Michał **CHROBAK**

WYSTĘPUJĄCE ZAGROŻENIA W POCZCIE ELEKTRONICZEJ

Streszczenie. W artykule omówiono niebezpieczeństwa związane z korzystaniem z poczty elektronicznej, takie jak podszywanie się pod nadawcę, podsłuchanie lub modyfikacja treści wiadomości. Przedstawiono skuteczne metody ochrony przed każdym z wymienionych zagrożeń do zastosowania w środowisku biznesowym.

Słowa kluczowe: korespondencja e-mail, podsłuchiwanie wiadomości, podszywanie się pod nadawcę, kryptografia, PGP, S/MIME.

1. WSTĘP

Poczta elektroniczna jest najstarszą metodą komunikacji w informatyce, wywodzącą się z lat ’60 kiedy do użytku weszły pierwsze systemu komputerowe umożliwiające użytkownikom zdalne zalogowanie się do nich. Pierwsze próby komunikacji polegały na prostym przesyłaniu plików z wiadomościami w obrębie takich komputerów. Wiadomości te nie posiadały żadnej ustandaryzowanej struktury ani formy przesyłu. Dopiero na początku lat ’70 powstał dokument RFC 561[1] definiujący format wiadomości oraz w tym samym czasie dedykowany program do ich przesyłania: mail. Do dzisiejszego dnia można wysyłać tym programem wiadomości zbudowanej wg zaleceń dokumentu RFC 561, pomimo że ich początki są sprzed ponad 40 lat. Należy wziąć pod uwagę, że wówczas nie było – tak jak dzisiaj - globalnej sieci zbudowane w głównej mierze z komputerów obsługiwanych przez jednego użytkownika. Wówczas dominował model scentralizowany, gdzie był jeden komputer, a użytkownicy łączyli się do niego poprzez terminale[1]. Przesył danych był w głównej mierze w obrębie zaufanej lokalizacji pomiędzy zaufanymi osobami. W związku z tym tworzące się fundamenty protokołu poczty elektronicznej nie były projektowane z myślą o bezpieczeństwie. Po latach zmian technologicznych w zakresie rozwiązań sieciowych i upowszechnieniu się komputerów, poczta w oryginalnej postaci nie jest dostosowana do obecnych warunków w zakresie bezpieczeństwa. Aby zmienić ten stan rzeczy, wprowadzono szereg usprawnień do protokołu pocztowego, tak po stronie serwerowej, niewidocznej dla użytkownika, jak i po stronie klienta, gdzie wymagane jest od użytkownika podjęcie stosownych kroków. W kolejnych rozdziałach opisano popularne ataki na pocztę elektroniczną, wybrane elementy z zakresu kryptografii oraz ich zastosowanie w celu ochrony przed napastnikami.

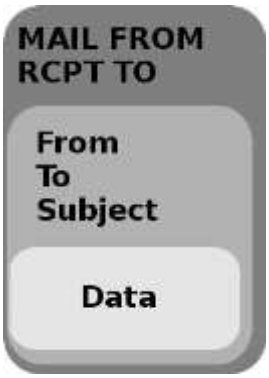
2. ATAKI NA POCZTĘ

2.1. Spoofing

W celu omówienia zagadnienia spoofingu w poczcie elektronicznej, niezbędne jest uprzednie omówienie minimalnego formatu wysyłanej wiadomości, którą przedstawiono na rysunku 1.

