

Krzysztof M. Brzeziński
Igor Margasiński
Krzysztof Szczypiorski
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa

Prywatne wojny w sieci: poddaj się, okop, negocjuj lub stań do walki

Motto:

"Get up, stand up, don't give up the fight.
Get up, stand up, stand up for your right"

Bob Marley

"...wystarczy mówić prawdę. Oczywiście są różne prawdy."
Umberto Eco, Zapiski na pudełku od zapafek.

STRESZCZENIE

Prywatność, którą użytkownik pragnie zachować także podczas nawigowania w sieci WWW, jest obecnie powszechnie naruszana. Tak rozumiana prywatność zostanie tu przedyskutowana w czterech kontekstach: na tle ogólniejszych tez dotyczących ochrony dóbr i ich naruszeń, w koncepcyjno-technicznym aspekcie skutecznych mechanizmów ochrony, w analogii do wzorców pojęciowych wypracowanych przez inne środowiska, oraz w aspekcie uwarunkowań mogących uzasadniać ataki na prywatność. Dla skuteczności rozważań, proponuje się tu (podobnie jak od lat czyni się np. w lingwistyce) oddzielenie metod i technik ochrony od ich emocjonalno-etycznego kontekstu (pragmatyki). Taki zabieg ułatwia definiowanie strategii ochrony oparte np. na mechanizmach uprawnionego ataku. Jako przykład szczególnie skutecznego mechanizmu ochrony, mającego cechy ataku na podmioty naruszające prywatność, zostanie przedstawiony oryginalny system VAST (*Versatile Anonymous SysTem for Web Users*).

ABSTRACT

A privacy - which is getting a premium factor among Web users - is globally violated today. The electronic privacy will be discussed in this paper in four dimensions: in a general context of goods protection and abuses, in the technical spectrum of methods and effective schemes, as an analogy to concept patterns presented in other domains, and also in a light of circumstances where the privacy violation can be accepted. To assure a competence of the analysis - we propose (like for example in linguistics) divide security means and protection techniques from their emotional and ethical context (pragmatics). This proceeding can allow us to define protection strategies based on authorized attack for example. We then submit the original approach to anonymity assurance: the VAST (*Versatile Anonymous SysTem for Web Users*) system, which represents highly effective protection mechanism and can be recognized as an attack scheme on parties violating privacy.

Słowa kluczowe – prywatność elektroniczna, zapewnianie prywatności, ataki sieciowe, bezpieczeństwo sieciowe

WPROWADZENIE

Dziedzina ochrony informacji, jak zresztą wiele innych dziedzin nauki, jest pełna pojęć o znaczeniu silnie uwarunkowanym przez kontekst. Wiele z tych pojęć zostało wprowadzonych w kontekście ściśle określonym (w tym - dotyczącym ich oceny etycznej). W rozważanej tu dziedzinie dokonywano już wielu prób definiowania i porządkowania pojęć i terminów [1,2,3,4]. W niniejszej pracy nie usiłujemy przedstawić kolejnej, "lepszej", całościowej taksonomii. Przyjrzymy się natomiast, w sposób możliwie wszechstronny, zaledwie jednemu z istotnych aspektów ochrony informacji, mianowicie **prywatności** użytkownika podczas korzystania z usługi WWW dostępnej w Internecie. Rozważymy do zagadnienie z *góry* - na tle ogólniejszych tez i spostrzeżeń dotyczących prywatności jako przykładu dobra chronionego, z *dołu* - wskazując uwarunkowania koncepcyjno-techniczne (w tym - oryginalną technikę) uzyskania i zachowania prywatności, oraz z *boku* - poszukując analogii i wzorców pojęciowych w pracach innych środowisk. Wobec istotnego

przewartościowania sposobu traktowania zagadnień prywatności po niedawnych atakach na podstawy państwa demokratycznego (ze swej istoty mającego tę prywatność respektować i chronić), może być odświeżające podejście, w którym eksponuje się słownikowe znaczenie terminów (nie obciążone balastem emocji), względność pojęcia "ataku" oraz naturalność i nieuchronność procesów poszukiwania przeciw-broni.

ATAK I OBRONA - OD PODSTAW

W tym miejscu dokonamy krótkiego przeglądu podstawowych, stosowanych dalej pojęć. Te pojęcia zostaną tu zdefiniowane w sposób nieco odmienny od najczęściej spotykanego w literaturze tematu: możliwie najbardziej zbliżony do słownikowego i nie obciążony konotacjami wynikającymi z emocjonalnego kontekstu.

Dogodnym punktem początkowym rozważań okazuje się termin "*intrusion detection*", w literaturze polskiej z reguły tłumaczony jako **wykrywanie włamań** [5]. W sensie szerokim, systemy wykrywania włamań (IDS, *Intrusion Detection Systems*), uznawane za mechanizm **obronny**, służą do reagowania na przypadki **niepożądanego aktywności** (*undesirable activity*) bądź **złamania (naruszenia) polityki bezpieczeństwa** (*violation of a security policy*), klasyfikowane jako **ataki**. Aktywności niepożądanego względem czego? Czym jest, w tym kontekście, "polityka"? W jakim znaczeniu występuje tu termin "bezpieczeństwo" i do jakiego stopnia jest to znaczenie naturalne, powszechnie przyjęte w języku codziennym? Jak się ma prywatność do występujących wyżej pojęć? Jak się atakuje prywatność? Czy "brak prywatności" także można zaatakować? Przedyskutowanie (i - w miarę możliwości - rozstrzygnięcie) tych wątpliwości jest celem dalszych rozważań.

"Włamanie" jest równoznaczne z przełamaniem pewnego *mechanizmu zabezpieczającego* (w rozumieniu technicznym). Zarówno w prawodawstwie, jak i w ogólnie przyjętym rozumieniu nie chodzi tu o przełamanie jedynie własnych skrupułów moralnych. Natomiast "**wtargnięcie**" jest słownikowo definiowane jako wkroczenie, bez zgody, zaproszenia bądź odpowiedniego powodu, w określony obszar. Aby mówić o wtargnięciu, obszar (praw, fragmentu architektury systemu, informacji), do którego następuje wtargnięcie, musi być uznany za **dobro chronione**, a ponadto dysponent tego dobra i ten, kto dopuszcza się wtargnięcia, muszą być różnymi podmiotami. To, w jaki sposób dobro jest chronione przed wtargnięciem, jest tu kwestią drugorzędną - wydaje się, że przestrzeń takich sposobów jest wyczerpująco podzielona na *mechanizmy* i *deklaracje*. Można bowiem wyobrazić sobie wtargnięcie bez włamania (wejście do obcego pomieszczenia przez otwarte okno, pomimo deklaracji o ochronie obiektu w postaci tablicy ostrzegającej). Wtargnięcie jest zatem pojęciem szerszym od włamania, a w dodatku - lepiej oddającym przedmiot naszych rozważań.

Do stwierdzenia wtargnięcia wystarczy sam fakt naruszenia obszaru chronionego. Strona ochraniająca nazwie stronę naruszającą **intruzem**. Wtargnięcie może nastąpić celowo i świadomie - wówczas wtargnięcie zostanie zakwalifikowane jako **atak**, a intruz stanie się atakującym. Jednakże bardzo kategoryczne stwierdzenia, stawiające znak równości między wszelkim wtargnięciem a atakiem z włamaniem, należy traktować z ostrożnością - wydaje się, że są one rezultatem silnych emocji leżących u podstaw rozwoju dziedziny "wykrywania włamań" (jeden z autorów dopuścił się kiedyś "ataku" na cudzy samochód Syrena, dokonując wtargnięcia przez włamanie: pokonał mechanizm zabezpieczający - klucz pasował, a samochód był zaparkowany obok i był tego samego koloru, co własny). Intencje intruza są rozstrzygane na innym poziomie rozważań: pragmatycznym (np. prawnym), a nie semantycznym.

