組込みセキュリティのしくみ（原理篇）

古城 隆、wolfSSL, Inc.

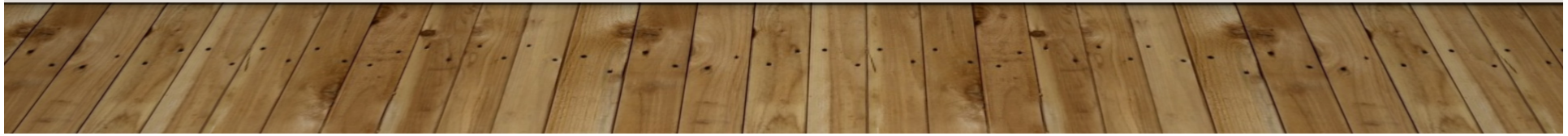
松原 豊、名古屋大学

概要

- SSL/TLSで使われている暗号技術や、プロトコル全体の流れをPythonで書かれたミニチュア版TLS（tinyTLS）を使って実際に動かしながら理解していきます。
- 共通鍵暗号、公開鍵暗号、ハッシュ、ディジタル署名、SSL証明書など個々の技術を一つづつ動かして動作を理解。
- 最後は全体のプロトコル・フローにつなげます。
- 聴講だけでもよいですが、Pythonが動作するPCがあれば、その場で自分で実際の動作を見て楽しみながらさらに理解を深めることもできるかも。

もくじ

1. とりあえず、メッセージを隠すにはどうしたらいいの？
2. でも、安全に秘密の暗号鍵を渡すにはどうしたらいいの
3. 今、通信しているあんたはホンモノのあんた？
4. でも、ホンモノのSSL/TLSって結構違うんでネ？



1. とりあえず、メッセージを隠すには？

- ネットワークの暗号化プログラムってどういう風になっているの？
- まずは、秘密の暗号鍵を使って、メッセージを暗号化、複合化してみましょう。
- 世界で一番簡単な共通鍵暗号のプログラムを作って、動かしてみます。

2. 安全に秘密の暗号鍵を渡すには？

- 秘密鍵を使って暗号通信するためには、まず、秘密鍵を安全に相手にわたさないといけませんね。
- 公開鍵暗号の原理を使って、ネットワークの相手側に秘密の暗号鍵を誰にも見破られないように渡してみます。
- 今、世界で一番使われているディフィー・ヘルマン (DH) という鍵合意のプログラムは意外に単純。実際に作って動かしてみよう。

3. あんたはホンモノのあんた？

- ネットワークのオレオレ詐欺にひっかからないために、公開鍵（SSL）証明書、そのもとになっているデジタル署名を使います。
- コピペ放題のネットとデジタルの世界でホンモノを確認する署名や証明書なんて、ホントに作れるの？
- 今一番広く使われているRSA公開鍵暗号の原理を使って、この(一見)難問に挑戦！でも、原理は意外に簡単。
- Pythonで作ったディジタル証明書に実際にディジタル署名や検証をしてみよう。

4. でも、現実は結構違うんでネ？

- というあなたのためのまとめセッション。
- インタネット・セキュリティの標準、SSL(Secure Sockets Layer)/TLS(Transport Layer Security) のハンドシェーク・プロトコル
- そのなかで、これまで説明、実験してきた原理がどんな風につかわれているか、ミニチュア版版TLS (tinyTLS) の形にまとめてみます。
- 最後はそれを使ってTLSクラアントとTLSサーバの間で秘密のメッセージを交換してみましょう。