VALSTYBINĖ
DUOMENŲ APSAUGOS
INSPEKCIJA

SAUGUS NARŠYMAS INTERNETE

Rekomendacija

Parengė
Egidijus Rasiulis
Valstybinės duomenų apsaugos inspekcijos
Informacijos ir technologijų skyriaus vyriausiasis specialistas

2017 m.

TURINYS

KAS YRA HTTPS?

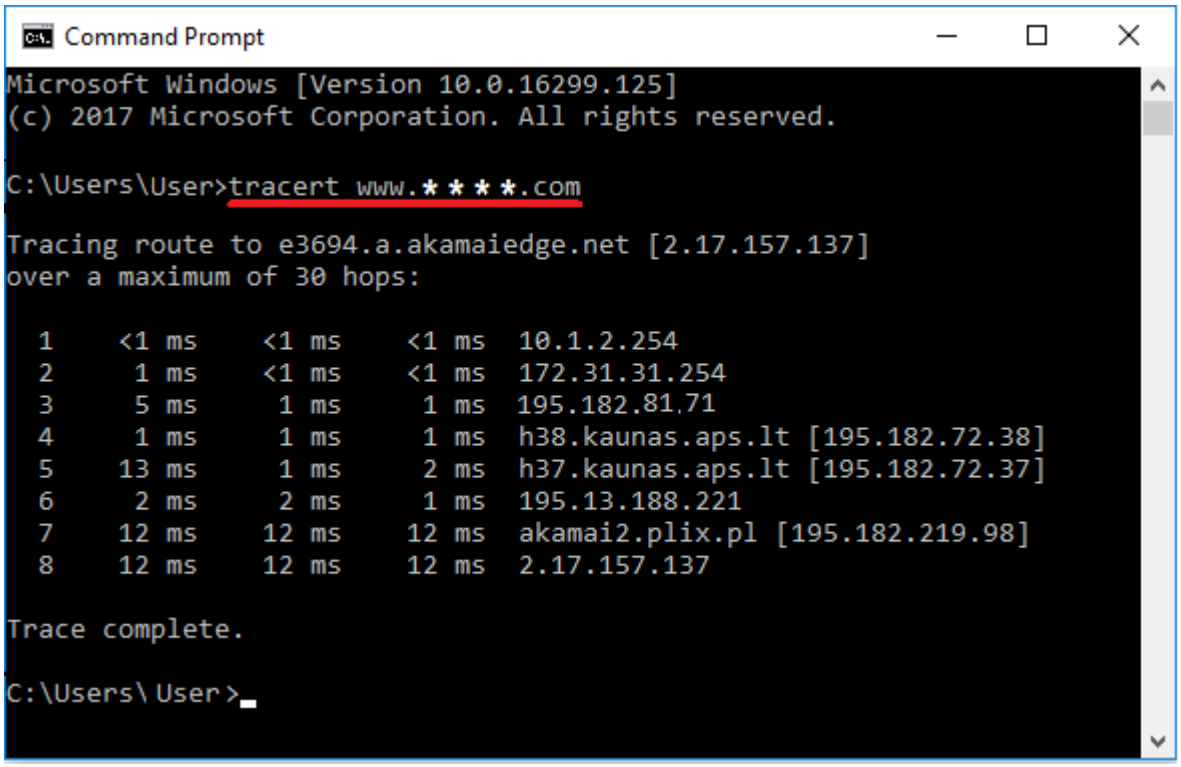
Asmens duomenų saugumas internete yra šių dienų aktualija. Mes apsipirkinėjame elektroninėse parduotuvėse, atliekame mokėjimus internetu, įvedame slaptažodžius į savo paskyras socialiniuose tinkluose ir galime bendrauti su valstybinėmis įstaigomis iš namų. Nors tai labai patogu, tačiau kyla rizika, kad perduodamus duomenis kas nors gali perimti. Tad kuo gali būti naudingas HTTPS protokolas?

Tam, kad skirtingi elektroniniai įrenginiai galėtų bendrauti vienas su kitu, informacijos perdavimui ir priėmimui reikalingos tam tikros taisyklės ir susitarimai, kurių įrenginiai laikysis. Tai yra vadinama duomenų perdavimo protokolu. Šiuo metu tinklinio ryšio tarp kompiuterių palaikymo protokolas yra TCP/IP, svetainių turinio priėmimo ir perdavimo protokolas visame žiniatinklyje yra HTTP (angl. *Hyper Text Transfer Protocol*) ir saugesnė jo versija HTTPS (angl. *Hyper Text Transfer Protocol Secure*).

Taigi, kai norite atverti jums rūpimą svetainę, jūsų naršyklė siunčia užklausą svetainės tarnybinei stočiai, naudodama HTTP protokolą, o tarnybinė stotis, apdorojusi užklausą, atsakymą persiunčia naršyklei, duomenis apdorodama pagal HTML taisykles, ir apdorotų duomenų rezultatas pateikiamas vartotojui į jo naršyklę, t. y. kompiuterio ekraną. Kiekvieną kartą spustelėję nuorodą internetiniame puslapyje, mes įvedame duomenis į įvairius laukus ir ši informacija perduodama į tarnybinę stotį, ten apdorojama ir siunčiamas atsakymas naršyklei. Taip bendrais bruožais atrodo sąveika tarp jūsų naršyklės ir svetainės tarnybinės stoties.

Duomenų mainų schema tarp naršyklės ir svetainės tarnybinės stoties nepriklauso nuo naudojamo įrenginio tipo ar jo operacinės sistemos. Veikimas yra vienodas tiek kompiuteryje, tiek ir išmaniajame telefone, planšetėje ar televizoriuje. Ir nesvarbu ar tai bus „Windows“, „macOS“ ar „Android“ operacinė sistema.

