити да су и поверљиви. То није нужно случај. Нарочито код виртуелних помоћника који се активирају гласом (нпр. Amazon Alexa, Google Assistant), подаци се могу послати у центре за обраду или чак ненамерно послати контактима [4] [5]. Када дође до таквих повреда, корисници се могу осећати изданим од стране ових уређаја и нерадо их користе јер су изградили погрешан ментални модел како уређај функционише.

Раздвајање сигурности од погодности отежава просечном кориснику да одреди колико је сигуран одређени паметан уређај.

Док су корисници упознати са обезбеђивањем физичке безбедности својих домова како би се заштитили, дигитална безбедност је релативно нов концепт. Упркос едукацији о овој теми, корисници могу претпоставити да је уређај сигурнији него што јесте јер можда не узимају у обзир како је сваки појединачни уређај повезан у њиховом дому, само да су уређаји у самом дому сигурни (да их је тешко украсти).

За већину корисника лакше је размишљати о физичкој безбедности него о дигиталној. У друштву је укорењено да власници кућа морају закључати врата и прозоре како би спречили провале. Да би то урадили, могу да купе браве и аларме, које након постављања треба само да одржавају. Ментални модел кућне сигурности је да брава или алармни систем након куповине функционишу првенствено сами. Не треба га редовно прегледавати или ажурирати и његово радно стање се лако може проверити погледом или додиром. Овај модел се може погрешно пренети на дигиталну безбедност.

Дигитална безбедност захтева сталну обазривост. Технологија је новија и стално се мења, тако да корисници паметних уређаја морају редовно да проверавају да ли постоје безбедносни пропусти и ажурирања. Сваки уређај представља потенцијалну улазну тачку у кућну мрежу корисника, а чињеница да су сви уређаји међусобно повезани значи да без довољно сигурности за сваки уређај, било који од њих може да се користи за приступ информацијама које се налазе у другим деловима система. Ово је посебно проблем када корисници уводе паметне уређаје као што су усисивачи који се раније нису сматрали безбедносном претњом. Ови уређаји су нови на тржишту, лако доступни и јефтини. Као резултат тога, они не морају нужно бити сигурни [6].

3 Паметни уређај је сигуран, али корисници немају контролу над подацима

Што се тиче другог питања, где паметан уређај може бити довољно безбедан, али се корисницима манипулише тако да произвођачима дозволе приступ већем броју података него што желе да поделе. Увођење Опште уредбе о заштити података ОУЗП (General Data Protection Regulation GDPR) је значајно помогло у регулисању контроле података, посебно са приватношћу и сигурношћу [7]. Добар је као метод контроле, посебно када омогућава корисницима да лако разумеју и контролишу своје податке. Али у стварности, тешко је проценити колико су корисници свесни шта се дешава са њиховим подацима јер нису били у могућности или не разумеју споразуме које склапају са технолошким компанијама. ОУЗП је ставио велики терет на компаније да избришу и контролишу податке од којих су раније можда остваривале профит. Није у њиховом интересу да дозволе корисницима да одустану од дељења својих личних података. Као резултат, прибегавају манипулацији корисницима како би задржали своје податке.

Пример за то је компанија Фејсбук. Фејсбук је већ неколико пута био ухваћен у прикупљању више података него што су корисници желели да поделе. Један од примера је да је друштвена мрежа имала посебне аранжмане са више од 150 компанија за размену личних података својих чланова. Речено је да су већина њих друге технолошке компаније, али на списку су, између осталих, били и телефонски продавци, произвођачи аутомобила и медијске организације. Фејсбук је сада прибегао коришћењу мрачних образаца корисничког искуства (UX) дизајнирани тако да се придржава ОУЗП и прикупља жељене податке. Тамни обрасци се дефинишу као ситуације у којима „дизајнери користе своје знање о људском понашању (нпр. психологија) и жеље крајњих корисника да примене варљиву функционалност која није у најбољем интересу корисника“ [8]. Ово може бити у облику сакривања опција, додавања куповина или трошкова у последњем тренутку у корпе за куповину или употребе трик питања како би убедили кориснике да изаберу опције које иначе не би одабрали.

