Introduction - IETF and Trends in Internet Security



I E T F®

Jari Arkko, IETF Chair (chair@ietf.org)
Expert, Ericsson Research (jari.arkko@ericsson.com)

Organisations & Roles







What the IETF Does



"Improving the Internet"

- Standards for core Internet technology
- Voluntary adoption of our standards
- A mix of volunteer participants (vendors, operators, academics, developers, policy/regulator people, …)
- Some of our most active areas of work today include real-time communications for the web, evolution of the web protocols, Internet of Things, and security in its various forms

Improving Security Technology for the Internet



- Security has always been a big part of IETF work
- Security for IETF protocols & tools for people to build secure networks and applications
- Surveillance revelations have caused a lot of discussion in last two years at the IETF
    - But not the first time such discussions arise

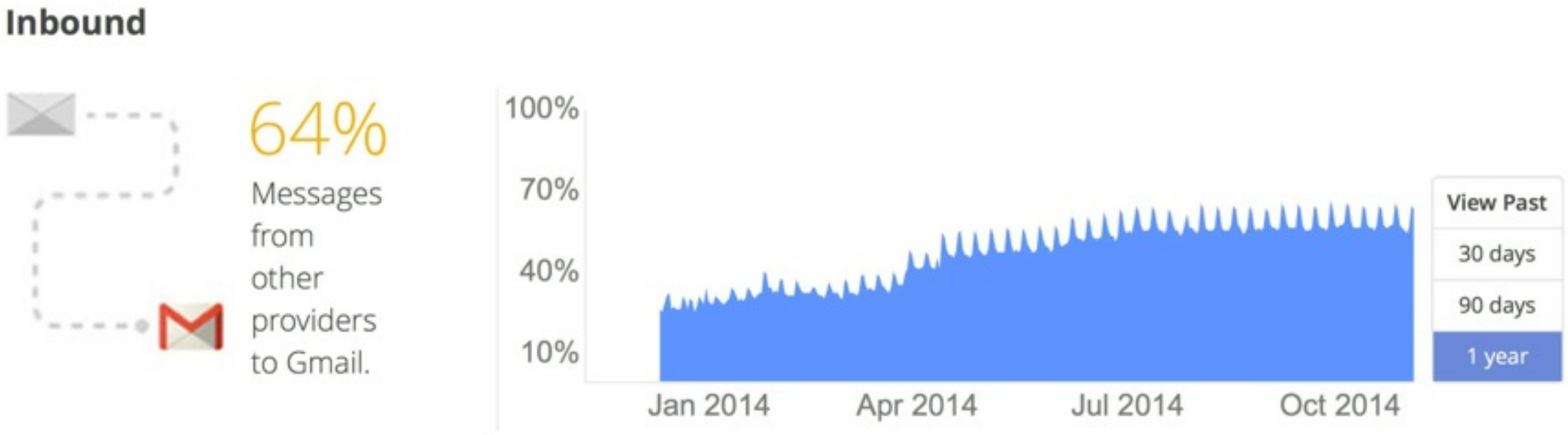
Encrypted Traffic In the Internet — Is There a Trend?



Making observations of what gets used in the Internet:

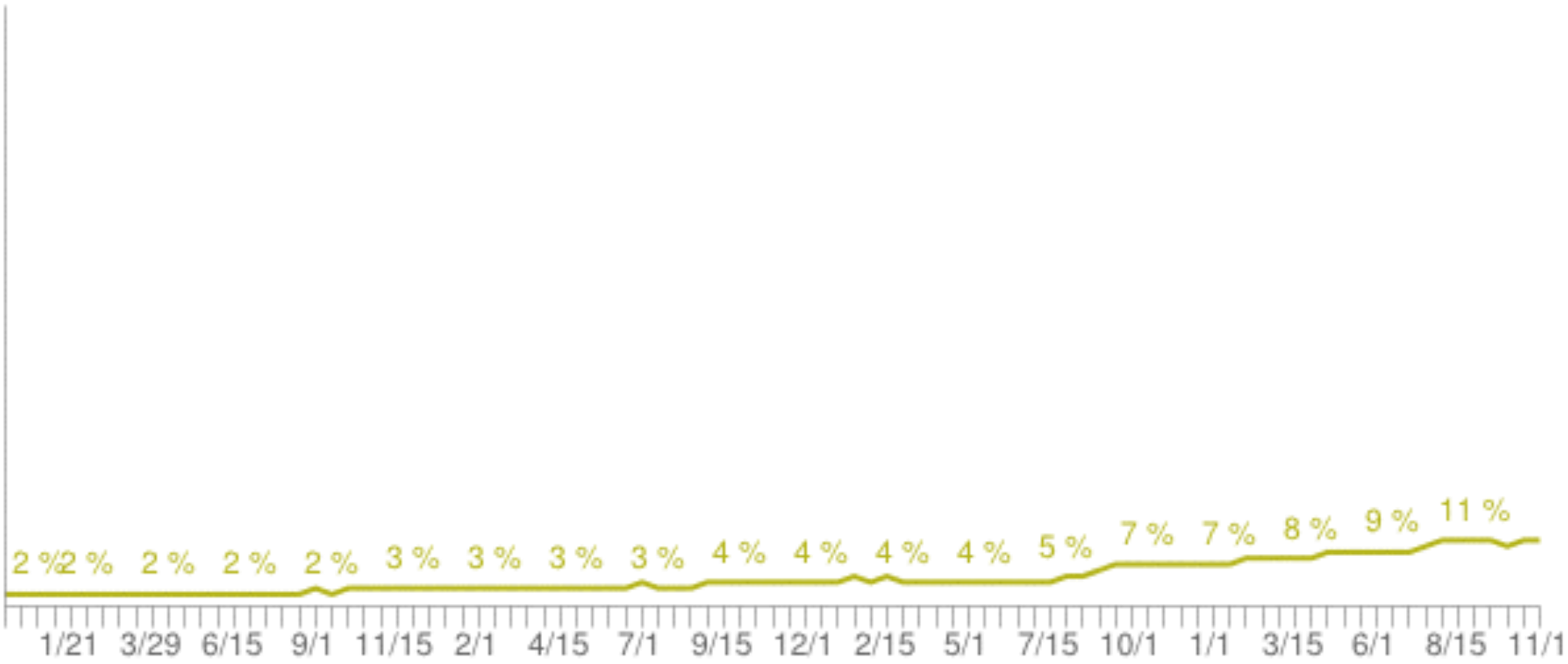
- Various statistics show an increase
  - Lots of variation, depending on what is measured
  - A sharper increase following Snowden affairs
  - But also a long-term increasing trend
- Significant part of traffic likely encrypted in the future (but not 100%)

Statistics Example 1



- Gmail traffic encrypted from other e-mail providers rises from 27% to 64% since early 2013 (source: Google)

Statistics Example 2



- Alexa top 1,000 HTTPS capability from 2010 to 2014 (Source: Httparchive)

- Note: cf. 50% of the top10 by default on HTTPS

Reasons for the Increase



There is no single reason:

- An application may wish to use security to prevent account hijacking, keep personalised content private, limit surveillance, business reasons, …

- But the use of security protocols may also incur cost and latency, or may not be needed

    - Some of these aspects may be improved with better technology

In any case, the increasing trend is likely to continue

Implications



- Long-term effects to the number of parties that see contents
- Secure traffic may also interact with network services, such as caching
- Useful technical things may need to be done in new ways

How to Work on Improvements?



- Do we have all the technical tools that we need?
- What can we do to improve security? Network operations?
- World still moves ahead on a voluntary basis on what technology is chosen and on what technology a particular party can adopt
- Important to understand the ecosystem works based on individual decisions of browser vendors, content providers, users, and network operators

End

Internet Architecture Board Statement on *Internet Confidentiality*

Russ Housley
IAB Chair

28 February 2015



IAB Statement released in November 2014

- **Internet Architecture Board** released a statement that encourages encryption at multiple places in the Internet protocol stack

  https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

- The statement is just five paragraphs

Paragraph 1: Background

In 1996, the IAB and IESG recognized that the growth of the Internet depended on users having confidence that the network would protect their private information. RFC 1984 documented this need. Since that time, we have seen evidence that the capabilities and activities of attackers are greater and more pervasive than previously known. The IAB now believes it is important for protocol designers, developers, and operators to make encryption the norm for Internet traffic. Encryption should be authenticated where possible, but even protocols providing confidentiality without authentication are useful in the face of pervasive surveillance as described in RFC 7258.