Svarbu žinoti, kad duomenų perdavimas HTTP protokolu turi reikšmingų trūkumų – visi duomenys tinkle perduodami atviru pavidalu per neapsaugotą ryšio kanalą. Šiuo atveju jūsų naršyklė neturi tiesioginio ryšio su svetainės tarnybine stotimi, o ryšys tarp naršyklės ir svetainės tarnybinės stoties vyksta per daugybę tarpinių tinklo taškų. Pirmiausia tai bus jūsų vietinis tinklas (jei jis yra), tada tinklas, kuris priklauso jūsų interneto paslaugų teikėjui, o po to bus kitų organizacijų tinklai su jų tinkline įranga, kol galiausiai pasieksite jums rūpimos svetainės tarnybinę stotį. Tai lengvai galite patikrinti ir patys, savo kompiuteryje pasirinkę „Windows“ „Command Prompt“ komandinės eilutės dialogo langą, kuriame įvedę komandą „tracert hostname“ („Linux“ ir „macOS“ operacinių sistemų vartotojams komanda būtų „traceroute hostname“). „Hostname“ vietoje įrašykite dominančios interneto svetainės adresą. Naudojant DNS tarnybinę stotį, bus nustatytas tarnybinės stoties IP adresas, sukurta paketų perdavimo grandinės dalis iki galutinio tinklinio taško. 1 pav. matyti, kad pabandžius patikrinti, kaip nueina užklausa iš jūsų kompiuterio iki internetinės svetainės www.****.com duomenų paketai praeina 8 skirtingus tinklo taškus.



1 pav. Maršruto patikrinimas „tracert“ komanda

Kai kam tai gali kelti nuostabą, tačiau jei koks nors asmuo, turintis piktų kėslų, prisijungs prie vieno iš grandinėje esančių tarpinių taškų, vedančių link svetainės tarnybinės stoties, jis galės perimti į svetainę jūsų perduodamą duomenų srautą, pavyzdžiui, slaptažodžius, jūsų įvestus kredito kortelių numerius ir kitą jūsų asmeninę informaciją. Esate ypač pažeidžiami, kai viešosiose vietose naudojatės atvirais belaidžiais tinklais (Wi-Fi). Naudojantis tokiais atvirais belaidžiais tinklais piktavalis gali įsibrauti tarp jūsų naršyklės ir svetainės tarnybinės stoties naudojant vadinamąją *„Man-In-The-Middle“ ataką*.

Tai nėra labai aktualu toms paprastoms informacinio pobūdžio svetainėms, kuriose lankytojai savo duomenų nepateikia, tačiau interneto bankams ir finansinėms institucijoms, socialinių tinklų, internetinių parduotuvių, elektroninio pašto paslaugas teikiančioms įmonėms, elektroninių mokėjimo sistemų ir kitų svetainių, kurios tvarko savo klientų asmens duomenis, tai yra tikras iššūkis ir nemažas galvos skausmas. Nors, kita vertus, prarasti prieigą prie mėgstamiausio forumo taip pat nėra labai malonus dalykas.

Šią problemą galėtų padėti spręsti HTTP**S** protokolo naudojimas. Koks skirtumas tarp HTTP ir HTTPS protokolų? HTTPS (angl. *HyperText Transfer Protocol Secure*) yra paprasto HTTP protokolo esamų galimybių praplėtimas perduodamus duomenis šifruojant SSL/TLS priemonėmis, todėl HTTP**S** laikomas saugiu protokolu.

Visos šiuolaikinės naršyklės žino, kaip, naudojant kriptografinius metodus, perduoti duomenis HTTPS protokolu. Senesnių naršyklių savininkai turėtų pagalvoti dėl savo naršyklių atnaujinimo, nes rizikuoja atidaryti svetaines, kurios vis dar naudoja pasenusius HTTP protokolus ir tokiu būdu rizikuoja atskleisti perduodamus duomenis bei sumažina savo duomenų saugumą.

Nors saugaus HTTP**S** protokolo naudojimas neišsprendžia duomenų srauto perėmimo galimybės pilna apimtimi, tačiau tai, kad visi duomenys perduodami šifruotu pavidalu, žymiai apriboja galimybes piktavaliui juos perimti, nes duomenis dar reikia suspėti iššifruoti žinant slaptą (privatų) raktą, o tai tampa beveik neįmanoma.

KAIP VEIKIA HTTPS?

Duomenys tarp vartotojo naršyklės ir svetainės tarnybinės stoties perduodami šifruotu pavidalu, naudojant SSL (TLS) šifravimo protokolus. Tam, kad naršyklė ir svetainės tarnybinė stotis galėtų saugiai komunikuoti, jos turi sukurti tarpusavyje užšifruotą ryšį. Šiam saugiam ryšiui užtikrinti būtina susitarti dėl privačių raktų, kuriais galima užšifruoti ir iššifruoti vienas kito perduotą informaciją. Problema kyla, nes tiesiog išsiųsti tokį raktą iš vieno kitam negalima, nes atvirai išsiųstas raktas nesaugiame interneto tinkle gali būti lengvai perimtas ir koks nors piktavalis gali iššifruoti duomenų srautą, pasinaudojęs šiuo perimtu slaptu raktu. Tai būtų tas pats, kaip garsiai padiktuoti savo slaptažodį nuo prisijungimo paskyros girdint svetimiems žmonėms.

Nors ši privačios komunikacijos užmezgimo problema yra sudėtinga, tačiau sprendimas yra – reikėtų naudoti kitiems nesuprantamą kalbą. Kalbant apie saugų ryšį kompiuterinėse technologijose, tam naudojama kriptografija.

Tarnybinėje stotyje įdiegto SSL sertifikato atveju, svetainės lankytojo naršyklė HTTPS protokolu klausdama tarnybinės stoties autentiškumo, gauna tarnybinės stoties autentifikacijos patvirtinimą. Po sėkmingo tarnybinės stoties savininko autentifikavimo svetainės lankytojo naršyklė ir tarnybinė stotis per gana trumpą laiką įvykdo gana sudėtingą raktų apsikeitimo procedūrą. Vykdant saugų HTTP**S** susijungimą, svetainės lankytojo naršyklė iš tarnybinės stoties gauna viešą užšifravimo 2048 bitų asimetrišką raktą, kuris duomenis gali užšifruoti, bet negali jų iššifruoti. Šis tarnybinės stoties viešasis raktas dalijamas visoms naršyklėms, kurios pateikia užklausą.