1 Terminal - urządzenie służące do łączenia się do zdalnych komputerów, na których są wykonywane wszystkie akcje użytkownika

inż. Michał **CHROBAK –** Ośrodek Badawczo-Rozwojowy Urządzeń Mechanicznych „OBRUM” sp. z o.o., Gliwice



MAIL FROM - nadawca wiadomości
RCPT TO - adresat wiadomości

From - nadawca wiadomości (dla klienta poczty)
To - adresat wiadomości (dla klienta poczty)

Subject - tytuł wiadomości

Rys. 1. Format wysyłanej wiadomości

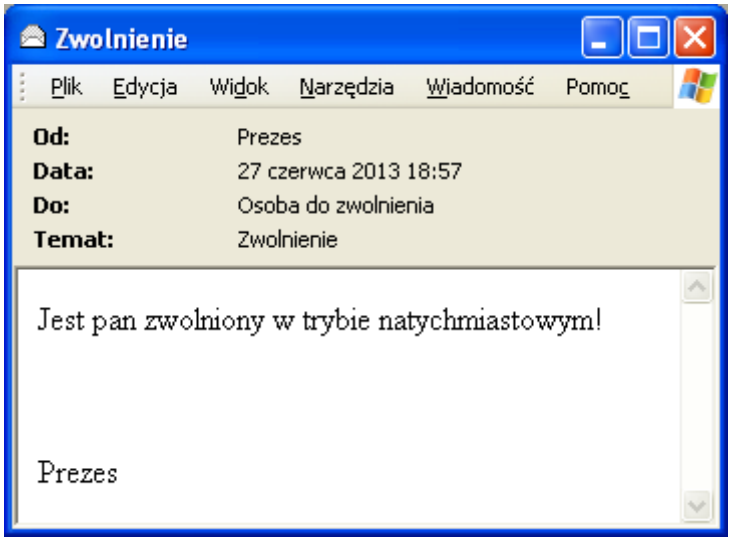
Jak widać na obrazku, dwa pola się powtarzają: *RCPT TO* z *To* oraz *MAIL FROM* z *From*. Przy wysyłaniu maili przeprowadzana jest "rozmowa" z serwerem pocztowym, w której w pierwszej kolejności informujemy serwer, kto jest nadawcą wiadomości (*MAIL FROM*) oraz do kogo serwer ma ją wysłać (*RCPT TO*). Serwer po zweryfikowaniu, że konto nadawcy istnieje w jego bazie, umożliwia wprowadzenie treści emaila, na którą składa się nagłówek i tekst wiadomości. W nagłówku znajdują się dane dla programów pocztowych, takie jak adresat (pole *To*), nadawca (pole *From*) czy temat emaila (pole *Subject*). W przeciwieństwie do pól *RCPT TO* i *MAIL FROM*, które służą do identyfikacji konta na serwerze i podaniu realnego odbiorcy, to pola *To* i *From* mają poinformować użytkownika o tym kto wysyłał wiadomość i do kogo. Z tego też powodu w pola *To* i *From* można wpisać np. 'Imię Nazwisko <imie.nazwisko@firma.pl>', dzięki czemu klient pocztowy pokaże czytelniejszą postać nadawcy i odbiorcy.

Spoofing bazuje na tym, że nie ma wymogu, aby adres w polu *MAIL FROM* był tym samym adresem co w polu *From*. W związku z tym, mając konto *oszust@spoof.com* można podać się za kogoś innego, np. *prezes@firma.pl.* Na wydruku kodu 1 przedstawiono ręczne wysłanie sfałszowanego maila, łącząc się do serwera pocztowego (wszelkie programy pocztowe wykonują te same kroki automatycznie), a na wydruku rysunku 2 tą samą wiadomość w programie pocztowym.

```
MAIL FROM: oszust@spoof.com
250 Ok
RCPT TO: ofiara@firma.pl
250 Ok
DATA
354 end with <CRLF>.<CRLF>
From: Prezes <prezes@firma.pl>
To: Osoba do zwolnienia <biedny-pracownik@firma.pl>
Subject: Zwolnienie
Jest pan zwolniony w trybie natychmiastowym!

Prezes
.
250 OK queued as AXQbfX
```

Kod 1: Ręczne wysyłanie e-maila na serwer



Rys. 2. Otrzymany sfałszowany e-mail

Jak widać wyżej, przy komunikacji z serwerem podano odmienne wartości w polach *MAIL FROM* i *From* oraz *RCPT TO* i *To*, co zaowocowało otrzymaniem maila, który wygląda jakby był wysłany z adresu *prezes@firma.pl*. Istotnym elementem jest to, że oszust połączył się z serwerem *spoof.com* i to na nim musiał mieć swoje konto (*oszust@spoof.com*), a nie na serwerach *firma.pl*.