Atak, jako działanie intencjonalne, można rozpatrywać jako proces rozciągły w czasie, złożony z powiązanych ze sobą faz:

- przygotowania,
- pokonywania zabezpieczeń (przełamywanie mechanizmu, zignorowanie deklaracji),
- momentu wtargnięcia,
- fazy trwającego naruszania dobra,
- wycofania.

Sposób (mechanizm, deklaracja) ochrony dobra (czyli **prewencji**) jest jedynie elementem szerszej **strategii ochrony**, w której nacisk może być położony na zniechęcenie do ataku bądź reagowanie na atak, który już nastąpił. Strategia reagowania może z kolei opierać się na wykryciu ataku w jego możliwie najwcześniejszej fazie (jeszcze przed pokonaniem zabezpieczeń), wykryciu momentu wtargnięcia (co może być trudne, gdyż nie zawsze jest to konkretna chwila), czy też wykryciu faktu naruszania dobra. W literaturze tematu [1] wylicza się, stojące zresztą na różnym poziomie abstrakcji i nie-ortogonalne względem siebie, generalne mechanizmy stosowane w strategii ochrony: poza wspomnianą już prewencją - **atak wyprzedzający** (*preemption*); **odstraszanie** (*deterrence*); **zmylenie** (*deflection*) - upewnienie atakującego o tym, że osiągnął cele swego ataku, bez istotnego uszczerbku dla chronionego dobra; **detekcję** (*detection*); **przeciwdziałanie** (*countermeasures*) dopuszczające możliwość **kontrataku**.

Poszczególni "aktorzy" operujący w przestrzeni rozważań (tu - w domenie korzystania z usług WWW w Internecie) starają się samodzielnie definiować obszary (dobra) chronione oraz wybierać sposób ochrony dóbr, których właścicielami bądź współwłaścicielami się czują. "Aktorzy" ci kierują się przy tym własnym interesem oraz ramami prawnymi i przyjętymi obyczajami. Jednym z istotnych trendów tego procesu jest zawłaszczanie przez podmioty gospodarcze przestrzeni publicznej, w której dotychczas funkcjonowały dobra (w tym - prywatność), już wcześniej chronione przez inne podmioty [6]. W przypadku niekompletności i słabości ram prawnych bądź nierespektowania obyczajów, naturalne sprzeczności interesów będą nieuchronnie rozstrzygane w drodze konfrontacji (jest to jedynie gorzkie stwierdzenie stanu rzeczy). Stąd terminologia militarna, uzasadniająca nawet atak w odpowiedzi na zagrożenie chronionego dobra, definiująca spiralę broni i przeciw-broni. Potraktujmy tu wtargnięcia i reakcję na nie (włącznie z atakiem zwrotnym) jako *mechanizmy*, a do bardzo istotnej kwestii ich dopuszczalności i wartościowania moralnego powrócimy przy końcu naszych rozważań.

SPOJRZENIE Z GÓRY - PRYWATNOŚĆ JAKO DOBRO CHRONIONE

Jednym z dóbr chronionych jest **prywatność** obywatela. W poszczególnych domenach życia społecznego to dobro jest chronione w różnym zakresie i w różny sposób, zarówno z mocy prawa, jak i własnymi siłami obywateli (choćby przez zasłanianie okien). Warto zauważyć, że potrzeba "prywatnej" ochrony prywatności silnie zależy od niezwykle licznych, trudno poddających się skatalogowaniu czynników. Na przykład zasłanianie okien jest oczywistością w Polsce, ale pozostaje praktyką niemal zupełnie niespotykaną i czasem wręcz uznawaną za niestosowność w Holandii (szerzej - w wielu krajach przesiąkniętych etyką protestancką), gdzie powszechnie i niemal ostentacyjnie demonstruje się, że się "nie ma nic do ukrycia".

Prywatność w sieci Internet, związana z odwiedzaniem stron WWW, ma swoją specyfikę, inną niż np. w kontekście używania poczty elektronicznej. Dla ustalenia uwagi przyjmijmy, że przeciwnikami ("aktorami" usług WWW, o sprzecznych interesach w zakresie prywatności) są: z jednej strony - użytkownik, a z drugiej - podmiot gospodarczy, budujący swą egzystencję na poznawaniu i wykorzystywaniu (głównie do celów handlowych) informacji o tożsamości i zwyczajach bądź preferencjach użytkowników. Jak zostanie pokazane dalej, nie jest to jedyna para przeciwników, jaką warto rozważyć.

Wykazana dalej łatwość w pełni zautomatyzowanego i globalnego pozyskiwania oraz przetwarzania danych o osobach korzystających z ogólnodostępnej sieci, to zjawisko odstraszaające użytkowników od poważnych zastosowań Internetu. Dane na ten temat, przytaczane np. w [7] pokazują, że większość konsumentów nie ufa przedsiębiorstwom przetwarzającym ich prywatne dane. Użytkownicy oczekują rozwiązań zapewniających ochronę ich prywatności w sieci publicznej. Ponad połowa ankietowanych przyznaje, że dopiero w przypadku pewności co do przestrzegania przez firmę polityki prywatności, poleciliby ich usługi znajomym lub rodzinie. Ponad 90% konsumentów zaznacza, że korzystaliby częściej z zakupów internetowych, gdyby polityka prywatności sklepu była poddana odpowiedniej kontroli. Według innych badań opinii publicznej, około 83% użytkowników nie korzysta ze sklepów internetowych, ponieważ nie jest dla nich jasne, co dzieje się z ich prywatnymi danymi, komu i do jakich celów są przekazywane, oraz

przez kogo ich zainteresowania i zwyczaje są obserwowane. Dla pełnego obrazu należy też zauważyć, że wykorzystywanie danych zdobywanych w wyżej opisany sposób przynosi ogromne, wręcz trudne do ogarnięcia zyski firmom wykorzystującym te dane bezpośrednio - do prowadzenia własnej działalności handlowej, bądź po prostu nimi handlujących (w roku 2000 obroty tylko jednej takiej firmy handlującej profilami danych o użytkownikach wyniosły 600 milionów dolarów!).

Z perspektywy użytkownika, dobrem chronionym jest własna prywatność. Wiele działań związanych z przeglądaniem stron WWW (np. transakcje dokonywane w sklepie internetowym) wymaga, co oczywiste, dobrowolnego odstąpienia od prywatności, na czas i w związku z danym działaniem oraz w stosunku do danego podmiotu (serwisu). Naruszenie prywatności wynikające z nieuprawnionego dalszego wykorzystania tak zdobytej informacji prowadzi do **kompromitacji** podmiotu - naruszenia o takiej naturze nie będą tu dalej rozpatrywane. Za atak na prywatność użytkownik mógłby uznać każde działanie, którego istotą jest uniemożliwienie mu zachowania prywatności.

Z perspektywy podmiotu gospodarczego, dobrem chronionym jest możliwość uzyskania interesujących ten podmiot informacji o użytkownikach usług WWW. Za atak na tak rozumiane dobro podmiot mógłby uznać każde działanie, którego istotą jest uniemożliwienie uzyskania tych informacji.

Załóżmy, że obie strony dążą z porównywalną determinacją do realizacji swych celów (czyli skutecznej ochrony przed wtargnięciem w obszar chronionego przez siebie dobra, rozumianego jak wyżej). Przy ochronie prywatności użytkownika współdziałają mechanizmy lokalne, implementowane w stacji użytkownika, oraz mechanizmy globalne (sieciowe) - odpowiednie struktury, protokoły i pomocnicze usługi zabezpieczeń. Jeśli te mechanizmy łącznie działają skutecznie, wówczas podmiot gospodarczy odczytuje to jako atak na dobro własne (atak, gdyż jest to ewidentnie działanie intencjonalne!). Podmiot musi wówczas przerwać ten atak - sprawić, by stał się nieskuteczny. Takie z kolei działanie, niezależnie od jego natury, zostanie odczytane przez użytkownika jako (skuteczny) atak na jego prywatność, co zapewne spowoduje przejście do fazy następujących po sobie kontrataków z obu stron (a następnie kontr-kontrataków itd).