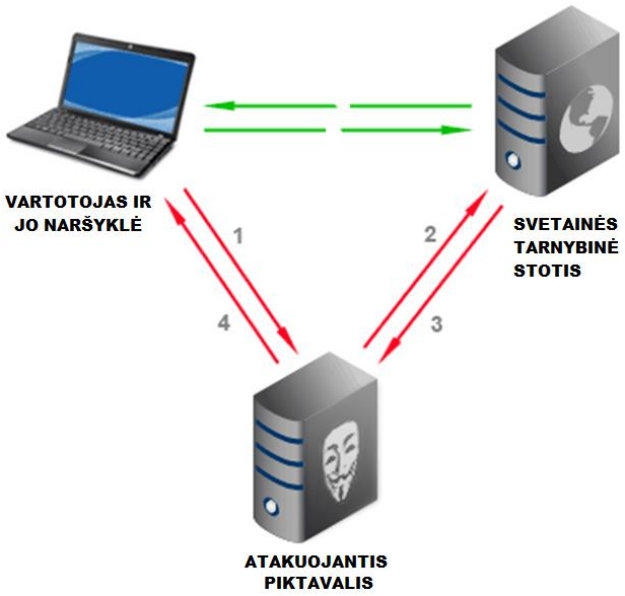
Duomenis iššifruoti gali tik privatus iššifravimo raktas, kuris saugomas tarnybinėje stotyje. Kol šis tarnybinės stoties privatus raktas nėra prarastas ar sugadintas, bet kas gali viešuoju raktu patikimai užšifruoti duomenis ir konfidencialiai juos perduoti tarnybinei stočiai. Svetainės lankytojo perduodamus užšifruotus duomenis išsišifruoti gali tik tarnybinė stotis savo privačiu raktu, tačiau niekas kitas tų duomenų iššifruoti negali. Po to, kai tarnybinė stotis pateikia svetainės lankytojo naršyklei savo viešą asimetrinį užšifravimo raktą, svetainės lankytojo naršyklė sukuria ir užšifruoja slaptą sesijos raktą. Šis tarnybinės stoties viešasis SSL sertifikato raktas naudojamas tik ryšio tarp tarnybinės stoties ir svetainės lankytojo naršyklės seanso pradžioje. Naršyklė, gavusi tarnybinės stoties viešąjį raktą, sukuria laikiną 256 bitų simetrišką sesijos raktą, kurs perduodamus duomenis gali ir užšifruoti, ir iššifruoti. Tada svetainės lankytojo naršyklė užšifruoja simetrišką raktą su gautu tarnybinės stoties viešuoju raktu ir išsiunčia užšifruotus duomenis tarnybinei stočiai.

Serveris gautą duomenų paketą išsišifruoja savo privačiu raktu ir tokiu būdu iš svetainės lankytojo naršyklės gauna simetrišką raktą. Po šios duomenų apsikeitimo operacijos tiek svetainės lankytojo naršyklė, tiek ir tarnybinė stotis žino tą patį simetrišką raktą. Taip sukuriamas simetriškas abipusis duomenų šifravimas ir iššifravimas. Toliau visi duomenys tarp tarnybinės stoties ir svetainės lankytojo naršyklės perduodami juos šifruojant simetrišku sesijos raktu. Atsižvelgiant į tai, kad simetriško rakto joks kitas ryšio dalyvis negali turėti, todėl duomenys tarp svetainės lankytojo naršyklės ir tarnybinės stoties perduodami visiškai saugiai.

Ši asimetrinio šifravimo, kaip vienakryptės matematinės funkcijos ypatybė, kurią lengvai galima apskaičiuoti tik viena kryptimi, vadinama Diffie-Hellmano algoritmu. Žinoma, šios duomenų mainų manipuliacijos sukuria papildomą apkrovą tarnybinei stočiai ir esant dideliam vartotojų srautui šiek tiek lėtina jos veikimą, tačiau tai atlikti reikia tik kartą ryšio seanso pradžioje. Net jei kas nors iš pašalinių perimtų išankstinį pasikeitimą pranešimais, tai jums nepakenktų. Tolimesnis pasikeitimas duomenimis yra šifruojamas naudojant gautą slaptą (privatų) raktą ir duomenis patikimai apsaugant nuo pašalinių. Ši procedūra vadinama simetriniu šifravimu.

KODĖL SVETAINEI REIKALINGAS IŠPLĖSTINIS SERTIFIKATAS SU AUTENTIFIKACIJOS PATVIRTINIMU?

Jei vis tik apgaulės (angl. *fishing*) ar virusinio įskiepio būdu piktavaliui pavyksta įsiterpti tarp jūsų naršyklės ir jus dominančios svetainės tarnybinės stoties, jis gali lengvai jūsų naršyklei prisistatyti kaip svetainės tarnybinė stotis, kuriai buvo pateikta užklausa gauti saugų ryšiui reikalingą raktą. Tuomet piktavalis gali kreiptis į svetainės tarnybinę stotį, į kurą buvo išsiųsta užklausa, prisistatyti kaip vartotojo naršyklė ir užmegzti privatų ryšį. Taip piktavalis gali gauti šifruotas užklausas iš naršyklės, iššifruoti jas ir vėl užšifruoti naudodamas kitą raktą bei persiųsti svetainės tarnybinei stočiai apsimetęs vartotojo naršykle. Piktavalis veiks kaip tarpininkas, visiškai kontroliuojantis ryšį, o naršyklė ir svetainės tarnybinė stotis apie tai net nežinos, galvodami, kad jie bendrauja tiesiogiai be jokių tarpininkų (2 pav.).



