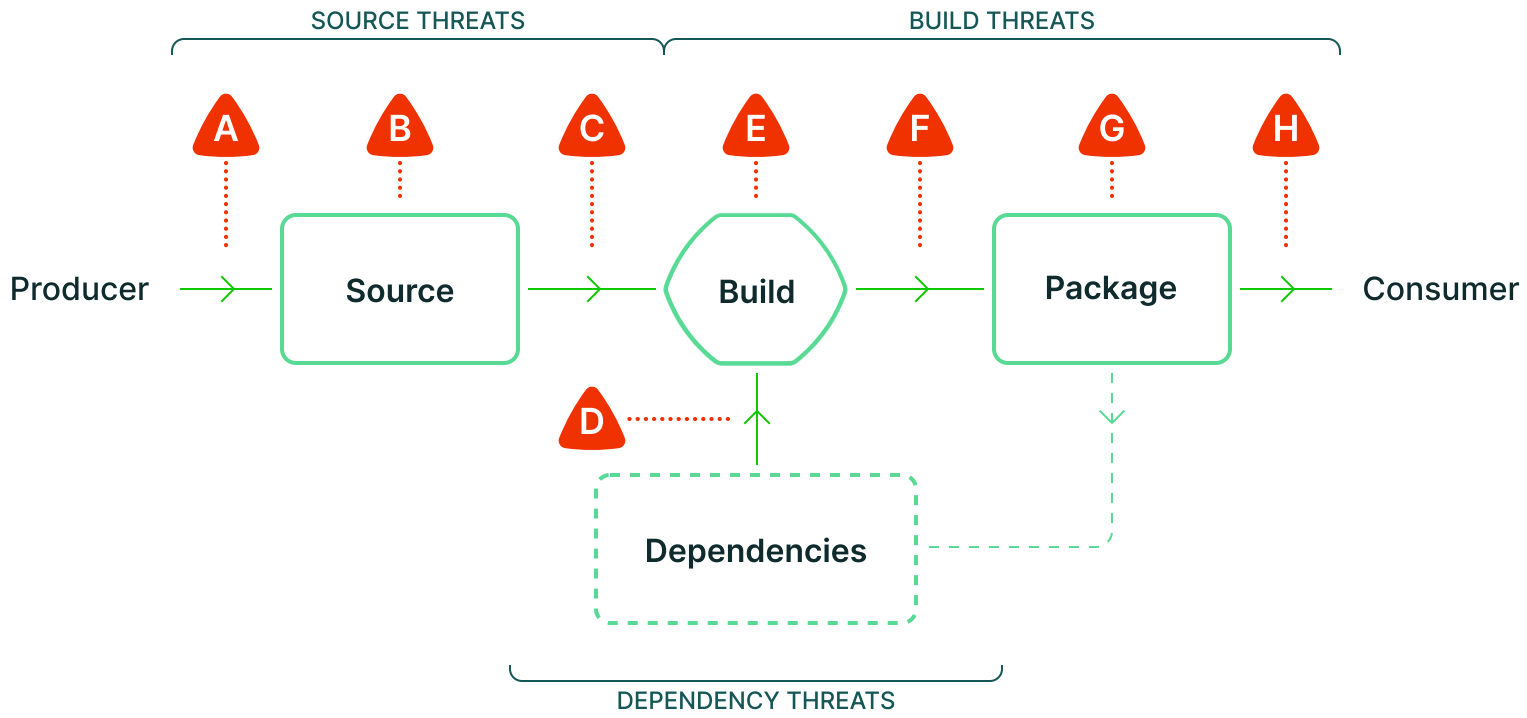
5 分で SLSA

2023/9/1 coord_e@coinsLT#1000

サプライチェーン脅威

- 落としてきたパッケージが本当にあなたの望むものであるのか？
- ソフトウェア開発者がソフトウェアを書いてからあなたの手元にパッケージが届くまでの間に、いくつもの attack surface が存在！



SOURCE THREATS

- **A** Submit unauthorized change
- **B** Compromise source repo
- **C** Build from modified source

DEPENDENCY THREATS

- **D** Use compromised dependency

BUILD THREATS

- **E** Compromise build process
- **F** Upload modified package
- **G** Compromise package repo
- **H** Use compromised package

https://slsa.dev/spec/v1.0/threats-overview

どうにかならないか。

- sha256sum -c？
- GPG で署名の検証？
- コード署名？

どうにかなっていないよなあ

- 検証できる情報が不十分
  - 結局 F~ 程度しか防げない
- 検証できる情報がものによりばらばら
  - 署名の意味もものによりばらばら
  - 決まったやりかたがない→自動で検証するのがむずかしい

SLSA: Supply-chain Levels for Software Artifacts

- https://slsa.dev/
    - organized within OpenSSF
- レベルがついたベストプラクティス集
- 各 Level に requirement と benefit が結びついている

登場人物

- Consumer
  - 生成されたソフトウェア成果物を使う
- Producer
  - ソフトウェアを開発している
- Platform
  - リポジトリのホストとか CI プロバイダ的なもの
  - 要は GitHub

信用関係

- Consumer は Producer を信用していない
  - Producer の制御下の入力はすべて Consumer が検査できるべき
- Consumer は Platform を信用している
  - どの Platform で生成されたかを認証できるべきだが、それ以外は何も要求しない
- Producer と Platform の間に明確なセキュリティ境界がある
- Consumer が信用する部分を Platform まで小さくするためのフレームワーク
  - > Trust platforms, verify artifacts
    > https://slsa.dev/spec/v1.0/principles
  - Level が上がるにつれて Producer への信用が減っていく

SLSA v1.0

- 4 月に v1.0 になった
  https://slsa.dev/blog/2023/04/slsa-v1-final
- v1.0 では “Provenance” の生成を中心に requirement が設定されている
  https://slsa.dev/spec/v1.0/requirements

Provenance

- ビルドの出力がどこでどのように生成されたかのメタデータ
- 例「このビルダーにこのパラメータをいれたらこれが出てきた」
    - 「**この Build platform で** Producer が**こうビルドした**結果が**これ**」
- Level 2 以降で、SLSA は Provenance が署名されていることを要求する
- SLSA では推奨される Provenance の形式も定めている

どうにかなるよ

- 検証できる情報が不十分？
  - どこでどうビルドされたかを Provenance に記録、そこに Build platform が署名
- 検証できる情報がものによりばらばら？
  - Provenance の形式に何らかの標準があればいい
  - → SLSA Provenance

https://slsa.dev/spec/v1.0/threats

どうなる？

1. 成果物を落とす
2. Provenance を落とす
3. 予期したリポジトリ/コミットからビルドされたものかどうか検証する
   https://github.com/slsa-framework/slsa-verifier

In Action(s)

- このスライドをビルドしているリポジトリ
  https://github.com/coord-e/slide-coinslt1000-slsa/
- いろいろなことがあって、GitHub Actions で SLSA Level 3 の Provenance が生成できるようになっている
- 簡単に雰囲気が出るので、やってみてね
  https://github.com/slsa-framework/slsa-github-generator