Romuald Swarcewicz

Zaufanie i pewność w e-biznesie (II)

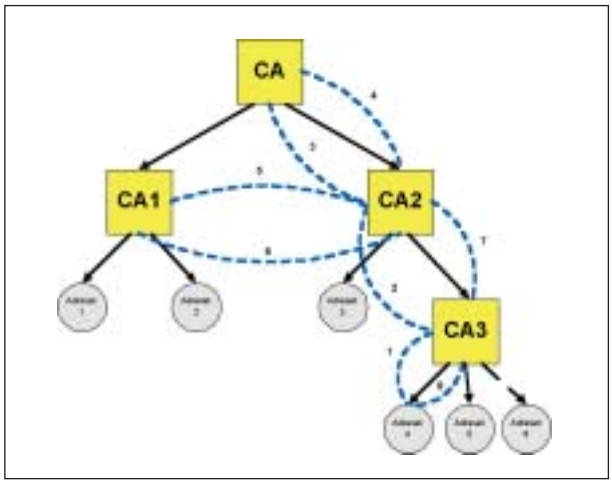
Fot. Nick Benjaminsz

Kryptografia, dziedzina wiedzy zajmująca się zagadnieniami utajniania informacji poprzez jej szyfrowanie, zaangażowana jest w dwa zagadnienia bezpieczeństwa: prywatności i autentyczności. W systemie kryptografii bardzo istotny jest klucz kryptograficzny, który służy do szyfrowania i deszyfrowania komunikatu. Szyfrowanie symetryczne posługuje się kluczem prywatnym, który jest taki sam dla nadawcy i odbiorcy. Obecnie używane klucze, uznawane za dające dostateczny poziom bezpieczeństwa mają długość 128 bitów. Szyfrowanie symetryczne zapewnia prywatność i autentyczność, ale jest bardzo kosztowne, gdyż wymaga unikalnych kluczy dla każdej komunikującej się pary. Tak więc jeżeli 10 jednostek chce komunikować się w ten sposób, potrzebne jest 45 kluczy, ale już przy 100 jednostkach potrzeba 4950 kluczy.

Przy szyfrowaniu asymetrycznym komunikujący się potrzebują dwu kluczy: publicznego, dostępnego dla wszystkich i prywatnego, specjalnego dla każdego uczestnika komunikacji. Klucz publiczny używany jest do zaszyfrowania komunikatu a prywatny do jego odszyfrowania. Cała kryptografia używająca klucza publicznego bazuje na założeniu, że na drodze obliczeń niemożliwe jest utworzenie prywatnego klucza z ekwiwalentnego klucza publicznego, podczas gdy rewers jest możliwy.

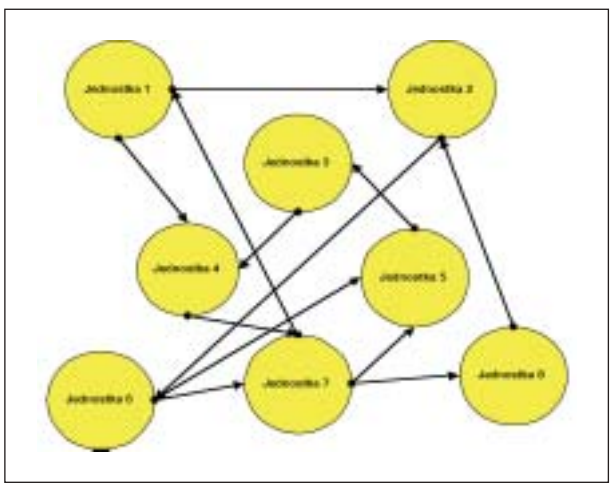
Opisana koncepcja szyfrowania kluczem publicznym wygląda rozsądnie, ale istnieje duży problem – jak jednostka może zaufać, że publicznie dostępny klucz jest autentycznym kluczem należącym do jednostki próbu-

Certyfikat decyduje tylko o jednej części zagadnienia zaufania, ale problemem do rozwiązania pozostaje jeszcze, jak wierzyć certyfikatowi.



