ガイダンス
セキュリティエンジニアリング特論 第1回

栗原 淳

兵庫県立大学大学院

2021-10-07

はじめに

シラバス

目標

現実のアプリケーション・サービスにおいて存在する脅威、および暗号他のセキュリティ技術の活用方法・最新動向を、ハンズオンや演習を交えながら講義する.
想定する脅威に対して、基礎を学んできた情報セキュリティの基盤技術を、適切に選択し、実際の製品に対して応用する能力の習得を目標とする.

ゴール

- サービスやシステムにおいて、あるセキュリティ要件が与えられた際に、標準技術の観点から適切に必要な暗号技術を選択・組み合わせることができる
- 標準技術となった背景、技術的観点、使い所などの観点から、標準技術・標準文書を読み解くことができる

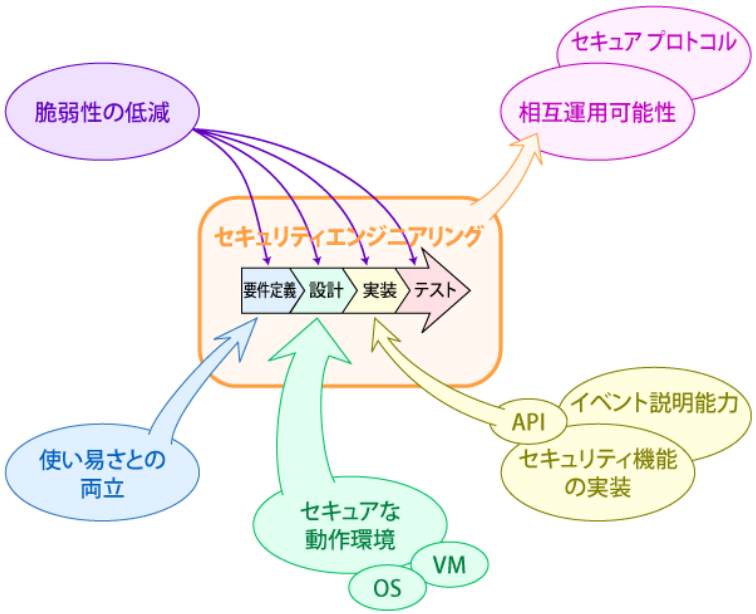

Figure: セキュリティエンジニアリング[1]

[1] https://www.ipa.go.jp/security/awareness/vendor/software.html

教員紹介

- 栗原 淳 (くりはらじゅん)
- 出身: 茨城県水戸市
- 学位: 博士 (工学, 東京工業大学)
- 経歴: 大企業から老舗研究機関、ベンチャーまで経験
  - 2006-2017 KDDI モバイル技術企画、KDDI 総合研究所 研究員
  - 2013-2014 Palo Alto Research Center 客員研究員
  - 2018- ゼタント 主任研究員
  - 2019- 国際電気通信基礎技術研究所 連携・客員研究員
  - 2020- 兵庫県立大学大学院

この講義は、研究・標準化の裏方，現場でのエンジニアリングの経験を生かしたものという位置付け.

通信・ネットワークにおけるセキュリティ技術を中心に研究開発

1. 秘密分散法 (情報の秘匿分散プロトコル) の設計・安全性解析
   - 超高速秘密分散法[2]の開発
   - 符号理論による秘密分散法の安全性解析手法の確立
2. 秘匿検索 (Private Information Retrieval) や セキュアネットワーク符号の設計・安全性解析
   - 符号化ストレージに対する秘匿検索手法の安全性解析
   - ネットワーク構造に非依存で、しかも「常に強安全」なセキュアネットワーク符号の設計
3. ネットワークアーキテクチャ、そのセキュリティプロトコルの開発
   - 情報指向ネットワークのアクセス制御フレームワーク、検閲回避プロトコルの開発
   - 匿名 Domain Name System (DNS) の開発

[2] https://www.kddi-research.jp/products/sproda.html

講義内容

講義内容

本講義では、「セキュリティエンジニアリング」と題して、**標準化された技術を対象としてエンジニアリングのキモである「技術選択」を行う勘所を学びます**.

- 前半: 情報セキュリティ標準技術の背景・使い所の説明に加えて、実際にコードを触って動作させて結果を確認するハンズオン講義形式．特にテーマはネットワーク・Web 系技術で利用されているセキュリティ標準について解説する予定．不定期にレポート課題を与える場合有.
- 後半: 講師+受講者の技術紹介プレゼンテーションによる輪講形式.