2 pav. „Man-In-The-Middle“ atakos schema

Šis pavyzdys akivaizdžiai įrodo būtinybę užtikrinti autentiškumą, nors autentiškumo patvirtinimas nėra toks jau paprastas. Įsivaizduokite, kad jums reikia susitikti su nepažįstamuoju, kurio niekada nematėte, bet jūs žinote tik jo vardą. Kaip įsitikinti, kad asmuo, kuris atvyko į susitikimą, yra būtent tas, kuriuo jis prisistato esąs? Nors galimybių yra daug, tačiau paprasčiausia yra paprašyti jo parodyti asmens tapatybę patvirtinantį dokumentą, pavyzdžiui, pasą, ir, jei vardas sutampa su tuo, kurio laukėte, tai tikėtina, kad tai tas asmuo ir yra. Pasu patikime todėl, kad tai oficialus dokumentas, išduotas visuotinai pripažįstamos institucijos piliečių identifikavimui.

Internete viskas vyksta panašiai. Siunčiant užklausą į svetainę ir naudojant šifravimą, labai svarbu įsitikinti, ar į mūsų užklausą atsakė tinkama svetainė, o ne ta, kuri tik apsimeta tokia esanti. Tokiam autentifikavimui patvirtinti yra skirtos specialios organizacijos, vadinamieji sertifikavimo centrai (angl. *Certificate Authority (CA)*). Jų užduotis – patikrinti ir patvirtinti (paliudyti) domeno egzistavimą ir jo valdymą. Jei įmonės, kuriai priklauso svetainė, patikra yra sėkminga, sertifikavimo centras išduoda savo parašu patvirtintą skaitmeninį sertifikatą. Kaip ir paso išdavimo atveju, viskas grįsta pasitikėjimu visuotinai pripažįstama organizacija. Naršyklėse iš anksto yra įdiegta informacija apie šiuo metu esamus (galiojančius) sertifikavimo centrus, kuriomis naršyklės pasitiki.

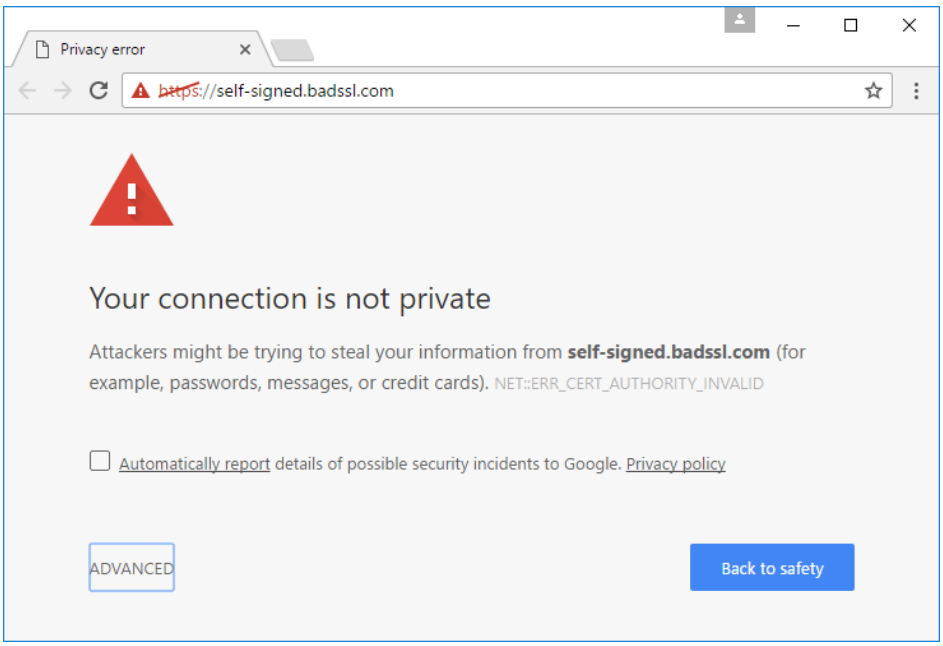
Taigi, svetainės skaitmeninis sertifikatas išsprendžia svetainės autentifikavimo problemą, o SSL/TLS protokolas šifravimu užtikrina saugų duomenų perdavimą atvirais ryšio kanalais. Tik esant tinkamam skaitmeniniam sertifikatui, kurį svetainėje patvirtina patikimas sertifikavimo centras, atsiranda galimybė užmegzti šifruotą HTTPS ryšį.

KAS, JEI SERTIFIKATAS NETURĖS PATVIRTINTOS AUTENTIFIKACIJOS?

Svarbiausias dalykas, ar naršyklės pasitiki pateikiamu sertifikatu, nes sertifikatą gali išduoti ir svetainės savininkas pats sau. Tokie sertifikatai vadinami savarankiškai pasirašytais sertifikatais.

Atrodytų, kad pakaktų vien užmegzti ryšį, tačiau naršyklės vien techniniu ryšiu nepasitiki, nes niekas nepaliudijo svetainės autentiškumo. Vartotojui naršyklė praneš (3 pav.), kad sertifikatas nėra patikimas jei:

- Svetainės sertifikatas yra pasirašytas savarankiškai;
- Išduotas nežinomo sertifikavimo centro;
- Domenas nesutampa;
- Pasibaigė sertifikato galiojimas.

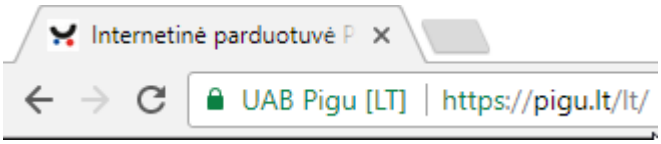


3 pav. Pranešimas apie nepatikimą sertifikatą

Kalbant apie svetainės sertifikato patikimumą, galima išskirti tris lygius: paprastas, įmonės patvirtinimo ir išplėstinis įmonės patvirtinimas. Esant paprastam SSL sertifikato patvirtinimui (angl. *Domain Validation (DV)*), jo išdavimo metu patikrinamas ir patvirtinamas svetainės domeno egzistavimas bei teisės į domeno nuosavybę atitiktis. Tai labiausiai paplitęs internetinių svetainių skaitmeninių sertifikatų tipas. Tačiau visais kitais atvejais to nepakanka. Įsivaizduokite, kad kas nors sukūrė gerai žinomos internetinės parduotuvės ar banko tos pačios išvaizdos ir labai panašaus domeno pavadinimo svetainės kopiją. Toks piktavalis gali teisėtai gauti paprastą skaitmeninį sertifikatą ir stengtis įtikinti nepastabius lankytojus jungtis prie šios svetainės turėdamas kėslų pavogti jų asmens duomenis.

