The Anatomy of a Dysfunctional Standards Body

Peter Gutmann, Independent Critic

John Doe #1 - #5, Various Organisations

Terminology

"Standards"

- Various different classes
- Standards-track ones that everyone ignores
- Informational-only ones that everyone implements
  - Is a mandatory standard that no-one bothers with really a standard?
- Some industry-wide standards remained in draft form for 20 years (RFC 8894)
- The SB uses confusingly gentle names for everything
  - A standard is a Request for Comments
  - The default status for standards is "Proposed Standard" (RFC 7127)
  - "Internet Drafts" are frequently used as full references (see above)
- I'll refer to them under the umbrella term "standards" to avoid getting bogged down in semantics

Terminology

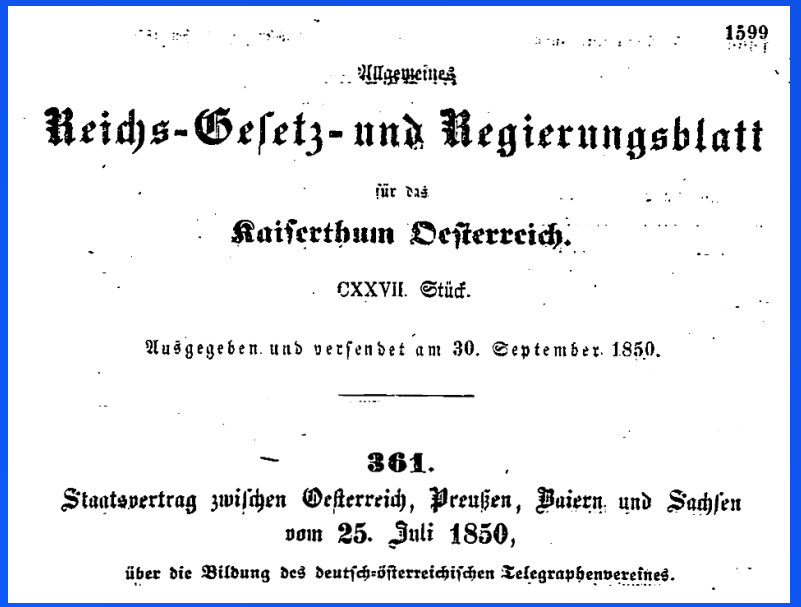
"Standards Body (SB) bureaucrats"

An official working in an organization or a government department
— Oxford Dictionary.

- Single-letter tags used to distinguish different individuals mentioned in case studies
- Commenting on the system, not on individuals

Occasional comparisons to what other standards bodies do, e.g. ISO, ITU, ETSI

- ITU is technically ITU-T, standardisation, not e.g. ITU-R, radio
- Admittedly some of these have had a lot more time to get their act sorted out



1599

Allgemeines

Reichs-Gesetz- und Regierungsblatt

für das

Kaiserthum Oesterreich.

CXXVII. Stück.

Ausgegeben und versendet am 30. September 1850.

361.

Staatsvertrag zwischen Oesterreich, Preußen, Baiern und Sachsen vom 25. Juli 1850,

über die Bildung des deutsch-österreichischen Telegraphenvereines.

Pay-to-play Standards

SB bureaucrats act as consultants to third parties who want pet standards

- SB bureaucrats also decide what gets adopted as a standard

Fast-track standards

- ISO: Submit an existing (non-ISO) standard for processing in (it's claimed) ¼ the usual time
- SB: Pay a SB bureaucrat to create one for you

Pay-to-play Standards (ctd)

Case study: The most heavily-documented instance of this…

- 2008-2009: `draft-rescorla-tls-extended-random-02.txt`
- Enabled the NSA Dual EC backdoor in TLS

Two authors

- An unknown, never-seen-before NSA employee
- The chair of the TLS working group

Pay-to-play Standards (ctd)

I should state that I only have fairly limited insight into the motivation for this extension. I was asked to help design something with a particular set of parameters in the way that would be most tasteful for TLS and that's what I did

- Translated: I was paid to get this past the TLS WG

This work was supported by the US Department of Defense

- Translated: The NSA bought this standard (well, draft)

The draft-rescorla-tls-extended-random-02.txt document was funded by the United States Department of Defense [NSA], requested by the United States Department of Defense [NSA], and coauthored by an NSA employee. It facilitates attacks on TLS implementations that use Dual EC. We have not found any way in which it increases security