Pewnym *novum* w powyższym rozumowaniu jest wyeksponowanie dualności pojęcia ataku i obrony. W sytuacji rzeczywiste przeciwstawnych interesów i niedoskonałych ram prawno-obyczajowych, ochrona realizowana przez jedną stronę jest przez drugą stronę odczytywana (z definicji) jako atak na jej interesy. Sposobem na przerwanie samonapędzającej się spirali wzajemnych ataków, która na razie wydaje się "stanem normalnym", może być (tu odwołajmy się do tytułu niniejszej pracy):

- a) **rezygnacja** jednej ze stron - chodzi tu w praktyce o rezygnację użytkownika z ochrony własnej prywatności.

Można przyjąć, że wielu (zwłaszcza niedoświadczonych) użytkowników nie w pełni jest świadomych tego, że ich prywatność *mogłaby być* (lepiej) chroniona - ich rezygnacja wynika z niedoinformowania. Z drugiej strony, rozważmy przywoływany już przykład holenderskich odsłoniętych okien - trudno przypuszczać, by Holendrzy nie byli świadomi istnienia żaluzji. Ta analogia zdaje się sugerować, że teza badaczy i praktyków ochrony prywatności o tym, że taka ochrona jest absolutną koniecznością i niezbywalnym prawem, jest pewnym nadużyciem (albo co najmniej skrótem myślowym). Powyższe stwierdzenie, wobec powszechności i bezczelności ataków na prywatność użytkowników Internetu ze strony podmiotów gospodarczych, jest oczywiście kontrowersyjne i prowokacyjne, ale czy nie należałoby jednak mieć go na uwadze?

- b) **"okopanie się"** użytkownika, w praktyce polegające na rezygnacji z korzystania z usług WWW w Internecie (tylko takie usługi są tu rozważane; w szczególności poczta elektroniczna nie musi zostać wykluczona).

Efekt "wylania dziecka z kąpielą" jest w tym przypadku ekstremalnie dotkliwy. Interesujące wydaje się poszukiwanie analogii z udanym atakiem typu *denial of service* - czyż w efekcie użytkownik nie został pozbawiony usług? Taki użytkownik staje się jednak bezwartościowy z punktu widzenia komercyjnego wykorzystania Internetu, bo nie przysparza już nikomu żadnego dochodu. Nie jest jednak nie do pomyślenia tak totalne skompromitowanie tego

medium komunikowania się, że zostanie ono po prostu porzucone, a jego funkcje przejmie inny, dziś jeszcze nieznan system, w którym zagadnienia prywatności znajdą skuteczniejsze i bardziej satysfakcjonujące rozwiązanie.

- c) taktyczne **negocjowanie** stanu, w którym interesy każdej ze stron są w równie satysfakcjonującym (bądź niesatysfakcjonującym!) stopniu zabezpieczone; przykładem mechanizmu implementacji tego trybu postępowania jest protokół P3P [7].
- d) opracowanie "bronii doskonałej" - mechanizmu ochrony, którego działanie ze swej istoty nie daje się zneutralizować żadnym znanym w danej chwili, ekonomicznie i technicznie racjonalnym mechanizmem kontrataku. Poniżej zostanie przedstawiona oryginalna koncepcja takiej właśnie "bronii doskonałej", czyli mechanizmu VAST.
- e) zasadnicza zmiana stosunków prawnych i społecznych; taki mechanizm, w gruncie rzeczy najbardziej racjonalny i pożądany, wykracza poza zakres dyskusji prowadzonej w niniejszej pracy, która zakłada określony stan rzeczy.

SPOJRZENIE Z DOŁU - MECHANIZMY ATAKU I OBRONY

Zagrożenia dla prywatności w architekturze WWW

Przeglądając internetowe strony WWW, nie pozostajemy anonimowi [7]. Zdarzenia odwiedzin oraz poszczególne kroki nawigacji są rejestrowane przez serwery WWW, z którymi następuje połączenie. Do typowych danych gromadzonych przez serwery należą: adres IP klienta, czas nadejścia żądania, adres URI przeglądanych zasobów, czas przesłania, nazwa klienta, informacje o błędach, informacje o przeglądarce użytkownika, oraz w przypadku, gdy przejście do strony nastąpiło przez odnośnik – adres URL poprzednio odwiedzanej strony (*refer link*). Wypełniając formularze przekazujemy serwerom WWW dalsze informacje.

Poszczególne odwołania użytkowników (w bezstanowym protokole HTTP [8]) wiązane są ze sobą najczęściej za pomocą mechanizmu zarządzania stanem HTTP – *Cookies* [9]. Serwery zapisują w ten sposób, na stacji użytkownika, dowolne informacje (najczęściej kodowane w tylko sobie znany sposób), aby przy kolejnych odwołaniach móc je odczytywać. Dzięki temu możliwe jest rejestrowanie ścieżek nawigacji poszczególnych użytkowników. Serwery mogą odczytywać tylko zapis *Cookies* dokonany przez siebie. Możliwe jest jednak globalne śledzenie nawigacji pomiędzy wieloma serwisami, np. z pomocą mechanizmu **bannerów**. W dziedzinie systemu WWW nośniki reklamy służą nie tylko do promowania określonych produktów – przekazywania użytkownikom informacji reklamowych i odnośników – ale również są przekaźnikiem informacji w drugim kierunku, czyli do organizacji umieszczającej bannery (takiej jak *DoubleClick*), która dzięki temu uzyskuje informacje o zainteresowaniach użytkowników. Na stronach WWW możliwe jest osadzanie elementów pochodzących od stron trzecich. W sieciach zrzeszających strony współpracujące ze sobą w tworzeniu profili użytkowników wyróżnić można centralny węzeł, z którego pochodzą bannery, czyli AdServer. Odwołując się do jednej ze stron z takiej sieci, w sposób niewidoczny odwołujemy się również do AdServera poprzez pobranie banneru. Temu odwołaniu towarzyszy na ogół zapis i odczyt odpowiednio preparowanych *cookies*.

Poza opisanymi mechanizmami, informacje o aktywności użytkownika mogą być także zdobywane poprzez podsłuchiwanie (*sniffing*) i analizę ruchu w określonych profilach sieci (także w wielu profilach naraz, co wymaga odpowiedniego korelowania takich informacji), a bezpośrednio dane o użytkowniku mogą być przesyłane w wyniku nieanonsowanego zainstalowania się w stacji użytkownika wrogiego programu (*malware*), np. typu **konia trojańskiego** (*Trojan Horse*).

Obszerne zbiory danych, uzyskane w sposób opisany powyżej, poddawane są następnie automatycznym procesom **odkrywania wiedzy**, w których stosuje się m.in. metody wywodzące się z teorii zbiorów rozmytych (*fuzzy sets*), sztucznych sieci neuronowych (*artificial neural networks*), algorytmów genetycznych (*genetic algorithms*) oraz teorii zbiorów przybliżonych (*rough set theory*).

