КИБЕРСИГУРНОСТ В "УМНИТЕ КЪЩИ"

ДОЦ. Д-Р ЛЮБЕН БОЯНОВ[1]

Абстракт: Навлизането на дигиталните технологии във всички сфери на обществото доведоха от една страна до значимо подобряване на условията за работа и живот благодарение тези технологии, а от друга – породиха редица проблеми, произтичащи от появяващата се зависимост на хората от същите тези технологии. Един от най-сериозните проблеми в съвременното дигитално общество е този за киберсигурността. Върху него се работи от много време насам, но поради сравнително ограниченият обхват на приложение на дигиталните технологии до скоро, той не криеше сериозни опасности за живота и средата на хората. В последните години дигиталната технология се появява и налага своите удобства все по-често в места, които са критични за хората – здравеопазването, дома, околната среда и др. Настоящата статия обръща внимание на киберзаплахите в т.нар. „умни къщи", като представя възможните заплахи и ги класифицира. Представени са различните начини за въздействие на недоброжелатели върху умните къщи и е описан проект, по който се работи у нас във връзка с предотвратяване на киберзаплахи в такава среда.

Въведение

От началото на 21 век се наблюдава повсеместно дигитализиране на нашия свят. То започна с масовото използване на персонални компютри, интернет, мобилни телефони, смартфони, таблети, безжични мрежи, и т.н. Развитието на електрониката и сензорните технологии доведоха до създаване и разпространение на малки, евтини и автономни безжични сензори и на пасивни и активни „идентификатори" от типа RFID. Всичко това намери място и в нашия дом, който с всеки изминал ден се превръща все повече в „умна къща". Този термин се употребява за жилища, в които са изградени системи за контрол, автоматизиране и оптимизиране управлението на:

- средата в дома (температура, влажност, чистота на въздуха, осветление, и т.н.);
- сигурността и безопасността в дома (аларма, възникване на пожар, изпускане на газ и т.н.);
- наблюдението на живущите в дома и тяхното здраве (деца, възрастни и болни);
- домашните уреди (климатик, печка, пералня, хладилник, телевизор и т.н.)
- разхода на енергия и други ресурси от бита (ток, газ, вода и т.н.)

Умните къщи до скоро бяха само за много заможни хора или чудаци, създаващи си различни удобства в дома, но съвременната тенденция е в друга посока. Например в САЩ през 2012 г са били инсталирани 1.5 милиона системи за автоматизация на дома, което е 2 пъти повече от 2011, като тендецията е този брой да нарасне на 8 милиона през 2017 г. [1]. Някои големи американски фирми вече предлагат интегрирани решения в това отношение [2]. Друга сериозна причина да очакваме нарастване на използването на новите технологии в дома е увеличаващата се цена на енергията и нарастващите екологични изисквания. Изследванията сочат, че е възможно едно средностатистическо домакинство да намали въглеродните си емисии със 71% , а годишните си разходи за енергия да станат два пъти по-ниски [3].

С развитието и навлизането на новите технологии, все по-голяма значимост придоби и осигуряването на сигурност от заплахите, произтичащи от тези технологии – т.нар. киберзаплахи. Проблемите с киберсигурността се отнасят към обема и произхода

[1] *Институт по информационни и комуникационни технологии – Българска академия на науките*

на данните в Интернет, мобилните устройства, различните устройства, свързани в мрежата и предоставяни услуги [4].

През последните години използването на компютри и Интернет в дома нарастна значително – според последните публикувани данни, в България над 50% от домакинствата у нас ползват Интернет, а 91% от използващите компютри правят това от дома [5]. Повече от половината от потребителите срещат проблеми при работата със световната мрежа, като само около 70% от тях ползват някакви средства за защита [5].

За разлика от служебното място, където има специалист по информационни технологии (системен администратор, а някъде и отдели по информационно осигуряване) в дома такъв най-често отсъства. А точно за дома хората имат най-високи изисвания за защита на своите информационни системи. При по-масовото дигитализиране на дома, тези изисквания ще стават все по-големи.

