tcpcrypt

April 7, 2016

Andrea Bittau, Dan Boneh, Daniel Giffin, Mike Hamburg,
Mark Handley, David Mazières, Quinn Slack, Eric Smith

What changed in protocol?

Nothing!

tcpcrypt is finally stabilizing…

tcpcrypt timeline

2010 original tcpcrypt	2014 tcpinc IETF-90	2015 tcpinc IETF-92	2015 tcpinc IETF-93	2015 tcpinc IETF-94
Built-in handshake in SYN, SYN-ACK				TCP-ENO
Packet based		Packet based	Stream based (TLV)	
Header protection		No header protection		
RSA	ECDHE			
AES, RC4	AES			
	STUN-like check to disable on fail			TCPINC-BCP

Most feedback is on exposition of draft—not protocol changes

- Separate out the “spec” from the “why” in draft.

- Harmonize terminology with TLS 1.3 spec (e.g., “ephemeral secret” instead of “pseudo-random” key).

- Question: separate negotiation for key exchange and symmetric cipher section vs. single negotiation for both?

- Question: if no randomness available yet, use plain-text TCP or delay tcpcrypt connections?

Question: separate code point for session resumption?

Approach 1: current specification. Use separate code point for session resumption

ENO	Session Resume 0x20 SESSION_ID	ECHDE P-521 0x22

getsockopt(TCP_ENO_NEGSPEC) -> 0x20

Problem: what cipher got resumed?

Approach 2: Use cipher ID followed by data to indicate resumption

ENO	Session Resume P-256 0x21 SESSION_ID	ECHDE P-521 0x22

getsockopt(TCP_ENO_NEGSPEC) -> 0x21

Effort shifting from draft to implementation

- New tcpcrypt release (v0.4) in February. People have been using it on all platforms.
    - Signed Windows implementation.
    - Signed OSX implementation.
    - Official Fedora package (thanks to Paul Wouters)
    - Official Debian package (thanks to Daniel Gillmor)

Hall of fame

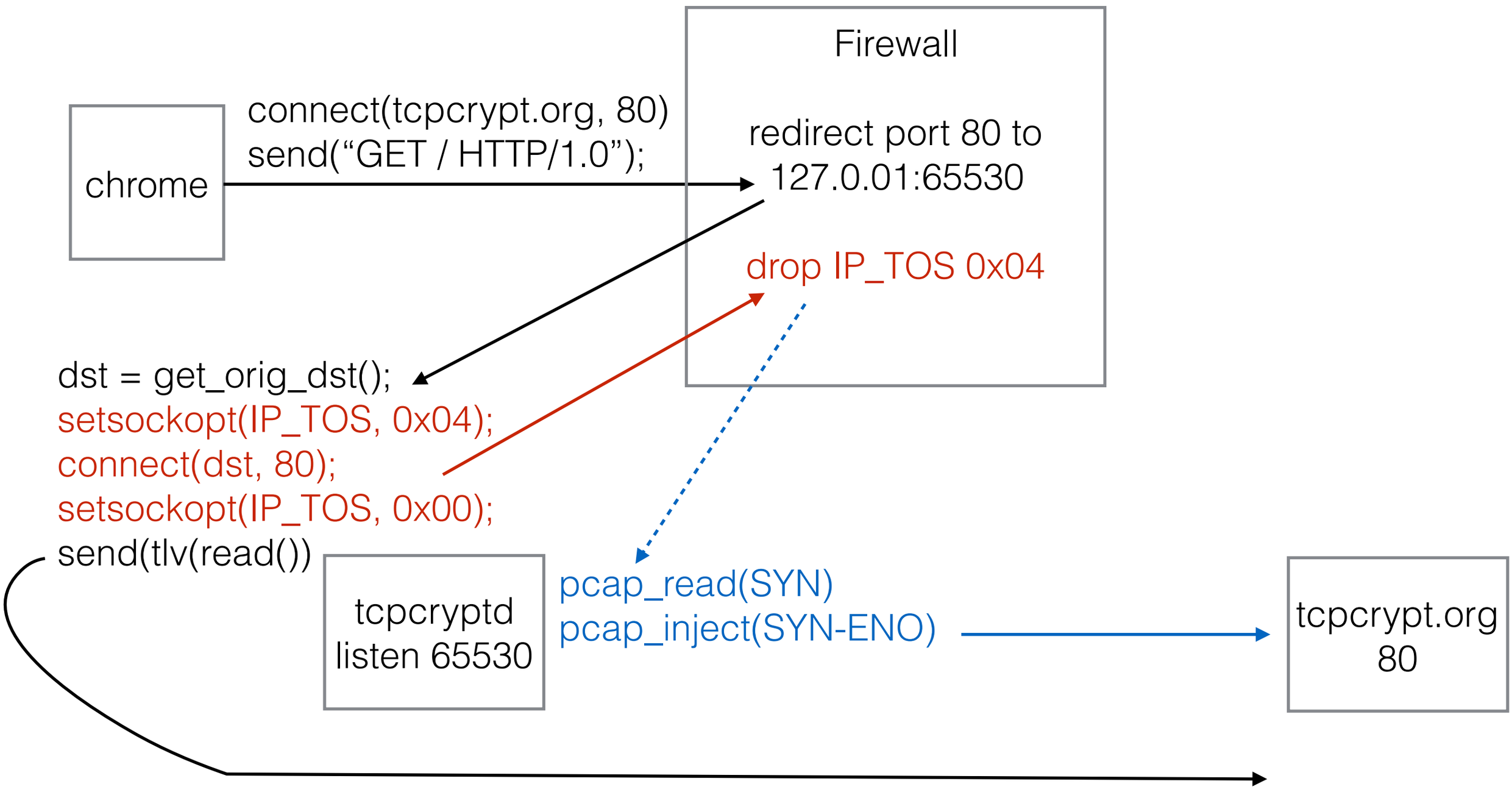
48% of the visitors to this website use tcpcrypt (37684 tcpcrypt hits). You're not one of them. Install tcpcrypt now and you'll be able to enter the hall of fame!