Paragraph 2: New Protocols

Newly designed protocols should prefer encryption to cleartext operation. There may be exceptions to this default, but it is important to recognize that protocols do not operate in isolation. Information leaked by one protocol can be made part of a more substantial body of information by cross-correlation of traffic observation. There are protocols which may as a result require encryption on the Internet even when it would not be a requirement for that protocol operating in isolation.

Paragraph 3: Deployment

We recommend that encryption be deployed throughout the protocol stack since there is not a single place within the stack where all kinds of communication can be protected.

Paragraph 4: Call to Action

The IAB urges protocol designers to design for confidential operation by default. We strongly encourage developers to include encryption in their implementations, and to make them encrypted by default. We similarly encourage network and service operators to deploy encryption where it is not yet deployed, and we urge firewall policy administrators to permit encrypted traffic.

Paragraph 5: Restore Trust

We believe that each of these changes will help restore the trust users must have in the Internet. We acknowledge that this will take time and trouble, though we believe recent successes in content delivery networks, messaging, and Internet application deployments demonstrate the feasibility of this migration. We also acknowledge that many network operations activities today, from traffic management and intrusion detection to spam prevention and policy enforcement, assume access to cleartext payload. For many of these activities there are no solutions yet, but the IAB will work with those affected to foster development of new approaches for these activities which allow us to move to an Internet where traffic is confidential by default.

Encryption Standards

- The IETF has already developed many security protocols for data in transit and data at rest:
  - IPsec, TLS, DTLS, OpenPGP, S/MIME, …
- Applications depend on these protocols:
  - Network Storage: iSCSI with IPsec
  - Web: HTTP with TLS
  - VoIP: SIP with DTLS
  - Email: SMTP, POP, and IMAP with TLS;
    Content with OpenPGP or S/MIME

Encryption Standard Deployment

- Expect improvements in the protocol standards themselves as well as their implementations
- Expect easier deployment
- Cost of infrastructure seems to be going down too

Thank You

Russ Housley
Phone: +1 703 435 1775
Email: housley@vigilsec.com

A Definition

From RFC7258/BCP188: “Pervasive Monitoring is an Attack”

> Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol meta-data such as headers. Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive monitoring. PM is distinguished by being indiscriminate and very large-scale, rather than by introducing new types of technical compromise.

What does RFC 7258 mean?

- RFC7258/BCP188 says that all IETF work will consider PM as an attack to be mitigated as part of our normal design processes for all protocol development
  - Note: this does not mean PM is always relevant nor that it's always practical to mitigate PM via protocol mechanisms, but if you can't, you need to be able to say why
- Took ~1000 emails to get rough consensus on that since countering PM is not free
    - Impacts on network management
    - Some folks scared of unreasonable security/privacy nerd dominance

Some PM Mitigations

- Improve code quality, open-source or not
  - More care with e.g. contacts, MISDN enrichment, TLS certificate handling
- Better and more use of crypto in protocols
  - UTA, Opportunistic Security (RFC7435), better usability for users, admins, ...
- Data minimisation in current protocols
  - DNS QNAME case, DHCP identifiers
- New protocols
  - e.g. certificate transparency (RFC6962), DPRIVE, TCPINC
- Traffic analysis mitigations
  - padding, routing: harder but we can put tooling in place
- Overall system designs
  - Avoid MitM attack middleboxes or clients, operating system/platform improvements
- Corporate and public policy



IETF scope

The PM Adversary

- Credible claims of attacks on mobile infrastructure (Belgacom, sysadmins, Bahamas, Gemalto)
  - Pattern to try/do everything – co-operating with and attacking infrastructure players at the same time
- In future, adversary may not be state actor, e.g. botnets, and more states will acquire capability
  - O(10) → O(1000) adversaries perhaps?
  - SDN/NFV etc will also virtualise infrastructure putting it more directly at risk, whenever assets are shared

