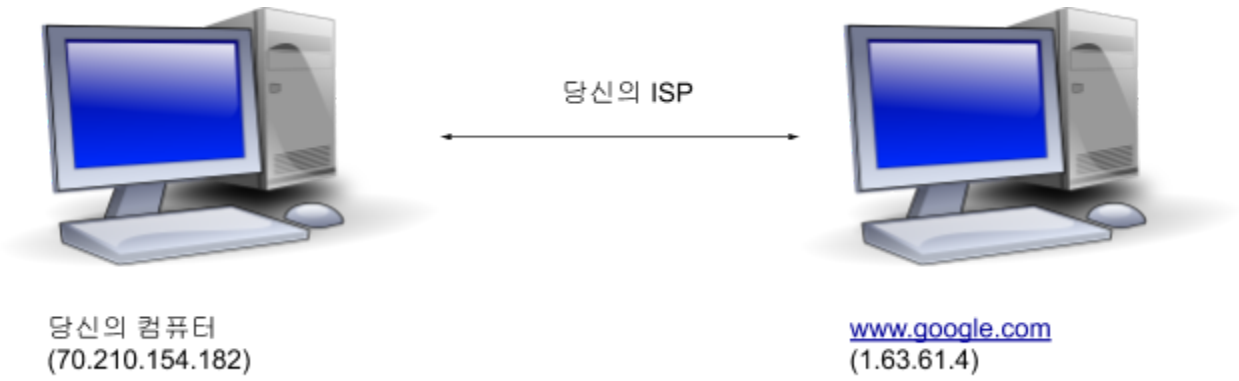
소개

자신을 정부의 감시에서 벗어나게 할 수 없다고 생각하는 것은 흔한 오인입니다. 할 수 있습니다. 정부에 의한 단속에 대한 공포가 자신의 의견을 내놓는 것을 막게 두지 마십시오. Ritser Privacy Toolkit은 당신에게 안전을 보장하고 정보를 알리기 위해 디자인되었습니다.

인터넷 작동 원리

인터넷에 있는 모든 컴퓨터는 서로의 통신을 위해 IP 주소를 가지고 있습니다. 웹 사이트들도 IP 주소를 가지고 있지만, 인터넷 브라우징을 편하게 만들기 위하여 IP 주소에 연결된 별개의 도메인 이름이 있습니다(예: www.facebook.com, www.google.com). 당신의 컴퓨터가 www.google.com에 검색을 실행하려 할 때, 연관된 IP를 찾아 정보를 얻기 위해 그 컴퓨터와 통신하며, 구글 검색이 실행됩니다.

당신의 컴퓨터를 인터넷에 연결해 주는 것은 당신의 ISP(internet service provider)입니다. 당신은 아마 휴대전화, TV, 혹은 광섬유 케이블을 이용하여 ISP에 연결하는 현대식을 하고 계실 겁니다. 당신의 인터넷은 인프라(혹은 하부구조)를 통하고, 그들은 당신이 보내는 모든 데이터와 정보를 보내는 IP 주소에 접근할 수 있습니다.



하지만 이것은 그들이 당신이 들어가는 웹 페이지를 알아야 한다는 것은 아닙니다. 당신이 데이터를 HTTPS로 암호화해두었을 경우 URL 주소(예: www.google.com/search?q=news)를 포함해 그들은 당신이 통하는 것을 볼 수 없습니다. 그들이 알 수 있는 것은 오직 당신이 연결한 IP 주소, 시각 및 송신한 암호화 된 데이터의 사이즈뿐입니다.

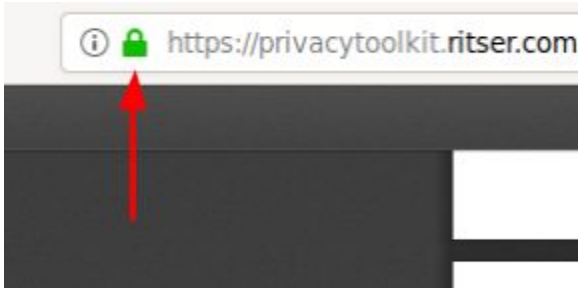
정부가 이미 추적 할 수 있는 것

정부가 추적할 수 있는 것을 짚어봅시다. 당신이 HTTPS를, 하지만 Tor는 사용하지 않는다고 가정할 경우, 당신의 정부는 당신이 언제 어떤 웹 사이트들을 사용하는지 추적할 수 있습니다. 예를 들어, 그들은 당신이 www.facebook.com의 IP 주소를 7:38 PM에 접속했다는 것은 알 수

있지만 어떠한 페이지와 계정들을 방문했는지 까지는 알지 못합니다. 그들은 오직 당신이 www.facebook.com을 방문했다는 것만을 알 겁니다.

