Contents

Edit

View

State: Private

Actions

Manage portlets

a few seconds ago

Sharing

i **Info** Changes saved

IETF 101, TLS 1.3

IETF 101 was organized in London this year. As usual, we, the hackers.mu team, participated remotely. This year, we were in as the TLS champions. Hence there was some more responsibilities and more planning needed.

How it began

As we had posted it in our events (https://hackers.mu/events/ietf-101-participation) section, this year, we went for the IETF 101 hackathon. As a reminder, last year, we even had 🔒The Register (https://www.theregister.co.uk/2017/10/26/hackers_mu_tls_1_3/) which wrote about our participation in the IETF 100 event to deliver TLS 1.3 implementations. We also had the 🔒IETF blog (https://www.ietf.org/blog/participating-ietf-hackathon-mauritius/?primary_topic=6&) which covered that as well.

We would have loved to go on site in London to do this but logistically, it would have been difficult, and quite expensive for all our members to go there so preparation to hack from Mauritius began some weeks before the big event. It was quite a rush as we were working on several other projects at the same time. We had to find a spot to get together and to the hackathon in the first place. A note about this, if there is anyone who wishes to sponsor a place where we can hack for a weekend once a while (when and if we have a hackathon planned), please do drop us a mail using the contact page (https://hackers.mu/contact-info).

Setting up

After all the planning for a space to hack, preparing the funds and logistics for it all, one week before DDay, the meteo announced that there could be a potential cyclone lurking around. Hence we decided to Perform the hackathon remotely, form each other's house. For this, the challenge becomes harder, as now, we obviously had communication issues to cope for as well as how to manage everything. But eventually we sorted it out! Trello and our Fb. We had slack and Jabber as well, but turns out, a lot were sending message through Fb, so we ended up using Fb for group conversation and Trello to manage our tasks.

What we worked on

We planned on working on the following:

<table>
<tr><th>Projects</th><th>IETF Draft || RFC</th></tr>
</table>

TLS 1.3	🔒The Transport Layer Security (TLS) Protocol Version 1.3 (https://tools.ietf.org/html/draft-ietf-tls-tls13-23)
DNS	🔒Pervasive Monitoring Is an Attack (https://tools.ietf.org/html/rfc7258)
http 451	🔒 An HTTP Status Code to Report Legal Obstacles (https://tools.ietf.org/html/rfc7725)

- Since OpenSSL pre release candidates were coming out with TLS 1.3 support, we had to work towards adding support for TLS 1.3 in as much software as we could.
- Loganaden and Codarren were interested in DNS security, hence worked on the DNS PRIVate Exchange (DPRIVE) Working Group develops mechanisms to provide confidentiality to DNS transactions, to address concerns surrounding pervasive monitoring.
- While those who wanted to work on http 451 focused on that.

TLS 1.3

	Project	Member	Gist/Pr
	GNU 🔒wget (https://www.gnu.org/software/wget/), is a free software package for retrieving files using HTTP, HTTPS, FTP and FTPS the most widely-used Internet protocols. It is a non-interactive commandline tool, so it may easily be called from scripts, cron jobs, terminals without X-Windows support, etc.	Loganaden Velvindron	

Nagios	nagios-plugins, 🔒check_http (https://www.monitoring-plugins.org/doc/man/check_http.html), tests the HTTP service on the specified host. It can test normal (http) and secure (https) servers, follow redirects, search for strings and regular expressions, check connection times, and report on certificate expiration times.	Rahul Golam	
Stunnel	🔒stunnel (https://www.stunnel.org/), stunnel is an open-source multi-platform application used to provide universal TLS/SSL tunneling service. stunnel can be used to provide secure encrypted connections for clients or servers that do not speak TLS or SSL natively. It runs on a variety of operating systems, including most Unix-like operating systems	Nitin Mutkawoa	
HTTPERF	🔒httpperf (https://github.com/httperf/httperf), is a tool for measuring web server performance. It provides a flexible facility for generating various HTTP workloads and for measuring server performance.	Muzaffar Auhamud	
git	🔒git (https://git-scm.com/), is a free and open source distributed version control system designed to handle everything from small to very large projects with speed and efficiency.	Loganaden Velvindron	
Nagios	🔒check_ssl_cert (https://github.com/matteocorti/check_ssl_cert), is a Nagios plugin to check an X.509 certificate: • checks if the server is running and delivers a valid certificate • checks if the CA matches a given pattern • checks the validity	Yasir Auleear	
aria2	🔒aria2c (https://aria2.github.io/), is a lightweight multi-protocol & multi-source command-line download utility. It supports HTTP/HTTPS, FTP, SFTP, BitTorrent and Metalink. aria2 can be manipulated via built-in JSON-RPC and XML-RPC interfaces.	Pirabarlen Cheenaramen	
paho	🔒Eclipse paho C library (https://www.eclipse.org/paho/), is a set of scalable open-source implementations of open and standard messaging protocols aimed at new, existing, and emerging applications for Machine-to-Machine (M2M) and Internet of Things (IoT)	Nitin Mutkawoa, Nigel Yong	
mercurial	🔒mercurial (https://www.mercurial-scm.org/), is a distributed revision-control tool for software developers. It is supported on Microsoft Windows and Unix-like systems, such as FreeBSD, macOS and Linux.	Codarren Velvindron	

	🔒 monit (https://mmonit.com/monit/), is a utility for managing and monitoring processes, programs, files, directories and filesystems on a Unix system. Monit conducts automatic maintenance and repair and can execute meaningful causal actions in error situations.	Codarren Velvindron	

Challenges that we had this year

While we did have some experience with draft 13 of TLS 1.3, we had quite some challenges this year. We had to keep up with the projects we were working on with and cope for new changes. As well as take into considerations the new changes related to draft 23 of TLS 1.3.

Testing was much more fine grained this time, and luckily we had WireShark around to catch any handshake issues, specially with that clienthello that caused some pain! But once we got the gist, it was all good.

Thanks to

-

-

-

NEWS (HTTPS://HACKERS.MU/NEWS)

Un membre de hackers.mu remporte le Grand Prix Drupal de Google Code-in (https://hackers.mu/news/un-membre-de-hackers-mu-remporte-le-grand-prix-drupal-de-google-code-in)

Feb 11, 2018

End of year 2017 review (https://hackers.mu/news/end-of-year-2017-review)

Jan 23, 2018

Lest we Forget (https://hackers.mu/news/lest-we-forget)

May 26, 2017

Operation Crypto Redemption (https://hackers.mu/news/operation-crypto-redemption)

Apr 06, 2017

Hackers.mu leads Mauritians for the Google code-in (https://hackers.mu/news/hackers-mu-leads-mauritians-for-the-google-code-in)

Feb 08, 2017

More news... (https://hackers.mu/news)

Site Map (https://hackers.mu/sitemap) Accessibility (https://hackers.mu/accessibility-info)

Contact (https://hackers.mu/contact-info)