SECURITY IN INTERNET OF THINGS

СИГУРНОСТ В ИНТЕРНЕТ НА НЕЩАТА

Tsvetomir Gyuretsov, Jordan Raychev, Georgi Hristov, Plamen Zahariev

Department of Telecommunications, University of Ruse "Angel Kanchev",
8 Studentska str., 7017 Ruse, Bulgaria, Phone: +359 082 888 817,
e-mail: {tsguyretsov, jraychev, ghristov, pzahariev}@uni-ruse.bg

Цветомир Гюрецов, Йордан Райчев, Георги Христов, Пламен Захариев

Катедра „Телекомуникации", Русенски университет „Ангел Кънчев",
ул. „Студентска" №8, 7017 Русе, България, тел.: +359 082 888 817,
e-mail: {tsguyretsov, jraychev, ghristov, pzahariev}@uni-ruse.bg

Keywords: Internet of Things, security, smart home, protection;

Резюме - Проблемът с кибер сигурността вълнува голяма част от разработчиците по целият свят. След обявяването на концепцията IoT компании по цял свят започват работа по откриване на нови методи за защита на разрастващата се мрежата от така наречените умни устройства. От съществена важност е откриването на нов вид гъвкава защита, която трябва да отговаря на следните основни изисквания – адаптивност към постоянно разширяващата се мрежа от устройства, приложимост на всяко едно от основните нива в концепцията IoT, непретенциозна към изчислителна мощност, да генерира минимален трафик в мрежата и най-важното да не ограничава приложението на този вид устройства.

Друг много важен аспект на който трябва да се обърне внимание е къде трябва да се съсредоточат усилията при имплементиране на тези защити. Разграничават се три ключови етапа при изграждане на надеждна защита свързана с интернет на нещата – защита на устройството, защита на облачната инфраструктура и защита на локалната мрежа. Всяка една от тези точки е от първостепенна важност за една добра и сигурна среда за използване на този вид нова технология. При евентуален проблем в един от тези слоеве, всички усилия свързани с разработването на нови протоколи, защитни стени и софтуерни продукти за защита биха били безсмислени. Тридесет години опит натрупан в изграждането и прилагането на защита на

познатите ни жични и безжични технологии е едно солидно начало и един летящ старт за разработчиците заели се с тази нелека задача. За жалост спецификата на идеологията IoT прави тези познати технологии неприложими, не и във вида в които ги познаваме.

Abstract – The problem with cyber security worries many developers around the globe. After Internet of things concepts were announced many companies around the world focused their work in developing new ways to secure fast growing network of smart devices. It is essential to find a new flexible protection which must meet the following basic requirements – adaptability to fast growing of network of devices, applicability of each main layer in the concept IoT, low computing power, low traffic over the network, and the most important thing - not limiting the application of smart devices.

Another very important aspect of which developers must focus is where to implement this security. Three layers can be distinguished when we talk about establishing reliable protection for Internet of Things – secure the devices, secure the cloud and secure the local network. All of these points are very important for applying good and secured core for using this new technology. In case of a problem in one of these layers all the effort related with developing of new protocols, fire walls or software products would be wasted. Many years of experience are accumulated in the establishment and implementation of the protection in the well-known wire and wireless technologies. This is a solid beginning and a running start for developers occupied with this hard task. Unfortunately the specifics of the ideology of Internet of Things makes this well-known technologies useless in the form we know them.

1. УВОД

От големи и модерни фабрики до болници, та дори и до нашите домове - умните устройства навлизат все повече в ежедневието на един съвременен човек. С развитието на технологиите, вече не е достатъчно тези устройства да са обособени като самостоятелна единица. Навлиза нуждата от комуникация и взаимодействие между тях, за да могат да предоставят едно по-добро обслужване на потребителите. Това от своя страна довежда до необходимост всички тези устройства да бъдат управлявани независимо от тяхното местоположение. Тази „инвазия“ на нови устройства носи със себе си много ползи и улеснява живота на всеки един, но пред нас се поставя един въпрос от съществена важност - безопасността.

Наличието на толкова устройства в мрежата открива нови хоризонти пред компютърните престъпници, предоставяйки им възможност за достъп до личната информация на потребителите. Нарастването на устройствата в мрежата, увеличава пропорционално възможните точки за експлоатиране, което от своя страна се оказва основен проблем пред който са изправени разработчиците на приложения.