만약 당신이 HTTPS를 *쓰지 않고 있다면*, 당신의 정부는 당신이 웹 사이트에 무엇을 보내는지도 추적할 수 있습니다. 이것은 암호와 URL 등을 포함합니다.

그렇다면 자신이 HTTPS를 사용하고 있는지 어떻게 알 수 있을까요? 보통은 HTTPS를 사용하고 있다면 밑의 그림처럼 당신의 브라우저가 잠금장치 모양을 표시할 겁니다.



HTTPS의 작동 원리는 당신의 브라우저와 웹 사이트 사이의 데이터를 암호화시키는 겁니다. 이것은 수학적 알고리즘을 이용하여 발신하는 도중에 데이터를 읽을 수 없도록 한다는 것을 의미합니다. 비록 최고의 정보기관들이라도 뚫기 힘들 정도로 현대의 암호화 알고리즘들은 안전하다 판단됩니다.

비 암호화된 연결(S 안 붙은 HTTP)은 이렇게 보입니다:

From: 70.210.154.182

To: 103.190.246.203 (baidu.com)

Time: 4:42 AM 2020-09-02

Data (70 bytes):

Webpage visited: baidu.com/account

Username: alex2

Password: password

암호화된 연결(HTTPS)은 이렇게 보입니다:

From: 70.210.154.182

To: 103.190.246.203 (baidu.com)

Time: 4:42 AM 2020-09-02

Data (68 bytes):

o866)F(Yu~1]TEjP47h6(vIEs!dq_'|/Sl^ZMbFriN_"LejUyUYZ%d?sRx;F##Coq9M&

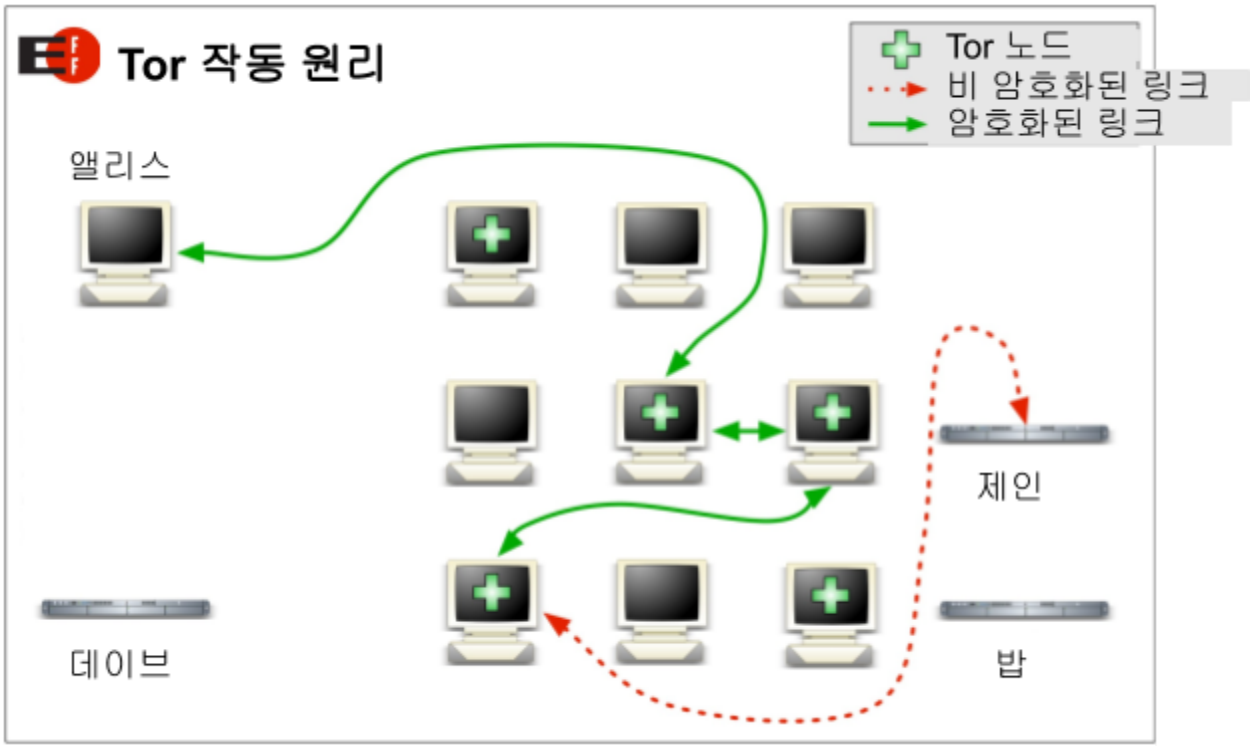
웹 사이트 소유자들의 도움을 받아 정부가 추적 할 수있는 것

그렇지만 HTTPS는 웹 사이트가 경찰에게 당신의 데이터를 주는 것을 막을 수는 없습니다. 당신이 접속한 인터넷 안의 모든 웹 사이트들은 당신의 IP 주소를 볼 수 있습니다. 만약 한 웹 사이트가 당신의 계정에 속해있는 IP 주소를 정부에게 넘기겠다고 결정하면, **그들은 당신의 실제 주소를 찾을 수 있습니다.** 당국이 당신의 온라인 계정에 속해있는 IP 주소를 찾을 수 없도록 하는 것은 중요합니다.