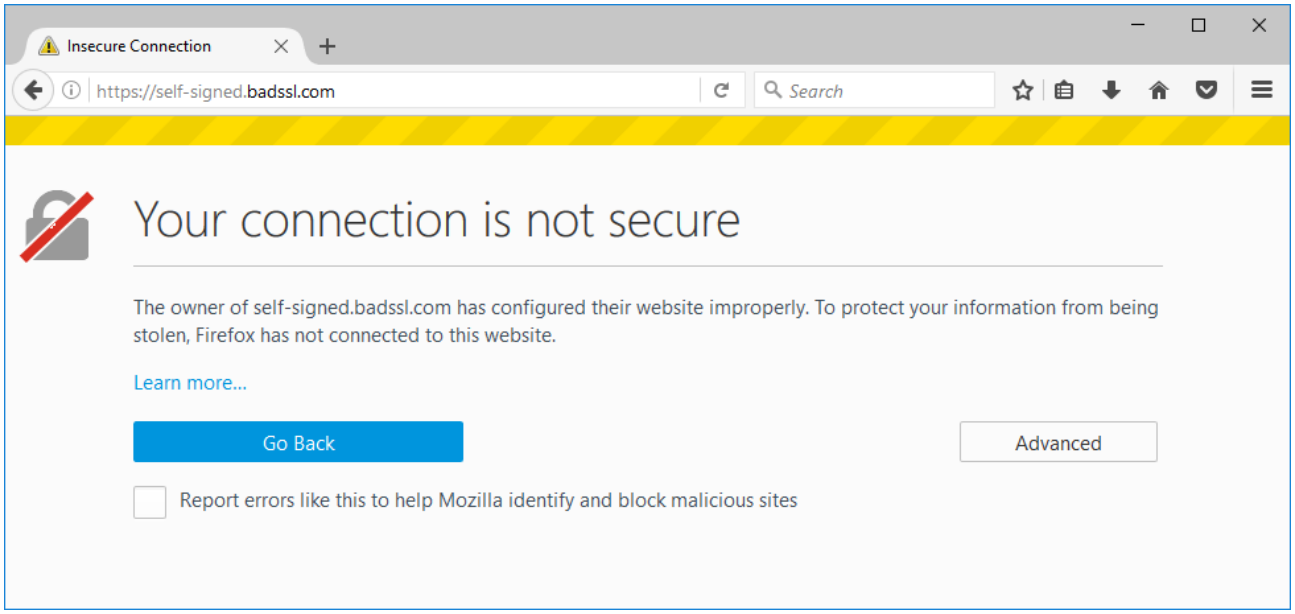
Svetainių savininkai, norėdami apsaugoti savo klientus nuo galimų piktavalių, gali užsakyti savo svetainės SSL sertifikatą, kuriuo papildomai yra patikrinama jų įmonė. Šiuo atveju sertifikavimo centras papildomai patvirtina įmonės egzistavimą, o sertifikatas liudija ne tik domeną, bet ir įmonės, kuriai jis yra išduotas, pavadinimą.

Sertifikatai su išplėstiniu patvirtinimu (angl. *Extended Validation (EV)*), kaip išplėstinio patvirtinimo santrumpa, yra brangesni ir sudėtingiau pasiekiami. Organizacijoms, norinčioms juos gauti, taikomi specialūs reikalavimai ir atliekami išsamūs patikrinimai. Juos paprastai užsako didelės įmonės, branginančios savo klientų pasitikėjimą, kurių reputacija yra labai svarbi ir joms yra būtina papildoma apsauga. Svetainės, turinčios išplėstinio patvirtinimo sertifikatus, naršyklėse turi papildomą skiriamąjį ženklą – žalios spalvos savo pavadinimą. Tokiais sertifikatais interneto vartotojai labiausiai pasitiki.



Taip pat pažymėtina, kad svetainių puslapiai nėra vientisi. Jie sudaryti iš atskirų dalių, tokių kaip tekstas, paveikslėliai, stilių įvairovė, programinis kodas ir pan. Visą tai yra sudėtinė puslapio dalis, kurie naršyklėje įkeliami atskirai. Tokiu būdu galima situacija, kai kiekvienas iš šių elementų bus svetainėje įkeliamas tuo protokolu, pavyzdžiui, HTTP, kuris aprašytas puslapio kode, vietoj to, koks yra naudojamas šiame puslapyje, pavyzdžiui, HTTPS.

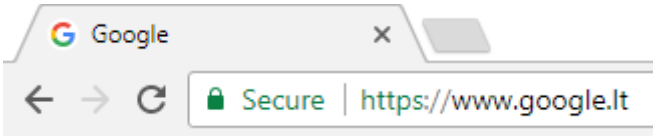
Jei atidarinėtume svetainę su apsaugotu HTTPS protokolu, o paveikslo užklausa būtų vykdoma su paprastu HTTP, tuomet naršyklė atveriamą puslapį traktuotų kaip skirtingo turinio, o tai, žinoma, mažintų sujungimo saugumą. Apie tai svetainė lankytojui praneša naršyklės adresų juostoje esančiu įspėjančiuoju ženklu apie pastebėtą klaidą. Spustelėję ant „Learn more“ nuorodos, pamatysite pranešimo detales.