W wydobywaniu wiedzy służącej do profilowania użytkowników systemu WWW, wyróżniane są na ogół trzy etapy: przetwarzanie wstępne, odkrywanie wzorców oraz analizowanie wzorców. Faza przetwarzania wstępnego opiera się na przekształcaniu danych o aktywności, treści stron

WWW oraz ich strukturze i wzajemnych powiązaniach, na formę abstraktu określającego ciąg działań dokonywanych przez użytkowników, a tak otrzymany ciąg zdarzeń dzielony jest na sesje. Rejestrację aktywności użytkowników może wspomagać zastosowanie mechanizmów wprowadzających dynamikę po stronie klienta, jak np. *JavaScript*. Na etapie odkrywania wzorców stosowane są m.in. metody statystyki matematycznej, wydobywania wiedzy (*Data Mining*), uczenia maszynowego (*Machine Learning*) i rozpoznawania obrazów (*Pattern Recognition*). W fazie analizy wzorców następuje odrzucanie wzorców nieinteresujących. W efekcie uzyskuje się **profile użytkowników** zawierające, poza danymi osobowymi użytkowników, także szczegółowe informacje o ich zainteresowaniach i zwyczajach.

Koncepcje zapewnienia prywatności

Prywatność, rozumiana jako zachowanie dla siebie informacji siebie dotyczącej, jest w sieci WWW nie do zrealizowania w co najmniej jednym aspekcie. Aktywność użytkownika jest z definicji widoczna dla wielu stron, np. węzłów pośredniczących i serwerów docelowych WWW (nawet przy założeniu, że nie dochodzi do podsłuchu komunikacji w łączach transmisyjnych). Dlatego w metodach ochrony prywatności, jakie rozważa się w kontekście architektur i usług WWW, nie chodzi o uniemożliwienie wykrycia tej aktywności, lecz o uniemożliwienie powiązania zaobserwowanej aktywności z konkretnym przypadkiem komunikacji pomiędzy danym użytkownikiem a danym usługodawcą (serwisem, stroną WWW). Taka **niepowiązawalność** (*unlinkability*) pozwala na zachowanie **anonimowości** użytkownika względem podmiotów, które obserwują jego aktywność.

W zapewnieniu tak rozumianej prywatności uczestniczą mechanizmy lokalne (działające u klienta) i mechanizmy sieciowe.

Mechanizmy lokalne, to: osobista **ściana przeciwogniowa** (*personal firewall*) nadzorująca wszelkie połączenia wychodzące i przychodzące, zarządzanie prawem do zapisu *cookies*, cykliczne działania utrzymaniowe (usuwanie wewnętrznych zapisów aktywności i plików *cookies*), blokowanie bannerów, wykrywanie koni trojańskich. Mechanizmy te pełnią jedynie rolę pomocniczą i samodzielnie są niezdolne do zapewnienia anonimowości (np. nie są w stanie ukryć adresu IP stacji).

Wśród mechanizmów sieciowych, opartych na zmodyfikowanej architekturze i (w niektórych przypadkach) specjalizowanych protokołach, obecnie najbardziej popularne są serwery pośredniczące i sieci wielu węzłów pośredniczących.

Serwer pośredniczący (*third party proxy server*) jest odległą maszyną, stanowiącą "trzecią stronę" pośredniczącą w pobieraniu zasobów z WWW. Umieszczenie węzła pośredniczącego pozwala na ukrywanie wszelkich informacji o kliencie przed serwerem docelowym (np. adres protokołu IP). Dodatkowo możliwe jest szyfrowanie przekazu pomiędzy klientem a serwerem pośredniczącym, dzięki czemu treść podejmowanej aktywności może zostać ukryta przed stronami mogącymi mieć dostęp do przekazywanych transakcji WWW (np. przed dostawcą usług internetowych – ISP). Serwer pośredniczący daje również szerokie możliwości kontroli nad komunikacją, w zakresie zbliżonym do zapewnianego przez lokalne mechanizmy osobistej ściany ogniowej: zarządzanie mechanizmem *cookies*, blokowanie niepożądanych dodatków (okien reklamowych), jak również usuwanie skryptów czy programów. Serwer pośredniczący może dokonywać dowolnych transformacji doręczanego dokumentu. Przykłady realizacji systemów serwera pośredniczącego to: *Anonymizer*, *Magusnet Proxy*, *Rewebber* oraz własny system *Lustro Weneckie* [10]. Wadą rozwiązań z serwerem pośredniczącym jest konieczność "zawierzenia na słowo", że skoncentrowane w takim serwerze dane o aktywności użytkownika nie są przez usługodawcę gromadzone ani wykorzystywane. W przypadku wykorzystania tej możliwości przez osoby zarządzające usługą, użytkownik narażony jest na straty poważniejsze, niż przy klasycznym przeglądaniu stron WWW. Co więcej, systemy z serwerem pośredniczącym nie zabezpieczają przed śledzeniem aktywności użytkowników usługi poprzez analizę korelacyjną ruchu "przed" i "za" takim serwerem. Ponadto niektóre technologie rozszerzające standard HTML (takie jak *JavaScript*),

zastosowane w przekazywanych plikach HTML, mogą umożliwić przeprowadzenie skutecznych ataków, całkowicie kompromitujących system serwera pośredniczącego.

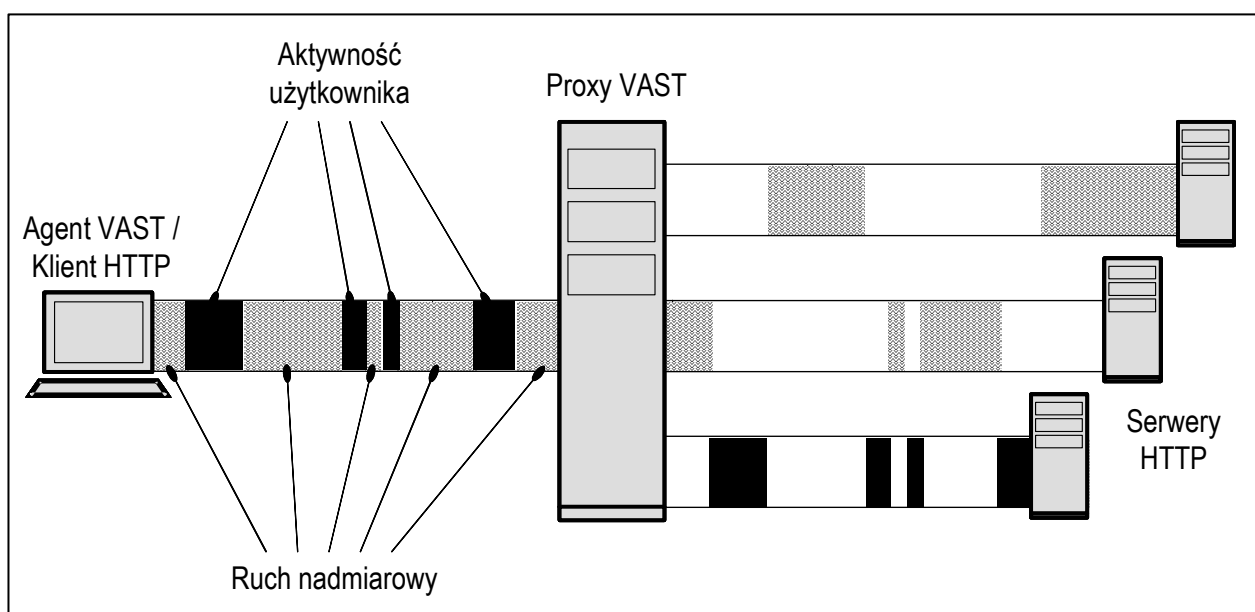
Próba usunięcia ograniczeń systemów opisanych wyżej poprzez rozproszenie miejsc przechowywania informacji o podejmowanej aktywności prowadzi do koncepcji **sieci wielu węzłów pośredniczących**. Wykorzystuje się, odpowiednio rozszerzoną, ideę Davida Chauma - *chaining with encryption*, opracowaną pierwotnie z myślą o zapewnieniu anonimowości użytkownikom poczty elektronicznej. Zakłada się, że każdy z węzłów sieci posiada ograniczoną wiedzę o przekazywanych zasobach, co można osiągnąć poprzez zastosowanie kryptografii asymetrycznej. Wielokrotne zaszyfrowanie danej wiadomości (np. zapytania do konkretnego serwera WWW) kluczami publicznymi kolejnych węzłów umożliwia przekazywanie danych pomiędzy komputerem użytkownika a serwisem internetowym tak, by żaden z węzłów nie wiedział jednocześnie o pierwotnym nadawcy i docelowym odbiorcy. Wybór trasy spośród dostępnych węzłów powinien przy tym mieć charakter losowy. Dzięki temu wędrujące w sieci pakiety wzajemnie się przeplatają, co ma prowadzić do uniemożliwienia ataku opartego na analizie ruchu. Omawiana tu koncepcja ma także wady, takie jak: kosztowna infrastruktura, poważne opóźnienia w przekazywaniu treści (bardzo dotkliwe w przypadku przeglądania stron WWW), konieczność instalacji dodatkowego oprogramowania w stacji użytkownika (co obniża zaufanie do usługi), a także brak rzeczywistej odporności na atak wykorzystujący technikę analizy ruchu (brak gwarancji, że poszczególne serwery sieci nie współpracują ze sobą w tym celu). Przykłady systemów tego typu, zastosowanych w kontekście usług WWW, to *Onion Routing*, *Crouds* i *Freedom* (pierwszy system komercyjny) [11].