Рискове и видове киберзаплахи

С въвеждането на интелигентните устройства в домовете ни, рисковете и заплахите за тях и респективно обитателите им ще растат. Домът и услугите в него представляват една силно хетерогенна среда, която поставя далеч по-големи предизвикателства за справяне с рисковете, отколото другите познати и масово използвани до момента киберпространства. Услугите, които умните къщи предоставят, особено от към гл.т. на здраве съдържат непознати до момента рискове. В телевизионен сериал, излъчен неотдавна бе показано как чрез нерегламентирано проникване в пейсмейкъра на висш политик се причинява инфаркт. Макар и това да бе само на филм, учени демонстрираха как е възможно подобно нещо да стане извън текста на сценариста [6]. Факт, който е достатъчно стряскащ като се има предвид, че само в САЩ в рамките на периода 2006-2011 са продадени над 4.6 милиона такъв тип устройства.

Една дефиниция на киберзаплаха я представя като „всеки идентифициран опит, насочен към достъп, извличане, подправяне, или нарушаване целостта, поверителността, сигурността или достъпа на данни, приложение или федерална система без законново право за това” [7]. В реалния живот, за дома заплаха може да е отворен прозорец или незаключена врата, забравена ютия, печка или течащ кран. В домовете на бъдещето, освен спрямо сигурността, домашните уреди и средата, с размери несъществуващи до сега, опасности могат да възникват и директно към здравето на обитателите им. Съвременни изследвания сочат, че киберзаплахите много бързо навлизат в ново появяващите се територии от дигиталното пространство – социални медии, мобилни устройства и облачни услуги [8], [9]. Това неизбежно ще стане и в най-близко бъдеще в домовете на бъдещето.

Киберзаплахите могат да се класифицират в няколко насоки:

- според намерението – непреднамерени и преднамерени. Първите се дължат на недостатъчно познание, обновяване на софтуера, проблеми с поддържката или апаратни грешки, които могат да навредят на системата, докато преднамерените са дело на хакери, шпиони, криминални лица и т.н.
- според обекта на атаката – целенасочени и нецеленасочени. Към първите спадат такива, които целят определена система или компонент от критична система, а към вторите – когато не е дефинирано кой точно ще попадне под заплахата (напр. вируси, червеи, зловреден софтуер и др.).
- според вида на атаката от гл.т. на последствия - критични, некритични и некритични, но опасни. Критичните блокират или изваждат от употреба цели

системи (може да са инфраструктурни), или отделни модули, оставяйки ги в частично или изцяло нефункциониращо състояние. Некритичните атаки не водят до промяна на състоянието на системата или нейни елементи (напр. извлича се информация за потребителите или системите с рекламни цели), а некритичните, но опасни са такива, които не причиняват вреда веднага, но това е възможно да се случи в последствие (кражба на пароли, самоличност и т.н.).