Употреба тамних образаца у UX дизајну није специфична само за Фејсбук. Тамни образци се лако имплементирају и широко су распрострањени. У овом тренутку једини начин борбе против њих, под условом да корисници желе да користе услуге које пружа дизајнер, је да истражу кроз опције читајући пажљиво. Реално, многи корисници то неће учинити. Количина напора која је потребна за борбу против мрачних образаца за сваку веб страницу и услугу навела би многе кориснике да једноставно заобиђу проблем и једноставно кликну на „прихвати“. Томе се надају дизајнери таквих интерфејса.

Такође је важно шта се дешава са прикупљеним подацима након што су прибављени од крајњег корисника. Без обзира да ли су подаци хаковани из несигурног система или уређаја, као у првом случају, или је корисник изманипулисан да се одрекне више података него што је намеравао, као у другом случају, крајњи резултат је исти. Компаније које су их прикупиле могу поново користити изворне податке или их продати трећим странама, а корисник нема контролу над овим,

или у неким случајевима чак и знање о томе. Све мере предострожности које се примењују од стране корисника могу само ограничити количину прикупљених података. Ради одговарајуће сигурности и приватности, овим питањима се морају позабавити произвођачи паметних уређаја и дизајнери њихових интерфејса.

У сценарију паметне куће, уместо да се мора ослањати на корисника да провери ниво безбедности паметних уређаја у свом дому, одговорност би требало да буде на произвођачу. Дизајн осетљив на вредност [9] и уговорни дизајн [10] су начини да заштите кориснике од нежељених последица коришћења технологије. ОУЗП је пример осигурања да корисници података и произвођачи технологије дизајном имплементирају приватност, и на неки начин безбедност података. Оно што је, међутим, потребно је ниво изнад овог. Потребан је етички дизајн који има на уму најбоље интересе корисника — избегавање тамних образаца и нуђење корисницима једноставних опција за њихову безбедност.

Произвођачи морају ставити своје кориснике на прво место и размотрити колико су њихови уређаји сигурни. Уређаји морају бити пројектовани имајући у виду концепт безбедности, како би се одговорило не само на питање „Може ли се неко идентификовати према овим подацима?“ али „Може ли се приступити овим подацима?“ и „Да ли би корисник желео да подели ове податке?“. С обзиром на брзину и разноликост развоја технологије, није увек одмах јасно у које сврхе се наизглед безазлени подаци могу користити у будућности. Неопходно је разговарати и применити заштитне мере за заштиту корисника данас од потенцијалних претњи сутрашњице.

4 Примери паметних уређаја

4.1 Паметан фрижидер

Паметан фрижидер је уређај који има могућност повезивања на интернет. У зависности од фрижидера који одаберете и бренда, паметан фрижидер може понудити неколико различитих практичних функција. Већина паметних фрижидера има могућност инсталирања апликације на мобилни телефон или друге уређаје како би омогућила власнику да види ажурирања на свом фрижидеру и када није кући.

Неке карактеристике паметних фрижидера:

Интерфејс екрана осетљивог на додир Екран осетљив на додир на паметном фрижидеру се може користити за приступ разним функцијама притиском на екран. Новији модели могу имати велики екран са рачунарском снагом сличној оној на Вашем лаптопу. Такође, паметан фрижидер може да има уграђене звучнике који могу побољшати искуство коришћења.

Могућност повезивања на интернет Паметан фрижидер има уграђен претраживач преко кога можемо да се повежемо на интернет и тражимо ствари које су нам потребне.

Унутрашња камера Унутрашња камера нам може омогућити да видимо шта се налази унутар фрижидера без да га сваки пут отварамо. Предност унутрашње камере је смањење трошкова

струје и храна се неће брзо кварити јер не улази топлота унутар фрижидера.