VAST - nowy mechanizm zapewnienia anonimowości

Próby pokonania niedoskonałości dotychczasowych rozwiązań podjęto opracowując nowy, oryginalny system **VAST** (*Versatile Anonymous SysTem for Web Users*) [11,12]. W założeniu ten system ma być rodzajem "broni doskonałej", pozwalającej na zwalczanie wszelkich prób przełamania anonimowości użytkownika usług WWW przez węzły pośredniczące i docelowe serwery WWW, dokonywanych także metodą prowadzenia podsłuchu i analizy ruchu.

System VAST składa się z dwóch podstawowych komponentów (rys.1):

- **agenta** działającego w środowisku przeglądarki WWW użytkownika;
- pojedynczego **serwera pośredniczącego**, zainstalowanego pomiędzy agentem a docelowymi serwerami WWW.



Rys.1. Architektura i działanie systemu VAST / VAST system scheme

Podstawą działania systemu VAST jest specyficzny mechanizm **generacji ruchu**

nadmiarowego. Pomędzy klientem HTTP a serwerem pośredniczącym przekazywane jest więcej stron, niż w istocie przegląda użytkownik. Wiedza o tym, które zasoby stanowią przedmiot zainteresowania internauty, jest dostępna tylko dla niego samego. Z przeglądarką użytkownika współpracuje *agent* (aplet Java), który generuje ruch nadmiarowy - w czasie, gdy użytkownik zapoznaje się z treścią stron, agent naśladuje jego typową aktywność, kierując do serwera pośredniczącego wybrane przez siebie zapytania. Ruch nadmiarowy nie pozostaje pod kontrolą człowieka - użytkownika i jest niezależny od jego rzeczywistych zainteresowań. W założeniu, charakter tego ruchu nie pozwala na jego odróżnienie od ruchu związanego z bezpośrednimi działaniami użytkownika. Dzięki temu, względem każdego podmiotu mogącego obserwować aktywność użytkownika uzyskuje się anonimowość wynikającą z niemożności przypisania temu użytkownikowi **intencji** wystosowania danego zapytania. Żadna obserwacja zachowań użytkownika nie dostarcza zatem spodziewanej, wartościowej informacji handlowej, a gdyby działania internauty uczynić przedmiotem *casusu* prawnego, wówczas dowody w postaci zaobserwowanej aktywności prowadziłyby do rozstrzygnięcia: "prawdopodobnie niewinny, *ergo* niewinny".

Funkcje komponentów architektury VAST, z których można wyczytać dalsze szczegóły proponowanego działania systemu, są następujące:

Agent:

- komunikacja z serwerem pośredniczącym z wykorzystaniem bezpiecznego połączenia SSL/TLS – *Secure Socket Layer / Transport Layer Security* [13];
- generowanie adresów URI (*Uniform Resource Identifier*) będących tłem dla adresów, które podaje użytkownik;
- przyjmowanie od użytkownika i przekazywanie do serwera pośredniczącego parametrów pracy (w szczególności adresów URI i ustawień poziomu bezpieczeństwa);
- przekazywanie adresów właściwych i nadmiarowych do serwera pośredniczącego;
- odbieranie zasobów dostarczanych przez serwer pośredniczący i oddzielanie tych, które zostały wskazane przez użytkownika od nadmiarowych;
- prezentacja w przeglądarce użytkownika właściwych (nie nadmiarowych) stron WWW;
- analiza poziomu anonimowości użytkownika na podstawie stosunku pobieranych zasobów wskazanych przez niego do ruchu nadmiarowego oraz informowanie użytkownika o aktualnym poziomie anonimowości.

Serwer pośredniczący:

- ukrywanie wszelkich danych o kliencie HTTP przed serwerem docelowym – w szczególności oryginalnego adresu protokołu IP;
- szyfrowanie wszelkich danych przekazywanych od i do agenta – w szczególności adresu URL zasobów przeglądanych przez użytkownika;
- opcjonalne szyfrowanie przekazu pomiędzy systemem a docelowym serwerem WWW;
- blokowanie *cookies*, skryptów, programów i apletów Java pochodzących z serwera docelowego.

Czym jest działanie systemu VAST, w świetle wcześniejszej dyskusji podstawowych problemów ataku i obrony? To intencjonalne działanie jest **atakami** na nieautoryzowane przejmowanie i przetwarzanie informacji o użytkowniku i jego zainteresowaniach. Poszczególne elementy koncepcji VAST stanowią przedmiot rozważań nad atakami i sposobami obrony przed nimi. Podmiot dążący do naruszenia prywatności użytkownika (czyli teraz - atakowany) dokonuje rejestrowania i analizowania aktywności w sieci. Te działania są zbliżone charakterem do działań systemu wykrywania naruszeń (IDS). Mechanizm dezorientowania takiego systemu przez ruch nadmiarowy można zakwalifikować jako atak typu *subterfuge* (fortel) [2]. Można także doszukiwać się analogii do metod unikania wykrycia ataku, nazwanych w [3]: *evasion* i *insertion*. Z drugiej strony, ruch nadmiarowy jako mechanizm **obronny** należałoby zakwalifikować do mechanizmów **zmylenia** (*deflection*) - podmiot zbierający dane może potraktować każdy zarejestrowany przez siebie wątek jako autentyczny, uzyskując przez to dane "pozorne". Należy jednak taką interpretację potraktować z przymrużeniem oka - po opublikowaniu niniejszego, jedynie wyjątkowo

nierozgarnięty podmiot da się w ten sposób zmylić (choć świadomość bycia zmylonym w tym przypadku nie zmniejsza dalszej skuteczności metody VAST!).

Czy system VAST jest poszukiwaną "bronią doskonałą" w walce o zachowanie prywatności? Argumenty przedstawione w [11,12], w których kolejno rozważa się wyobrażalne kontr-ataki na VAST, wydają się potwierdzać bardzo wysoką skuteczność tego systemu w obecnym stanie wiedzy.

