SoftEther VPN を用いたソーシャルアプリケーション実行環境の構築

海沼直紀[†] 新城靖[†] 登大遊[†]
櫻井孝一[†] 佐藤聡[†] 中井央[†]

1. はじめに

Social Networking Service(SNS) は世界中のユーザが利用しており、有用なコミュニケーションツールとして普及している。SNS 上のアプリケーションの多くは Web アプリケーションとして実装されている。

LAN 上で動作するアプリケーションを SNS のアプリケーションとして利用したいという要求がある。この要求を満たすものとして Social VPN[1] が提案されている。このシステムでは SNS ユーザの計算機を P2P 型の VPN で接続できる。その際、認証に用いるパスワードを各ユーザに配布する代わりに SNS のパスワードを使うことができる。しかし、この Social VPN を利用するためには専用のソフトウェアが必要であり、利用できる環境が限られてしまう。また、この Social VPN のユーザインタフェースでは SNS のサーバで認証をしていることが確認できないという問題がある。さらに、アプリケーションのバイナリをどのように配布し、安全に実行するかという問題もある。

本研究では SoftEther VPN を用いたソーシャルアプリケーション実行環境を構築する。本研究では、Facebook, Twitter, 及び Google+による VPN の認証機能を SoftEther VPN に付加し、SNS のグループ内のユーザ間で VPN を簡単に導入できるようにする。認証はブラウザによるインターフェースで行い、ユーザが SNS のサーバで認証をしていることを確認できるようにする。また、SNS のユーザ名を含むホスト名を利用可能にする。さらに、Web アプリケーションを利用するときに、VPN の認証と Web アプリケーションの認証を連携させ、認証が 1 回で済むようにする。

2. SoftEther VPN

本研究で用いる VPN ソフトウェアは SoftEther VPN[2] である。このソフトウェアは、イーサネット通信の仕組みをソフトウェアで実装することにより、VPN を実現している。スイッチングハブは仮想ハブ、LAN カードは仮想 LAN カードとして実装されている。

本研究では認証方法に署名済み証明書認証という方法を使用する。これは、サーバに信頼する認証局を登録し、クライアントがその認証局で署名された X.509 証明書と、対応する秘密鍵を保持していることを確認する方法である。

SoftEther VPN ではクライアントに IP アドレスを割り当てるために、内部の DHCP サーバを使う方法の他に仮想ハブと同一のセグメントにある既設の DHCP サーバを用いる方法がある。

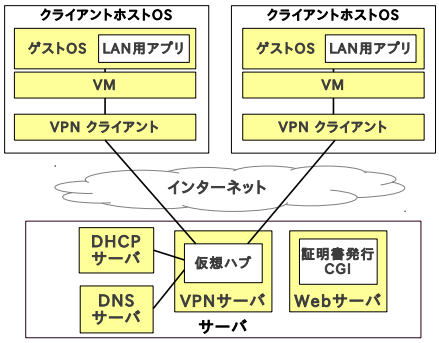

図 1 構築する実行環境

3. ソーシャルアプリケーション実行環境

本研究では図 1 に示すネットワークを構成する。ユーザはまずブラウザで VPN サーバと同一のホストで動作している SNS アプリケーションを実行し、SNS の認証を行う。次に VPN 制御プログラムを起動する。VPN 制御プログラムは先の SNS アプリケーションの証明書発行スクリプトを実行する。これはサーバに用意された認証局で証明書を発行し、それをクライアントに送る。VPN 制御プログラムはこの証明書を VPN クライアントに登録する。最後に VPN 制御プログラムは仮想計算機を実行し、それが利用する TAP デバイスを SoftEther VPN の仮想 LAN カードに接続する。

この後実行されたゲスト OS は、DHCP サーバから

† 筑波大学

図 2 ブラウザを用いたユーザインタフェース

IP アドレスを取得し、VPN サーバで動いている IP アドレス登録スクリプトを実行する。このスクリプトは VPN サーバのユーザ情報から SNS のユーザ名を取得し、それを元に生成したホスト名の正引きと逆引きを DNS サーバに登録する。例えばユーザ名が Alice の場合は Alice.social-vmvpn のようなホスト名になる。

