

Bezpieczeństwo systemów komputerowych

Omijanie filtrów sieciowych

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

9 grudnia 2011

Na podstawie wykładu Marka Marczykowskiego z 2009 r.

Korzystanie z płatnego punktu dostępowego Wi-Fi

- ▶ Płatny punkt dostępowy zabezpieczony jest za pomocą filtra sieciowego.
- ▶ Dopóki nie zapłacimy, każde odwołanie do dowolnej strony www wyświetla informację o konieczności uiszczenia opłaty.
- ▶ Najprościej byłoby, gdyby filtr sieciowy przechwytywał komunikaty DNS i zawsze zwracał adres lokalnego serwera WWW, wyświetlającego tę informację.
- ▶ Niestety niektóre popularne systemy operacyjne zapamiętują takie tłumaczenie adresów i po zapłaceniu nadal nie byłoby można korzystać z serwisów www.
- ▶ Dlatego filtr sieciowy musi przepuszczać ruch DNS, a w celu wyświetlenia strony z informacją o opłacie musi przykierowywać ruch HTTP.

Bezpłatne korzystanie z punktu dostępowego Wi-Fi

- ▶ Skoro ruch DNS nie jest blokowany, to po co płacić?
- ▶ Nabywamy domenę i instalujemy swój serwer DNS, który będzie pośrednikiem.
- ▶ W komunikatach DNS jest dość miejsca, aby tunelować dowolny ruch.
- ▶ Pośrednik nie może sam nic do nas wysłać – trzeba go cyklicznie odpytywać.
- ▶ Istnieją gotowe programy, np. NSTX.
- ▶ Filtr sieciowy może bronić się, ograniczając węzłowi liczbę odwołań do DNS w jednostce czasu.

Tunelowanie ruchu w ICMP

- ▶ W polu danych komunikatu *echo request* (*ping*) można wysłać dowolne dane.
- ▶ W polu komunikatu *echo response* (*pong*) serwer odsyła odpowiedź.
- ▶ Trzeba gdzieś zainstalować serwer-pośrednik.
- ▶ Pośrednik nie może sam do nas nic wysłać – trzeba go regularnie „pingować”.
- ▶ Pingtunnel: TCP w ICMP,
<http://www.cs.uit.no/~daniels/PingTunnel>