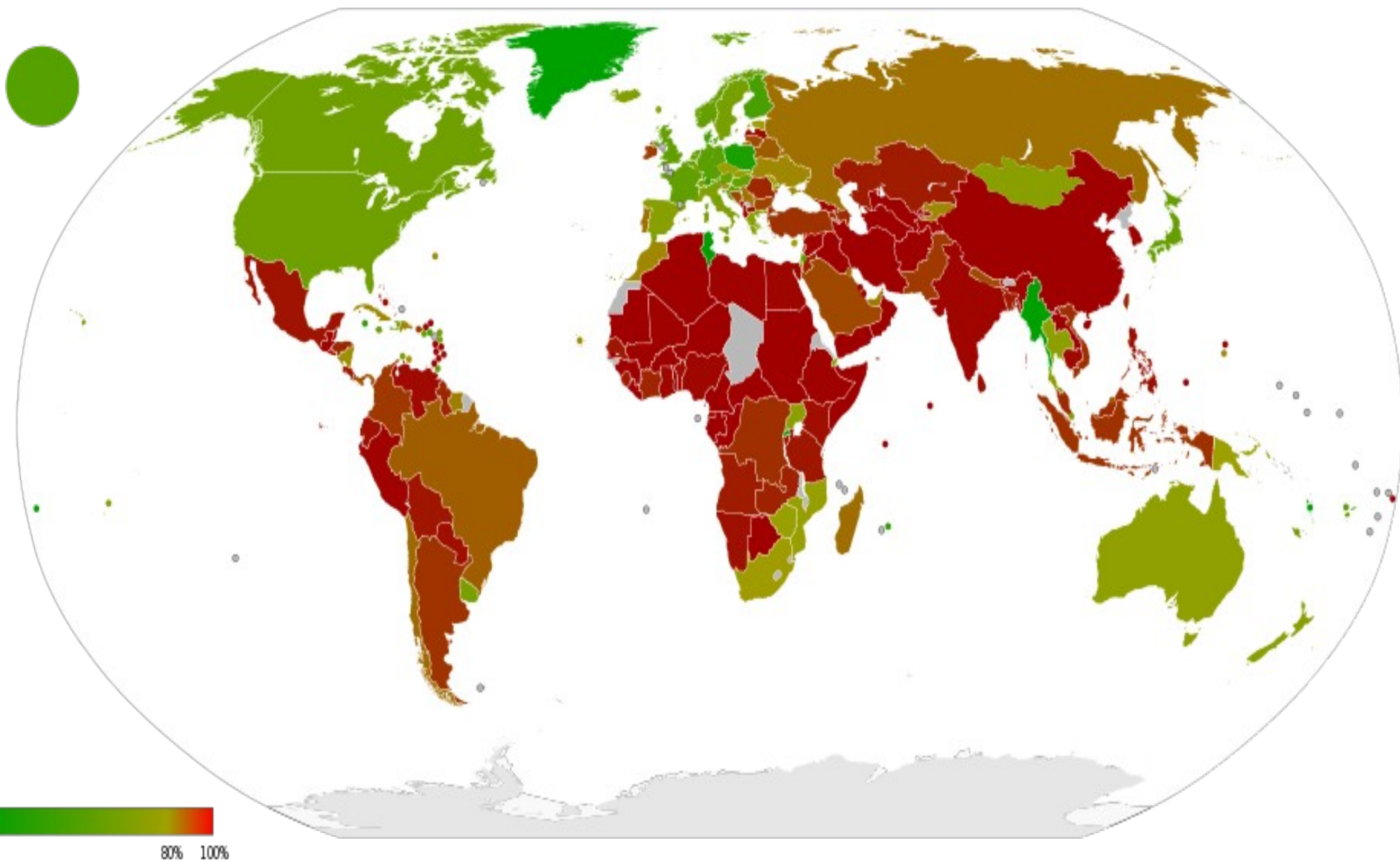


Sposoby walki ze spamem w portalu WP.PL

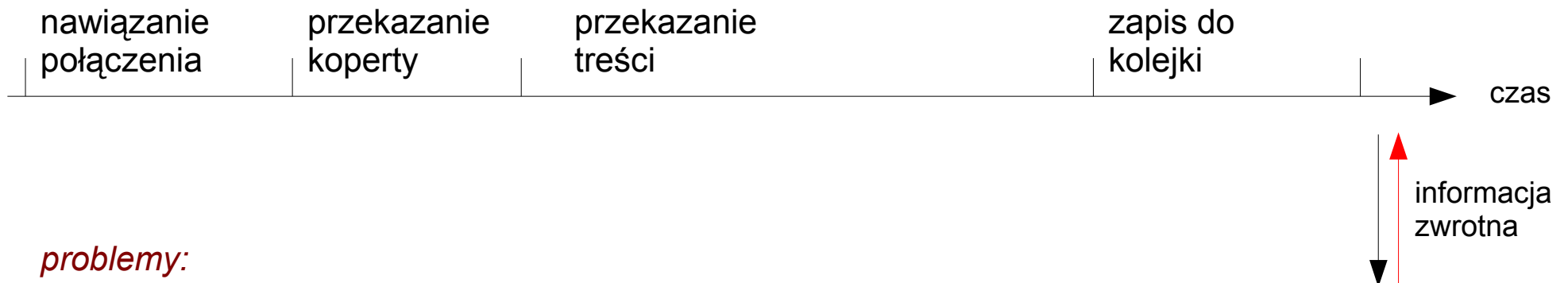
Andrzej Butkiewicz
abutkiewicz@wp-sa.pl

Wirtualna Polska S.A.



<u>ratio</u>	<u>rejected</u>	<u>accepted</u>	<u>total</u>	<u>country</u>
100	1040	0	1040	Togo (TG)
100	528	0	528	Yemen (YE)
100	329	0	329	Northern Mariana Islands (MP)
100	292	0	292	Afghanistan (AF)
100	273	0	273	Sudan (SD)
.....				
37.4432	12536	20944	33480	Denmark (DK)
37.3736	2254	3777	6031	Finland (FI)
23.3831	47	154	201	Cayman Islands (KY)