4. ブラウザによるユーザインタフェース

本研究ではブラウザを用いたユーザインタフェースを作成する。SNS の認証をブラウザで行うことにより、ユーザは確かに SNS のサーバで認証をしたことを確認できる。また、既にブラウザで SNS の認証をしていた場合、ユーザ名とパスワードの入力は必要ない。ユーザは VPN サーバで動いている SNS アプリケーションを実行し、認証を終えると図 2 のような証明書取得のための乱数を含む URL が書かれた Web ページが表示される。ユーザは Web ブラウザのアドオンの接続ボタンを押して VPN 制御プログラムを実行する。VPN 制御プログラムはこの URL を用いて証明書を取得し、VPN 接続をする。

5. ユーザ認証の連携

VPN 内でユーザ認証の必要な Web アプリケーションを使用する場合、VPN と、Web アプリケーションで 2 回の認証をする必要があり、不便である。この問題を解決するために、本研究では VPN の認証と Web アプリケーションの認証を連携させる。本研究では Apache HTTP Server の認証モジュールを作成する。このモジュールは、まず、環境変数 REMOTE_ADDR からユーザの IP アドレスを取得し、その IP アドレスを用いて VPN 内の DNS サーバに問い合わせる。次に、DNS サーバは SNS のユーザ名を含むホスト名をモジュールに返す。このホスト名は 3 章で述べたように、VPN サーバから得られたものであり、信頼できる。最後に、モジュールはホスト名からユーザ名を取り出し、ユーザ名を環境変数 REMOTE_USER に入れる。Web サーバから実行された Web アプリケーションは環境変数 REMOTE_USER からユーザ名を取り出して利用できる。

6. 関 連 研 究

Social VPN[1] という研究は、SNS の基盤を利用した VPN ソフトウェアを作成している。VPN には IP over P2P を用いている。また、この Social VPN を利用するには専用のソフトウェアが必要である。本研究とは VPN に SoftEther VPN を用いている点、仮想計算機を用いているので、ゲスト OS に VPN クライアントをインストールする必要がない点、及びブラウザを用いたユーザインタフェースを作成している点で異なる。

Virtual private social networks[3] という研究は、既存の Web ベースのソーシャルネットワークで外部には偽の情報を表示して、内部のユーザにだけ本来の情報を表示する。ただし、内部のユーザに本来の情報を予めメールで送る必要がある。これに対して本研究では、内部の情報をメールではなくユーザが管理しているコンピュータに置ける点、及び LAN 上で動作する Web 以外のアプリケーションを利用できる点で異なる。

7. お わ り に

本研究では SoftEther VPN を用いたソーシャルアプリケーション実行環境の構築をする。SNS のアカウントを用いた VPN の認証機能を作成し VPN を簡単に導入できるようにする。また、ブラウザを用いたユーザインタフェースを作成し、SNS のサーバで認証をしていることを確認できるようにする。さらに、VPN の認証と Web アプリケーションの認証を連携させ、認証が 1 回で済むようにする。

今後はユーザインターフェースを完成させ、どのユーザの VPN サーバを使用して通信するのかを決定する機能の作成、及び認証連携のための Apache HTTP Server のモジュールの作成を行う。

参 考 文 献

1) Figueiredo, R., Boykin, P., Juste, P. and Wolinsky, D.: Integrating Overlay and Social Networks for Seamless P2P Networking, *Workshop on Enabling Technologies: IEEE 17th Infrastructure for Collaborative Enterprises*, pp. 93 –98 (2008).
2) : SoftEther VPN プロジェクト, `http://ja.softether.org`.
3) Conti, M., Hasani, A. and Crispo, B.: Virtual private social networks, *The first ACM conference on Data and application security and privacy*, pp. 39–50 (2011).