SPOJRZENIE Z BOKU - ANALOGIE I WZORCE POJĘCIOWE

Dotychczasowa teoria i praktyka wykrywania i reagowania na wtargnięcia, zaledwie tu zasygnalizowana, rozwijała się w dużej mierze w sposób spontaniczny, w reakcji (czasem z konieczności pospiesznej) na kolejno pojawiające się zagrożenia. Dotychczasowe osiągnięcia tej dziedziny możnaby zatem określić, nic nie ujmując z ich wagi i ogromnego praktycznego znaczenia, jako katalog metod i technik oraz spostrzeżeń co do ich skuteczności w danych warunkach (w odniesieniu do równoległe katalogowanych konkretnych typów zagrożeń). Można jednak (i warto) poszukiwać także bardziej ogólnych ram pojęciowych i modeli teoretycznych, zdolnych (choćby w części) do opisywania rozważanych tu zjawisk.

"Wtargnięcie" sugeruje aktywność - jest określonym zachowaniem systemu, którego częścią jest intruz. Nawet atak na prywatność, polegający po prostu na nieuprawnionym użyciu informacji dostępnej w danym węzle, opiera się na tym, że ta informacja została tam, pośrednio lub bezpośrednio, *dostarczona*, bądź też że dostarczony został agent atakującego (np. *cookie*), a pozyskana informacja będzie mogła być zwrotnie "*przemycona*" z tego węzła do strony atakującej. Oznacza to, że w kręgu naszego zainteresowania jest **zachowanie** (*behaviour*) reaktywnego systemu rozproszonego, wyrażane w terminach sekwencji, zależności czasowych i zawartości wiadomości - pakietów wymienianych pomiędzy węzłami (a więc dających się zauważyć - monitorować). Problem oceny tak określonego zachowania systemu jest istotnie odmienny od problemów kryptograficznych - do jego rozważania jest stosowany zupełnie inny aparat koncepcyjny i formalny [14]. Jeśli więc pominąć kryptografię, która w przypadku rozważanego tu problemu prywatności w sieci WWW pełni dość ograniczoną rolę (w systemie VAST - szyfrowanie komunikacji pomiędzy agentem i serwerem pośredniczącym), pomocne ramy pojęciowe można znaleźć m.in. w pracach na temat:

- teorii **klas własności** dotyczących zachowania systemu reaktywnego (bądź też wykonania programu współbieżnego) [15]; istnieje silny związek z **logikami temporalnymi**, odpowiednimi do wyrażania takich własności [16];
- zarządzania sieciami telekomunikacyjnymi (*network management*) zwłaszcza w zakresie **zarządzania błędami** (*fault management*) [17];
- metod weryfikacji i walidacji własności systemów rozproszonych (głównie telekomunikacyjnych) metodami **testowania biernego** [18,19] oraz wykorzystywania tych metod m.in. do wykrywania błędów w systemach telekomunikacyjnych [20];
- metodyki EM (*Execution Monitoring*) zabezpieczenia systemu (obliczeniowego) przed wykonaniem operacji prowadzącej do złamania *polityki bezpieczeństwa* [21];
- tradycyjnej metodyki testowania implementacji protokołów telekomunikacyjnych, w zakresie specyfikowania **celu testu** i wydawania **werdyktu** [22,23].

Dla ilustracji, prześledźmy krótko jeden tylko wątek tych innych prac. Zdefiniujmy konkretne zachowanie systemu, bądź krótko - **wykonanie** (*execution, system run*) jako sekwencję zdarzeń, którą nazwiemy **śladem** (ang. *trace*). Istota zdarzeń jest tu drugorzędna i zależy od przyjętego poziomu abstrakcji: w domenie tradycyjnie pojmowanej informatyki mogą to być np. operacje bądź wywołania systemowe, a w domenie tu rozważanej - wystąpienia wiadomości (pakietów) w danych przekrojach sieci. System może w różnych (a nawet tych samych - niedeterminizm) okolicznościach wykazywać różne zachowanie - generować różne ślady. Można zdefiniować *a priori* konkretny (być może nieskończony) zbiór śladów i badać, czy stwierdzone (zaobserwowane) zachowanie systemu należy do tego właśnie zbioru. **Własność** (*property*) definiuje się po prostu jako zbiór śladów *P*, przy czym żąda się dodatkowo, by przynależność śladu do tego zbioru mogła

zostać ustalona na podstawie tego i tylko tego śladu. Powiemy, że *system ma własność P*, jeśli *każde* wykonanie tego systemu generuje ślad należący do zbioru *P*.

Ślad może być w ogólności nieskończony i taki właśnie przypadek jest najczęściej rozważany w teorii. W istocie, rzeczywisty system reaktywny może wykonać się tylko "raz" - w odróżnieniu od systemów o naturze obliczeniowej, nie ma tu mowy o kolejnej próbie, resetowaniu, ponawianiu obliczeń itp. Natomiast jest również prawdą, że zachowanie reaktywne protokołów telekomunikacyjnych i usług sieciowych jest ze swej natury **rekurentne** (nawracające) - sesje są ustanawiane i likwidowane, połączenia są zestawiane i rozłączane. W praktyce właśnie takie wariantowe fragmenty zachowania, przeplatające się w nieskończoność w "jedynym" zachowaniu systemu, mogą stanowić elementy zbioru *P*. Ta obserwacja pozwala sensownie mówić o wielu kolejnych zachowaniach (wykonaniach) rozważanego systemu.

Stwierdzenie, czy dany, właśnie zaobserwowany ślad należy do zbioru *P*, może wymagać odniesienia się do innych (wcześniejszych) wykonań systemu. Mówimy wówczas nie o własności, a o **polityce** (*policy*). Nie każda polityka jest własnością. Zidentyfikowane tu wyżej teorie dostarczają głównie instrumentów badania *własności*, natomiast w "internetowej" praktyce badania zachowań bardzo istotną rolę pełnią mechanizmy oceny, czy system, poza posiadaniem odpowiednich *własności*, dodatkowo *stosuje się do polityki* (zachowuje politykę) *P*. Te mechanizmy, dotyczące w istocie **meta-zachowania** (czyli zachowania zachowań), silnie zależą od celu badania zachowania. Na przykład, jak już wspomniano, w kontekście ochrony prywatności (a dokładniej - ataku na prywatność) rozważa się procesy odkrywania wiedzy, których dwa etapy: odkrywanie wzorców i analizowanie wzorców można potraktować jako dotyczące *polityki*.

Identyfikowane tu prace dotyczą głównie własności, a nie polityk. Jednak nawet w tym ograniczonym zakresie wnoszą istotne uporządkowanie do przestrzeni rozważań nad wtargnięciami.

Wyróżnia się dwie generalne klasy własności zachowania [15]: **bezpieczeństwa** (ang. *safety*) i **żywołności** (ang. *liveness*). Własności te zwykle parafrazuje się w następujący sposób:

- własność bezpieczeństwa P_S : "zła rzecz (*bad thing*) nie zdarzy się nigdy",
- własność żywołności P_L : "dobra rzecz (*good thing*) koniecznie się zdarzy (w końcu musi zajść)";

Wiolacja (naruszenie, zaprzeczenie) własności bezpieczeństwa jest nienaprawialna, niezbita (*irremediable, irrefutable*): skończony prefiks śladu, demonstrujący złamanie własności (zajście *złej rzeczy*) nie może zostać uzupełniony tak, by cały ślad nieskończony był elementem P_S . Natomiast każdy skończony prefiks śladu systemu posiadającego własność żywołności, w którym *dobra rzecz* nie zaszła, może zostać uzupełniony do nieskończonego śladu w którym *dobra rzecz* zachodzi. Warto zauważyć, że np. dla potrzeb testowania implementacji te cechy są parafrazowane jeszcze inaczej: wykrycie "błędu" podczas testu ostatecznie dowodzi niepoprawności implementacji, natomiast niewykrycie "błędu" nie stanowi dowodu poprawności implementacji.

