平成 18 年度情報処理軽井沢セミナー

南山大学 教育・研究事務部 情報システム課
小島　一人

１．　課題タイトル

「認証技術を知る －PKI を中心として－」

２．１の概要

大学等において各種ネットワークサービスを設計･運用していくうえで必要となる, PKI（Public Key Infrastructure：公開鍵基盤）を中心とした認証関連の専門的知識や最新技術を修得する.

実習では, 証明書の正しい解釈の仕方（データフォーマットから認証パスの検証まで）や既成アプリケーションでの SSL/TLS 認証, S/MIME 等の環境構築等を行う. PKI を中心とした認証技術について、技術・実装に止まらず最新の動向や運用設計等も網羅した幅広い知見を身につけ, 所属機関のネットワークサービスに適切な形で PKI を導入することができることを目標とする.

３．講義・演習とその成果

何を計画し、今後どのように進めていくか。セミナーでの発表＋今後の展望について

セミナーは以下の内容で, PKI の技術についての解説とそれに関する演習を実施した.

1. PKI の技術(基礎編)

   PKI に係る基本的な用語について解説に続いて, PKI 技術についての解説があった.

   - 署名者(Subscriber)
   - 検証者(Relying Party)
   - 認証局の信頼
   - PKI の構成
   - 証明書発行
   - X.509 証明書拡張
   - PKI の信頼性

2. PKI の技術(応用編)

   PKI を相互運用するさいに必要な技術等について解説があった.

   - 証明書検証の技術
   - 認証局と HSM(Hardware Security Module)
   - PKI によるネットワーク認証技術
   - 電子署名法と電子署名の展開
   - 公的個人認証サービス

3. PKI の技術(補足編)
4. PKI 実習編

   各編で解説のあった技術を理解するために, 演習では以下の 2 つの実習を実施した.

   ・証明書の発行と認証パスの構築検証
   ・電子署名とタイムスタンプ

   証明書の発行と認証パスの構築

   JNSA(日本ネットワークセキュリティ協会)相互運用テストスィートを利用して, 証明書を発行し, 発行した証明書について認証パスを構築できるかどうかをいくつかの場合について検証した.

   電子署名とタイムスタンプ

   FileSign を使用してファイルに署名をつけ, その署名を検証できるかどうかについて実習した. またタイムスタンプをつけた場合の検証についても実施した.

5. 課題

このセミナーの課題は，所属している組織で実際に PKI を運用することを想定し，具体的な運用案と実現するさいに解決しなければならない問題等について検討することであった．

PKI の具体的な運用の検討の案として，学内の利用者認証にハードウェアトークンを利用した PKI を使用することを検討し，運用する場合の前提条件および問題点について検討した．

現在大学内のシステムは，すべてユーザ名とパスワードによる利用者認証を使用している．学外から利用する場合に，ユーザ名とパスワードだけ利用者認証することに不安があり，より安心できる認証方式を検討している．利用者認証をハードウェアトークン利用 PKI による利用者認証へ移行することにより，この問題が解決できると考える．

具体的には以下の利用者認証に PKI を使用することを検討する．

- 学外からの利用時の認証
- ネットワーク利用時の認証
  - 無線 LAN
  - 有線 LAN
- 他大学との連携

前提条件

利用者認証として使用することを考慮すると，以下の条件が導入の前提条件として考えられる．

- すべての利用者がハードウェアトークンを所有すること
  代理利用(なりすまし)ができないことが重要となるので，MOC(Match On Card)でない IC カードでは防止できず，防止できなければパスワード認証の代わりにはできない．
  - ネットワーク機器が 802.1X に対応していること
  - 利用者端末の OS を限定できること

実現に向けての検討課題

PKI を実現する前に検討しなければならない課題として以下の点が考えられる．

- ハードウェアトークン配布時の問題点
  - 配布時の本人確認
    特に大学以外の利用者の対応について検討する必要がある．
    非常勤教員
    名誉教員・名誉職員
  - 学生への配布
    学生に配布する場合，配付する時期を検討する必要がある．教務システムを利用するには 4 月から使えることが必要だが，入学から授業開始までは 1 週間程の時間しかない．
  - 大学以外で利用することを考えるとリーダの必要のない，USB トークンが有効だが，携帯されない可能性がある．
- すべてのシステムで利用できるかどうかの確認が必要である．
  - 現在の事務システムは PKI 認証に対応できないので，次期開発(2010 年を予定)で対応する．
  - 対応できないシステムをどうするか．
- 証明書の失効が正しく扱われなければ，不正利用を防止できない．
  - ネットワーク機器では証明書の失効に対応していないものがある．
- 認証局(Certificate Authority，CA)をどこで運用するかを検討する必要がある．また Registration Authority(RA)をどこが担当するかについても検討が必要である．
  - 学生　　学生課
  - 留学生　国際教育センター
  - 教職員　人事課

  情報センタは認証サービスの利用者であり，証明書の発行機関ではない．

大学(学園)全体での導入には検討すべき課題がおおいが，まずはできるところから試験運用を開始し，事務システムへの対応を含めた学内の運用体制について検討する．

４．セミナーで学んだ技術及び知識

参考になった URL とその簡単な内容紹介

これまで PKI については関連する用語についての理解にとどまり，証明書を使って認証

をする意味について，十分な理解ができていなかったが，セミナーの中では，公開鍵暗号などの基礎的な技術だけではなく，以下の点について理解できた．

- 証明書を信頼できるかどうか
  - 証明書を信頼できるとはどういうことか
  - 証明書の確認方法(証明書の認証パスの生成)
  - 第三者機関発行の証明書を信頼してよいかどうか．
    - 実在証明がされているかどうか
  - 相互運用する場合の問題

参考になった URL

独立行政法人情報処理推進機構(IPA)

PKI 関連技術解説

http://www.ipa.go.jp/security/pki/index.html

電子政府情報セキュリティ相互運用支援技術の開発(相互運用テストスィート)

http://www.ipa.go.jp/security/fy14/development/pki/interop.html

５．事前準備として知っておいた方が良かったと思われること

不足していたソフトウェアや予習事項等

今回のセミナーでは，PKI 技術の基礎から解説いただいたので，特に不足していたと感じることはなかった．事前に公開された資料にもう少し目を通しておけば，余裕を持って講師の話を聞くことができたのではないかと思う．

６．セミナーの感想

今回のセミナーでは PKI 技術の基礎から相互運用を含めた応用技術について説明があり，PKI について理解を深めることができ，また設備等も整った会場で受講でき大変充実したセミナーであった．今後もこのようなセミナーが開催されることを期待したい．これまでは PKI 運用に関しては，技術的な側面でしか捕らえていなかったが，特に技術的な問題を解決するだけではなく，運用ポリシー等についても組織内での調整を含めた十分な検討が必要だということを感じた．

７．備考、その他

PKI 導入にはまだ解決すべき問題が多く，前途多難な感が強いが，運用開始できるように努力したい.他大学との認証連携の要望も出ており，大学間連携電子認証基盤に向けた「UPKI イニシアティブ」についても動向を追っていきたい．