— "Dual EC DRBG", `https://projectbullrun.org/dual-ec/ext-rand.html`

Pay-to-play Standards (ctd)

Preceded by an earlier draft

- `draft-rescorla-tls-opaque-prf-input-00.txt`, again by the NSA employee and the TLS WG chair, precursor to `draft-rescorla-tls-extended-random-00.txt`

Succeeded by more drafts and a confusing RFC

> OpaquePRF merely enables the [backdoor] accelerator. At no point does it mandate that the extension convey the output of a CSPRNG, and it hints at uses for the extension that don't involve extending randomness.
>
> Extended Random mandates the accelerator. The only thing you're allowed to embed in an Extended Random blob is CSPRNG output
>
> — Thomas Ptacek, `https://sockpuppet.org/blog/2015/08/04/is-extended-random-malicious/`

Pay-to-play Standards (ctd)

For such a tiny set of proposed extensions with such an impact (if only on the news cycle), these proposals generated a pitiful amount of discussion and virtually no skepticism from the IETF

— Thomas Ptacek, https://sockpuppet.org/blog/2015/08/04/is-extended-random-malicious/

Pay-to-play Standards (ctd)

How to spot a pay-to-play standard

- No obvious purpose

  This standard for storing key bits upside down exists to provide a standard for storing key bits upside down

  – There are standards whose abstracts actually say approximately this, just with more words

- Mostly created, and driven by, a SB bureaucrat

  – Possibly co-authored by someone never seen before in the WG

- Passed the relevant WG with little to no debate, shepherded by the SB bureaucrat

- Another sure sign:

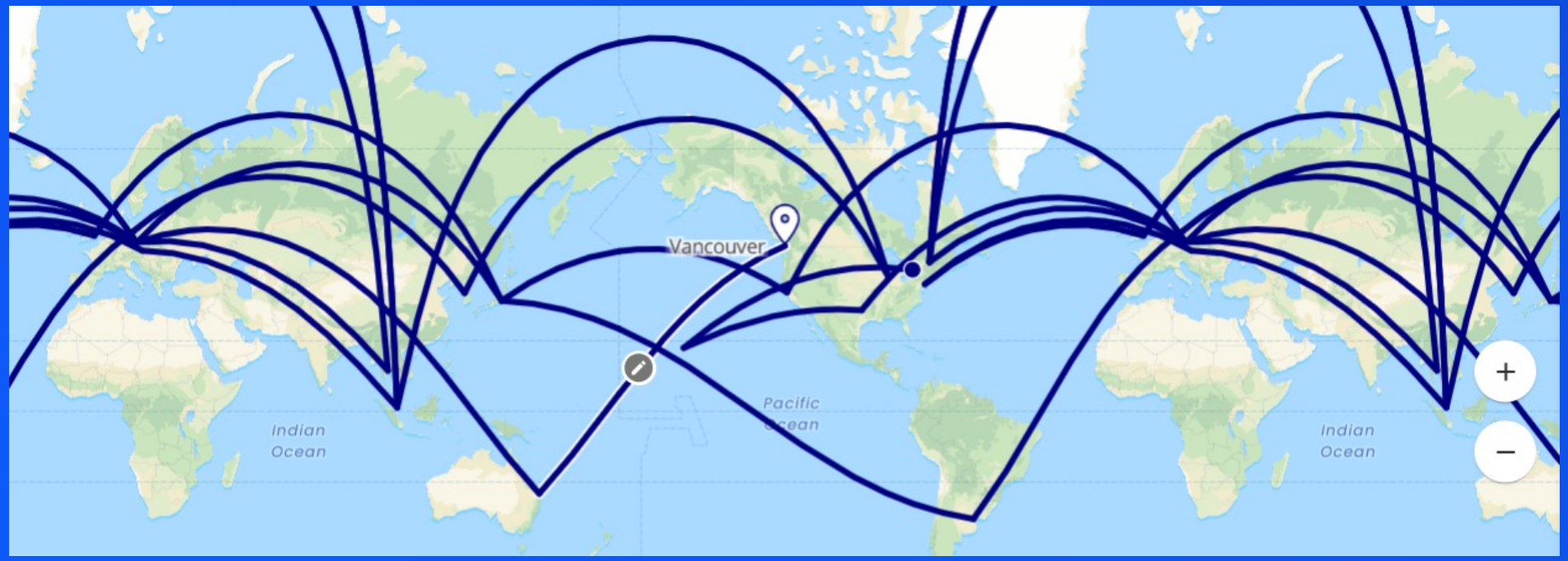
Is anybody aware of [standard published 15 years ago] implementations? →
I am aware of one that is proprietary
— Question + answer on LAMPS