21.8501	137	490	627	Liechtenstein (LI)
21.5884	193	701	894	Mauritius (MU)
16	24	126	150	Asia/Pacific Region (AP)
13.8364	686389	4274360	4960749	Poland (PL)
0.3184	1	313	314	Andorra (AD)
0	0	1	1	Rwanda (RW)
0	0	1	1	Myanmar (MM)
0	0	1	1	Greenland (GL)

Zarys transakcji SMTP



problemy:

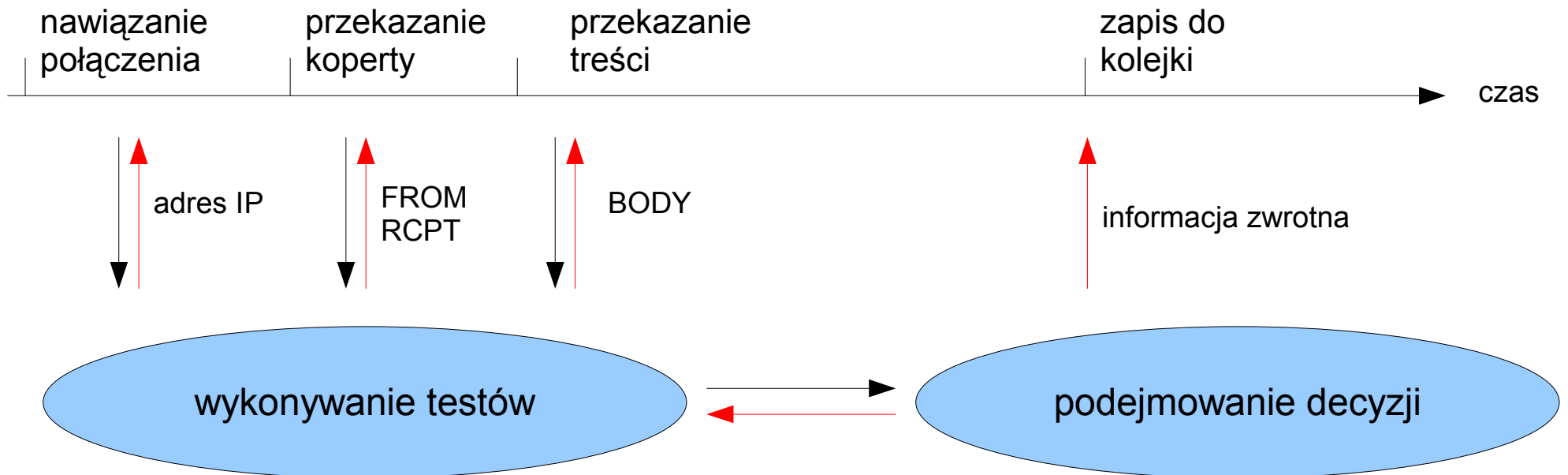
- brak możliwości odrzucenia maila we wczesnej fazie transakcji SMTP
- utrudnione dodawanie kolejnych mechanizmów AS
- utrudnione przekazywanie wyników z innych mechanizmów AS