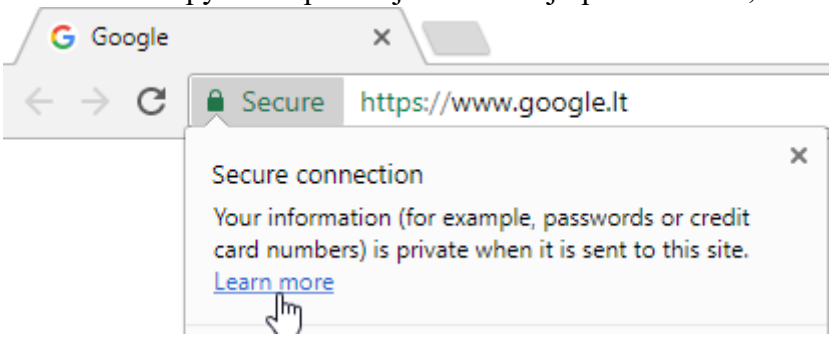
HTTPS ryšiu bandant įkelti „JavaScript“ kodą arba svetainės CSS stiliaus failus HTTP protokolu, naršyklė tokį puslapį blokuotų, interpretuodama tai kaip rimtą pažeidžiamumą. Likusi įkelta puslapio dalis laikoma saugi, tačiau ji gali veikti nekorektiškai dėl ne nepilnai įkeltų puslapio turinio elementų. Jei vis tik nepaisant saugos perspėjimų norima šiuos elementus atidaryti, galima informaciniame pranešime paspausti atitinkamas nuorodas. Naršyklė atnaujins puslapio įkėlimą, bet visą puslapį pažymės kaip nesaugų.

KAIP PATIKRINTI SSL SERTIFIKATĄ „CHROME“ NARŠYKLĖJE

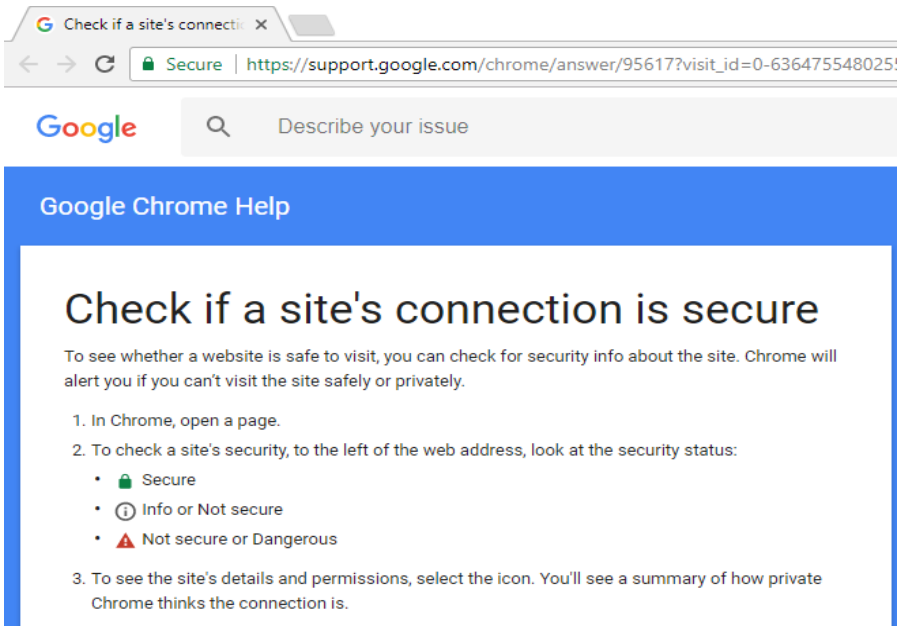
„Chrome“ naršyklėje saugus HTTPS protokolo ryšys matyti naršyklės adresų juostoje, kai spynelės piktograma yra žalia, o užrašas yra „Saugu“ (angl. *Secure*).



Ant spynelės spustelėjus dešiniuoju pelės klavišu, iššoka meniu:

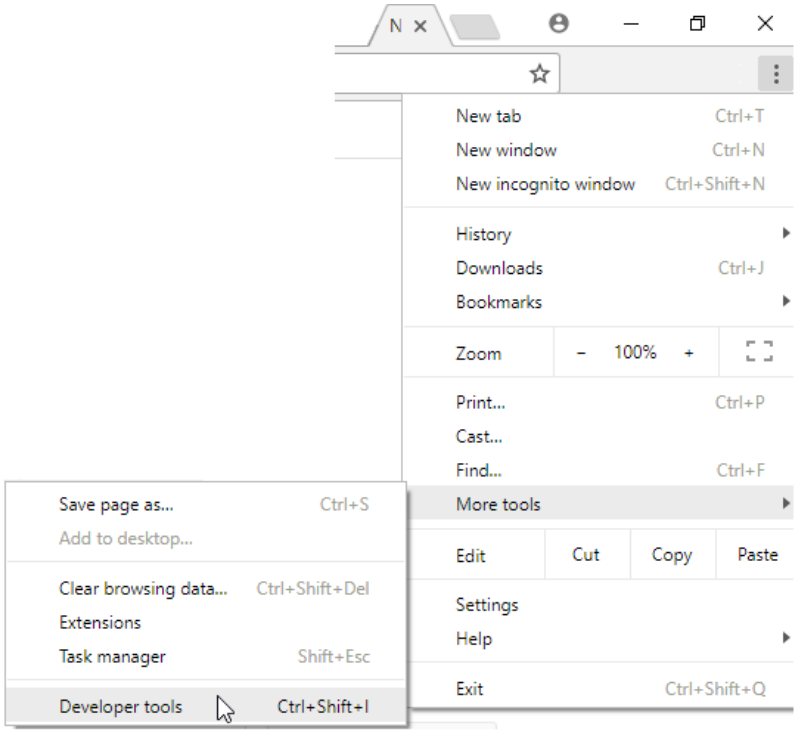


Norėdami detaliau patikrinti spynele žymimą saugaus ryšio pranešimą, spaudžiame nuorodą „Sužinokite daugiau“ (angl. *Learn more*), kuri apibūdina, kad ryšys yra saugus (4 pav.).