База рецепата Имамо могућност чувања рецепата са интернета. Такође, фрижидер нам може читати кораке за неки рецепт или можемо пустити видео који објашњава кораке рецепта.

4.2 Паметан усисивач

Роботски усисивач, који се некад назива робовак (Robovac), је самостални усисивач који има ограничен систем за усисавање подова у комбинацији са сензорима и роботским погонима са програмабилним контролерима и рутинама чишћења. Рани дизајни су укључивали ручно управљање путем даљинског управљача и режим „самовожње“ који је омогућавао машини да самостално чисти без људске контроле. Неки дизајни користе окретне четке да би досегнули уске углове, а неки укључују низ функција за (брисање, УВ стерилизација, итд.) чишћење заједно са функцијом усисавања. Новији модели користе вештачку интелигенцију и дубоко учење за боље мапирање, идентификацију објеката и чишћење на основу догађаја.

Неке карактеристике паметних усисивача:

Не морамо бити код куће да би кренуо да чисти Имати роботски усисивач у свом животу значи да никада не морамо да одвајамо време за усисавање куће. Могу се програмирати да обилазе кућу док нисмо кући. Такође, можемо правити распореде према коме ће он сам кренути са своје станице да чисти и када нисмо код куће.

Самостално се пуни Ови усисивачи се враћају на своју станицу ради поновног пуњења на крају сваког циклуса чишћења. Све док је њихова станица за пуњење укључена, никада не морамо да бринемо да ли ће се искључити током чишћења. Неки модели ће чак престати са чишћењем и вратити се на прикључну станицу ако открију да је батерија празна.

Флексибилни су за чишћење више врста површина Роботски усисивачи су дизајнирани да се прилагођавају различитим површинама помоћу својих сензора који детектују промене на подним површинама. Можемо их пустити да се крећу свуда по нашој кући и са лакоћом се носе са променама површине.

Уграђени сензори који детектују прљавштину на одређеном месту Роботски усисивачи имају уграђене сензоре који могу да открију који делови наше куће захтевају додатни рад, и усисивач ће након тога направити додатне пролазе преко тог подручја. Простори са великим прометом као што су ходници, улази и играонице добиће додатну пажњу која им је потребна да би били чисти.

4.3 Паметна камера

Паметне камере су типичне бежичне камере које раде више од снимања снимака и слика. Ови уређаји имају додатне функције које нам могу помоћи да пратимо статус своје куће чак и када смо удаљени хиљадама километара.

Неке карактеристике паметне камере:

Препознавање лица Способност паметне камере за препознавање лица је једна од најзначајнијих предности инсталирања овог типа система сајбер безбедности. Помоћу овог уређаја можемо да будемо сигурни да добијамо само упозорења за стварне претње тако што ћемо отпремити слике своје породице и пријатеља или их означити као несумњиве на снимку.

Комуникација Поред снимања слика, паметне камере су такође опремљене системима за аудио надзор који нам омогућавају да слушамо разговоре или пазимо на другу сумњиву буку у окружењу наше куће. Ако откријемо да се нешто лоше спрема у окружењу наше куће, можемо изненадити лопове тако што ћемо разговарати са њима и вербално их отерати како би помислили да сте у својој кући.

Детекција покрета Ови уређаји су опремљени сензорима који детектују кретање и аутоматски се крећу ка извору кретања. Затим ради са функцијом препознавања лица да идентификује да ли је особа споља пријатељ или непријатељ и да нас упозори на њено присуство путем апликације за паметне телефоне. Такође има ноћни вид како би били сигурни да је наша кућа заштићена током целог дана.

5 Предности и мане паметне куће

5.1 Предности

Паметне куће могу побољшати квалитет живота становника пружањем различитих услуга које му помажу у свакодневном животу.