特に前半の内容は、**本職エンジニア向けの講義をベースとしたものを提供**する予定です．[3]

[3] その講義の資料は講師の Slideshare https://www.slideshare.net/JunKurihara2 および GitHub で大体公開してあります.

本講義の目的

目的

- 適切な標準技術の選択方法と、「組み合わせてセキュアなシステム設計を行う」というエンジニアリングの理解
- 最新のセキュリティ標準技術の知識の獲得

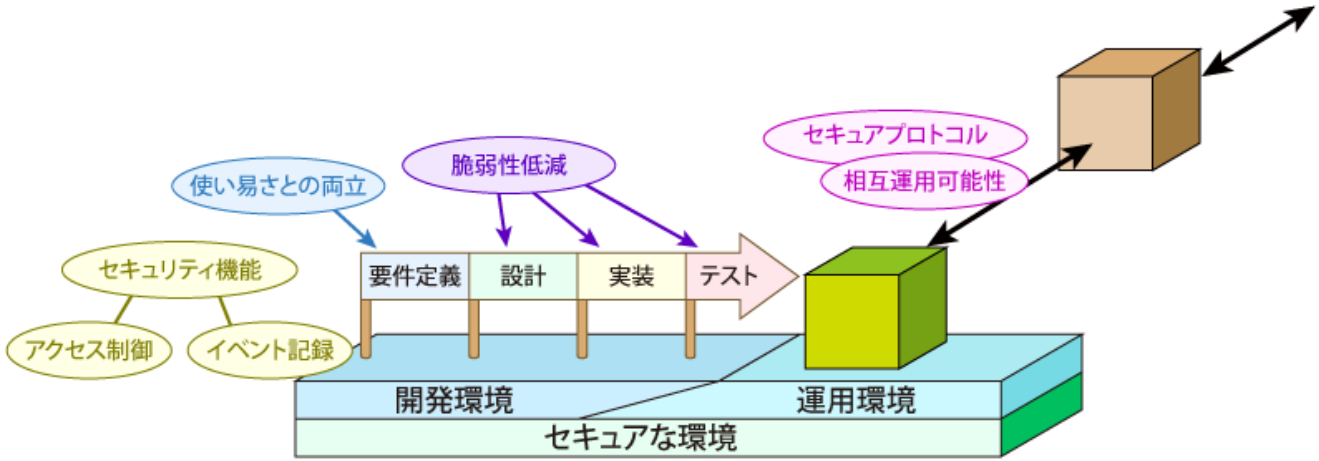

Figure: ソフトウェアエンジニアリングフロー[4]

エンジニアリングでは採用技術選択やその使い方に標準規格が深く関連.

[4] https://www.ipa.go.jp/security/awareness/vendor/software.html

スケジュール (予定)

- 第 1 回: ガイダンス ← イマココ
- 第 2 回: ソフトウェアエンジニアリングにおけるセキュリティ技術 (標準規格・文書，標準規格の例，環境準備)
- 第 3–6 回: 「標準規格」としての暗号プリミティブ (共通鍵暗号，公開鍵暗号，署名など) とその利用方法・技術選択
  ⇒ 「Web で安全な End-to-End 暗号化システムを構築するには」
- 第 7–9 回: 「標準規格」として認証技術とその使い方
  ⇒ 「次世代のパスワードレス認証技術規格 “FIDO2” を追いかける」
- 第 10–15 回: 講師+受講者による標準技術紹介プレゼンテーション

時間があれば、「認証+認可」を実現する OpenID Connect (+OAuth2.0) の解説や、コードベースでセキュア DNS 規格の紹介などを行う。

プレゼンテーション (最終課題) について

セキュリティ・プライバシに関する標準規格やデファクト標準について 1 つ選び，以下の観点から講師と他の受講者に紹介してください．プレゼン資料は作成すること．標準技術の解析論文の紹介を行っても良い．質疑含めて 20 分〜30 分を予定．

プレゼンの観点

- その技術・規格が生まれた経緯と背景 (他技術や社会状況との関連)
- 技術そのものの紹介
- その技術の使い所・使い方，メリットデメリット
- 現在のステータス (実装は進んでいるのか・どの環境で実装が存在するのか，アップデートは検討されているのか，など)