4 pav. Langas, paaiškinantis pranešimų apie saugias ir nesaugias svetaines žymėjimą

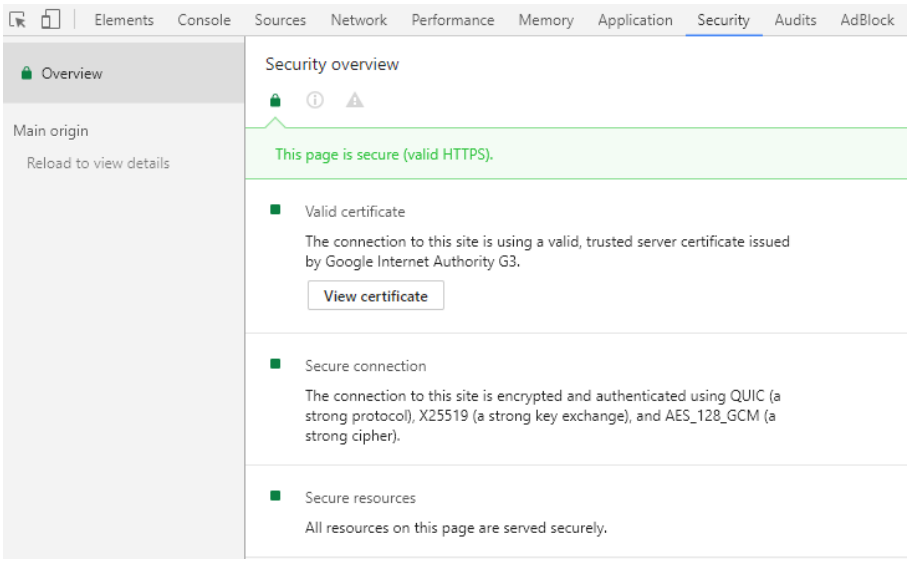
Pasiekti detalesnes SSL sertifikato savybes galima per bendrąjį naršyklės nustatymų meniu (5 pav.). Tai pamatysite spustelėję piktogramą su vertikaliu daugtaškiu, esančiu naršyklės dešinėje adreso juostos pusėje.



5 pav. Iššokantis meniu detalesnėms SSL sertifikato savybėms pasiekti

Iš išsiskleidusio meniu pasirenkame „Papildomi įrankiai“ (angl. *More Tools*), iš kurių renkamės „Kūrėjo įrankiai“ (angl. *Developer Tools*).

Atsidariusiame lanke pasirenkame skirtuką „Sauga“ (angl. *Security*). Čia galite pamatyti saugaus susijungimo (angl. *Security Connection*) savybes (6 pav.), o taip pat mygtuką „Peržiūrėti sertifikatą“ (angl. *View Sertificate*).

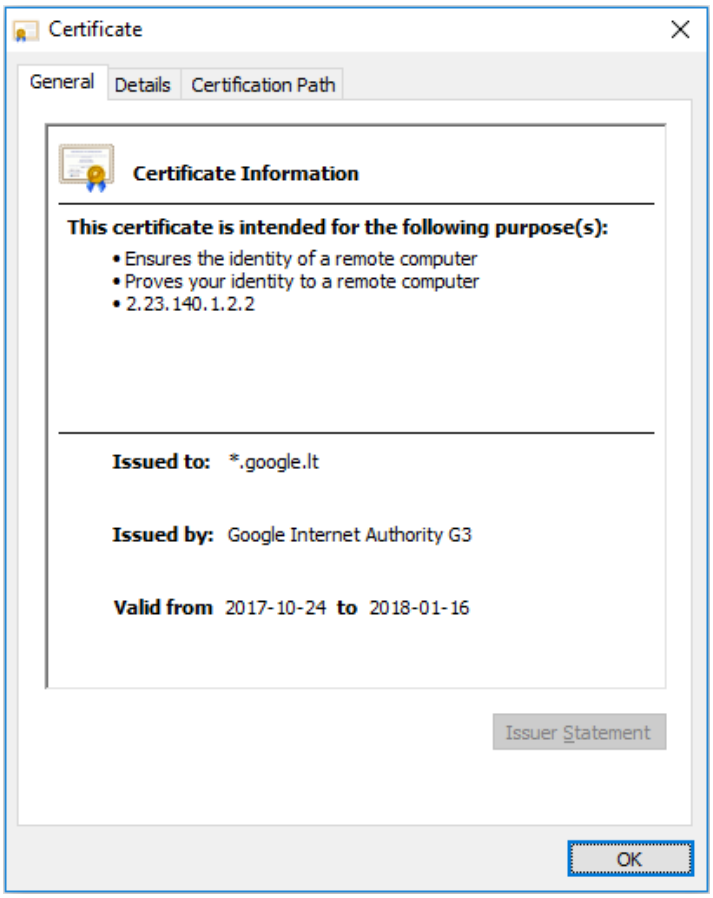


6 pav. Skirtuko „Sauga“ langas

Paspaudę mygtuką „Peržiūrėti sertifikatą“, matysite langą su SSL sertifikato savybėmis. Atsidaro langas su informacija apie sertifikatą (7 pav.).

Skirtuke „Bendra“ (angl. *General*) yra pagrindinė informacija apie sertifikatą: sertifikato paskirtis, kas ir kam šį sertifikatą išdavė bei nurodomas sertifikato galiojimo laikas. Šiuo atveju jis išduotas:

- Nuotolinio kompiuterio (tinklalapio) nustatymui;
- „Google.lt“ domenui ir jo subdomenams (8 pav.);
- „Google“ interneto administravimo G3 sertifikavimo centrui;
- Išduotas laikotarpiui nuo 2017-10-24 iki 2018-01-16.