Паметну кућу можемо да користимо за контролу окружења, она је аутоматизована контролом неких уређаја, попут оних који се користе за осветљење и грејање, на основу различитих климатских услова. Новије технологије омогућавају праћење унутрашњег окружења и активности корисника куће. Такође, могу независно да предузимају унапред програмиране радње ида управљају уређајима према унапред дефинисаним обрасцима, независно или према захтевима корисника.

Потпуна контрола свих паметних уређаја са једним паметним уређајем Ово значи да све док поседујемо паметан телефон или неки други паметан уређај и исправну интернет везу, већину уређаја у својој кући можемо контролисати са једне централне тачке. Ово нам даје потпуну контролу над нашом кућом и чак можемо да прилагодимо неколико подешавања у другим просторијама. Ако не желимо да идемо на неко место у кући да бисмо променили подешавања уређаја, можемо то да урадимо директно са свог места због софистицираног међусобног повезивања кућних апарата.

Обавештења у случају опасности Паметне куће нам такође омогућавају да будемо обавештени у случају да постоје проблеми са нашом кућом. На пример, ако неко покуша да нам насилно уђе

у кућу, добићемо обавештење на паметном телефону да је неовлашћена особа на нашем имању. Ово може помоћи да се ухвати лопов јер полиција може бити обавештена у реалном времену.

Уштеда времена Пошто се са једним паметним уређајем могу контролисати сви паметни уређаји у нашој кући, вероватно ћемо на дуже време уштедети доста времена. Не морамо бити физички присутни кући да би кренула нека радња да се одвија. Потребно је само да дамо команду, и да наставимо да радимо нешто друго. Ово доста помаже људима који немају пуно времена.

5.2 Мане

Свака паметна кућа има доста добрих предности, али увек постоје мане које могу бити мање или више опасне.

Значајни трошкови инсталације Један недостатак паметних кућа је то што могу бити прилично скупе. Могу постојати значајни трошкови инсталације који могу износити више хиљада долара. У зависности од квалитета система, можда чак и нема ограничења и многи људи можда неће бити вољни да потроше ову количину новца на свој дом. Међутим, паметне куће нам такође могу уштедети новац на дуге стазе због уштеде енергије.

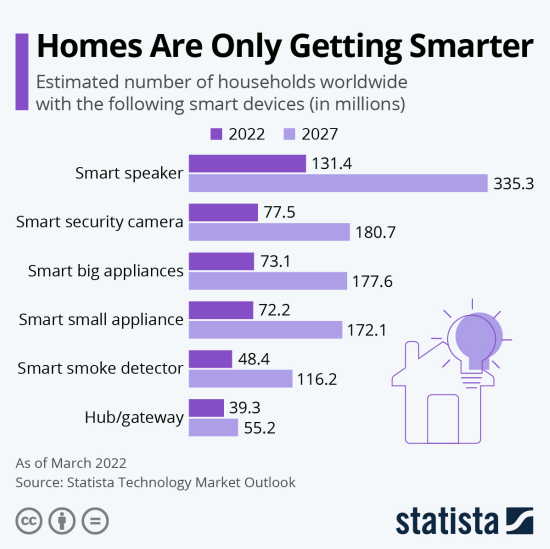
Поуздана интернет мрежа Још једна мана паметних кућа је да им је потребна поуздана интернет веза да би исправно радиле. На пример, ако живимо у области где је интернет веза прилично лоша, можда ћемо имати озбиљне проблеме јер наши паметни кућни уређаји можда неће реаговати на начин на који желимо.

Брига о безбедности Такође постоје и неки безбедносни проблеми повезани са технологијама паметних кућа. На пример, провалници би могли да хакују у наш систем паметне куће и отворе браву како би добили приступ нашем дому. Постоји могућност и да хакери упадну у наш систем и да нам украду све личне податке, или да виде када нисмо код куће да би могли да нам провале у кућу.

