Netflix Web Audit

Sarah Larbi, Megan Horan, Victoria Thomson, Cody Kajardi

With 89 million paying members worldwide, and 8.3 billion dollars in global streaming revenues, Netflix has reached unprecedented levels of user engagement and traffic. Checking the security and procedures of the website is of the utmost important due to the sheer number of users on the site. Building off of this, following the requirements set forth by the ISA, four attack vectors were scrutinized: acting as a man-in-the-middle on unencrypted network traffic, gaining access to the server and learning everything the server knows, gaining access to the client and learn what the client knows, and hacking into a certificate authority. While most of Netflix is served on HTTPS using secure encryptions, an interesting point of potential inquiry arose around the websites' uses of cookies: questioning the validity of Netflix's use of third party cookies, and the potential ignorance of users' options in terms of privacy.

While attempting to analyze the effectiveness of the attack vectors on Netflix, most were rendered irrelevant due to Netflix's security measures. Fortunately for users, Netflix securely encrypts all of its traffic. All of Netflix's form pages, such as login, search, and customer support, are served over HTTPS with a strong key exchange ECDHE_RSA with P-256 and a cipher that uses AES_128_GCM. Netflix uses up to date security algorithms to encrypt their pages, and there is very little that the ISA would be able to gain from eavesdropping on TCP packets between Netflix and its users. If Netflix were to not encrypt all of their traffic, then in theory the ISA would be able to gain a lot of information about the user including their login credentials, billing information, viewing preferences, and potentially even their facebook information.

Further, if the ISA could carry out an attack on the server and gain all the data the server knows, they would have access to what people's interests and preferences are, for not only would their username, password, and payment information be known, but all of the data and preferences gathered by Netflix would become compromised. Server attacks are commonly used for information theft, and this has some potentially serious drawbacks. Depending on what the ISA would do with the information it gained access to, whether that be modification or just acquisition, an attack such as this one could have several outcomes. If detectable modifications occurred on a user's account (i.e. new unusual viewing preferences), then this may result in a tarnished name for Netflix, associating the service with the idea that they are not protecting information, and user's may be less inclined to trust the site in the future. Similarly, if you could gain access to the client you would gain the same information as from the server attack, but this attack is hard to execute since Netflix is served over HTTPS and there are few browser vulnerabilities.

Due to poorly designed web browsers that will accept any trusted certificate regardless of the unexpectedness of the CA, a successful attack with a bogus certificate proves to be extremely dangerous. Once the bogus certificate is accepted, the ISA would gain the ability of eavesdropping on all of a user's SSL/TLS Netflix traffic on the network. The purpose of these SSL certificates is to verify that the websites customers visit are the valid, intended websites. Issuing a bogus trusted certificate allows an attacker such as the ISA to impersonate a site, in this case Netflix, and the user is unsuspecting because they have been told they are participating in trusted communication. If the ISA can succeed in such an attack, then everything becomes very visible and information is being sent completely in the clear. Similarly to a successful Man In The Middle Attack on HTTP connections, the ISA would gain valuable user information such as their username/password, viewing habits, billing information, etc. Given that many of these aforementioned attack vectors hold no weight with Netflix's strong security features, other facets of Netflix's website provoked further inquiry.

One area of Netflix that could potentially be interesting to unsuspecting users is Netflix's policies on cookies. There are three kinds of cookies that Netflix keeps track of: essential, performance and functionality cookies, and advertising cookies. Essential cookies are used to identify and keep track of users and prevent against fraud; performance and functionality cookies help to personalize the user's experience, keeping track of things like "popular pages, conversion rates, viewing patterns, [and] click-through"[1] among other things; and advertising cookies, which cataloge a user's information and their movements to other third party advertisers, in order to create more specified ads.