Przy komunikacji z serwerem linie zaczynające się od liczb są wysyłane przez serwer po wprowadzeniu polecenia przez użytkownika i oznaczają czy serwer przyjął polecenie (kod 250, 354) lub wystąpił błąd (powyżej brak takiego przypadku). Komenda *DATA* informuje serwer, że kolejne linie ma traktować jako treść wiadomości.

Gdyby ofiara chciała odpowiedzieć na tak sfałszowaną wiadomość, odpowiedź nie zostałaby wysłana na skrzynkę oszusta (*oszust@spoof.com*), a na adres podszywanej osoby (*pre-zes@firma.pl*). Może to doprowadzić do wykrycia oszustwa, dlatego też oszuści stosują czasem dodatkowe pole nagłówkowe przy polach *From* i *To*, a mianowicie *Reply-to*, który wskazuje na jaki adres należy odesłać wiadomość (adres ten jest widoczny przy adresie nadawcy i odbiorcy w klientach pocztowych).

2.2. Phishing

Phishing jest niejako rozwinięciem *spoofingu*, gdzie oszust, oprócz modyfikacji nagłówków, stara się nakłonić ofiarę w treści emaila do uzyskania poufnych informacji. Może się podszywać pod autorytet (przełożony), osobę zaufaną (administrator), instytucję (serwis pocztowy lub bankowy) lub interesującą osobę (atrakcyjna kobieta / mężczyzna) w celu zwrócenia uwagi na wiadomość. Często towarzyszy temu odpowiedni temat wiadomości:

- „Natychmiastowa potrzeba podania hasła” (od przełożonego),
- „Łatka na krytyczną dziurę w systemie” (od administratora),
- „Przekroczono ujemne saldo na koncie” (od banku),
- „Nasze fotki z szalonego weekendu!” (od atrakcyjnej kobiety / mężczyzny).

Również zawartość wiadomości może być różnych rodzajów, poczynając od emaili nakazujących wykonanie jakichś akcji (przełożony każe podać hasło), poprzez uruchomienie

załączonego programu (aktualizacja usuwająca rzekomą lukę w bezpieczeństwie), odwiedzenie strony, której adres jest zawarty w mailu (link do fałszywej strony banku, gdzie można sprawdzić swoje saldo), kończąc na zachęcaniu do otwarcia dokumentów lub obrazków (zdjęcia od atrakcyjnej kobiety / mężczyzny). Wszystkie te akcje są związane z podstawionym przez oszusta elementem, łudząco podobnym do oryginalnego.

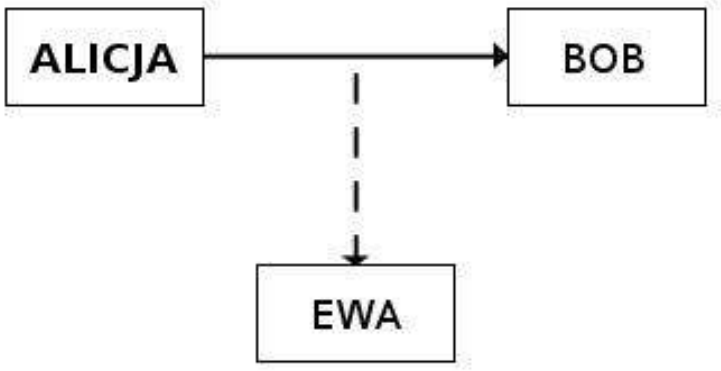
Jak widać *phishing* w głównej mierze bazuje na *socjotechnice*, czyli technikach manipulacji człowiekiem - najsłabszym ogniwem w systemie bezpieczeństwa.