Pay-to-Play Participation

Many of the important decisions are made at pay-to-play meetings

Recent IETF meetings were held in

- Bangkok
- Brisbane
- Buenos Aires
- Dublin
- Madrid
- Montreal
- Prague
- Seoul
- Vienna
- Yokohama



Pay-to-Play Participation (ctd)

If your employer has enough resources to send you, you get to participate

- If your employer can send enough people to stack the room, all the better

Pay-to-Play Participation (ctd)

Case study: Manager at a smaller company shells out to send an employee to a pay-to-play

- Google posters on the walls
- Everyone in Google shirts
- Google sponsors the lunch
- Any attempt to provide an alternative view gets shouted down

- "Please don't ever send me to one of these again"

Approx. cost for employee to pay-to-play (economy airfare + accommodation + registration + wages) = AUD 10,000

- Google are easily spending a six-figure sum per pay-to-play to stack the room

Pay-to-Play Participation (ctd)

Some working groups have been entirely captured by players representing a single industry segment

Case study: TLS WG

- Nothing exists outside the web
  - (A few minor exceptions like telcos who do their own thing anyway)

Could folks on the [TLS WG] list who work in embedded, SCADA, industrial control […] who have also posted to the list at least once in the last six months, a very low barrier, please identify themselves?

[Two week wait to give people plenty of time to respond]

<<<Crickets>>>

Pay-to-Play Participation (ctd)

All other participants have left the group

- Their input doesn't get heard, so why waste time participating?
- "Please don't ever send me to one of these again"
- The group is left as an echo chamber

[…] non-starter as web browsers […] fix the reasons why web browsers […] the web browser vendors […]

— CFRG list comment, responding to a message that talked specifically about non-browser TLS use, e.g. SCADA/embedded

Pay-to-Play Participation (ctd)

ISO has a Systematic Review process to ensure that their standards are globally relevant

The standards can be used/implemented as broadly as possible by affected industries and other stakeholders in markets around the world

— Guidance on the Systematic Review process in ISO

- WTO Technical Barriers to Trade Agreement (WTO/TBT) creates an obligation to do this

Pay-to-Play Participation (ctd)

Case study: HTTP/2

- HTTP/1 is the universal substrate for the Internet
  - Everything imaginable use HTTP/1 to carry it
  - Port 80 is always open for business
- HTTP/2 is designed to optimise content delivery for large content providers
  - Think HTTP4Google
- HTTP/3 even more so

Concern that when HTTP/2 appeared users would automatically ask for it because 2 > 1 and so we need 2

Pay-to-Play Participation (ctd)

Representative from multinational organisation requests a header flag to still allow HTTP/2 to be used as a universal substrate

- Flag indicates “this is merely a substrate, not an optimised advertising distribution medium”
- Response: “Let them eat HTTP/1”

Forks HTTP

- HTTP/2 for web content providers
- HTTP/1 for the rest of ~~us~~ them

Result was predictable…

- “When is X going to support HTTP/2?”
- “Why don’t you support HTTP/2 yet, it’s been around for ages?”
- “All the browsers support HTTP/2, why don’t you?”

Pay-to-Play Participation (ctd)