The performance and functionality cookies are used to find trends in what users are watching, what potential tv shows they should make, and how they should market them to new users. It takes user analysis and specialization to new levels, tracking when users watch, how long they watch, and even browsing and scrolling behavior. This affords Netflix unprecedented access to user engagement, a facet inherent to their rampant success and longevity. For example, if Netflix notices a spike in trends with a certain tv show, they might go ahead and reboot a show or create a whole new show based on the data supplied to them through user's actions on the site. [2] This behavior is exactly what resulted in the creation of what is now Netflix's most viewed television series, House of Cards. Big Data collected from users is what determined the show would be a hit *a full year* before its production. The show was originally a BBC miniseries and when Netflix was given the opportunity to remake it they simply looked at their data, observed that original watchers of the show were also viewers of movies starring Kevin Spacey, and they knew then and there that there existed an audience using there service that was almost guaranteed to watch the show. Netflix's communication director even said, "We know what people watch on Netflix and we're able with a high degree of confidence to understand how big a likely audience is for a given show based on people's viewing habits."[3] The importance of this trend monitoring is the reason why Netflix will not allow you to watch in incognito mode, since it relies on the data to make sure it creates a unique user experience and affords feedback for future endeavours .

[1] https://www.netflix.com/

[2] https://blog.kissmetrics.com/how-netflix-uses-analytics/

[3] https://www.fastcodesign.com/1671893/the-secret-sauce-behind-netflixs-hit-house-of-cards-big-data

In regards to the third party cookies, Netflix also sends their advertising cookies to companies such as DoubleClick, Facebook, Google Adwords, SiteScout, and other advertising companies. Netflix does afford you the ability to turn off third party cookies, but the user would have to go out of their way to find this small clause and would also need a basic understanding of what third party cookies even are to be able to take advantage of this choice. While Netflix's use of essential and performance cookies are essential to its success, the morality of the third party advertisers and their relationship to Netflix becomes murky as you dig deeper.

Using a Firefox add-ons such as Ghostery or Lightbeam, it is evident that all of this user information *is* indeed being given to a handful of third-party websites. However, in the Netflix privacy policy it states that they do not *sell* user information. Their policy also states that "[m]any of the advertising cookies associated with [their] service belong to [their] Service Providers." What's the benefit of sharing this information with these third party agencies? Turns out, Netflix is trying to create deals with broadband providers to avoid paying for their traffic. "Netflix had hoped to achieve agreements with major broadband providers that would allow the company to exchange traffic with the providers at no charge – and according to news reports, it was successful in achieving such agreements with some smaller broadband providers, including Cablevision, but other major providers including AT&T, Verizon and Time Warner have refused to make such agreements." [4] The morality of this comes into question when we consider the possibility that Netflix is sharing this data in *exchange* for free service and that the two events are not independent of one another. This is simply speculation, but it does seem counterintuitive that Netflix would simply give away customer info: there would be no incentive for Netflix to just give away a wealth of data that third party advertisers would most surely benefit from. The privacy policy claims cookies are being used to "create a better user experience" and are valuable for advertising purposes, but given that Netflix does not support advertisements on their service specifically, what is their interest in aiding third-parties in targeted advertising?

Overall, this report strove to delve deeper into a website that had become a constant part of the lives of countless individuals, who spend large swaths of their time clicking, watching and consuming. A consumption that provides Netflix and multiple third party advertisers with an extensive exposure to its users lives. What does this all mean for users? The main takeaway is the Netflix provides secure and encrypted data, which is good news for your privacy from malicious adversaries. But what about your privacy from Netflix? The score on that front is less than ideal: a user has little privacy from Netflix and its third party connections. Everything you click, down to when you pause and if you stick with a show to its finale are all tracked, documented and manipulated by Netflix. Although this does afford you little privacy on what you click and what you watch, it does allow Netflix the resources and capability to keep creating

[4] http://www.telecompetitor.com/netflix-comcast-deal-relies-third-party-data-centers-interconnection/

content and allowing it to cement itself as an enduring, relevant service that many users have come to rely on.

Sources:
https://www.usatoday.com/story/tech/news/2017/01/18/netflix-shares-up-q4-subscriber-additions/96710172/
https://www.netflix.com/
http://www.telecompetitor.com/netflix-comcast-deal-relies-third-party-data-centers-interconnection/
http://resources.infosecinstitute.com/cybercrime-exploits-digital-certificates/
https://blog.kissmetrics.com/how-netflix-uses-analytics/
https://www.fastcodesign.com/1671893/the-secret-sauce-behind-netflixs-hit-house-of-cards-big-data
http://theemon.com/top-10-web-server-attacks-impact-and-prevention/
https://www.honeynet.org/node/157