Rank	Date	Message	User agent
1126	Apr 1	yes [SID: 9FDDCE25407424D843C49E843B30BF71705D3971EFA50ED13C58A130D03203EC]	Windows/Chrome
1125	Mar 29	Finally got it to work!! [SID: F8F3C3190FB952AD0FE49F38D05EEADA3872D19251EDA45C6AF52FA5A95461FE]	Windows/Firefox
1124	Mar 28	thy's VM suddenly works! [SID: 7CD463E3375910C87CECE032D506A9BA41BF700D27C6BAC23BCF6EE5BC799C66]	Linux/Firefox
1123	Mar 28	thy use Ubuntu 14.04LTS, kernel version 4.2.0, network config: eth0 Link encap:Ethernet HWaddr bc:ee:7b:9c:25:58 inet addr:192.168.0.246 Bcast:192.168.255.255 Mask:255.255.0.0 inet6 addr: fe80::beee:7bff:fe9c:2558/64 Scop [SID: 1048075C852A5B93B759BA55051121567 65D55870A3AEF92DA60A4C58DE5DC8F]	Linux/Firefox
1122	Mar 20	Hi [SID: 31091E8CA06FB396BA686DCE0712AD97382FA7E068D4F24B3A76DDDE486E52A2]	Linux/Firefox
1121	Mar 20	[SID: 5D26050D5D63E4513C3A53896165082D74A0F82816D149387A633DB4CC2E7EA0]	Linux/Firefox
1120	Mar 20	ok [SID: B879AAABDB838B8F16DE1E49F1381C80A332EA764143A31266043600428DCC95]	Windows/Firefox
1119	Mar 20	che bello, sono molto felice, sprizzo gioia da tutti i pori yeeeee [SID: D13D5F07E24A400304C85A15A9E4A5F71513C9D67DE383E81D90B33D350BA0C]	Windows/Chrome
1118	Mar 20	Hello Encrypted World. [SID: DFC56D70D4933AEEA494E4786B4282FF57A61686A4F77751E7CE490E906D4E78]	Mac/Safari
1117	Mar 19	hi 623 [SID: DD3759A453A780D821DB29429023D03446385045 31A4076EBDE875DCCA475B1A]	Mac/Chrome
1116	Mar	Excellent!	Linux/Chrome

Notes for a user-space implementation

- Problem: how do we add ENO to the 3-way handshake
  - Can’t use DIVERT - OSX no longer supports it.
  - Firewall (drop) handshake. tcpcryptd eavesdrops it using PCAP, adds ENO option to packet, and resends it via PCAP.
    - Use IP-TOS to signal handshake to firewall so it can match packets to drop.
- Problem: how do we TLV data?
  - Use REDIRECT to proxy connection via tcpcryptd and TLV payload. Just like transparent proxies (e.g., Squid).
  - Windows doesn’t support REDIRECT. We implemented it using DIVERT. Similar to NAT, but always send to 127.0.0.1:rdr_port.

tcpcrypt packet flow



What's next?

- Address feedback in draft. More people to edit draft?
- Mirja's call for implementations. Anyone up for it?
- Start a new clean implementation. Existing implementation organically grew from DIVERT code and original tcpcrypt spec (which are fundamentally different).
- Write a kernel implementation
  - FreeBSD
  - Linux