PLANTS BoF: Charter

IETF 124 Montreal

Devon O'Brien

Current PLANTS Charter Text:

https://github.com/davidben/merkle-tree-certs/blob/main/charter-ietf-plants.md

Content Warning: Plant Puns

PLANTS Charter - Initial Draft

https://github.com/davidben/merkle-tree-certs/commit/f11f6bc1e9ddb810a388813d49319128b24bebdf

The goal of the PLANTS Working Group is to mitigate the costs of large post-quantum signatures on PKIs with Certificate Transparency (RFC 6962 and RFC 9162), as used in interactive protocols like TLS (RFC 8446). In such protocols today, X.509 certificates demonstrate to the relying party that some trusted certification authority (CA) has associated a public key with some application identifier (e.g., a DNS name). Certificate Transparency then provides public auditing, with log artifacts that demonstrate to the relying party the certificate is visible to monitors in some public log.

Large post-quantum signatures and keys add significant costs to these protocols:

- Each log entry contains a public key and signature. This added size to every log entry increases log operator costs, as well as costs to others in the transparency ecosystem.
- Certificates and log artifacts carry signatures from the CA and a quorum of logs. The added size increases latency to the TLS handshake.

The PLANTS Working Group will prune these costs by defining a new certificate and transparent log construction, with comparable security, privacy, and transparency properties to the status quo. In doing so, the Working Group may extend X.509 (e.g. new extensions or signature algorithms). As appropriate, the PLANTS Working Group will liaise with the LAMPS Working Group to ensure adequate lighting for this work and help it grow.

Overgrowth in signature overhead additionally impacts the use of the keys in the protocol (e.g. the TLS CertificateVerify message). These components can be cultivated separately from the PKI and are not in scope for this Working Group.

The PLANTS Working Group will additionally define how authenticating parties can provision its certificates with ACME, and how to use its certificates in TLS. As needed, the Working Group may define extensions to ACME and TLS to achieve this. It is expected to liaise with the TLS and ACME Working Groups for cross-pollination.

Though not the primary focus, the PLANTS Working Group may consider other properties of transparent PKIs to improve over the status quo, such as monitoring and revocation, in the course of its work. If concrete, feasible improvements are identified, the Working Group may recharter to seed new, secondary deliverables.

Initial Charter Feedback

PQ Signature Cost

- Mitigating cost of large PQ signatures "too vague" [1]
- Focus less on cost of PQ signatures and more on design tradeoffs [2]
- Constraining scope to PQ signature cost might exclude other improvements for PKI, CT not directly related to PQ [4]

Initial Charter Feedback

Security, Privacy, Transparency Properties

- Issues with specifying "comparable security, privacy, and transparency as the status quo." [1]
- "Comparable" will result in charter lawyering / bikeshedding [3]

Initial Charter Feedback

CT Log Operation

- Log operator costs are less of a concern than PQ signature size [4]
- Log operator costs are currently a serious issue with CT

PLANTS Charter - Second Draft

- Define "what we're building": a CA-built log of key/identifier bindings, and certs defined relative to that log.
- Expanded scope to optionally include improvements to auditing, monitoring, certificate revocation
- Evaluating tradeoffs pertaining to security, privacy, transparency, performance, and deployment properties
- Clarified liaison relationships with other WGs
- Initial deliverables are to define the following mechanisms:
    1. A transparency log structure, maintained by a CA, containing the key/identifier bindings that the CA has certified.
    2. Certificate constructions to prove to relying parties that a binding is both in the CA's view of the log and publicly monitorable.
    3. How the certificate constructions may be provisioned with ACME and used in TLS.

Charter V2 Discussion

- Charter should extend RFC5280, not X.509 and should also consider non-X.509 based solutions [5]
- Disambiguation of private PKIs, Enterprise PKIs, IoT PKIs [6]
- PQ signature sizes aren't, in fact, a real problem and widespread TLS performance benchmarks do not measure the right data [7]
- TLS is primary use case; alternative use cases can be discussed and re-chartered into scope, if necessary [8] [9] [10] [11] ...
- Charter should state how PQC size growth will be addressed [12]

Charter V2 Changes

- **Require N>1 collusion for transparency**
  - https://github.com/davidben/merkle-tree-certs/pull/132
- **Logs should be externally monitorable**
  - https://github.com/davidben/merkle-tree-certs/pull/133
- **Clarify where private or limited-scope PKIs fit in**
  - https://github.com/davidben/merkle-tree-certs/pull/134
- **Require two interoperable implementations**
  - https://github.com/davidben/merkle-tree-certs/pull/135
- **Use batching language**
  - https://github.com/davidben/merkle-tree-certs/pull/138
- **State how PQ size growth will be addressed**
  - https://github.com/davidben/merkle-tree-certs/pull/141

Questions to consider

- Not all concerns stated on-list have been addressed with language changes, have we appropriately bucketed "Charter" and "Non-Charter" concerns?
- Does the charter adequately scope intended protocol usage (e.g. non-TLS)?
- Does the charter properly address different kinds of PKIs?
- Did we land on an appropriate balance re: addressing revocation mechanisms?
- Should additional Merkle Tree constructions be added to PLANTS scope or transplanted to other f(l)ora?

Refs

- [1] https://mailarchive.ietf.org/arch/msg/plants/BP4EvHSsigx5ygEbypGjVbd4GD4/
- [2] https://mailarchive.ietf.org/arch/msg/plants/IhC9oyx3AY7Ld6XtjfzoAEQZ3aY/
- [3] https://mailarchive.ietf.org/arch/msg/plants/aGtp0cfgmh7cNUfh9t-vvXyEpNM/
- [4] https://mailarchive.ietf.org/arch/msg/plants/VFHZwG11E3zFz81Of49V29Q_MGw/
- [5] https://mailarchive.ietf.org/arch/msg/plants/nhJq4nF_wpAPDcOlCY2X90VJoo0/
- [6] https://mailarchive.ietf.org/arch/msg/plants/D-QFkYg1Pcs5fclO12uf5KQh9XQ/
- [7] https://mailarchive.ietf.org/arch/msg/plants/BCJamp94rqOXJHHh7QcuRZMwSxk/
- [8] https://mailarchive.ietf.org/arch/msg/plants/D1QQ1SKIjvOuK0CWBNJ7rq9FHGk/
- [9] https://mailarchive.ietf.org/arch/msg/plants/85hmhleTjGRlYv4NWr28ULuLYMI/
- [10] https://mailarchive.ietf.org/arch/msg/plants/e8HefWFFXhNhf1yuPvekiCKMNKg/
- [11] https://mailarchive.ietf.org/arch/msg/plants/yfnXFWUZ3S9RcLS0mYhDKjcVKFE/
- [12] https://mailarchive.ietf.org/arch/msg/plants/Yk1KqbeUpmGFkZPdCUbJUk4jQd8/