2.3. Podsłuch

Podsłuch wiadomości jest najmniej wyrafinowaną metodą ataku na pocztę elektroniczną, jednak muszą być spełnione oczywiste ku temu warunki: atakujący musi być albo w tej samej sieci lokalnej (np. w domu, w firmie lub sieciach bezprzewodowych na lotniskach czy kawiarniach) albo musi mieć bezpośredni kontakt z medium, którym przesyłana jest wiadomość. Drugi przypadek jest stosunkowo rzadko spotykany, gdyż wymaga od napastnika fizycznego dostania się do sieci jednej z osób biorących udział w komunikacji lub u dostawców internetowych, którzy pośredniczą w transmisji. Istnieją jeszcze inne, bardziej zaawansowane metody podsłuchu, jednak ze względu na ograniczoną ilość miejsca skupiono się na omówieniu powyższych metod.

Zdecydowanie łatwiej jest przeprowadzić podsłuch w sieci lokalnej. Jeszcze kilkanaście lat temu, kiedy sieci były zbudowane o koncentratory (ang. *hub'y*), podsłuchiwanie danych w sieciach było bardzo proste. W takiej sieci dane wysyłane z jednego węzła były rozsyłane do wszystkich węzłów w sieci, więc każdy mógł podsłuchać co w danej chwili jest transmitowane. W dzisiejszych czasach, w sieciach opartych o przełączniki (ang. s*witche*) komunikacja pomiędzy dwoma węzłami przebiega bezpośrednio - dane nie trafiają do żadnych innych węzłów. Dlatego też jednym z pierwszych kroków napastnika jest albo atak na przełącznik, aby ten zaczął zachowywać się jak koncentrator, albo zmuszenie dwóch węzłów w sieci do przesyłania wszystkich danych przez komputer atakującego (tymi węzłami może być np. komputer ofiary oraz serwer pocztowy, atak taki nazywany jest *Man in the Middle*). W obu przypadkach po udanym ataku, napastnik ma dostęp do całego ruchu ofiary, w tym do przesyłanych wiadomości, a przy ataku *Man in the Middle* dodatkowo ma możliwość modyfikacji przesyłanych wiadomości, czyli naruszenia ich integralności.

Na rysunku 3 przedstawiono sytuację, kiedy Alicja wysyła do Boba dane, które są zarazem podsłuchiwane przez Ewe[2].



Rys. 3. Podsłuchiwanie Danych

2 Alicja i Bob - klasyczne akronimy do opisywania systemów kryptograficznych, gdzie Alicja i Bob są elementami przesyłającymi sobie dane, a Ewa elementem ingerującym w ten przesył

2.4 Naruszenie integralności

Naruszenie integralności występuje wówczas, kiedy napastnik po uprzednim przekierowaniu ruchu pomiędzy dwoma węzłami w sieci w taki sposób, aby przechodził przez jego komputer, przeprowadza modyfikację wiadomości. Jest to zatem połączenie podsłuchu wraz ze *spoofingiem* z wyeliminowaniem pewnych wad tego drugiego. Mianowicie przy klasycznym *spoofingu* odbiorca wiadomości jest w stanie obejrzeć techniczne nagłówki wiadomości, które normalnie nie są wyświetlane. W tych właśnie nagłówkach podany jest adres komputera, który wysłał wiadomość oraz jakim kontem pocztowym posłużył się do nadania wiadomości (wartość pola *MAIL FROM*). Przy podsłuchu typu *Man in the Middle* (który jest warunkiem koniecznym przy tym ataku), wszelkie nagłówki poczty elektronicznej (techniczne oraz zwykłe) pozostają w niezmienionej formie. Kiedy przy takim podsłuchu napastnik zacznie modyfikować wiadomość - nie zostawi to żadnych dodatkowych śladów umożliwiających zdemaskowanie incydentu.

