Mgr inż. Mateusz Kozłowski
ORCID: 0009-0005-6899-0244
e-mail: mk@mko.is

BEZPIECZNY TRANSPORT DANYCH W SIECI

Streszczenie

Artykuł porusza tematykę szyfrowania danych w trakcie transportu w relacji klient-serwer oraz przedstawia korzyści płynące z tego rozwiązania. Omówione zostają również zagrożenia oraz niedoskonałości popularnych protokołów, które wymagają modernizacji. W szczególności omówione zostaną aspekty prywatności użytkownika oraz technicznie możliwości analizy ruchu sieciowego. W początkowych fazach powstawania Internetu poufność transmisji nie była kluczowa, ponieważ bardzo mało osób miało dostęp do samej sieci, a sam fakt powstania rozległej sieci był ogromnym wynalazkiem. Na szczęście rozwój technologii zaadresował ten problem i stworzył mechanizm pozwalający na zachowanie poufności w transmisji na linii klient – serwer. Mechanizm ten jest znany w świecie informatyki jako TLS (*Transport Layer Security*). Rozwiązanie to zapewnia bezpieczeństwo komunikacji poprzez szyfrowanie przesyłanych danych. Jest to szczególnie ważne w kontekście przesyłania informacji tj. loginy i hasła, pliki lub korespondencja prywatna.

Słowa kluczowe: poufność danych, szyfrowanie, protokoły sieciowe.

UWAGI OGÓLNE

Codziennie przez sieć Internet przepływają ogromne ilości danych. Według statystyk dostępnych na platformie Statista, rocznie wytwarzane jest około 403 milionów terabajtów danych[1]. Ogromna część tych danych to ruch sieciowy składający się na codzienne przeglądanie Internetu przez użytkowników końcowych. Przeciętny użytkownik najczęściej wykorzystuje sieć Internet do komunikacji z innymi ludźmi, jako źródło wiedzy o różnych faktach lub wydarzeniach oraz do szeroko pojętej rozrywki. Bardzo często Internet jest również wykorzystywany do załatwiania spraw bieżących tj. zakupy, realizacja płatności cyklicznych, rezerwacje biletów[2]. Mało osób zastanawia się jak dużo cennych danych jest przekazywane przez sieć, które w przypadku dostania się w niepowołane ręce mogą stać się źródłem wielu problemów. W początkowych

[1] https://www.statista.com/statistics/871513/worldwide-data-created/ [dostęp: 21.01.2025 r.]
[2] C. Chou et al., A Review of the Research on Internet Addiction, Educational Psychology Review 2005, vol. 17, no. 4, 2005, s. 363.

fazach powstawania Internetu poufność transmisji nie była kluczowa, ponieważ bardzo mało osób miało dostęp do samej sieci, a sam fakt powstania rozległej sieci był ogromnym wynalazkiem. Na szczęście rozwój technologii zaadresował ten problem i stworzył mechanizm pozwalający na zachowanie poufności w transmisji na linii klient – serwer. Mechanizm ten jest znany w świecie informatyki jako TLS (*Transport Layer Security*)[3]. Rozwiązanie to zapewnia bezpieczeństwo komunikacji poprzez szyfrowanie przesyłanych danych. Jest to szczególnie ważne w kontekście przesyłania informacji tj. loginy i hasła, pliki lub korespondencja prywatna. Mechanizm TLS został wdrożony w różnych popularnych protokołach tj. HTTP(S), IMAP(S), SMTP(S), FTP(S) – to właśnie litera „S" na ich końcu informuje o implementacji szyfrowania. Istotne jest, żeby mieć na uwadze, że poufność transmisji nie gwarantuje, że serwer, z którym prowadzona jest komunikacja jest zaufany. Protokoły gwarantują, że dane na trasie klient – serwer, nawet w przypadku przechwycenia, nie będą możliwe do odczytania.