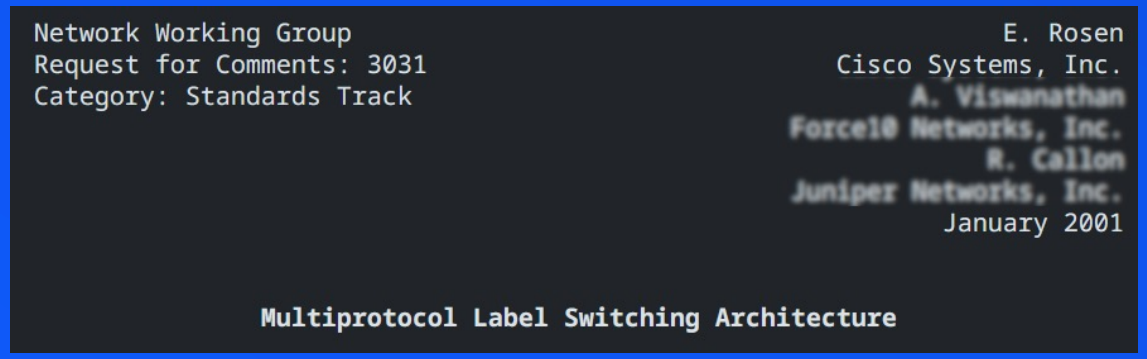
In contrast, ITU participation needs to be backed by a country

- Admittedly not perfect, e.g. leads to countries pushing geopolitical issues
- No names mentioned but you can guess who

Pay-to-Play Participation (ctd)

Solves the problem of WG stacking

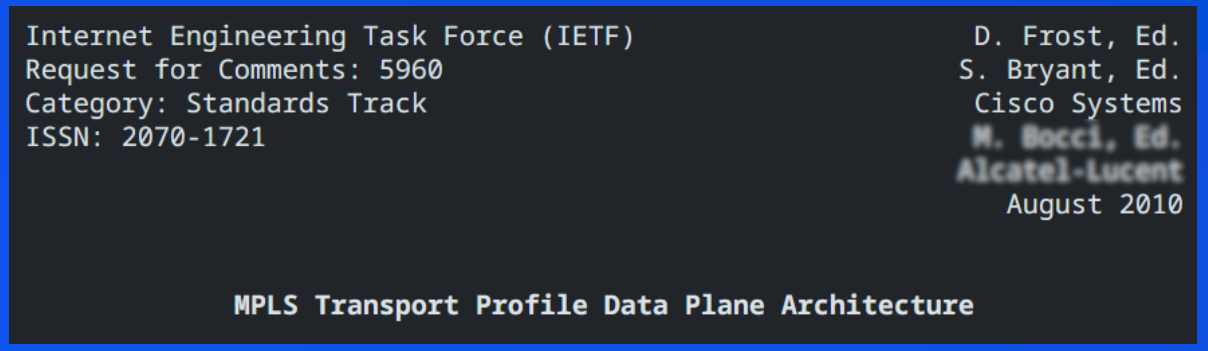
- Cisco couldn't force through their ideas on MPLS in the ITU which upset them no end



Network Working Group
Request for Comments: 3031
Category: Standards Track

E. Rosen
Cisco Systems, Inc.
A. Viswanathan
Force10 Networks, Inc.
R. Callon
Juniper Networks, Inc.
January 2001

Multiprotocol Label Switching Architecture



Internet Engineering Task Force (IETF)
Request for Comments: 5960
Category: Standards Track
ISSN: 2070-1721

D. Frost, Ed.
S. Bryant, Ed.
Cisco Systems
M. Bocci, Ed.
Alcatel-Lucent
August 2010

MPLS Transport Profile Data Plane Architecture

- No problem doing it with the IETF
  - VRRP vs.CARP fiasco, slew of Cisco pet standards like EST which have no reason to exist apart from being Cisco pet standards, etc

Cisco is also by far the largest employer of IETF contributors for all of the last 20 years

- 35% of all RFC authors came from just 10 companies

The bureaucrats giveth, the bureaucrats taketh away

Alongside promoting standards, the SB bureaucrats can block any standard for any reason

Case study: TLS-EtM

- Fixes a long-standing, well-known flaw in TLS
- Swaps older MAC-then-Encrypt (MtE) for Encrypt-then-MAC (EtM)
- A few lines of code changed to swap the order of two crypto ops
- A no-brainer of an RFC, more boilerplate than actual content
  - MAC first, encrypt second → encrypt first, MAC second

The bureaucrats giveth, the bureaucrats taketh away (ctd)

Pretty simple right?