2. СЪСТОЯНИЕ НА ПРОБЛЕМА

Какво всъщност представлява интернет на нещата? Какви са устройствата, които изграждат тази мрежа? Това са важни въпроси на които трябва да се намери отговор преди да се започне изграждане на цялостна концепция за защита. Интернет на нещата представляват устройства с вградени управляващи системи, които комуникират помежду си и взаимодействат с заобикалящата ги среда посредством локалната мрежа или облачната среда. Важно е да се обърне внимание на думите „вградена управляваща система“. Тук трябва да се изясни това понятие. Вградена управляваща система е съвкупност от хардуер и софтуер с тясно специализирана задача за изпълнение. Тя се състои от микропроцесор, програма записана във вътрешната ROM памет и входно-изходни устройства за взаимодействие с околната среда. PLC контролерите са пример за вградена управляваща система. Много често тези системи се проектират така, че да имат изчислителна мощност съобразена с задачата, която ще изпълняват. Тук може да се открои първия основен проблем, който се поставя при разработването на една нова система за сигурност, а именно ограничените хардуерни възможности на устройствата използвани за изграждане на интернет на нещата. Това ограничение прави трудно приложимо, а дори и невъзможно използването на blacklisting подхода, който е един от най-широко разпространените подходи за борба със зловреден софтуер в момента. Най-просто казано blacklisting представлява списък с приложения, които се смятат за зловредни и съответно тяхното изпълнение не се разрешава. Основен проблем – твърде обемисти файлове за съхранение. От друга страна имаме така наречения whitelisting подход. Този подход обратно на blacklisting метода използва списъци с разрешени програми и приложения които може да се изпълняват. В допълнение се използва и хеширане за по-голяма сигурност. Проблемите на този подход се изразяват в необходимостта от по-високо процесорно време за изпълнение на съответната задача.

Друг аспект, който трябва да се вземе под внимание е постоянно разрастващата се мрежа на IoT. С увеличаване на активните устройства в мрежата се увеличава и броят на възлите, които могат да бъдат подложени на кибер атака. Това се оказва основен момент, който трябва да се вземе под внимание при разработване на нови механизми за сигурност. Те трябва да са гъвкави и адаптивни към тази постоянно развиваща се среда. Това разрастване носи със себе си и друг основен проблем – значителното увеличение на мрежовия трафик. Защитният механизъм, който трябва да се приложи трябва да генерира минимално количество трафик в мрежата. В противен случай

увеличаването броя на устройствата ще увеличи и трафика в мрежата, което се дължи на огромното количество служебна информация, която се предава между IoT устройствата. През 2015 година Forrester Global Business Technographics публикува проучване, фиг. 1., което представя най-големите заплахи за инженерите работещи в сферата на мрежовата сигурност в IoT.

Фиг. 1. Проучване на Forrester Global Business Technographics

В проучването участват 2053 специалисти от който 69% са силно загрижени от пробив на външни хакери. От проучването става ясно, че по-голяма част от мрежовите специалисти насочват вниманието си към заплахи, като DDOS (Distributed Denial Of Service), препращани на данни към трето лица и проблеми свързани с оторизацията на страните участващи в комуникационния процес. Това са една част от основните проблеми пред разработването на нова “умна“ защита приложима в интернет на нещата, но остава въпроса с живота на тази защита. Остава въпроса с приложението на тази нова сигурност спрямо времето. Според учени от университета в Станфорд тази нова защита трябва да е с цикъл на използване поне 20 години. Тоест при разработването трябва да се вземе под предвид как ще се развие света на IT технологиите в следващите двадесет години и да се имплементира такъв тип защита, която ще остане неуязвима в този период от време. От табл. 1., се вижда, че по-известните криптографски алгоритми има продължителност на живот между 15 и 20 г., а някой и повече.

Проблемите са поставени, но къде трябва да бъде имплементирана тази нова защита? Разграничават се три основни слоя, които могат да бъдат подложени на кибер атака – облачната инфраструктура, локалната мрежа или самото устройство. Този многослоен подход би гарантирал високо ниво на сигурност за цялата мрежа от умни устройства. От тяхното първоначално стартиране до преминаването им в работен режим.