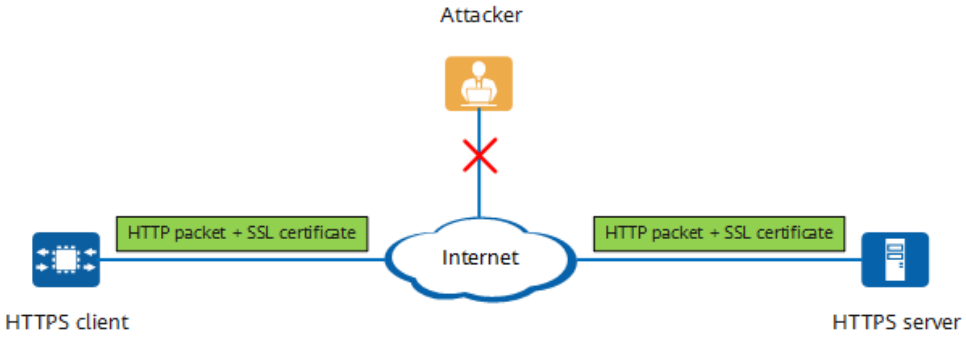

Figura 1 Przykładowy przebieg transmisji HTTPS, źródło: https://info.support.huawei.com/info-finder/encyclopedia/en/SSL.html (dostęp 21.01.2025 r.)

Nie ma jednak gwarancji, że w przypadku przejęcia kontroli nad serwerem atakujący będzie mógł je odczytać w momencie gdy dotrą na serwer docelowy. Sam fakt wystąpienia komunikacji szyfrowanej nie daje nam pewności, czy na pewno rozmawiamy z zaufanym serwerem – tutaj największym zagrożeniem staje się phishing[4]. Atakujący tworząc stronę Internetową na wzór np. bankowości elektronicznej kopiują jej wygląd i uruchamiają ją z wykorzystaniem fałszywej domeny często, z nazwy podobnej do oryginału[5]. W związku z ogólną dostępnością bezpłatnych certyfikatów SSL atakujący mogą bez kosztowo i bez dodatkowej weryfikacji wygenerować ważny rozpoznawany przez najpopularniejsze przeglądarki certyfikat SSL i w ten sposób zapewnić poufną

[3] S. Holtmanns, Mobile Web Service Security, Journal of Information Warfare 2004, vol. 3, no. 1, s. 44.
[4] A.S. Malish, Navigating Cyber Coverages for Modern Day Cybercrimes, Tort Trial & Insurance Practice Law Journal 2019, vol. 54, no. 3, s. 916.
[5] M. Boyle, Information Assurance Standards: A Cornerstone for Cyber Defense.Journal of Information Warfare 2014, vol. 13, no. 2, s. 18.

transmisję na linii klient – serwer[6]. Efektem tego zabiegu będzie kłódka widoczną w oknie przeglądarki, które może sugerować „bezpieczeństwo" połączenia. Mając na uwadze powyższe istotnym elementem edukacji użytkowników nt. bezpiecznego poruszania się po sieci jest naświetlanie im różnicy pomiędzy poufnością, a bezpieczeństwem połączenia.