- The TLS WG chairs kept blocking its adoption when the work was nearly complete

After endless to-and-fro I applied the nuclear option

> The WG chairs have refused to accept a draft containing a simple, straightforward fix to a serious problem in TLS' crypto, one that has rough consensus and running code. I therefore propose a vote of no-confidence in the TLS WG chairs, since I have no confidence that they're acting in the best interests of TLS development and TLS users

Suddenly the objections went away and it passed without any more problems

The bureaucrats giveth, the bureaucrats taketh away (ctd)

Case study: TLS-LTS

- Long-term support profile for TLS 1.2 in long-lived devices
- Think SCADA, industrial control, etc
- 10-20 year or more lifetimes
- Just a list of common-sense known-good things to do

First posted in 2016

- Asked to delay publication until TLS 1.3 was finished so as not to interfere with the 1.3 process

Waited some years for TLS 1.3 to be published

- At the same time TLS feature freeze, `draft-ietf-tls-tls12-frozen`, was written
- LTS was explicitly excluded from the feature freeze

The bureaucrats giveth, the bureaucrats taketh away (ctd)

"We've got TLS 1.3 now, we can't have LTS, put it through the independent track"

- Put it through the independent track, assessed by a single SB bureaucrat
- The same SB bureaucrat who told me to put it through the independent track assessed it

Asked to clear a series of seemingly arbitrary hurdles that no other TLS RFC has ever had to clear

- Would probably have prevented half the TLS RFCs from being published

The bureaucrats giveth, the bureaucrats taketh away (ctd)

Was eventually rejected on the basis that `-frozen` doesn't permit it

- Pointed out that LTS was excluded from `-frozen`
- `-frozen` co-author also pointed out that it didn't apply to TLS

"If you don't like it, there's a dispute process you can follow"

- An SB bureaucrat gets to decide whether another SB bureaucrat's actions are OK
- I wonder if the SB bureaucrat who told me to put it through the independent track and then rejected it once it got to the independent track will also be the one who gets to decide whether their actions were appropriate?

SB is working to make it even harder to ever dispute anything (modpod)

The bureaucrats giveth, the bureaucrats taketh away (ctd)

After nine years on this one draft I haven't yet been able to work up the energy to start another round

- What's the point, it's a hopeless case
- The SB bureaucrats can arbitrarily block anything they feel like

“The SB Doesn’t Vote”

This is technically correct

- The plebs don’t get a vote in anything

The SB bureaucrats all get one

- Feudalism: It’s your count that votes

XXXX has entered the following ballot position for draft-YYYY: No Objection

“The SB Doesn’t Vote” (ctd)

Anyone who can attend the pay-to-plays also gets a vote

- Votes are taken by measuring the volume of people humming
  - Initially done to help a blind participant who couldn’t see hands being raised
  - In theory needs confirmation on the mailing list, but it’s a case of more what you’d call guidelines than actual rules

More and more of our actions are now indistinguishable from voting
— RFC 7282

- They’re not indistinguishable from voting they *are* voting
- Well, voting by a highly privileged subset anyway

“The SB Doesn’t Vote” (ctd)

Important decisions are made at the pay-to-plays and announced as a fait accompli on the mailing list later on

> We all decided at the meeting in Tahiti last week to do X

Case study: My own work-in-progress, which later became RFC 7366, was debated without my knowledge at a pay-to-play

> This topic was discussed at the TLS WG meeting in Vancouver. Your proposed approach had no support in the room. [...] there has been some support on the list

- “We talked about this behind your back at the pay-to-play. Although people supported it on the mailing list, for some odd reason no-one at the pay-to-play did”
- (This led to the vote-of-no-confidence call)

“The SB Doesn’t Vote” (ctd)

ITU works by consensus: Do we have consensus?

- No objection → Approved
- Objection → Noted but approved
- Opposed → Typically need to retry
  - Rarely, in order to move forward, approved with a note of dissent
- Worst-case → Vote, *a sign that you’ve failed* since there’s no consensus

The SB doesn’t vote, except that it does (well, a privileged subset votes)

The ITU votes, except that it doesn’t (unless the consensus process has failed)

The Revolving Door

> The movement of high-level employees from public-sector jobs to private-sector jobs and vice versa
>
> — Investopedia

In the SB, it's within the SB

- SB bureaucrats typically serve two-year terms (RFC 8713)
- At the end of the two years, they move sideways (or upwards) into another position
- Even if they put NSA backdoors into a security standard, they still get given another position

The Revolving Door (ctd)