Istotną różnicą pomiędzy tym atakiem, a *spoofingiem* jest fakt, że tutaj modyfikować można tylko już wysłane wiadomości, natomiast w przypadku *spoofingu* napastnik sam generuje fałszywą wiadomość.

Na rysunku 4 zobrazowano atak *Man in the Middle*, gdzie Ewa jest wpięta w kanał komunikacyjny między Alicją i Bobem.

Rys. 4. Atak Man in the Middle

3. OCHRONA PRZED ATAKAMI Z UŻYCIEM KRYPTOGRAFII

W poprzednim rozdziale przedstawiono 3 główne problemy poczty elektronicznej:

- brak pewności, czy nadawca jest faktycznie tym za kogo się podaje (uwierzytelnianie),
- brak pewności, że nikt niepowołany nie przeczytał wiadomości (poufność),
- brak pewności, czy wiadomość dotarła do odbiorcy w niezmienionej postaci (integralność).

Za pomocą kryptografii można rozwiązać te problemy, stosując szyfrowanie lub cyfrowe podpisywanie wiadomości. Oba te elementy bazują na kryptografii asymetrycznej.

3.1. Kryptografia asymetryczna

W procesie szyfrowania asymetrycznego potrzebne są dwa elementy, zwane kluczem publicznym i kluczem prywatnym. Są to w istocie bardzo długie ciągi znaków umieszczone w pliku tekstowym. Cechą charakterystyczną w kryptografii asymetrycznej jest to, iż jednym kluczem następuje szyfrowanie, a drugim deszyfrowanie (nie ma znaczenia czy szyfrowano kluczem prywatnym czy publicznym). Nazwy kluczy biorą się od tego, że jeden z nich (publiczny) jest udostępniany ogółowi, a drugi (prywatny) musi pozostać u właściciela.

Algorytmy stosowane przy kryptografii asymetrycznej są tak skonstruowane, że klucz publiczny jest generowany na podstawie prywatnego (stąd powiązanie pomiędzy tymi kluczami do szyfrowania i deszyfrowania), jednak wygenerowanie klucza prywatnego na podstawie klucza publicznego jest jak najbardziej trudne obliczeniowo.

3.2. Podpisywanie i szyfrowanie wiadomości

Szyfrowanie różni się tym od podpisywania, że podpisaną wiadomość może przeczytać każdy (nie jest potrzebny klucz) i opcjonalnie zweryfikować nadawcę oraz integralność wiadomości. Natomiast przy wiadomości zaszyfrowanej nie ma możliwości jej odczytania bez posiadania klucza, a więc wzbogaca podpisywanie o element poufności.

W sytuacji kiedy Alicja chciałaby wysłać zaszyfrowaną wiadomość do Boba:

1. Alicja uzyskuje publiczny klucz Boba (od niego samego lub z ogólnie dostępnych źródeł).
2. Alicja szyfruje swoją wiadomość kluczem publicznym Boba i wysyła do niego tak powstały szyfrogram.
3. Bob dostaje szyfrogram od Alicji i deszyfruje go swoim kluczem prywatnym, otrzymując oryginalną wiadomość.
4. Natomiast w przypadku podpisywania swojej wiadomości przez Alicję i weryfikację tejże przez Boba.
5. Alicja tworzy skrót[3] swojej wiadomości i szyfruje ten skrót swoim kluczem prywatnym. Wynik tej operacji jest właśnie podpisem i jest dołączany do wiadomości.
6. Bob po otrzymaniu wiadomości od Alicji również wylicza skrót wiadomości (bez podpisu) tym samym algorytmem co Alicja.
7. Bob deszyfruje kluczem publicznym Alicji otrzymany od niej podpis i sprawdza czy skrót, który on sam wyliczył jest tym samym, który dostał w postaci zaszyfrowanej od Alicji.