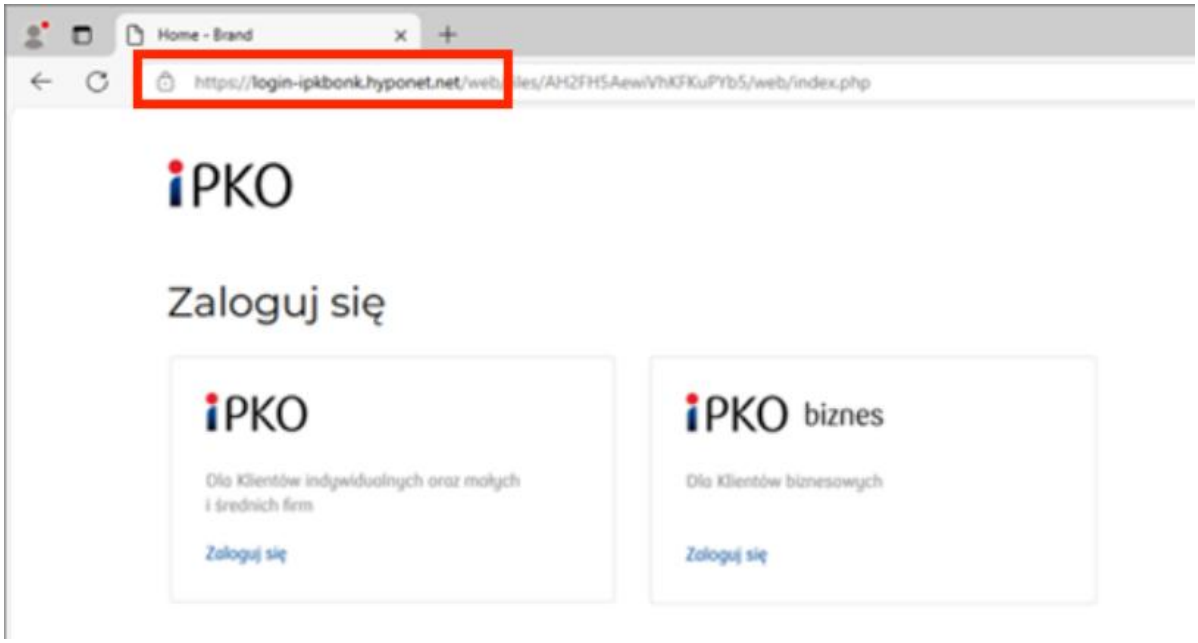

Figura 2 Przykładowy phishing z wykorzystaniem poufnej transmisji (HTTPS), źródło: https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf/362-ostrzezenia/918-przeglad-wybranych-oszustw-internetowych-grudzien-2024 (dostęp: 21.01.2025 r.)

[6] Ch. Mudler, Improving Early Phishing Detection using SSL & WHOIS data: an Application to PhishDetect for Civil Society Protection, https://research.tue.nl/en/studentTheses/improving-early-phishing-detection-using-ssl-whois-data [dostęp:21.01.2025]

Kilka lat temu przeglądarki posiadały funkcjonalność, która wskazywała poziom walidacji certyfikatu tj. jak wiele danych zostało zweryfikowane przez dostawcę. W celu uzyskania bezpłatnego certyfikatu SSL wystarczy potwierdzenie posiadania dostępu do domeny, a dokładnie do serwerów DNS. Przykładowa weryfikacja polega na dodaniu wpisu do strefy celem zweryfikowania dostępu. W przypadku ataków typu phishing jest to rozwiązanie idealne, ponieważ domeny wykorzystywane przez atakującego są rejestrowane tylko na potrzeby oszustwa i posiada nad nimi pełną kontrolę – z tego względu weryfikacja nie stanowi problemu. Firmy nadal inwestują w środki celem uzyskania bardziej wnikliwej weryfikacji tj. dane rejestrowe spółki. W takim przypadku w certyfikacie umieszcza się dodatkowe pola, które gwarantują, że podmiot faktycznie istnieje i złożył do urzędu stosowne dokumenty. Na ten moment przeglądarki wycofały się ze wskazywania wprost jaki poziom walidacji został zastosowany i weryfikacja tego faktu wymaga otwarcia szczegółowych informacji w przeglądarce[7].

Rosnąca popularność protokołów szyfrowanych rozpoczęła dyskusję dot. Bezpieczeństwa i prywatności użytkowników na innych płaszczyznach. Kolejnym protokołem bez którego Internet nie mógłby funkcjonować jest wcześniej wymieniony DNS (z ang. Domain Name System)[8]. Co do zasady nie jest on szyfrowany i całość komunikacji przebiega w trybie jawnym. Prowadzi to do niebezpieczeństwa ingerencji w integralność oraz poufność komunikacji. Atakujący w przypadku posiadania odpowiedni środków techniczny ma możliwość podsłuchiwania ruchu oraz modyfikowania go bez wiedzy użytkownika. Może to być szczególnie groźnie w przypadku niedoświadczanych użytkowników, którzy nie wykryją anomalii w zachowaniu sieci. Problem ten został zaadresowany przez wprowadzenie mechanizmów tj. DNS-over-HTTPS (w skrócie DoH) oraz DNS-over-TLS (w skrócie DoT). Mechanizmy te gwarantują, że klient pytający o dane dot. Domeny otrzyma niezmodyfikowaną odpowiedź, a zapytanie teoretycznie pozostanie prywatne. Mechanizm ten został szeroko przyjęty przez najpopularniejsze przeglądarki internetowe, które posiadają wbudowaną funkcjonalność tego typu.[9]