Беспомоћност ако технологија откаже Наш технолошки напредак се може сматрати добрим јер може побољшати квалитет живота сваког од нас. Међутим, постоје и неки проблеми у вези са технологијом. На пример, можда ћемо бити прилично беспомоћни ако наша технологија паметне куће откаже. Пошто смо се увек ослањали на ову технологију да функционише и прилагодили своје понашање, можда ћемо се осећати изгубљено у случају да наша технологија паметне куће више неће радити.

Није погодна за све домове Многи људи једноставно не воле идеју о паметном кући. Поготово старија генерација која је прилично скептична по питању тога. Пошто често чујемо о слабостима тих система који провалницима олакшавају улазак у нашу кућу, многи људи се могу уздржати од тих технологија паметних кућа и радије се ослањају на своје браве старе школе, чак и ако су те браве такође прилично несигурне.

6 Статистике



Слика 2: Статистике колико се данас користе паметни уређаји, и колико ће се користити у будућности

Неке занимљиве статистике:

- До 2023. године, аутоматизација индустрије паметних кућа у америчким домовима биће 53,9%
- Статистике показују да ће глобално тржиште паметних домова у 2022. години износити 53,5 милијарди долара
- Са обимом продаје од 23 милијарде долара, Сједињене Америчке Државе су највећи потрошач паметних технологија
- Пројекције показују да ће продор паметних звучника порасти за 55% до 2022. године
- Процене показују да ће домаћинства потрошити 19,4 милијарде долара на куповину паметних безбедносних система

7 Закључак

У овом раду поменули смо неке од позитивних и негативних страна паметне куће. Паметне куће могу да нам живот учине много једноставнијим, поготово у областима здравствене неге, али долазе и са одређеним ризицима. Ако корисници са опрезом и разумевањем рукују паметним уређајима, негативне стране ће постати скоро занемарљиве. Када би посматрали паметне куће са стране етике утилитаризма правила, где је нагласак на укупној срећи а не на томе шта се дешава појединачним учесницима, дошли би до закључка да паметне куће доносе добро. Поготово ако узмемо у обзир да део корисника и није свестан свих (или је одлучан да их игнорише) негативних аспеката паметних кућа.

Литература

[1] "Smart Appliances (worldwide)," Statista (online), 2019. [Online]. Available: https://www.statista.com/outlook/389/100/smart-appliances/worldwide.

[2] J. Robbins, *"If technology is a parasite masquerading as a symbiont – Are We the Host?," IEEE Technol. Soc. Mag., vol. 38, no. 3, pp. 24–33, Sep. 2019.*

[3] "Amazon Alexa vs Google Assistant: Which voice assistant should you get?," Which? (online), 2019. [Online].Available: https://www.which.co.uk/news/2019/11/amazon-alexa-vs-google-assistant-which-ai-helper-is-the-best-for-black-friday/. [Accessed: 29-Nov-2019].

[4] L. Temple, *"How new guidelines on smart devices will help protect consumers from being hacked," Which? (online), 2018.*

[5] A. Woodruff, S. E. Fox, S. Rousso-Schindler, and J. Warshaw, *"A qualitative exploration of perceptions of algorithmic fairness," in Proc. 36th ACM Conf. Hum. Factors Comput. Syst., pp. 1–14, 2018.*

[6] A. Laughlin, *"The cheap security cameras inviting hackers into your home," Which? (online), 2019*

[7] ICO, emph"Guide to the General Data Protection Regulation (GDPR)," Information Commissioner's Office (online), 2018. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/. [Accessed: 27-Jun-2018].

[8] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt and A. L. Toombs *"The Dark (Patterns) side of UX Design," in Proc. 2018 CHI Conference on Human Factors in Computing Systems - CHI '18, 2018, Apr. 2018, pp.1–14.*

[9] B. Friedman and P. Kahn, *"Value sensitive design: Theory and methods," Univ. Washingt. Tech., pp. 1–8, Dec. 2002.*

[10] J. Pitt, *"Design contractualism for pervasive/affective computing," Technol. Soc. Mag. IEEE, vol. 31, no. 4, pp. 22–29, 2012.*