IETF100 PKI分野報告

2017年12月15日

IETF100 報告会

伊藤　忠彦（セコム株式会社）

自己紹介

- 伊藤忠彦 （セコム株式会社　IS研究所）
  - ルート認証局構築業務など
    - CA/BForum等でも活動
  - 暗号プロトコル・鍵管理に関する検討
    - 低リソースデバイス（IoTデバイス等）
    - 長期的な鍵管理に関する検討
      - 量子コンピュータの影響等も
  - IETF現地参加は2度目（94、100）
    - 95～99はリモート

もくじ

- **TRANS WGでの議論について**
  - 伊藤の発表
    - I-Dはじめて書きました
  - Short Signatureについて
- **CFRGでの発表について**
  - 量子コンピュータ関連

IETF 100 TRANSWG 当日資料

Use of Name Redaction for Mass Devices

Tadahiko Ito (Secom)

https://datatracker.ietf.org/meeting/100/materials/slides-100-trans-name-redaction-for-mass-devices/

Background

- draft-strad-trans-redaction-01
  - Name Relation was taken out of 6962-bis.(IETF97)
  - Expired (July 21, 2017)
  - Discussion was focusing on privacy

- My motivation
  - Some IoT devices might be outside the scope of “CT for web PKI”
  - We should have interoperability with “none-web PKI certificates”
    - Increase in IoT devices and scalability issue
    - security
  - Seems fine with same mechanisms as draft-strad-trans-redaction-01

https://datatracker.ietf.org/meeting/100/materials/slides-100-trans-name-redaction-for-mass-devices/

We use server certificates for many devices

- Increase in Devices-to-Devices Communication is expected
  - one of the communication parties will use server certificate.

- Surveillance Cameras
  - We do not need a surveillance system for surveillance cameras
    - Need of TLS for confidentiality
  - Viewed / Connected by consumer devices (i.e. smart phone)
    - Want to tie to public root
  - Over the air firmware / certificate update
    - e.g.) issue one month certificate,

https://datatracker.ietf.org/meeting/100/materials/slides-100-trans-name-redaction-for-mass-devices/

To make devices management easier

- Information for physical identification
  - Geometry information, model or lot number of Product
    - Sometime, people miss-install or miss-behave
  - Want to describe important information on the certificate, to manage the IoT devices
- Security
  - Above information is useful for
    - physical attack against devices
    - construct botnet
  - hiding them for security is “security through obscurity”?
  - Attack surface may increase with CT

https://datatracker.ietf.org/meeting/100/materials/slides-100-trans-name-redaction-for-mass-devices/

Do we need other mechanisms to deal with IoT devices?

- Current Mechanisms (draft-strad-trans-redaction-01)
  - Wild card
    - may not work with IoT devices at all
  - Use of name constraint intermediate
    - seems fit with my situation
  - Use of domain Label name redaction
    - Able to determine service provider / device vendor without showing identity of devices.
- Is it enough?
  - Do we have any better mechanisms?

https://datatracker.ietf.org/meeting/100/materials/slides-100-trans-name-redaction-for-mass-devices/

	Plain method (Current CT)	Tec-Const Intermediate	Domain Label Redaction
Monitor	Can detect mississue	can not detect misissue	Can detect misissue
Log Server	Massive data	Not much difference	Massive Data
Browser	No change	implementation cost	High Implementation cost
CA	No change	Need constrained intermediate CAs	Implementation cost
Service Provider / Device Vendor	Can not put geo-information on cert.	Can put geo-information on cert.	Can put geo-information on cert.

https://datatracker.ietf.org/meeting/100/materials/slides-100-trans-name-redaction-for-mass-devices/

反応

- IETFで議論するべき事案であるという事に
  - ハムの結果
- 最近のTRANS　WGに対するgoogleの姿勢についてあれこれ。

Short signature
TRANS + side meeting

- 有効期間数日の証明書を（ACMEで）発行
  - 有効期間数日だから、失効しなくてよい。
  - ★同一の対象に発行する証明書（群）の鍵ペアは同じ
  - CDNで利用したい？

- 新たなPKIを作るような試み
  - さすがに大変なのではないかという雰囲気
  - 失効しないPKIについての知見は余り貯まっていない。多くの議論を行わなければいけない。
  - OCSP（stapling）との差分とは…
    - 結局、通信の流れは変わらない
      - OCSPを問い合わせるか、証明書を取りに行くか。
    - 新たに実装する必要はあるのか？

- サイドミーティングでは、凄く濃い議論が展開されました。

LAMP

- CAAの(path)Discoveryについて
  - RFC6844
    - web.example.com CNAME www.example.com
    - www.example.com CNAME cdn.example.com
    - Web.example.com
    - www.example.com
    - cdn.example.net
    - example.net
    - .net
- SHAKEのoidについての議論
  - 可変長の出力をどうoidで扱うか
  - SHAKEはやるとして、何故未だにDSAあるの？
  - Id-dsa-with-shake128
    - 2.16.840.1.101.3.4.3

CFRG

- 量子コンピュータでの暗号解読の実現可能性について
  - とりあえず、調査中とのこと。
  - 対策についても纏めて欲しいと要望
    - 今回のスコープ外