Alpern i Schneider dowiedli, że *każda* własność może być przedstawiona jako koniunkcja odpowiedniej własności bezpieczeństwa i żywołności (twierdzenie o dekompozycji [15]). Formułowanie interesujących własności (np. w logice temporalnej bądź z użyciem języka MSC lub reprezentacji automatowej) i badanie ich spełnienia przez określony obiekt jest istotą obszernej dziedziny weryfikacji i walidacji systemów. Opracowano skuteczne metody takich działań, właściwe dla określonej fazy rozwoju systemu [24]: dla fazy, w której system można przedstawić jako formalny obiekt matematyczny - badanie metodami np. eksploracji grafu osiągalności, a dla fazy obiektu zaimplementowanego - monitorowanie i testowanie. Wykrywanie wtargnięć jako określonych zachowań systemu rzeczywistego można zaklasyfikować jako szczególny wariant problemu testowania. W testowaniu zwykle zakłada się, że formalna specyfikacja zachowania dopuszczalnego ("dobrego") jest dana i stanowiła wzorzec przy implementowaniu systemu. W takim ujęciu, testowanie może być uznawane za problem **weryfikacji**. W przypadku porównywania z zachowaniem pożądanym (bądź niepożądanym), ale zdefiniowanym "z zewnątrz", niezależnie od wcześniejszych działań rozwojowych, testowanie jawi się jako mechanizm **walidacji**.

W dotychczasowej teorii i praktyce testowania (np. w "matce" metod testowych w telekomunikacji - testowaniu zgodności [23]):

- (a) definiuje się wzorzec w postaci wszystkich dopuszczalnych zachowań; *złą rzeczą* będzie wykazanie przez testowaną implementację zachowania innego, niż należące do tego wzorca (czyli naruszenie własności bezpieczeństwa);
- (b) definiuje się **cel** testu jako własność zbliżoną do żywotności (w domenie śladów skończonych); jest to *dobra rzecz*, która ma zajść - nie kiedyś w przyszłości, lecz podczas danego testu;
- (c) zaobserwowanemu zachowaniu przypisuje się werdykt PASS, jeśli własność bezpieczeństwa nie została naruszona, a własność "żywotności" została potwierdzona; werdykt FAIL, jeśli własność bezpieczeństwa została naruszona; a werdykt INCONCLUSIVE, jeśli własność bezpieczeństwa wprawdzie nie została naruszona, ale własność "żywotności" nie została potwierdzona.

Poszukując zastosowania wyżej opisanych pojęć i mechanizmów w domenie naruszeń, możemy stwierdzić co następuje:

- (a) jako *złą rzecz* można traktować zachowanie odmienne od ustalonego zbioru wzorców poprawnych; wykrycie takiego zachowania (w dziedzinie testowania - FAIL) jest *sukcesem* (a więc - PASS) systemu IDS, klasyfikowanego jako *specification-based* [1];
- (b) jako *dobrą rzecz* można (przewrotnie!) potraktować zachowanie zgodne z jedną ze zbioru **sygnatur** znanych ataków; wykrycie takiego zachowania (PASS) jest sukcesem systemu IDS klasyfikowanego jako *signature-based* [1];
- (c) komplementarne połączenie strategii (a) i (b) daje podstawy do rozróżniania pomiędzy **anomalią** (odpowiednik INCONCLUSIVE w testowaniu) i zachowaniem traktowanym jak atak (odpowiednik werdyktu FAIL).

SPOJRZENIE ZZA CIEMNYCH OKULARÓW - POLICJANCI I ZŁODZIEJE

Konflikt interesów w zakresie prywatności jako dobra chronionego występuje nie tylko pomiędzy użytkownikiem a podmiotem gospodarczym, lecz także między np. terrorystą (lub dewiantem) a państwem, oszustem finansowym a bankami, oraz - z zastrzeżeniami - pracownikiem a pracodawcą, itp. Nie ulega wątpliwości, że w takich relacjach komfort prywatności musi zostać skonfrontowany z innym dobrem; w tej konfrontacji prywatność może okazać się "złą", a to inne dobro - "dobre". Terrorysta potraktuje własną prywatność (anonimowość) jako dobro, które musi być za wszelką cenę ochronione, zaś państwo uczyni (bo musi uczynić) wszystko, włącznie ze skutecznym atakiem, by w obszar tego dobra wtargnąć. Ograniczenie prawa do samodzielnej ochrony prywatności obywateli (na wypadek konieczności naruszenia tej prywatności przez służby państwowe w imię wyższego dobra) zawsze występowało i przejawiało się np. w zakazie posiadania ciężkiej broni (do ochrony posesji) bądź zakazie stosowania do celów cywilnych systemów kryptograficznych o "mocy" (długości klucza) przekraczającej określoną wartość [4].

Po atakach terrorystycznych z dnia 11 września 2001 r. nastąpiło przewartościowanie, które na próby zachowywania prywatności rzuciło odium praktyki podejrzanej i niebezpiecznej. Zbiory danych uzyskiwanych m.in. z obserwacji aktywności internetowej obywateli wykorzystuje się już nie tylko do prowadzenia agresywnych akcji marketingowych, ale też np. do uniemożliwiania wstępu do samolotów określonym osobom, nawet nie skazanym ani nie będącym w stanie formalnego oskarżenia. Te i podobne praktyki, choć traktowane z oburzeniem przez grupy obrońców praw obywatelskich, legalistów i wielu zwykłych obywateli, nie są jednak *powszechnie* potępiane, a w każdym razie nie na tyle powszechnie, by uznać je za działania *niewspółmierne* do zagrożenia (na pewno nie spotkają się z potępieniem ze strony rodzin poległych pasażerów zaatakowanych samolotów). Zarazem powszechnie uważa się, że ataki "uprawnionych" służb państwowych na prywatność obywateli są (co najmniej od czasu wspomnianych wyżej zdarzeń) prowadzone bezkarnie i bez żadnej kontroli. Tymczasem prawodawstwo telekomunikacyjne demokratycznych państw (także w Polsce) od wielu lat nakazuje udostępnianie wyznaczonym agencjom państwa (LEA, *Law Enforcement Agencies*) środków technicznych, umożliwiających przechwytywanie informacji umożliwiającej identyfikację komunikujących się stron, w razie potrzeby łącznie z treścią prowadzonej korespondencji. Takie działania są określane jako *lawful intercept*. Wraz z wprowadzeniem komunikacji pakietowej (np. w sieci WWW), skomplikowały się

uwarunkowania prawno-techniczne takich działań. Nikła jest świadomość, jak bardzo takie ataki na prywatność są w rzeczywistości obwarowane różnymi zastrzeżeniami i ograniczeniami. Na przykład, w [25] dyskutuje się problemy i sposoby udostępniania uprawnionym agendom jedynie tych informacji ze strumienia komunikacji pakietowej, do których poznanie zostaną one autoryzowane ("*...by providing law enforcement only with the information to which it is lawfully entitled*"), co okazuje się rzeczą technicznie bardzo złożoną. Co prawda, jest znamienne, że [25] jest pracą niepublikowaną...

Możnaby uznać, że przedstawiony wcześniej system VAST, pozwalający zachować anonimowość podczas nawigowania w Internecie, jest potężnym narzędziem mogącym znaleźć złowrogi zastosowanie. Jednakże system ten ma interesującą cechę: jego "moc" ochrony prywatności radykalnie i automatycznie maleje (właściwie - zanika), gdy użytkownik odwiedza strony WWW o charakterze "przestępczym". Aktywność takiego użytkownika nie będzie skutecznie ukrywana przez ruch nadmiarowy. Zapytania generowane przez agenta systemu VAST wybierane są z odnośników dostarczanych przez popularne narzędzia wyszukujące. Strony WWW, które nie należą do tego zbioru (a strony o treściach przestępczych nie są zazwyczaj indeksowane), stanowiąc będą łatwo wykrywalny kontrast.