There is one very practical use for the term limits…

Case study: PKI protocol uses

```
Encrypt( Sign( Message ) )
```

- Encrypt is 3DES (it's an old protocol) or AES
- Signing uses SHA-1 (see "old protocol")
  - This is encrypted inside the AES envelope
  - Would then require the ability to create a real-time SHA-1 collision on non-chosen data, which no-one knows how to do

The Revolving Door (ctd)

Doc is in the final stages before publication

- E objects to the use of SHA-1 even though you'd need a real-time break of AES just to be able to then attempt a real-time break of SHA-1

After many messages back and forth that got nowhere, looked up E's remaining time in office

- Around a year

Waited one year

- Resubmitted to the next interchangeable bureaucrat in line
- Passed without comment

The Revolving Door (ctd)

Waiting out an SB bureaucrats's term of office is a very effective strategy if you have the patience

- Since decisions are arbitrary, the next one can be the opposite of what the current one was

The Revolving Door (ctd)

SB bureaucrats are appointed by other SB bureaucrats

- NomCom, IESG
- Everything is decided at the pay-to-plays

Most of the work will take place during IETF 123 and IETF 124

- In theory can do it via phone, but I've been unable to locate anyone who's reported success with this

I've only participated in two days of remote meetings and I was so appalled at the pointlessness of engaging that I now pay someone else to do it simply so we have a spy in the room

— John Doe #3

The Revolving Door (ctd)

Only the usual suspects get to be on the NomCom

- Need to have attended M of the last N pay-to-plays

It's your count that votes again

- Regular participants don't get a say

This system relies on a "credit" market. Positions in the selection committees rotate. The barons serving on the committees in any one competition agree to give some of the jobs to [others] who are not on the committees, in the expectation that these professors will reciprocate in the next round […] Professors who have accumulated credit […] are afraid of [criticizing others] for in future rounds their acolytes would suffer retaliation

— Diego Gambetta, "Codes of the Underworld"

The Revolving Door (ctd)

Positions like AD (Area Director) are practically a full-time job

- In theory anyone can apply, but …
- … need to be either independently wealthy or have your employer pay for it
- Positions invariably go to representatives of large vendors or people who have made a business out of getting standards through the SB

ITU SBs are appointed by the same consensus process as standards

- Everyone gets their say, appointment by consensus not cabal
- Attempt to make it geographically balanced, gender-balanced
- Conscious replacement of old guard by new blood
- Outreach to industry to get participation

The Clown Car

Politicians like omnibus bills because everyone tries to get their stuff attached to must-pass legislation

- Similarly, authors want to get their stuff into must-pass working groups

This used to be PKIX

- PKI was fashionable so everyone with a crazy idea tried to launder it through PKIX
- Result: Seventy RFCs totalling 2,356 pages.
  - Many of these, including full standards-track ones, have no known implementations

No real consensus and no running code

The Clown Car (ctd)

Case study: CMP interop

6.21 Use of TCP/IP as the transport protocol

Issue: The use of TCP/IP as the transport protocol is under specified in RFC 2510. For example, the polling protocol is incomplete and ambiguous.

Resolution: TBD

6.22 Purpose of publicKeyMac in POPOSigningKeyInput

Issue: It is unclear what is the purpose of the publicKeyMac in POPOSigningKeyInput. When should it be checked? What attack(s) does it protect against? Should it always be there or is it used in lieu of other mechanisms.

Resolution: TBD

The Clown Car (ctd)

Results of the interop

- “This protocol does not work”

Runs can end with

- CA cryptographically convinced a certificate was issued
- Client cryptographically convinced a certificate wasn’t issued

The Clown Car (ctd)

Resolution

1. Don't run any further interops

   If we stop testing right now, we'd have very few cases

2. "We'll push it through as a standard and then people will have to figure out how to get it to work"

This is why the first version of CMP is version 2

- It's also why most people have never heard of PKIX' flagship certificate management protocol

John Doe #4: Shades of the IKEv2 saga

John Doe #6: Some RFCs made it through to last call before anyone noticed they couldn't be implemented

The Clown Car (ctd)

Alongside the 70 RFCs probably around 200 drafts

- Couldn’t find any archive of them
- Based on extrapolating from one year of RFCs : drafts

I have a pile of them stored on archival media

- There’s some really wacky stuff in there

The Clown Car (ctd)

I didn't help the case with things like PARP, Peter's Active Revocation Protocol, `draft-ietf-pkix-parp-01.txt`

```
PARPObject ::= CHOICE {
    activeXControl   [0] OCTET STRING,
    javaApplet       [1] OCTET STRING,
    win95            [2] OCTET STRING
    }
```

To check a certificate's validity, the ActiveX control or Java applet is extracted from the extension and executed. Since the validity checking is performed entirely by the code contained within the extension, there is no need for tedious protocol specification and interoperability testing, as anything which can run ActiveX or Java can verify a certificate.

