دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

اینترنت اشیا

گزارش پروژه ی کارشناسی

محمد مهدی امینی

استاد

دکتر منشیی

۱۳۹۶

فهرست مطالب

فهرست تصاویر

فهرست جداول

فصل اول

UPNP

۱ـ۱ معرفی

Universal Plug and Play (UPnP) یک پرتوکل distributed است که بر اساس TCP/IP و در لایه ی Application بر اساس تکنولوژی های وب مثل Simple Object Access Protocol (SOAP), HTTP, HTTPU و XML کار می کند. یک دستگاه با بکارگیری UPnP می تواند تا حد امکان بدون نیاز به هیچ تنظیماتی (Zero-Configuration) به یک شبکه متصل شود، آدرس IP دریافت کند، نام خود را به بقیه ی موجودیت های شبکه اعلام کند، قابلیت ها و توانایی هایش را به اطلاع دیگر موجودیت های شبکه برساند، به درخواست ها درباره ی قابلیت هایش پاسخ دهد و درباره ی حظور و قابلیت های دیگر موجودیت های شبکه سوال بپرسد.

این پرتوکل طوری طراحی شده تا بتواند در انواع مختلف شبکه ها مثل شبکه های خانگی، تجاری کوچک و تجاری در اندازه ی بزرگ کار کند.

UPnP برای اجرا محدودیتی خاصی نسبت به پلتفرم (سیستم عامل و زبان برنامه نویسی) و لینک ارتباطی(خط تلفن، خط برق و ...) ندارد.

۱ـ۲ مشکلاتی که استفاده از این پرتوکل در محیط اینترنت اشیا را با مشکل مواجه می کند

در محیط اینترنت اشیا نه تنها منابع شبکه مثل پهنای باند محدود است بلکه منابع دستگاه ها مثل توان پردازشی و منبع تغذیه نیز محدود است. از طرفی تعداد دستگاه هایی که با این ویژگی ها با هم در ارتباط هستند، بسیار زیاد است که در واقع باعث تولید حجم زیادی از مبادله ی پیام می شود. با در نظر گرفتن این ویژگی ها به بررسی نکاتی می پردازیم که دربردارنده ی دلایل عدم تناسب UPnP با اینترنت اشیا است.

در بعضی از بخش های UPnP پیام های Multicast با مدل P۲P ارسال می شود که باعث افزایش مصرف منابع شبکه در حظور تعداد زیاد دستگاه می شود.

در سال ۲۰۱۱ یک ابزار طراحی شد که به کمک آن ممکن است به دستگاه هایی که از UPnP استفاده می کنند (اگرچه پشت NAT هستند) درخواست ارسال کرد. این ابزار امکان ارسال درخواست PortMapping به یک آدرس IP بیرونی را از طریق دستگاه مورد نظر که پشت NAT قرار دارد، فراهم می کند. در سال ۲۰۱۳ یک بررسی که ۶ ماه به طول انجامید و طی آن سیگنال های دستگاه هایی مبنی بر حظورشان در اینترنت را منتشر می کردند، شمرده شد. وجود ۶۹۰۰ دستگاه از ۱۵۰۰ شرکت مختلف که با ۸۱ میلیون آدرس به اینترنت متصل بودند، شمرده شدند که ٪۸۰ آنها مسیریاب ها بودند. و بقیه Printer, Webcam و دروبین های نظارتی بودند. بسیاری از این دستگاه ها قابل دسترسی و سو استفاده بودند.

در مرحله ی شناسایی سرویس (Service Discovery) این پرتوکل از پرتوکل Simple Service Discovery Protocol (SSDP) استفاده می کند. وقتی یک دستگاه به شبکه اضافه شد و آدرس IP دریافت کرد، می تواند بر اساس SSDP توانایی ها و سرویس هایی که ارایه می دهد را در شبکه تبلیغ کند که از طریق ارسال پیام های Alive انجام می شود. در نتیجه دستگاه ها باید به تعداد بالا در دوره های زمانی کوتاه پیام های Alive ارسال کنند که باعث هدر شدن منابع شبکه و دستگاه می شود.

در سال ۲۰۱۴ مشخص شد که می توان از SSDP برای اجرای حمله ی DDOS استفاده کرد. این حمله به SSDP reflection attack with amplification معروف شد. بسیاری از دستگاه ها مثل مسیریاب های خانگی یک آسیب پذیری مربوط به UPnP دارند که به حمله کننده امکان می دهد پاسخ یک درخواست را از پورت ۱۹۰۰ (که مربوط به SSDP) است به یک مقصد خاص و دلخواه ارسال کند. با استفاده از یک شبکه ی Botnet به اندازه ی کافی بزرگ، می توان تعدادی کافی بسته به این شکل تولید کرد که پهنای باند استاندارد یک موجودیت شبکه را کاملا مورد استفاده قرار دهد. در نتیجه بسته های واقعی و سالم امکان دسترسی به موجودیت هدف را نخواهند داشت. با توجه به اینکه اینترنت اشیا محیطی تشکیل شده از تعداد زیادی دستگاه است، استفاده از UPnP می تواند منجر به ایجاد یک Botnet بسیار بزرگ و آماده ی حمله شود.

در پرتوکل UPnP امکان اهراز هویت وجود ندارد. برای حل این مساله هر دستگاهی که می خواهد از این پرتوکل استفاده کند، باید یک سرویس جداگانه به نام Device Security Service را پیاده سازی(استفاده) کند. متاسفانه بسیاری از دستگاه هایی که از UPnP استفاده می کنند، این مکانیزم اهراز هویت را پیاده سازی نکرده اند. این فقدان باعث بروز آسیب پذیری در برخی از مسیریاب ها و دیوارهای آتش می شود. برای مثال برخی نسخه ها Adobe Flash که امکان اجرا در بیرون از مرورگر وب را دارند، می توانند یک نوع خاص از درخواست HTTP را تولید کنند که به مسیریابی که UPnP را بکار برده اجازه می دهد تا توسط یک وب سایت خراب کار کنترل شود. برای اجرا شدن این حمله فقط کافی است سایت خراب کار توسط سیستم اجرا کننده ی Flash باز شود.

کتاب‌نامه

[1] Washer, Peter. *Learning Internet of Things*. Packt, 2015.

[2] us cert.gov, UDP-Based Amplification Attacks. https://www.us-cert.gov/ncas/alerts/ta14-017a, 2016.

[3] Lee Myers, Senior Manager of Security Operations Christopher Cooley, Cyber Intelligence Analyst. Guide to ddos attacks, 2016.

[4] MICROSOFT, Overview of UPnP Architecture. https://msdn.microsoft.com/en-us/library/windows/desktop/aa382261(v=vs.85).aspx.

[5] gnucitizen, Hacking The Interwebs. http://www.gnucitizen.org/blog/hacking-the-interwebs, 2008.

[6] The H Security, Millions of devices vulnerable via UPnP Update. http://webcache.googleusercontent.com/search?q=cache:l1wpyg99wfmj:www.h-online.com/security/news/item/millions-of-devices-vulnerable-via-upnp-update-1794032.html, 2013.

[7] hdmoore, Whitepaper: Security Flaws in Universal Plug and Play: Unplug, Don't Play. https://community.rapid7.com/docs/doc-2150, 2013.

[8] Joel Lee, What Is UPnP and Explains], Why Is It Dangerous? [MakeUseOf. http://www.makeuseof.com/tag/what-is-upnp-and-why-is-it-dangerous-makeuseof-explains/, 2013.

[9] upnp hacks.org, Frequently Asked Questions. http://www.upnp-hacks.org/faq.html.