[7] https://www.troyhunt.com/extended-validation-certificates-are-dead/ [dostęp: 21.01.2025 r.]
[8] C. Sample, A. Karamanian, Culture and Cyber Behaviours: DNS Defending, Journal of Information Warfare 2015, vol. 14, no. 4, s. 60; J. Sherman, Addressing and the domain name system, The politics of internet security: private industry and the future of the web, Atlantic Council, 2020, s. 6–21.
[9] C. L. Romera, DNS Over HTTPS Traffic Analysis and Detection, Universitat Oberta de Catalunya, http://hdl.handle.net/10609/119946 [dostęp 21.01.2025]

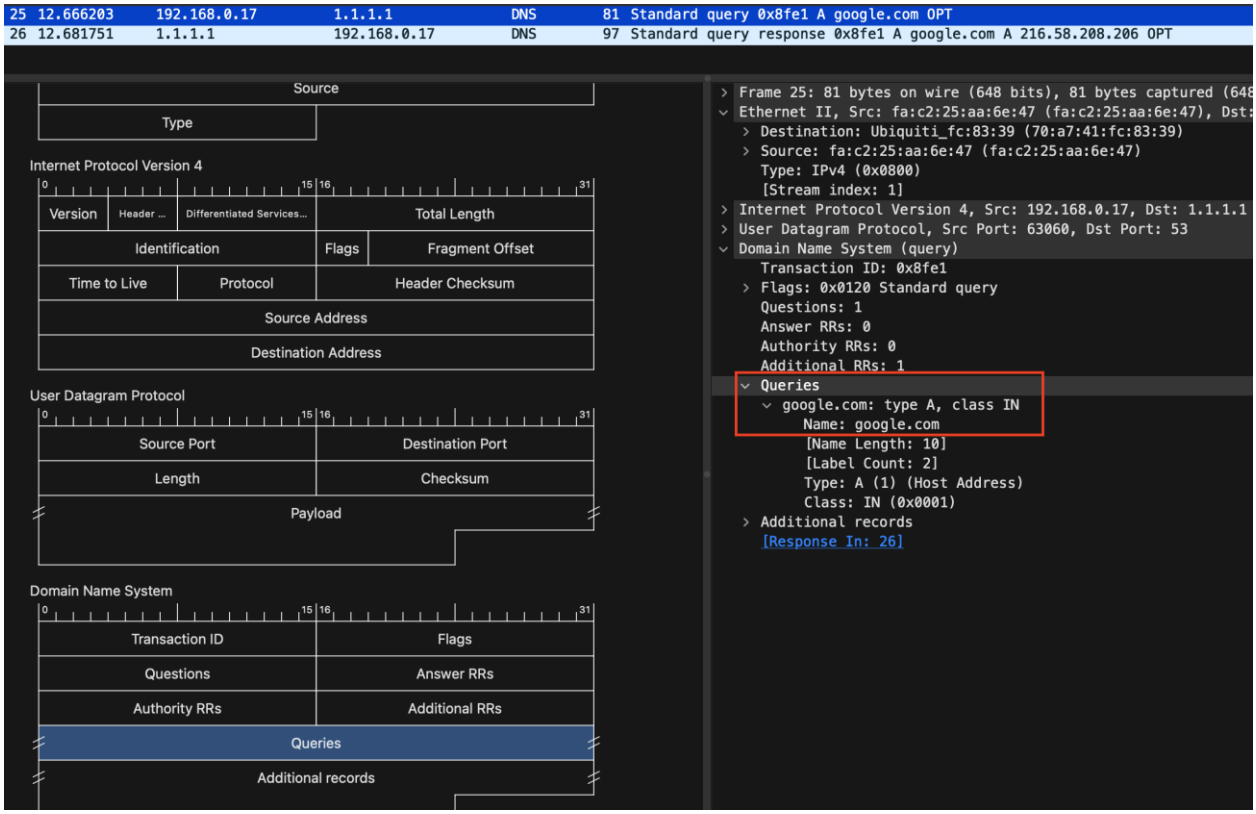

Figura 3 Przykładowy nieszyfrowany ruch DNS, opracowanie własne

Mechanizmy zapewniające prywatność i integralność zapytań DNS są bez wątpienia bardzo ważnym mechanizmem zwiększającym bezpieczeństwo użytkownika. Należy jednak pamiętać, że kolejnym etapem nawiązania bezpiecznego połączenia jest wykonanie zapytania na przekazany przez serwer DNS adres IP, które będzie zawierało w sobie informację dot. jaką domenę planujemy odwiedzić. Wynika to z faktu, że na wskazanym adresie IP może być utrzymywane więcej niż jedna strona internetowa – jest to szczególnie istotne wobec aktualnego rozwoju rozwiązań chmurowych tj. *Content Delivery Network* – świadcząc w ramach swojej infrastruktury usługi dla milionów klientów[10].