Co robić ze spamem?

- odrzucać
 - DNSBL
 - Reputacje IP
 - DNS-check
 - ...
- oznaczać (poźniej decyduje użytkownik)
 - Analiza treści (np. Bayes, DCC)
 - Reputacje IP

Ogólna architektura systemu AS



problemy:

- utrudnione dodawanie kolejnych mechanizmów AS

Transakcja SMTP

- Nawiązanie połączenia
 - Dane wejściowe:
 - adres IP
 - data/czas połączenia
 - OS fingerprint
 - Testy do wykonania:
 - DNSBL
 - antyflooding
 - DNS-check
 - reputacje IP
 - reputacje OS fingerprint

Transakcja SMTP

- Przekazanie koperty
 - Dane wejściowe:
 - FROM
 - RCPT TO
 - ilość RCPT TO
 - Testy do wykonania:
 - blacklist
 - SPF
 - DNS-check (FROM, RCPT)
 - antyflooding
 - greylisting

Transakcja SMTP

- Przesłanie treści
 - Dane wejściowe:
 - From:
 - To:
 - Subject:
 - wielkość maila
 - treść maila
 - Testy do wykonania:
 - DCC (distributed checksum clearinghouse)
 - bayesian filter
 - antyflooding (np. wielkość maila)
 - SURBL

Czarne listy (DNSBL)

- Działanie
 - lista adresów IP będących np. źródłem spamu
- Zalety:
 - możliwość odrzucenia dużej ilości spamu bez obciążenia systemu kolejkowania
 - niewielki narzut wydajnościowy
- Wady:
 - preferowane utrzymywanie baz we własnej infrastrukturze
 - wykonywanie synchronizacji baz
 - w zależności od jakości DNSBL mogą pojawić się skargi od użytkowników sieci osiedlowych i zakładowych

WP jest mirrorem Spamhaus Project

SBL - Spamhaus Block List

lista IP potwierdzonych źródeł spamu

XBL – Exploits Block List

lista IP zarażonych wirusami/trojanami z wbudowanymi silnikami spamu itp.

PBL – Policy Block List

zakresy IP z których nie powinny być generowane połączenia SMTP bez autoryzacji, dotyczy to głównie dynamicznych IP u końcowych użytkowników

Mechanizm SURBL

- Działanie
 - Lista URLi prowadzących do stron używanych w przesyłkach spamowych
- Zalety
 - wysoka skuteczność
 - możliwość ochrony przed spamem z linkowanymi obrazkami
- Wady:
 - skomplikowana implementacja, narzut wydajnościowy na parsowanie maila
 - konieczność synchronizowania bazy

Mechanizm “antyyflood”

- Działanie
 - Obserwacja wcześniej określonych zdarzeń w jednostce czasu i stosowna reakcja
- Zalety:
 - możliwość ochrony przed atakiem niewykrywalnym przez klasyfikatory treści
 - możliwość ochrony nie tylko przed spamem lecz również przed atakami DoS
- Wady:
 - narzut wydajnościowy na analizę real-time przetwarzanych zdarzeń
 - (czasami) problematyczny tuning