Rys. 3. *Hierarchiczny model PKI*

jącej skomunikować się? Z tego powodu konieczne jest posiadanie właściwego systemu zarządzania kluczem, aby można było go używać bezpiecznie. PKI (*Public Key Infrastructure*) – infrastruktura publicznego klucza definiuje strukturę publicznego klucza otrzymywanego przez jednostkę w celu szyfrowania informacji dostarczającej cyfrowego certyfikatu identyfikującego jednostkę i organizację obsługującą. Innymi słowy PKI definiuje strukturę dla zarządzania kryptograficznym kluczem. W celu ustalenia związku pomiędzy jednostką i jego publicznym kluczem, PKI używa strukturę danych nazywaną certyfikatem, który łączy tożsamość jednostki z jego publicznym kluczem i jednocześnie zawiera informację, jak użyć publicznego klucza. Certyfikat decyduje tylko o jednej części zagadnienia zaufania, ale problemem do rozwiązania pozostaje jeszcze, jak wierzyć certyfikatowi. Zaakceptowanym rozwiązaniem w PKI tego zagadnienia jest skorzystanie z zaufanej jednostki certyfikującej zwanej Certificate Authority (CA). CA cyfrowo podpisuje certyfikat i wysyła go do żądającego podmiotu.



Rys. 4. *Sieciowy model PKI*

Dostępne i proponowane są różne modele PKI. Różnią się konfiguracją, regułami ufności i elastycznością. Rozpatrując konfigurację i reguły ufności rozróżniamy dwie kategorie PKI: hierarchiczną i sieciową.

Model hierarchiczny to taki, w którym każdy CA ma relacje nadrzędne i podrzędne, jak widać to na rys. 3.

Niebieskie linie przerywane pokazują drogi prośby o klucz i przesyłu klucza. Model hierarchiczny ma prostą strukturę i jednokierunkowe relacje zaufania. Zaletami tego modelu są: skalowalność, przystępne tworzenie jednokierunkowych dróg certyfikacji i to, że drogi certyfikacji są krótkie. Natomiast do wad modelu możemy zaliczyć: bardzo silne oparcie na pojedynczym punkcie, korzeniu CA. Jeżeli korzeń CA załamie się, to cała hierarchia upadnie, umowa z jednym CA może być nierealna, wszystkie organizacje lub kraje nie mogą bowiem ufać jednej jednostce zaufania.

Model sieciowy jest alternatywą dla tradycyjnego modelu hierarchicznego PKI. W tym modelu wszystkie jednostki w sieci mogą być jednostkami zaufania - jednostkami certyfikującymi. Zaufanie jest tu dwukierunkowe i jednostki tworzą sieć zaufania, często jest on nazywany jako „web zaufania". Jednostką w tym modelu może być zarówno normalny użytkownik, jak i CA. Dowolna jednostka w sieci może wydać certyfikat innej jednostce, a żadna z jednostek nie może dyktować innej typu certyfikatu, jaki ona wydaje. Model przedstawiono na rys. 4.

Zaletami tego modelu są:

- łatwe dołączenie nowego zbioru użytkowników
- załamanie jednego punktu nie powoduje degradacji całej sieci, ponieważ istnieje wiele dróg zaufania lub certyfikatów pomiędzy uczestnikami
- bardzo łatwo przywrócić stan zaufania po degradacji jednego punktu
- niezwykle łatwo jest dołączyć oddzielnie rozwijany PKI.

Wadami modelu to:

- dwukierunkowe relacje zaufania czynią model bardziej złożony w stosunku do hierarchicznego
- budowanie drogi certyfikacji od certyfikatu użytkownika do punktu zaufania jest niedeterministyczne

- użytkownik sieci musi raczej określić, jaka aplikacja certyfikatu może być użyta za podstawę zawartości certyfikatu, aniżeli lokalizować CA w PKI.

System zarządzania kluczem musi zapewniać użytkownikowi otrzymanie autentycznego klucza, możliwego do użycia w celach kryptograficznych. Zarządzanie kluczem może być więc rozpatrywane jako synonim zarządzania zaufaniem.

Większość implementacji PKI obecnie bazuje na hierarchicznym modelu, w którym jednostka otrzymuje klucz publiczny w formie certyfikatu od CA, w którym jest zarejestrowana. Współczesna generacja mobilnej komunikacji polega również na centralnej autoryzacji. Gdy nastąpi jej rozwój, przejdzie do nowej topologii sieci, której popularność rośnie. Ta nowa topologia sieci jest siecią doraźną, a jej przykładem są *Jini* i *bluetooth*.