PM is not everything

- PM is far from the only security or privacy issue on which we need to work
  - Spam, malware, DDoS, …
  - But mitigations for PM can also help a lot with other problems
- And some PM mitigations will make life harder, e.g. inbound malware detection
  - Balancing those competing requirements will be an ongoing task
- Hypothesis: If we work to address PM, and prioritise services and mechanisms that mitigate PM and that are also effective against other attacks then we will be doing the “right thing”

GSMA/IETF Questions

- What's the best way for us to work together to ensure we improve the Internet?
- How to capture and reflect operational requirements from GSMA in IETF work on PM?
- How to establish effects of Internet protocol changes and trends (e.g. more crypto) on operator networks?
- What current work items can we collaborate on in the near/medium term?
- What new work may need to be initiated?
- Are there useful ways in which we can “visit” one another?

Backup

IETF (Re)Action

- Overall: snowdonia has re-energised folks to do better on security and privacy in general (and not solely in response to PM)
  - Side meeting in Berlin @ IETF-87 (July 2013)
  - Tech plenary, major discussion @ IETF-88 (Nov 2013)
  - STRINT workshop before IETF-89 (Feb 2014)
    - (W) https://tools.ietf.org/html/draft-iab-strint-report
  - Topic at many meetings/BoFs @ IETF-89 (July 2014)
  - Starting to see results from IETF-90 (Nov 2014) onwards...
- Unsurprisingly this is similar to the more broad technical community reaction

IETF work related to PM

- RFC 7258/BCP188 published after major IETF LC debate – sets the basis for further actions
- RFC 7435 defines “Opportunistic Security” - less gold-plating, more deployment
- IAB Statement on Internet Confidentiality: basically: encrypt everything!
- New working groups established:
  - UTA: update BCPs on how to “Use TLS in Applications”
  - DPRIVE: “DNS Privacy”- unthinkable before snowdonia
  - TCPINC: “TCP INCreased security”: tcpcrypt proposed two years earlier but rejected
    - Mistakenly, including by me, as ack'd at mic @ IETF-88, bummer
- IAB re-factored security and privacy programme
  - Developing PM threat model document
- Stuff not going so well (yet!)
  - Old-RFC privacy/PM review team – go back and see what needs fixing, sadly moribund
  - Endymail email list for discussion of ways IETF can help those working on new e2e interpersonal messaging solutions

Other relevant IETF Things

- TLS 1.3 aiming for better handshake encryption properties and learning from previous TLS problems in various ways
- HTTP/2.0, the major deployment model for which seems to be to run much much more HTTP traffic over TLS
- Extension to HTTP/2.0 defining opportunistic security way of sending http URI schemed content over TLS
- DHCP privacy considerations work
- DNS Query Minimisation
- Negatively: deprecate RC4 in TLS, SSL3, ...
- And since all this is IETF stuff, you can (and please do) join in and help if you're willing and able – that's how to make it better!
  - Even a small amount of good opertator input is hugely valuable (but you need to be able to deal with a noisy environment;-)

Opportunistic Security RFC 7435

- IETF modus operandi has (in practice) been to define mandatory to implement security that works for higher security environments

  => often hard/expensive to deploy => often not used => cleartext often sent even when better options exist

- Opportunistic Security (OS) aims to evaluate these trade-offs on a connection-by-connection basis, explicitly allowing for e.g. unauthenticated endpoints for confidentiality (open-channel key exchange) as an option that is better than cleartext
- I (personally) hope that this concept is followed very often and is fleshed out to the point where we end up with a new security development approach that is based around OS
  - Not there yet: TLS deprecation of RC4 was interesting because of differing perspectives from web and mail folks about what conclusion to draw when following the OS approach