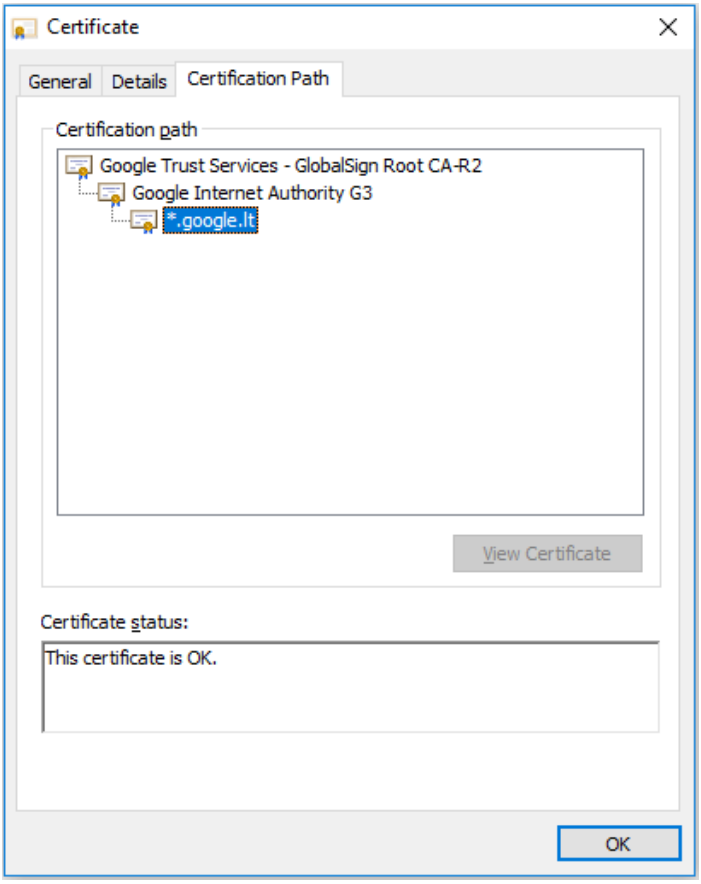


7 pav. Skirtuko „Bendrasis“ (angl. General) langas

Skirtuke „Sertifikavimo kelias“ (angl. *Sertification Path*) galite pamatyti, kas kurį sertifikatą patvirtino (8 pav.).

Yra nemažai aukščiausio lygio sertifikavimo centrų. Tarpusavyje patvirtinami įgaliojimai išduoti sertifikatus matosi iš grandinėlės, kuri parodyta žemiau.

Šiuo atveju domeno * „google.lt“ SSL sertifikatas buvo išduotas „Google Internet Authority G3“ sertifikavimo institucijos, kuri jį atitinkamai pasirašė su savo skaitmeniniu parašu. „Google Internet Authority G3“ sertifikatą pasirašė ir kita sertifikavimo institucija – „Google Trust Services – GlobalSign Root CA-R2“.



8 pav. Skirtuko „Sertifikavimo kelias“ (angl. Sertification Path) langas

REKOMENDACIJOS

Žinant, kam reikalingas HTTPS protokolas, reikia pripažinti, kad duomenų srauto šifravimo technologija yra žinoma jau senai, ir ją senai naudojo interneto bankų, mokėjimo sistemų, didelių elektroninių parduotuvių savininkai, kuriems svarbu užtikrinti lankytojų privačios informacijos saugą. Pastaruoju metu situacija pradėjo pastebimai keistis – svetainių, kurios naudoja šifruotą HTTPS ryšį, sparčiai daugėja, įskaitant ir tas svetaines, kurios savo veikloje lankytojo asmens duomenų nenaudoja. Internetinės paieškos sistemų politika verčia svetainių savininkus įdiegti saugų protokolą į savo svetaines. Pavyzdžiui, „Google“ pareiškus, kad nuo 2017 metų svetainių, kurios neturės įsidiegusios saugaus protokolo, reitingai paieškos sistemoje mažės, o „Chrome“ naršyklės tokias svetaines pažymės kaip nesaugias. Kita vertus, toks perėjimas sukuria techninių problemų ir iššūkių, todėl daugelis senesnių svetainių savininkų pereina prie saugaus ryšio protokolo ne taip greitai, kaip to norėtų vartotojai. Migracijos procesas link saugių protokolų sparčiai įsibėgėja ir netolimoje ateityje HTTPS visiškai pakeis nesaugų HTTP.

Saugiam naršymui internete svarbu laikytis šių rekomendacijų:

1. Internete teikdami savo asmens duomenis, visada paisykite saugumo reikalavimų. Būkite apdairūs, ypač jei prie šios informacijos turi prieigą bet kuris vartotojas.

2. Apdairiai naudokitės tomis elektroninėmis paslaugomis, kurioms reikia Jūsų asmens duomenų. Prieš pateikdami savo asmens duomenis įsitikinkite, kad interneto svetainė, kuriai teikiami duomenys, yra patikima. Jei elektroniniu paštu gaunate nenumatytą laišką, kuriame prašoma pateikti savo asmens duomenis ir (arba) slaptažodį, – būkite budrūs. Tai dar vienas būdas piktavaliams gauti prieigą prie Jūsų duomenų.

3. Venkite puslapių, kuriuose turite registruoti savo paskyras, užsakyti ir sumokėti už prekes, jei adresai prasideda „http://...“, vietoj „https://....“. Interneto svetainėje, kurios adresas prasideda „https://...“, ryšio duomenys yra šifruojami. Tai, kad ryšys su interneto svetaine ar jos dalimi yra saugus, dažnai parodo mažas pakabinamos spynelės simbolis. „Chrome“ naršyklėje greitai sertifikato peržiūrai naudokite klavišų kombinaciją [CTRL] + [Shift] + „I“.

4. Jungiantis prie savo internetinio banko ar elektroninio pašto paskyros įsitikinkite, kad adresas yra toks, kuriuo įprastai jungiatės. Nenaudokite klaidinančių nuorodų, kurios gali atidaryti fiktyvias interneto svetaines.

5. Nepageidaujami reklaminiai pranešimai ir kitas elektroninio pašto šlamštas (angl. *spam*) ne tik užpildo asmeninio elektroninio pašto erdvę, tačiau su jais gali atkeliauti virusai, suteikiantys neteisėtą prieigą prie Jūsų kompiuterio. Rekomenduojama neatidarinėti prisegtų failų ar nuorodų, gautų elektroniniu paštu iš nepažįstamųjų.

6. Naudokitės tik patikimu interneto ryšiu. Viešose vietose venkite nežinomų tinklų, kurie gali būti piktavalių spąstai. Junkitės prie konkretaus pavadinimo tinklo su *Wi-Fi* tinklo prisijungimo slaptažodžiu. Prisijungę prie viešo *Wi-Fi* venkite naudotis elektronine bankininkyste ar apsipirkimo internetu.

7. Apie internete esamas grėsmes informuokite savo vaikus, suteikite jiems žinių apie saugų elgesį elektroninėje erdvėje.