ТАБЛИЦА 1. ПРОДЪЛЖИТЕЛНОСТ НА ЖИВОТ НА АЛГОРИТМИ ЗА КРИПТИРАНЕ

	Алгоритъм	Година на разработване	Година на разбиване	Време на използване
Симетрични алгоритми	DES[16]	1979	1994	16 години
	RC4[4]	1994	2013	19 години
	RC2[13]	1996	1997	1 година
	3DES[14]	1998	2015	17 години
	AES	1998	-	повече от 18 години
	Camellia	2000	-	повече от 18 години
Хеш функции	MD5[17]	1992	2004	12 години
	SHA-1[17]	1995	2004	9 години
	SHA-256	2000	-	повече от 16 години

Защитния механизъм трябва да се прилага веднага щом устройството бъде захранено и свързано към мрежата. Чрез криптографски методи и дигитален подпис устройството се удостоверява в мрежата, че има разрешение за достъп и може да функционира. Този дигитален подпис се имплементира в софтуера от разработчиците му, в противен случай устройство без правилния ключ за автентичност няма да има достъп до мрежата. Това е една важна първа стъпка за установяване на надеждна защита. След като първият етап е направен и устройството се е идентифицирало следва да се приложи политика за достъп. На всяко устройство трябва да се даде достъп само до ресурсите, които са му нужни за изпълнение на неговите операции. При правилно прилагане, този механизъм би намалил щетите до минимум при установена уязвимост. Така недоброжелателя ще има достъп само до ресурсите до които има достъп и устройството, но не и до цялата мрежа. При изпращане и получаване на данни трябва да се приложи политика за идентификация. Мрежовият трафик трябва да се генерира само от устройствата, които имат позволение за изпращане и получаване. Това също позволява да се изгради и йерархия при обслужването на данните. Този метод за защита може да се постигне на база потребителско име и пароли за всяко устройство. Всяка парола и потребителско име се вграждат в софтуера и така след стартиране на устройството то ще може да комуникира в мрежата. Това улеснява и системната поддръжка на цялата мрежа от устройства. По всяко едно време системният администратор на база анализ състоянието на мрежата или други фактури може да промени, както политиките за достъп така и трафика на данни от едно или група устройства.

До тук предложените методи са главно за защита на мрежата от устройството. Погледнато от обратната страна атаката може да бъде насочена към самите устройства. Ако хакер установи връзка с дадено устройство от мрежата той може да започне да му подава грешна информация, което би довело до фатални последици не само за цялата мрежова инфраструктура, но и за хората, които работят около тях. Този проблем налага използването на някакъв вид защитна стена или антивирусна програма, които да филтрират трафика на данни изпратен към устройството и да блокира атаките на зловреден софтуер.

Всички от изброените методи не биха били ефективни без постоянно обновяване на софтуера и базата от рестрикции. Тези регулярни обновления трябва да се направят така, че да не натоварват калната мрежа. Също така отново трябва да се наложат рестрикции от гледна точка на това кой и как може да извършва това обновяване.

3. ЗАКЛЮЧЕНИЕ

Разработването и внедряването на защита от този вид е комплекса работа изискваща впрягането на усилия на разработчици от различни нива и типове сигурност. Предоставянето на една сигурна среда за работа на този вид умни устройства е от съществена важност за налагането на идеологията интернет на нещата. Разработването на един нов вид защита отговаряща на поставените изисквания и предизвикателства ще отвори една нова страница и ще промени цялостната концепция на мрежовата сигурност.

4. БЛАГОДАРНОСТИ

Публикуваните резултати са получени при работа по проект ФНИ-16-РУ-10 “Създаване на прототип на роботизирана безпилотна летателна платформа за отдалечен мониторинг на критична инфраструктура” и проект ФНИ-16-ФЕЕА-04 "Изследване влиянието на местоположението на контролерите в управляващата равнина върху производителността на софтуерно-дефинираните мрежи", финансирани от Фонд „Научни изследвания“ на РУ „Ангел Кънчев“.

5. ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Stanford University, Secure Internet of Things, 2016
[2] Wind River, Security in the internet of things. Lessons from the past for the connected future, 2015
[3] Cloud Security Alliance, Security Guidance for Early Adopters of the Internet of Things (IoT), April 2015
[4] Rose K., Eldridge S., Chapin L.,The Internet of Things: An Overview, October 015
[5] Levis Ph., Secure Internet of Things Project, August 2014