3.3. Dystrybucja kluczy publicznych - PGP i S/MIME

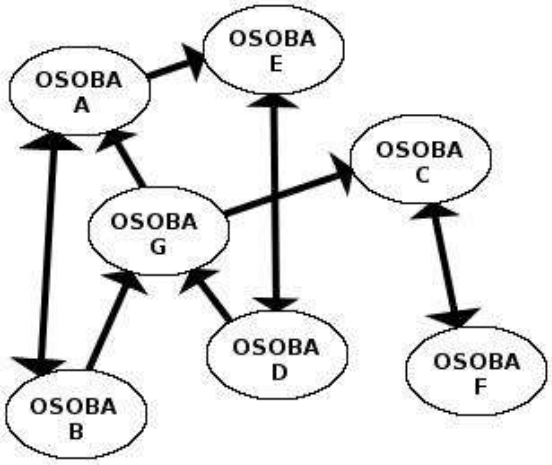
Fundamentalnym elementem przy kryptografii asymetrycznej jest dostęp do kluczy publicznych. Rodzi to jednak problemy z weryfikacją, czy dany klucz publiczny faktycznie należy do osoby, której chcemy wysłać wiadomość. Aby rozwiązać ten problem stosuje się:

1) wzajemną sieć zaufania (ang. *Web of Trust (WoT)*) – PGP,
2) zaufany autorytet, zbudowany na bazie infrastruktury klucza publicznego (ang. *Public Key Infrastructure (PKI)*) - S/MIME,
3) bezpośredni i pośredni przesył kluczy pomiędzy zainteresowanymi osobami - PGP i S/MIME.

PGP[2] oraz S/MIME[3] to technologie mające na celu poprawę bezpieczeństwa poczty elektronicznej. Oba standardy opierają się o kryptografię asymetryczną, jednak nie są one ze sobą kompatybilne. S/MIME charakteryzuje się tym, że wykorzystuje certyfikaty wystawione przez zaufane centrum, a PGP tym, że certyfikat zdobywa zaufanie poprzez innych użytkowników którzy dokonują weryfikacji.

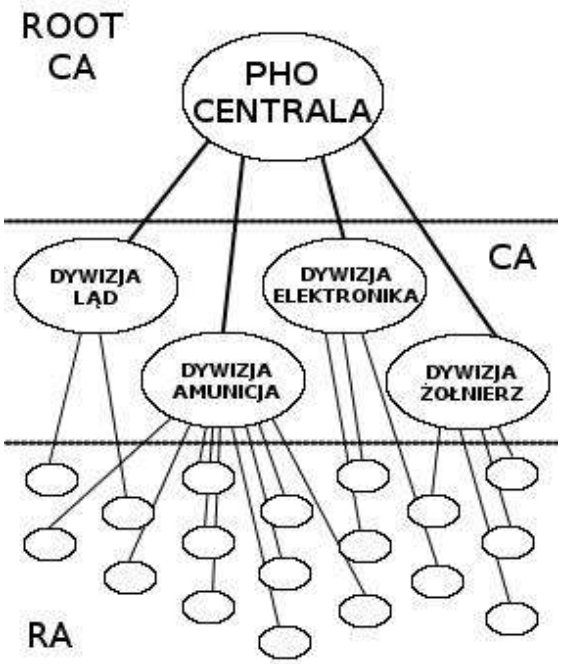
Sieć zaufania działa na zasadzie poświadczenia osób będących w tej sieci o autentyczności danego klucza. Realizowane jest to poprzez cyfrowe podpisywanie kluczy: jeśli osoba A jest pewna że klucz K_B należy do osoby B, podpisuje go swoim kluczem K_A, jeśli osoba C zweryfikowała klucz osoby A, wówczas klucz K_A osoby A jest podpisany kluczem K_C osoby C itd. Tworzy to sieć zaufania jak na rysunku 5.