Sender Policy Framework

- **Działanie:**
 - Maile wysyłane z danej domeny mogą pochodzić tylko ze ściśle określonych adresów IP
- **Zalety:**
 - prosty sposób na walkę z podszywaniem się
 - bardzo prosta implementacja pasywnej części SPF (rekord TXT)
 - stosunkowo prosta implementacja aktywnej części SPF (dostępne biblioteki)
- **Wady:**
 - w przypadku obsługi forwardów konieczność stosowania SRS
 - konieczność utrzymywania rekordu TXT (zmiana IP itp.)

Distributed Checksum Clearinghouse

- Działanie:
 - Z różnych fragmentów maila liczona jest suma kontrolna, która następnie zapisywana jest w bazie celem określenia ilości powtórzeń danej części maila.
- Zalety:
 - rozproszona sieć repozytoriów
 - klasyfikowanie maili o zmiennej lecz podobnej treści
 - funkcja greylistingu
 - funkcja reputacji IP
- Wady:
 - podłączenie do ogólnej sieci DCC (o ile to wada)
 - dedykowane serwery DCC

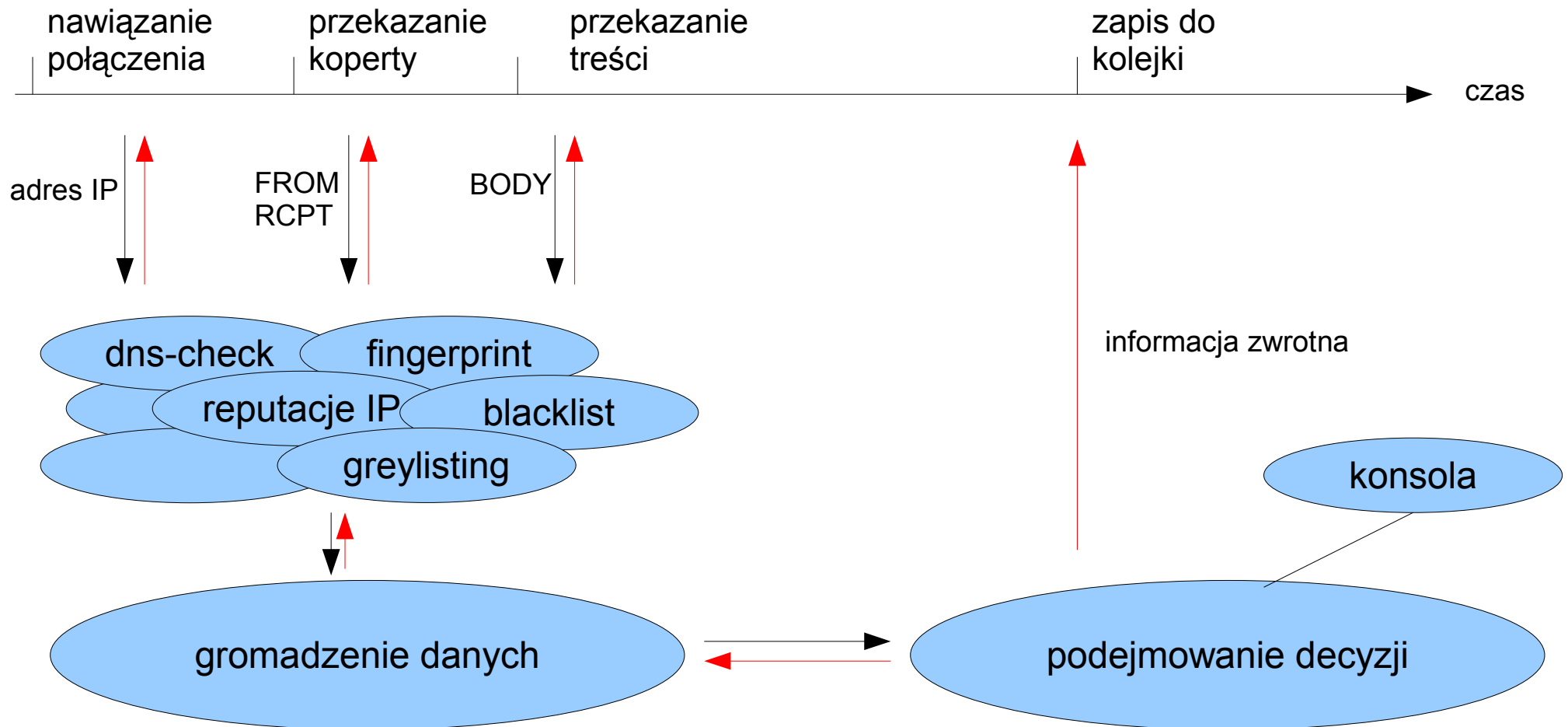
greylisting

- Działanie:
 - Dla każdego po raz pierwszy wysłanego maila generowany jest błąd tymczasowy. Dopiero kolejne wysłanie tego maila (retransmisja) może zakończyć się powodzeniem.
- Zalety:
 - Wysoka skuteczność
- Wady:
 - Skomplikowana implementacja (utrzymywanie repozytoriów tripletów)
 - Problemy przy współpracy z niektórymi MTA (zbyt długie czasy retransmisji lub jej brak)

OS fingerprinting

- Działanie:
 - zakładając, że systemy Windows nie pracują na ogół jako MTA i nie powinny łączyć się do MX'a wykrywamy takie połączenia w czasie rzeczywistym i uznajemy za prawdopodobne źródło spamu.
- Zalety:
 - bardzo wysoka skuteczność
 - niewielki narzut wydajnościowy
 - prosta konstrukcja
- Wady:
 - konieczność utrzymywania “białej listy” hostów Windows, które pracują jako MTA

Ogólna architektura systemu AS