The Clown Car (ctd)

[The win95 option] includes a complete Windows 95 installation in the extension which, when run, installs Win95 on the machine, locates and downloads whatever support is necessary for ActiveX and/or Java (typically a copy of MSIE), and then performs a PARP verification as described above.

CAs that include the Win95 option should be aware that this may lead to a small increase in certificate size.

The Clown Car (ctd)

This was only slightly sillier than some other drafts, e.g. the one for including theme music in certificates, `draft-ietf-pkix-logotypes`

```
LogotypeAudio ::= SEQUENCE {
  audioDetails ::= SEQUENCE {
  mediaType      IA5String,-- MIME media type name
  ... }
  audioInfo ::= SEQUENCE {
  fileSize       INTEGER,-- In octets
  playTime       INTEGER,-- In milliseconds
  channels       INTEGER,-- 1=mono, 2=stereo, 4=quad
  sampleRate[3] INTEGER OPTIONAL,-- Samples per sec
  ... }
  }
```

- Eventually became standards-track RFC 3709

The Clown Car (ctd)

This was serious

My counter-proposal for scratch-n-sniff certificates slightly less so

> The new logotype would be implemented in the form of scratch-n-sniff certificates, and will assist relying parties in making informed decisions as to whether a particular certificate is trustworthy and relevant for its intended usage. Service providers and product vendors invest a lot of money and resources into creating a strong relation between positive user experiences and easily recognizable scents such as grilled beef, fresh air, and cordite, allowing easy and familiar branding of certificates

- Most of this text is straight from standards-track RFC 3709
- If you can have musical certificates then you should also be allowed scented certificates

The Clown Car (ctd)

Now it's TLS

- 60 RFCs
  - No, that's not an error, *sixty* RFCs for four TLS versions
- 32 further RFC drafts in progress

That's just under *two thousand pages* of standards documents

- This is what it would look like if printed

Should overtake PKIX in a year or two

- This is *not* a feature

TLS 1.3 is essentially made of extensions

- People can tack on anything they want

The Clown Car (ctd)

Attestation in TLS, PEM file formats for Client Hello, Workload Identifier Scope Hint, Merkle Tree Certificates, OpenPGP keys for TLS, Certificate Compression, Delegated Credentials, Kerberos Cipher Suites, Bootstrapping ECH with DNS, Key Share Prediction, Trust Anchor Identifiers, and every post-quantum idea you've ever heard of and several you haven't

John Doe #2: If you want to see a real clown car, take a look at OAuth

- (I don't follow OAuth but I've heard bad things)

> Last month I reached the painful conclusion that I can no longer be associated with the OAuth 2.0 standard. I resigned my role as lead author and editor, withdraw my name from the specification, and left the working group [...] It is bad enough that I no longer want to be associated with it. It is the biggest professional disappointment of my career
>
> — Resignation note of Alan Smithee, former lead author and editor of the OAuth specification

The Clown Car (ctd)

Not TLS in this case but deserves honourable mention

Security Considerations

The use of this cipher and MAC combination has a KNOWN SECURITY VULNERABILITY […] This is a breach of the SSH transport protocol's security guarantee

— `draft-ietf-sshm-chacha20-poly1305-01`, Standards Track RFC

- This standard, once published, will mandate a CVE'd security vulnerability (CVE-2023-48795) for SSH
  - The standard indicates that you should mitigate the security vulnerability that it contains before deploying
  - A recent study found that almost no-one gets this mitigation right
- For once I am at a loss for words
  - (This almost never happens)

The Clown Show

Where there's a clown car, there's also going to be a clown show

```
RSAPrivateKey ::= SEQUENCE {
    version           Version,
    modulus           INTEGER, -- n
    publicExponent    INTEGER, -- e
    privateExponent   INTEGER, -- d
    prime1            INTEGER, -- p
    prime2            INTEGER, -- q
    exponent1         INTEGER, -- d mod (p-1)
    exponent2         INTEGER, -- d mod (q-1)
    coefficient       INTEGER, -- (inverse of q) mod p
}
```

