Will address TLS 1.3’s:

What's
Where's
How's
We promise:

Not too Technical
Lots o’ Links
Lame Nerd Humor
Whence does it come?

The plot of sum of Order for Year. Color shows details about Org. The marks are labeled by Milestone.
Who’s **implementing** 1.3?

Open source!

Browsers!

Test servers available!
Where are the specifications?

- Working copy
- Official I-D
Where does it sit?

X marks the spot!

<table>
<thead>
<tr>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>IP</td>
</tr>
</tbody>
</table>
What does it do?

Begone Eve!

Mallory No More!

From xkcd.com
Wat, Wat! There’s how many protocols!? 

![Diagram showing TCP, TLS, Handshake, Alert, Application Data, Record, Application]
Wat! Wat! You don’t need to use all the protocols?

Application Shim

- QUIC
- TLS
- UDP
- IP

QUIC does not use TLS’ Application Data
What was wrong with the previous versions?

Lucky 13
BEAST
Freak
Logjam
Drown

Crime
Breach
Triple
Handshake
Poodle
Sweet32

...
What were the design goals?
Why is it more secure?

HERE'S TO THE SECURITY RESEARCHERS
What did you remove to make it more secure?

- SHA-1
- Compression
- Stream Ciphers
- Static RSA Key Exchange
- Renegotiation
- Block Ciphers
Why is it more secure?

Record Payload Algorithms: AEAD-only

Key Establishment Algorithms: (EC)DHE or PSK

Convergence of PSK, Session Resumption, Session Tickets and 0-RTT

TLS1.2

>100 Cipher Suites

TLS1.3

005
What algorithms are supported?

AEAD: AES-GCM, AES-CCM, CHACHA20-Poly1305

ECs:

Sig: p256, p384, p521, EdDSA (25519 and 448)

KE Groups: p256, p384, p521, 25519, 448

Named FFDHE Groups

RSA-PSS Signatures
How do you specify ciphers?

OLD: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

NEW: a la carte

IANA Registry will include Recommended column
Come again - it’s faster?

TLS1.2

Handshake

Handshake

Handshake

AppData

TLS1.3

Handshake

Handshake

AppData

AppData

HTTP starts here
What are the normal modes?

1-RTT

Resumption (PSK)
Is that *all* you got?

**TLS1.3 0-RTT Data**

HTTP starts here

PFS starts here

**WARNING: 0-RTT Data is replayable and not PFS!**
It supports record protection?

Padding for Length Hiding

Unencrypted ContentType and Version no longer meaningful
You turned PFS on!?

Perfect Forward Secrecy is the default.

Also available with PSK modes.
You’re encrypting more early though, right!?
What’s not to like!?
TLS1.3-related drafts

TLS1.3 Test Vectors

- Working copy
- Official I-D

DTLS1.3

- Working copy
- Official I-D
please tell us what you thought about this session:
https://www.surveymonkey.com/r/100t1s