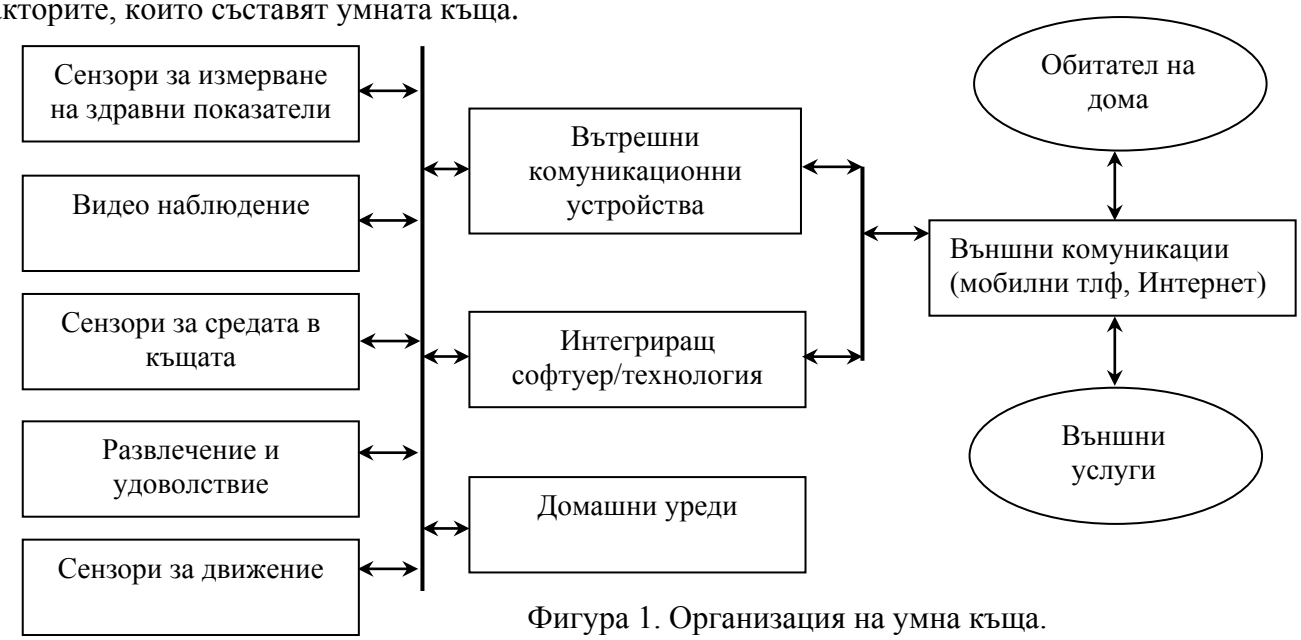
Наскоро публикуваната Червена книга за изследвания в областта на системната сигурност [10] представя ценностите, на които хората обръщат най-голямо внимание, като на първите четири места с изброените киберзаплахи към тях са:

- живот – заплахи спрямо транспорта, системите за реакции при спешни случаи;
- здраве – заплахите към все по-навлизащите информационни технологи в здравето;
- околна среда – заплахи свързани със замърсяване, пожари и др.;
- лично пространство на индивидите.

Тези четири области са ключови в развитието на „умните къщи“, като към тях спадат още заплахи към сензорните технологии (най-често използвани в домовете на бъдещето), вградените системи и умната среда (smart environment).

Опасности за умните къщи

На Фигура 1 е представена организацията на устройствата, системите и факторите, които съставят умната къща.



Фигура 1. Организация на умна къща.

В Таблица 1 са представени основните услуги, възли и системи на „умната къща“, както и опасностите спрямо тях.

В областта на здравните грижи се използват сензори на различни принципи, микроелектромеханичните системи (MEMS – micro-electromechanical systems) и Радиочестотната идентификация (RFID - Radio Frequency Identification). При грижите за хора с увреждания и деца, най-често се използва видеонаблюдение, а за състоянието на средата в къщата - оптически, акустични и електромагнитни сензори. Като за източници на данни се използват сензорни технологии и видеонаблюдение.

В областта на комуникациите, в „умните къщи“ се използват технологии като Етернет, WiFi, Bluetooth, RFID, ZigBee и инфрачервени комуникации.