[10] F. Musiani, Decentralizing DNS: Peers, Infrastructure, and Internet Governance, Georgetown Journal of International Affairs 2013, s. 111.

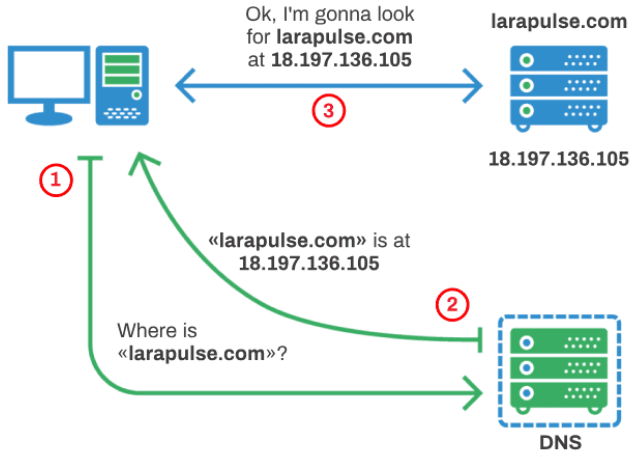

Figura 4 Schemat przedstawiający przepływy sieciowe niezbędne do uruchomienia strony internetowej, źródło: https://blog.larapulse.com/network/how-dns-servers-work (dostęp: 21.01.2025 r.)

Wskazany parametr nazywany jest *Server Name Extension* i pozwala na identyfikację domeny, o którą prosi klient. Następnie następuje wymiana certyfikatów i dalszy ruch jest szyfrowany. Problem ten został wstępnie zaadresowany przez firmę CloudFlare, która przyczyniła się do prac oraz popularyzacji dodatkowego rozszerzenia dla protokołu TLS o nazwie *Encrypted Client Hello* (w skrócie ECH)[11]. Mechanizm ten ma zagwarantować poufność komunikacji już na wczesnym etapie wymiany informacji o certyfikacie, przez co nie będzie konieczności umieszczania w formie jawnej informacji o odpytywanej domenie. Rozwiązanie to nie jest jeszcze szeroko stosowane[12].

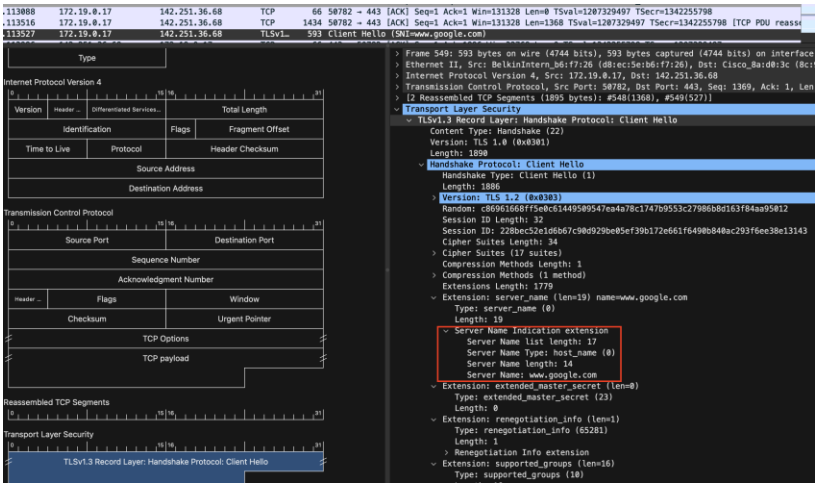

Figura 5 Przykładowy szyfrowany ruch HTTPS, opracowanie własne

[11] N. Meysenburg et al., Encryption, Evaluating the Digital Standard: How to Assess the Security of the Internet of Things, New America, 2020, s. 119.
[12] https://blog.cloudflare.com/encrypted-client-hello/ [dostęp: 21.01.2025 r.]