PODSUMOWANIE

Tezy niniejszej pracy mogą być przez wielu uznane za prowokacyjne, jako sugerujące "relatywizm etyczny". Łatwo stwierdzić, że w niemal całej literaturze dotyczącej różnych patologii w Internecie, termin "*atak*" jest stosowany z zabarwieniem pejoratywnym, na oznaczenie agresywnego, złośliwego, nielegalnego działania, przed którym podmioty działające legalnie i w dobrej wierze mogą i mają prawo się chronić, stosując różnego rodzaju działania *prewencyjne*. Wśród takich działań wymienia się wprawdzie także atak prewencyjny bądź zwrotny [1], ale czyni się to z wieloma zastrzeżeniami i jakby z zawstyżeniem. Twierdzimy tu, że taka "poprawność polityczna" w zakresie samo-ograniczeń pojęciowych w istocie działa na niekorzyść zastosowań powszechnie uznawanych za społecznie pożądane.

Nie mamy wątpliwości, że komercyjnie motywowane ataki na prywatność obywateli w związku z ich aktywnością w Internecie są powszechne, bezczelne, nękające, stojące na granicy legalności (nie zawsze bezpośrednio nielegalne, gdyż, wbrew popularnej opinii, zbiór danych o obywatelu, którego posiadanie i przetwarzanie jest obwarowane uregulowaniami prawnymi, jest dość precyzyjnie określony). Paradoksalnie, te ataki prowadzą do skutków będących zaprzeczeniem ich pierwotnej motywacji (nieufność użytkowników przekłada się na zmniejszenie komercyjnego znaczenia Internetu). W sytuacji niedoskonałych regulacji i powszechnego "upadku obyczajów", obywatel ma prawo ochraniać swe dobro, jakim jest prywatność, wszelkimi **skutecznymi** środkami pozostającymi we właściwej proporcji do zagrożenia, w tym - środkami aktywnymi, które pod względem *technicznym* można zakwalifikować jako atak. Takim środkiem jest, opisany wyżej, system VAST. Zarazem nie mamy także wątpliwości, że prywatność (a więc także płynący z jej zachowania komfort psychiczny) nie leży wcale najwyżej w hierarchii wartości i dóbr, które podlegają (bądź powinny podlegać) ochronie. Jednakże roztrząsanie tej filozoficznej kwestii w pracy o charakterze metodyczno-technicznym wydaje się jałowe.

Charakterystyczne dla dziedziny specyfikowania i weryfikowania własności terminy: *zła rzecz* i *dobra rzecz* niosą w sobie ładunek emocjonalny i rzeczywiście w takim kontekście są często stosowane. Tymczasem, w teorii weryfikacji/walidacji własności są to terminy używane roboczo, jako nazwy pewnych klas napisów matematycznych. Nie-wartościujące ich traktowanie jest w istocie niezbędne dla rozwoju tej dziedziny i pozwala bez skrępowania korzystać z jej wyników (także dla, quasi-objektywnie postrzeganego, globalnego *dobra* społecznego). Ekstrapolując, także atak i obronę (i poszczególne techniki ich zaimplementowania) warto, dla skuteczności rozważań, rozpatrywać z podziałem na aspekt **syntaktyczny** (jako wzorce zachowań pomiędzy podmiotami), **semantyczny** (co, dla chronionego dobra, oznacza, że dany wzorzec zachowania wystąpił) oraz **pragmatyczny** (czy to dobrze, że taki wzorzec wystąpił, i czy powinien był w danym kontekście wystąpić). Takie warstwy rozważań są charakterystyczne np. dla **lingwistyki** [26] - a czyż sieć

WWW nie jest przestrzenią komunikowania się, w której funkcjonuje specyficzny język?

LITERATURA

- [1] S. Axelsson, *"Research in Intrusion-Detection Systems: A Survey"*, Dept. of Computer Engineering, Chalmers Univ. of Technology, TR:98-17, Dec.15, 1998 (rev. Aug.19, 1999)
- [2] S. Axelsson, *"Intrusion Detection Systems: A Survey and Taxonomy"*, Dept. of Computer Engineering, Chalmers Univ. of Technology, TR:99-15, March 2000
- [3] T. Ptacek, T. Newsham, *"Insertion, evasion, and denial of service: Eluding network intrusion detection"*, Technical report, Secure networks Inc., Jan. 1998
- [4] K. Szczypiorski, R. Kossowski, *"Trendy w ochronie informacji"*, Przegląd Telekomunikacyjny, Nr 5, 2002
- [5] P. Kijewski, K. Szczypiorski, *"Bezpieczeństwo w sieciach TCP/IP"*, Przegląd Telekomunikacyjny, Nr 5-6, 2001
- [6] N. Klein, *"No Logo"*, Świat Literacki, Warszawa, 2004
- [7] I. Margasiński, K. Szczypiorski, *"Prywatność z protokołem P3P w transakcjach online"*, ENIGMA 2004, Warszawa, 2004
- [8] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, *"HyperText Transfer Protocol – HTTP/1.1"*, RFC 2616, 1999
- [9] D. Kristol, L. Montulli, *"HTTP State Management Mechanism"*, RFC 2965, October 2000
- [10] I. Margasiński, *"Zapewnianie anonimowości przy przeglądaniu stron WWW"*, KST'02, Bydgoszcz, 2002
- [11] I. Margasiński, K. Szczypiorski, *"VAST - metoda zapewnienia wszechstronnej anonimowości dla użytkowników systemu WWW"*, ENIGMA 2003, Warszawa, 2003
- [12] I. Margasiński, K. Szczypiorski, *"VAST - Versatile Anonymous System for Web Users"*, Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems. Springer-Verlag, 2004
- [13] T. Dierks, C. Allen, *"The TLS-Protocol Version 1.0"*, RFC 2246, 1999
- [14] K. Schneider, *"Verification of Reactive Systems"*, Springer, 2004
- [15] B. Kindler, *"Safety and Liveness Properties: A survey"*, EATCS-Bulletin, vol.53, June 1994
- [16] A. P. Sistla, *"Safety, Liveness and Fairness in Temporal Logic"*, Formal Aspects in Computing, vol.6, 1994
- [17] E. Ayanoglu, D. Lee, *"Reading notes on network management. Part 1: Fault Management"*, Bell Labs, Lucent Technologies, June 4, 1998
- [18] K. M. Brzeziński, *"Technologia testowania biernego w pomiarach własności sieci"*, Współczesne problemy sieci komputerowych: nowe technologie. WNT, 2004
- [19] A. N. Netravali, K. K. Sabnani, R. Viswanathan, *"Correct Passive Testing Algorithms and Complete Fault Coverage"*, FORTE 2003, LNCS 2767, pp.303-318
- [20] D. Lee, A. N. Netravali, K. K. Sabnani, B. Sugla, A. John, *"Passive testing and applications to network management"*, Proc. 1997 International Conference on Network Protocols (ICNP'97)
- [21] F. B. Schneider, *"Enforceable Security Policies"*, ACM Trans. on Information and System Security, Vol.3, No.1, Feb.2000
- [22] K. M. Brzeziński, Z. Łapkiewicz, *"Testowanie systemów telekomunikacyjnych: metodologia i praktyka"*, KST'96, Bydgoszcz, 1996
- [23] ISO/IEC 9646, *"Conformance Testing Methodology and Framework"*
- [24] K. M. Brzeziński, *"Ewolucja protokołów telekomunikacyjnych"*, Przegląd Telekomunikacyjny, nr 1, 2000
- [25] K. Bhargavan, C. A. Gunter, *"Network Event Recognition for Packet-Mode Surveillance"*, praca niepublikowana
- [26] Z. Saloni, M. Świdziński, *"Składnia współczesnego języka polskiego"*, PWN, 1998