Услуги на „умната къща“	Възможни опасности	Критични за атака възли	Последствия от възможна атака
Здравни грижи	Не се взима лекарство, не работи пейсмейкър и др.	Сензори, видеонаблюдение, комуникационна система, интегрираща система, външни комуникации	Критични
Грижи за деца/хора с увреждания	Има нужда от внимание	Сензори, видеонаблюдение, комуникационна система, интегрираща система, външни комуникации	Критични
Охрана и безопасност	Нерегламентирано проникване	Сензори, видеонаблюдение, комуникационна система, интегрираща система, външни комуникации	Критични
Среда в къщата	Пожар, наводнение, изтичане на газ	Сензори, видеонаблюдение, комуникационна система, интегрираща система, външни комуникации	Критични
Умни домашни уреди	Работи без да прекъсне, прекъсва работа	Сензори, видеонаблюдение, комуникационна система, интегрираща система	Некритични, некритични но опасни
Лично пространство	Нарушаване на личното пространство, кражба на данни	Видеонаблюдение, комуникационна система, интегрираща система, външни комуникации	Некритични, но опасни
Развлечения и удоволствия	Нефункциониране на системата за развлечение и удобства	Сензори, комуникационна система, интегрираща система	Некритични

Таблица 1. Услуги, опасности и критични възли в „умните къщи“.

Все още няма стандартни и масово използвани системи за интеграция, като една от възможните такива е [11], която има за цел да прави възможно управлението и контрола на множеството хетерогенни системи в умната къща.

Възможните последствия от кибератаките могат да бъдат:

- нарушен достъп до услуга (DoS) – било то чрез въздействие върху сензорните устройства или устройствата за видеонаблюдение или върху комуникационната система,
- нарушена цялост или модифицирани данни, които се предават в комуникационната среда;
- нарушена поверителност на системата, получавайки неоторизиран достъп до мрежовите ресурси или до ресурсите на системата за интеграция.

За справяне с атаките е необходимо:

- да може да се установи наличието на атака;
- да има надеждни средства с идентификация , автентикация и контрол на достъпа;
- да има сигурни и ефикасни комуникационни протоколи;
- да има сигурни интегриращи системи и системи за външна комуникация.

Проект за киберсигурност в домовете на бъдещето у нас

По темите, свързани със сигурността в умни къщи се работи и у нас. От края на 2012 г. се изпълнява проект с такава насоченост, финансиран от Фонд „ Научни изследвания“ към Министерството на образованието, младежтта и науката. Координатор и водещ проекта е научен колектив от Института по информационни и комуникационни технологии към БАН, в партньорство с ВУ „Колеж по телекомуникации и пощи“ и фирма Висенси ООД. Проектът цели:

1) да се изследват начините за откриване на заплахи към потребителите чрез експериментално подбран пакет от сценарии. Те емулират различни дейности, при използване на сензорните мрежи в умната къща и прилагат симулационни модели с участието на апаратни системи за мониторинг на зададени техно- и био- параметри

2) да се анализират, интегрират и практически валидират получените експериментални и моделни данни в единна методология за идентифицикация на заплахите в „умните къщи“ [12, 13].

През първата година на проекта бяха извършени поредица от експерименти със сензорни системи, които ще бъдат вложени в изграждания физически модел на умна къща (работи се в рамките на една стая). Разработени са концептуални модели на комуникационната среда и е създадена методологическа рамка за идентификация на кибер заплахи в домовете на бъдещето. Предложен е симулационен, агентноориентиран модел за пакет от експерно подбрани сценарии.

Оборудваната стая има интелигентно сензорно и гласово управление на осветеността и звуковия фон, което дава възможности за провеждане на експерименти с контролирано въздействие от страна на средата върху потребителите. По този начин става възможно изследване на потребителската психо-физиологична динамика при забавление и рекреативни дейности. Допълнително е изградена е система за следене на биопараметри на обитателите на стаята като ЕКГ ритъм, телесна температура, положение в пространството и др. Следят се физически параметри на средата в стаята като температура, влажност, осветеност, наличие на прахови частици, състав на въздуха (с акцент върху концентрация на CO и CO2) и радиационния фон. Посредством централизирана вътрешна мрежа се наблюдава мрежовия трафик на свързаните устройства и консумацията на електроенергия. Предстои цялостно интегриране на системата и проиграване на различните сценарии за идентифициране на явни и скрити киберзаплахи.