PKCS #1, in global use for 30+ years

- Newer formats like PKCS #15 only store *p*, *q*
- The rest can be recalculated from that and the public values

The Clown Show (ctd)

Week 1: D points out that there's a side-channel vulnerability there

- An attacker who has the plaintext private key sitting in memory can determine the length of values like *p* and *q* with a timing attack
  - Recovering p and q is what you do to break RSA via factorisation, $n = p \times q$
- This length value can also be computed by taking the length of the public value *n* and dividing by 2
- Or by looking up the value in the appropriate standard, e.g. FIPS 186

Using methods 1 and 2, p and q with lengths of 1024 or 1536 bits may be generated

— FIPS 186, B.3.1, "Criteria for IFC Key Pairs"

The Clown Show (ctd)

In case you're not already shaking your head at this point, it means…

1. An attacker who walks straight past the plaintext private key sitting unprotected in memory
2. Can possibly compute, via a timing attack
3. A publicly-available value of no use in recovering the private key
4. Which, in case it hasn't been mentioned before, is sitting there unprotected in memory

Several people point out that this "vulnerability" is imaginary

- Saying that it's nonsensical might lead to a code-of-conduct complaint

The Clown Show (ctd)

Week 2: S asks what will be done about this "unfixable sidechannel"

- More baffled responses by people explaining that it's an imaginary problem

Week 3: C, a secdir (Security Area Directorate) reviewer, asks whether the "concerns with the RSA format [will] be addressed"

- More responses, including "please explain how an attacker who walks straight past the plaintext private key and then carries out a potential side-channel attack that confirms a publicly-known value (sizeof(n)/2) of no use to the attacker is a problem"

The Clown Show (ctd)

Week 4: The debate continues…

LAMPS, successor to PKIX, continuing the PKIX tradition of facepalm-inducing discussions

How to Fix This

Burn it down and start again

- OK, maybe a bit drastic

Single biggest problem is the pay-to-play nature of the SB

- The SB is a (well-)paid standards manufacturer
  - Just under ten thousand so far
- As long as there's money to be made from creating them, the flow will never stop

Discontinue the pay-to-play meetings

- Everything is done on the mailing lists where anyone can participate

How to Fix This

John Doe #1: Alternatively, all pay-to-plays are online so everyone can participate

- Money or access to visas should not be a proxy for the value of your contribution
- Still means people will have to be up at 2am to be able to participate

ITU has remote participation

- Round-robin'd across time zones so everyone gets a chance to be inconvenienced equally
- Plenary/final decision does require physical presence

How to Fix This (ctd)

Second biggest problem is the unelected SB bureaucrats

- An SB bureaucrat can arbitrarily block, or alternatively push through, anything they like

SB bureaucrats creating paid standards must disclose in the standard who paid them for it and how much

- Admittedly this didn't help with the Extended Random / Dual EC backdoor (the text essentially says "The NSA paid for this backdoor"), so maybe more is needed

John Doe #4: Being shown to be dishonest or failing to do their job properly results in an ethics investigation followed potentially by a ban *including the organisation backing them*

- (I think this would be very difficult to enforce)

How to Fix This (ctd)

One vote per organisation

- Can still be manipulated, c.f. Microsoft with Office Open XML
- “Google will generously fund your attendance, and I’m sure you’ll know which way to vote when the time comes”

There should be a reason why a vote is accepted

- If you can’t show active participation, you don’t get a vote
- Attempts to address the above issue

How to Fix This (ctd)

Implement postmortem reviews

- If a huge amount of effort has gone into creating a standard that no-one uses, something has gone seriously wrong
- Determine why and fix the process

ISO standards have this built in

> If the results of the [5-yearly] Systematic Review show that a standard is not widely used around the world (by at least 5 countries), its global relevance is called into question and it would likely be proposed for withdrawal
>
> — Guidance on the Systematic Review process in ISO

Endnote

This is an ongoing work

- Everyone who reviewed the drafts had something they wanted to add
- This will probably continue for the foreseeable future

Expect changes from the current version you're reading

Note on sources for figures given: Several were taken from "Characterising the IETF Through the Lens of RFC Deployment", 2021