OS example: Deprecating RC4

- RC4 past sell-by date: agreed by all
- For the web ~15% of https sites were using TLS/RC4 (FF 2014 measurement)
  - When RC4 zapped 99% of those just picked a better option (AES, 3DES)
- SMTP+STARTTLS between MTAs
  - There is a widely deployed MTA that only does RC4, 3DES is buggy and won't work (so I'm told)
  - Zapping RC4 means emails will be sent in clear between MTAs when one is the buggy one
- So – which is better: deprecate RC4 entirely or add this and possibly other caveats?
  - IETF rough consensus was to deprecate entirely, but some mail folks were in the rough
- Interesting example implying conclusion from following OS protocol design pattern will depend on scope
  - OS requires us each to figure out some kind of utility or objective function and where those differ enough, different well meaning folks will reach different conclusions
  - Any way to produce evidence as to what's the best thing to do for things like this?
- It is OK that it is harder to figure out what to do when following the OS approach

IAB Statement

"We recommend that encryption be deployed throughout the protocol stack since there is not a single place within the stack where all kinds of communication can be protected.

The IAB urges protocol designers to design for confidential operation by default. We strongly encourage developers to include encryption in their implementations, and to make them encrypted by default. We similarly encourage network and service operators to deploy encryption where it is not yet deployed, and we urge firewall policy administrators to permit encrypted traffic."

(W) https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

Non-IETF Things Relevant to IETF

- Internet Research Task Force (IRTF) CFRG work on additional elliptic curves for TLS that perform better and have better side-channel resistance
  - Basically: consider last decade of academic crypto work on ECC
  - Has adopted Curve25519, more tbd
- IEEE 802 have started work on privacy and are considering e.g. MAC address randomisation
  - Collaborating with IETF
- W3C TAG statement on “Securing the Web”
  - Builds on RFC7258 and IAB statement
  - (S) https://www.w3.org/2001/tag/doc/web-https
- Cryptech – (W) https://cryptech.is/
  - Aiming to build open-source h/w crypto module to help increase confidence
- … there are loads more

More References (1)

- General IETF stuff:
- https://www.ietf.org/
- https://www.ietf.org/newcomers.html
- Working group details for WG <foo>:
  - https://tools.ietf.org/wg/<foo> - links to charter, docs, mail archive etc
  - Suggested <foo> values:
    - tls, dprive, tcpinc, httpbis, uta

References (2)

- Relevant IETF non-wg lists:
  - All of them (loads): https://www.ietf.org/list/nonwg.html
  - Perpass – triage list for PM related stuff:
    - https://www.ietf.org/mailman/listinfo/perpass
  - Secruity area list (saag)
    - https://www.ietf.org/mailman/listinfo/perpass
  - Possible e2e interpersonal messaging discussion
    - https://www.ietf.org/mailman/listinfo/endymail
  - General privacy discussion
    - https://www.ietf.org/mailman/listinfo/ietf-privacy
- IRTF:
  - https://www.irtf.org/
  - IRTF Crypto Research Forum Goup: https://irtf.org/cfrg

References (3)

- Videos (ISOC hint:-)
  - IETF youtube stuff in general
  - https://www.youtube.com/user/ietf/videos?sort=p&view=0&flow=grid
- Nov'13 IETF technical plenary video
  - https://www.youtube.com/watch?v=oV71hhEpQ20
- Dan york videos 5 minute summaries of IETF meetings
  - There are loads but these are about PM
  - https://www.youtube.com/watch?v=HG54EsHYKr0
  - https://www.youtube.com/watch?v=fbjs_6Mz-6s
- STRINT workshop
  - Has all 66 position papers
  - https://www.w3.org/2014/strint/

References (4)

- IEEE Internet Computing “soapbox” column on why PM is bad:
  - http://www.computer.org/csdl/mags/ic/2014/04/mic2014040004.pdf
- Some Internet drafts not referenced above:
  - PM Threat model
    - https://tools.ietf.org/html/draft-iab-privsec-confidentiality-threat
  - DNS Privacy problem statement
    - https://tools.ietf.org/wg/dprive/draft-ietf-dprive-problem-statement/
  - “Modern” TLS best current practices
    - https://tools.ietf.org/html/draft-ietf-uta-tls-bcp