Моделът, върху който ще се развиват възможните сценарии за киберзаплахи включва данни, събрани от допитвания у нас и в чужбина и съдържа пет основни направления, всяко от които съдържа различни компоненти. Избрани бяха направленията: „Устройства“, „Дейности“, „Комуникационна среда“, „Характеристики на средата“ и „Характеристики на човешкия фактор“. Всяко направление се състои от определен брой специфични за него компоненти. Направлението „Устройства“ включва умни мобилни устройства (смартфони, таблети и т.н.), системи за домашно забавление

(игрови конзоли, роботи и т.н.) и автоматични домашни системи (аларми, сензорни системи и т.н.). Направлението „Дейности“ включва: забавления, комуникация, ежедневна работа и поддържане на домакинството. Направлението „комуникационна среда“ включва кабелни, безжични мрежи и социални мрежи. Направлението „Характеристики на околната среда“ включва физически (състав на въздуха, налягане, температура и т.н.), структурни (вътрешен дизайн, налично пространство и т.н.) и функционални (ергономични, функционални и т.н.) характеристики. Направлението „Човешки фактор“ включва биопоказатели (умствена дейност, сърдечен ритъм и т.н.), място (местонахождение, изминато разстояние в стаята и т.н.) и емоции (влияние на аромат, звук и т.н.). На базата на сценарии, които включват комбинация от различни компоненти на направленията ще бъдат идентифицирани различните киберзаплахи. Един примерен сценарий включва: „Система за домашно забавление“->“Забавление“->“Кабелни мрежи“->“Структурни“->“Място“. На базата на различно зададени тегла на връзките между компонентите на дейностите се извършва оценка на наблюдавания сценарий, който служи за по нататъшно системно изследване.

Заключение

С навлизането на дигиталните технологии в дома навлизат и опасностите, които тези технологии биха могли да доведат със себе си – отказ от услуги, забавяне или нарушаване на критична комуникация или известяване, нефункциониране на критични за здравето и сигурността на обитателите възли, опасности от проникване в личното пространство на индивида. А домът все още е важна за човека крепост, която той трябва да може да опази на всяка цена от вмешателство в нея, без да се лишава от удобствата, които модерните информационни технологии предлагат.

Литература:

[1] ABI Research, 1.5 Million home automation systems installed in the US this year, New York, https://www.abiresearch.com/press/15-million-home-automation-systems-installed-in-th

[2]O‘Brien, AT&T launches Digital Life home automation and security platform, April 2013, http://www.engadget.com/2013/04/26/atandt-launches-digital-life-home-automation-and-security-platform/

[3] http://www.navigantresearch.com/blog/articles/smart-house-in-japan

[4] Боянов Л., Минчев З., Боянов К., Някои киберзаплахи в дигиталното общество, Автоматика и Информатика, ISSN 0861-7562, Год. XLVI, 4/2012, стр. 43-48.

[5] http://www.nsi.bg/otrasal.php?otr=17&a1=2405&a2=2406&a3=2409

[6] Computerworld, October 2012, http://www.computerworld.com/s/article/9232477/Pacemaker_hack_can_deliver_deadly_830_volt_jolt

[7] U.S. Department of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise 3, March 2010, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf

[8] Symantec Corp., Internet Security Threat Report 2013, Volume 18, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[9] Sophos, Security Threat Report 2013, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

[10] The Red Book. The SysSec Consortium, 2013, http://www.red-book.eu/m/documents/syssec_red_book.pdf

[11] Dixon C, Mahajan R, Agarwal S, Brush A, Bongshin L, Saroiu S, Bahl V, An Operating System for the Home, Microsoft Research – Publications, Microsoft, April 2012.

[12] Minchev Z, Boyanov L, Georgiev S, Security of future smart homes. Cyber-physical threats identification perspectives, Сборник материали с резултатите от изпълнението на задачите по проект HOME/2010/CIPS/AG/019, част 2, София, 2013 стр. 165-169

[13] http://smarthomesbg.com