3 Skrót - ang. hash - ciąg znaków o stałej długości, jednoznacznie identyfikujący dane z którego liczony jest skrót. W zależności od stosowanego algorytmu, skrót ma długość najczęściej kilkudziesięciu znaków



Rys. 5. Sieć zaufania

Infrastruktura klucza publicznego[4] opiera się o zewnętrzny autorytet, który uznaje się za zaufany i w przypadku kiedy ten autorytet poświadcza o danej osobie, to również jest ona zaufana. PKI jest zbudowana hierarchicznie, gdzie głównym elementem jest Urząd Certyfikacyjny (ang. *Certification Authority (CA)*), który na bazie klucza użytkownika tworzy mu odpowiedni certyfikat podpisany przez siebie. Jednak nim *CA* wyda taki certyfikat, musi najpierw zweryfikować osobę, której klucze będzie podpisywać - ten element zapewnia że osobom z certyfikatami można zaufać. W zależności od potrzeb, może być kilka Urzędów Certyfikacyjnych: jeden główny (ang. *Root CA*) oraz kilka pośrednich (*CA*) mogących w imieniu głównego Urzędu wydawać certyfikaty. Oprócz samych Urzędów Certyfikacyjnych może również wystąpić Urząd Rejestrujących (ang. *Registration Authority (RA)*), który zbiera wnioski i zajmuje się weryfikacją osób ubiegających się o certyfikat. Przykładową infrastrukturę klucza publicznego przedstawiono na rysunku 6.



Rys. 6. Infrastruktura klucza publicznego

Ostatnią metodą dzielenia się kluczami publicznymi jest umieszczanie ich na specjalnie do tego przygotowanych serwerach (tzw. Serwery Kluczy [5]), przesłanie ich bezpośrednio pomiędzy sobą lub umieszczenie ich na własnej stronie www.

4. PODSUMOWANIE

Pomimo ogromnej popularności poczty elektronicznej jest ona zarazem podatna na wiele rodzajów zagrożeń. Na przestrzeni lat starano się wdrożyć wiele mechanizmów poprawiających bezpieczeństwo poczty, jednak żadne z nich, które wymagało interakcji użytkownika nie zyskało popularności. Powodów jest kilka, a główne to brak świadomości odnośnie zagrożenia oraz (tak wydaje się na pierwszy rzut oka) skomplikowany proces wdrożenia PGP lub S/MIME. W rzeczywistości, po zaznajomieniu się ze sposobem funkcjonowania PKI i WoT, w prosty sposób można zacząć korzystać z tych technologii. W sieci istnieje wiele serwisów, które w łatwy sposób umożliwiają wdrożenie zarówno, jeśli chodzi o wygenerowanie kluczy, uzyskanie certyfikatów, jak i opis w jaki sposób należy je zaimportować do programu pocztowego.

5. LITERATURA

[1] Bhushan A., Pogran K., Tomlinson R., White J.,: RFC 561 - Mail Headers, 5 wrzesień 1973, http://tools.ietf.org/html/rfc561.

[2] Callas J., Donnerhacke L., Finney H., Shaw D., Thayer R.: RFC 4880 – OpenPGP, listopad 2007, http://tools.ietf.org/html/rfc4880.

[3] Ramsdell B., Turner S.: RFC 5751 – S/MIME, styczeń 2010, http://tools.ietf.org/html/rfc5751.

[4] Cooper D., Santesson S., Farrel S., Boeyen S., Housley R., Polk W.: RFC 5280 – PKI, maj 2008, http://tools.ietf.org/html/rfc5280.

[5] Serwer Kluczy MIT http://pgp.mit.edu/

HAZARDS PRESENT IN ELECTRONIC MAIL

Abstract. The paper discusses the hazards encountered when using electronic mail, such as sender impersonation, message interception or modification. Effective methods of protection against such risks in the business environment are also presented.

Keywords: e-mail correspondence, message interception, sender impersonation, cryptography, PGP, S/MIME