Sieci doraźne są nowym paradygmatem komunikacji bezprzewodowej dla urządzeń mobilnych. Sieć doraźna nie ma stałej infrastruktury takiej jak – stacja bazowa lub mobilne centrum przełączające. Mobilne urządzenia komunikują się ze sobą drogą radiową w ramach zasięgu i tworzą między sobą infrastrukturę, która może zmieniać się w czasie. Oznacza to, że urządzenie przejmuje odpowiedzialność pośredniego węzła, jest więc zarówno terminalem jak i routerem. Cele zabezpieczeń są identyczne dla wszystkich typów sieci, zarówno stacjonarnych jak radiowych.

Zagrożenie sieci doraźnych można podzielić na dwie kategorie: zagrożenie podstawowej komunikacji i mechanizmów kierowania oraz zagrożenie mechanizmu zarządzania kluczem. **Przed atakiem zagrożenia komunikacyjnego można zabezpieczyć się właściwą techniką kryptograficzną.** Dla właściwego działania technik kryptograficznych najpierw powinna zadziałać infrastruktura zarządzania kluczem. Jeśli infrastruktura ta jest zdegradowana, wówczas urządzenie nie może ufać kluczowi, który otrzymuje do celów kryptografii i bez tego zaufania nie ma możliwości szyfrowania komunikatu. Znane są trzy metody zarządzania kluczem:

Kryptografia progowa jest systemem zbiorowego udziału w **prywatnym kluczu** wymagającym współpracy grupy przy szyfrowaniu. W sieci doraźnej zakłada się specjalne węzły zwane serwerami. Każdy serwer ma własny prywatny klucz publiczny i przechowuje publiczne klucze wszystkich węzłów w sieci. Oznacza to, że każdy serwer zna publiczne klucze wszystkich innych serwerów i to umożliwia im ustalenie bezpiecznego połączenia wśród siebie. Gdy jakaś jednostka otrzymuje szyfrowany tekst, to wysyła go do każdego z serwerów posiadającego część grupowego prywatnego klucza. Każdy z serwerów odszyfrowuje ten tekst i wysyła z powrotem do nadawcy. Nadawca odzyskuje pełny tekst z jego odszyfrowanych części. Zaufanie zależy od ilości serwerów. System zostaje więc nienaruszony, nawet gdy kilka z serwerów zostanie uszkodzonych.

Umowny klucz. Grupa ludzi zakłada mobilną sieć, a ich urządzenia pozwalają na klucz, który uzgodnią. Klucz powinien być tajny i musi zapewniać standardowe bezpieczeństwo w doraźnej sieci. Zarządzanie kluczem rozpoczyna się od przekazania tradycyjną drogą słabego tajnego klucza. Gdy słaby tajny klucz jest znany, dwa urządzenia mogą transmitować szereg zaszyfrowanych komunikatów, najpierw używając słabego tajnego klucza i później stopniowo używając swojego publicznego klucza. Gdy przekonają się, że komunikują się z właściwym urządzeniem, końcowy klucz staje się współdzielonym prywatnym kluczem pomiędzy dwoma urządzeniami. Ta sama procedura jest powtarzana wśród innych urządzeń tak, że każde z nich otrzymuje współdzielony prywatny klucz.

Samoorganizujący się PKI. Ten projekt wymaga, aby każda jednostka utrzymywała małą bazę certyfikatów wybranych spośród używanych algorytmów. Kiedy jednostka potrzebuje publiczny klucz innej jednostki, to łączą one swoje bazy i próbują znaleźć właściwy łańcuch certyfikatów z tych baz. **Projekt zakłada prawdopodobieństwo pewności, że w połączonej bazie znajduje się taki certyfikat.**

PKI urzeczywistnia koncepcję dystrybucji zaufania w sieciach informatycznych. Nowsze projekty stopniowo migrują z dziedziny sieci stałych do obszaru sieci mobilnych. Prowadzone są intensywne prace nad rozwojem komunikacji mobilnej, której udział w e-biznesie będzie rósł. Zaufanie w sieciach mobilnych staje się istotnym problemem wynikającym z faktu, że brak w nich jednostki certyfikującej, zarządzającej siecią.