「プレゼン=みんなでレベルアップしよう」というものでもあるので，是非伝えることに重点をおいてください．

プレゼンテーマの選び方

- 対象となる標準規格は自由に選んでもらって構いませんが，講義で説明済 (予定)[5]のものは，原則対象から外してください．例えば以下のようなものを対象とすると良いかもしれません．
  - OpenPGP (RFC)
  - S/MIME (RFC)
  - JSON Web Key / JSON Web Token (W3C)
  - DNS over TLS / DNS over HTTPS (RFC)
  - Trusted Platform Module (ISO/IEC)
- 現状でも使われていれば，枯れた技術でも構いません．ただし，曖昧な技術 (例えば，「RSA 暗号」) ではなく，利用するに際して明確に仕様が規定されている技術 (例えば，「RSAES-PKCS1-v1_5」[6]) を対象としてください．
- もちろんテーマ選びは講師に相談しても構いません．
  むしろ相談推奨．

[5] AES と暗号利用モード関連・Hash/MAC 関連・公開鍵暗号化/署名アルゴリズム関連・FIDO 関連

[6] RSA 暗号を安全に使うためのパディングを含めた暗号化スキーム．RFC8017 を参照．

受講について

講義の進め方 (予定)

- 毎週木曜日 10:40am〜に実施．場所は以下の基準で選択し，都度 Slack にて周知する．
  - **コードに触れるハンズオンの回**:
    ⇒ 情報演習室で実施．受講者数によっては 602[7]．
    なるべくオンライン (Zoom) を併用，状況次第で変更．
  - **コードに触れない座学・プレゼンの回** (第 1-2 回他):
    ⇒ 演習室+オンライン (Zoom)，講義室へ来る必要はない．
    状況次第でオンライン (Zoom) のみへ変更．
- 連絡形式: 基本的に Slack 中心．ユニパは障害時の予備．
  - 業務連絡: Slack
  - 資料配布: 前日までに GitHub/SlideShare で公開，もしくは Slack で配布
  - 不定期レポート: Dropbox File Request，もしくは Slack で受領

[7] 栗原の居室向いの学生部屋

成績

評価対象

- プレゼンテーション (20 分〜30 分): 70%
- 不定期レポート・議論参加: 30%

⇒ 単位取得のためにはプレゼンテーション以外は出席不要[8]だが，プレゼンを行わない場合は単位取得不可能．

⇒ 不定期に簡単なレポート課題有．他受講者のプレゼンへの積極的な質疑・議論は加点対象．

[8] ですがエンジニアになりたい人は取り組んで欲しいです．

受講上の注意点

- 講義では Web 系の技術 (FIDO2 WebAuthn など) を中心に紹介するので，Node.js および UNIX 系コマンドを多用します．また，コードは基本的に GitHub に置きます．そのため，Node.js (Java/TypeScript), Bash 等のシェル, Git などが最低限使えると受講が楽です．[9][10]
- 講義内容についていくためには基礎的なプログラミング能力を要求します[11]が，成績には大きく関係しないようにします．環境構築やプログラミング言語自体の解説はほぼ行いません．
- プレゼンテーションをスケジュール前半などで早めにやりたい人は申し出てください．申し出ない場合は，スケジュールの後半で割り振ります．

---

[9] シェルや Git は学んで損はないでしょう．ソフトウェア開発においては Linux/macOS の方が苦労はしません．Windows を使う場合は WSL2 か、仮想マシンに Linux を入れて対処してください．

[10] 低レイヤの技術を紹介する際には Rust/Go/Python 等も使います．

[11] 「非同期プログラミング」という言葉を調べておくとネットワーク・Web 系技術になじめます．

SARS-CoV-2 (新型コロナウイルス) 感染拡大防止

- 少しでも体調が悪ければ講義室に来ないでください
  - 前述の通り，講義の「出席点」はありません．不定期レポートは出席せずに出しても構いません．
  - なるべくオンラインを併用します．
  - 栗原の作った資料・サンプルコードは GitHub でフル公開します．
- 教員がちょっとでも体調不良の場合は，休講とします．
  ⇒ 講義前に Slack (and ユニパ) を確認してください．
- 講義室での感染拡大防止策に協力をお願いします．

参考書

情報セキュリティ関係の教科書，
および下記の標準化団体 (の文書群)

- **IETF RFC** [12] ←特にこれをよく参照
- ISO/IEC JTC1
- ITU-T SG17
- W3C (特に WebAuthn WG/WebCrypto WG)
- PKCS; Public Key Cryptography Standards
- NIST FIPS および SP800
- FIDO Alliance
- OpenID Foundation
- 3GPP
- ...

[12] https://www.rfc-editor.org/rfc-index.html