페이스북, 레딧, 구글 등의 큰 웹 사이트들은 정부가 사용자의 데이터를 요청할 경우 처리하기 위한 절차가 준비돼 있습니다. 일반적으로 그들은 권위주의 정부들의 법을 무시하기 때문에 주로 이 절차 과정은 다소 투명하고 공정합니다. 예를 들어, 구글은 2014년과 2018년 사이에 3건의 사용자 데이터를 이집트에서 요청받았지만 모두 거절했습니다.

웹 사이트에서 신원 숨기기

그런데도 자신의 안전을 다국적 영리 기업에 맡긴다는 것은 현명한 생각이 아닙니다. 당신의 안전이 위험한 나라에 살고 있거나 당신의 신원이 공개될 경우, Tor(이 툴킷에 포함)를 사용하는 것이 현명합니다. Tor는 당신의 인터넷 트래픽을 웹 사이트에 도달하기 전 다른 컴퓨터들을 거치는 것으로 당신의 IP 주소를 숨겨 줍니다. 웹 사이트들은 당신의 것이 아닌 마지막으로 거친 컴퓨터의 IP를 볼 수 있을 것입니다. 당신이 Tor를 사용한다는 것을 정부는 알지만, 그들은 당신이 무엇을 Tor를 통해 보내는지, 또 누구랑 통신하는지는 알지 못합니다.



Tor를 사용하는 또 다른 이점은 당신이 어떤 웹 사이트를 액세스하는지 ISP는 모르기 때문에 차단할 수 없다는 것입니다.

Tor도 빈틈이 없는 것은 아닙니다. 정부가 당신의 대략적인 위치를 알고 있고, 웹 사이트 소유자가 당신이 Tor를 사용하고 있다는 것을 그들에게 알려 주면 당신이 웹 사이트를 볼 때와 동시에 해당 장소에서 Tor에 액세스 한 사람을 확인하여 당신의 실제 신원을 얻을 수 있습니다. FBI는 이전에 이것을 해왔지만 거의 문제가 되지 않습니다. 이것이 걱정될 경우 공용 WiFi를 사용할 수 있습니다.

사이드 노트: VPN은 온라인에서 당신의 익명성을 유지하는 데 Tor만큼 효과적이지 않습니다.

당연한 것

일반적으로 사람들을 잡히게 하는 것은 정부가 그들의 IP 주소를 얻는 것이 아닙니다. 자신의 정체성을 드러내거나 친구에게 자신의 정체성을 드러내는 무언가를 인터넷에 제출하는 것입니다. 바보 같은 실수들이 사람들을 붙잡히게 합니다. 다음은 당신이 항상 수행해야 할 몇 가지 예입니다.

1. 이야기를 제출 할 때는 모호하게 하고 세부 사항을 구성하십시오. 보유한 형제자매 수와 같은 작은 정보로 인해 신원을 알아낼 수 있습니다.
2. 인터넷에 사진을 제출할 경우 **각별히** 주의하십시오. 모든 사진에서 EXIF 데이터를 제거하고 사용자를 식별하는 데 사용될 수있는 세부 정보가 없도록 확인하십시오.

3. 다른 사람이 내 컴퓨터를 사용한다면 히스토리가 저장되지 않도록 확인하십시오. 신원을 유출 할 수 있는 어떤 것도 컴퓨터에 저장하지 마십시오.
4. 익명의 신원에 사용하는 계정에 가입할 때 실명을 사용하지 마십시오.
5. 실생활에서 아는 사람들에게 익명의 신원을 밝히지 마십시오.
6. 익명의 신원을 통해 아는 사람들에게 실제 신원을 밝히지 마십시오.

결론

익명의 Reddit 또는 Facebook 계정을 만든다면 때때로 안전을 유지할 수 있습니다. 그러나 당신의 삶이 그것에 의존한다면 이 회사들을 신뢰하는 것이 좋지 않을 수 있습니다. 자신 있게 익명을 유지하려면 Tor를 사용하십시오. PrivacyTools는 다른 개인 정보 보호 지향 소프트웨어를 위한 좋은 리소스입니다.

그리고 기억하십시오 : 자신의 안전에 대한 책임은 오직 당신에게만 있습니다.