Bez wątpienia bezpieczeństwo użytkownika oraz poufność i integralność jego komunikacji będzie w najbliższych lata bardzo istotnym tematem, który wymusi wypracowanie nowych standardów. Jest to szczególnie ważne ze względu na coraz bardziej surowe ustawodawstwo, które wymusza ograniczanie zbierania danych oraz nakłada wysokie kary w przypadku wykrycia zaniedbań. Należy mieć na uwadze, że przy odpowiednich siłach i środkach istnieje możliwość profilowania użytkowników na podstawie zapisu jego ruchu sieciowego. Nie ma konieczności poznawania faktycznej treści komunikacji w momencie gdy można ustalić z jakich stron internetowych korzysta, w jakich godzinach to robi oraz ile czasu na nich spędza. Oczywiście analiza takiego ruchu wymaga dostępu do łącza, po których jest prowadzona transmisja, jednak w przypadku odpowiedniego zaangażowania i zaplecza technicznego jest to technicznie wykonalne.

Lista figur

Bibliografia

Boyle M., Information Assurance Standards: A Cornerstone for Cyber Defense.Journal of Information Warfare 2014, vol. 13, no. 2.
Chou C. et al., A Review of the Research on Internet Addiction, Educational Psychology Review 2005, vol. 17, no. 4, 2005.
Holtmanns S., Mobile Web Service Security, Journal of Information Warfare 2004, vol. 3, no. 1.
https://blog.cloudflare.com/encrypted-client-hello/ [dostęp: 21.01.2025 r.]
https://www.statista.com/statistics/871513/worldwide-data-created/ [dostęp: 21.01.2025 r.]
https://www.troyhunt.com/extended-validation-certificates-are-dead/ [dostęp: 21.01.2025 r.]
Malish A.S., Navigating Cyber Coverages for Modern Day Cybercrimes, Tort Trial & Insurance Practice Law Journal 2019, vol. 54, no. 3.
Meysenburg N. et al., Encryption, Evaluating the Digital Standard: How to Assess the Security of the Internet of Things, New America 2020.
Mudler Ch., Improving Early Phishing Detection using SSL & WHOIS data: an Application to PhishDetect for Civil Society Protection, https://research.tue.nl/en/studentTheses/improving-early-phishing-detection-using-ssl-whois-data [dostęp:21.01.2025]
Musiani F., Decentralizing DNS: Peers, Infrastructure, and Internet Governance, Georgetown Journal of International Affairs 2013.
Romera C. L., DNS Over HTTPS Traffic Analysis and Detection, Universitat Oberta de Catalunya, http://hdl.handle.net/10609/119946 [dostęp 21.01.2025]
Sample C., Karamanian A., Culture and Cyber Behaviours: DNS Defending, Journal of Information Warfare 2015, vol. 14, no. 4.
Sherman J., Addressing and the domain name system, The politics of internet security: private industry and the future of the web, Atlantic Council 2020.

SECURE NETWORK DATA TRANSPORT

Abstract

The article discusses the topic of data encryption during transport in client-server communication and presents the benefits of this solution. It also covers the threats and imperfections of popular protocols that require modernization. In particular, aspects of user privacy and technical possibilities of network traffic analysis will be discussed. In the early phases of the Internet, the confidentiality of transmissions was not crucial, as very few people had access to the network itself, and the creation of the vast network itself was a huge invention. Fortunately, the development of technology addressed this problem and created a mechanism to maintain confidentiality in client-server transmissions. This mechanism is known in the IT world as TLS (Transport Layer Security). This solution ensures the security of communication by encrypting the transmitted data. This is especially important in the context of transmitting information, i.e. logins and passwords, files or private correspondence.

Keywords: data confidentiality, encryption, network protocol.