Przykład polityki antyspamowej

- **IF** (IP==a.b.c.d/24) **AND** (TIME>00:00 **AND** TIME<07:00) **AND** (dns-check-ip) **AND** (DCC) **THEN** MarkSpam();
- **IF** (dns-check-ip) **AND** (DCC) **AND** (Bayes) **THEN** Reject();
- **IF** (IP==localnetwork) **THEN** Skip();

Zastosowania:

- sterowanie poziomem zabezpieczeń w zależności od sieci z której pochodzi połączenie (np. sieci z dynamicznie przydzielanymi IP)
- sterowanie w zależności od daty (np. święta) czy pory dnia
- sterowanie w zależności od parametrów zdefiniowanych dla konkretnego użytkownika lokalnego (np. użytkownik komercyjny lub darmowy)
- sterowanie w zależności od ilości wysłanych maili (w przypadku przekroczenia pewnej granicy zwiększamy czułość systemu AS)

Wagowy system klasyfikacji

- Każdy z mechanizmów (testów) otrzymuje wagę, np:
 - obecność na blacklist (+2)
 - negatywny test SPF (+2)
 - negatywny test bayes (+3)
 - Reputacje poniżej pewnego poziomu (+5)
- Dla danych warunków definiujemy politykę AS:
 - na podstawie adresu źródłowego (mark: 4, reject: 8)
 - na podstawie informacji o własnym użytkowniku (1, 3)
 - na podstawie daty/czasu nadejścia maila (5, 8)
 - Itp...
- Mail zostaje oceniony na podstawie sumy punktów

Kilka rad dla admina dużego środowiska

- lepiej odrzucać spam niż go oznaczać i przechowywać gdyż oszczędzamy sieć, dyski oraz procesory.
- należy stosować wiele różnych mechanizmów zabezpieczających w różnych fazach transakcji SMTP
- koniecznie trzeba analizować feedback (np. w postaci skarg od użytkowników ;)) i na tej podstawie wykonywać tuning systemów AS
- prowadzić statystyki działania systemów AS i regularnie wyciągać wnioski z ich obserwacji.
- Uczestniczyć w wymianie informacji (np. Messaging Anti-Abuse Working Group - MAAWG)

Pytania... ?