Alors aujourd'hui nous allons parler de CH avec Arnaud Tadehi.
Bonjour Arnaud.
Bonjour à tous.
Pour discuter avec lui, les contributeurs de No Limit Sécu sont Paul Amar.
Et bonjour.
Nicolas Rue.
Bonjour.
Hervé Chauheur.
Bonjour.
Et Christophe Renard.
Bonjour.
Alors Arnaud nous avons déjà réalisé un épisode ensemble mais pour les
auditeurs qui ne l'auraient pas suivi et ce que tu voudrais bien te présenter.
Oui, alors je suis Arnaud Tadehi, je suis basé en Suisse, à Genève et je fais deux choses dans la vie.
D'abord je travaille pour la société Symantec chez Bandcom.
Je fais deux choses dans la vie.
Une je fais du conseil exécutif auprès des clients.
L'autre je le passe à la moitié de mon temps à la standardisation internationale,
notamment l'IETF et l'Union internationale des Télécom.
Alors Arnaud, qu'est-ce qui se cache derrière ces trois lettres énigmatiques
ECH ?
Alors d'abord ECH, ça veut dire Encryptus Client Rello et ça parle du protocole TLS.
Et en fait c'est la fin de ce qu'on appellera le chiffrement de bout en bout de toute la situation.
La fin du chiffrement de bout en bout, c'est-à-dire ?
Alors avant TLS 1.2, qui était un protocole qu'on connaît avec beaucoup de limites,
il y avait beaucoup trop de choses qui étaient dans le clair.
Et donc l'IETF, Internet Engineering Task Force, a décidé de, dans Snowden,
quand le cas de Snowden s'est révélé, de chiffrer le maximum d'observat possible.
Donc TLS 1.3 a chiffré le certificat XS9.
Ensuite, DOH, DOT et DOQ, qui sont DNS Over HTTP, DNS Over PIC et DNS Over TLS,
ont chiffré l'accès du client au réserveur de TLS.
Et il restait à chiffrer les éléments de ce qu'on appelle le clientelot dans la session TLS,
qui était encore dans le clair, et notamment le fameux SNI, qui veut dire server name indication.
Je lui ai dit plein de mots barbares là, mais en gros, depuis 2017, quand TLS 1.3 a démarré,
il y a eu tout un mouvement qui s'est organisé pour chiffrer tous les observables qui étaient utilisés,
qui sont utilisés par la Défense Sécuritaire Résoudre, en particulier, pour pouvoir faire de la
défense.
C'était motivé par le fait que ces données laissaient passer trop de chauds d'emplaires,
il y a tellement trop de choses qui atteignent la vie privée des gens,
donc c'était un problème de remettre la privérité sur la vie privée ou de dépendre de la session.
Et ce qu'on peut expliquer, comment ça marche sur les virtuallos, c'est en fait,
comme plusieurs services web, enfin plusieurs nom de domaine peuvent être générés à la même
adresse IP,
quand un client contacte un nom de domaine, enfin, un server web ou HTTPS, il va dire,

je connecte à tel adresse IP, mais je demande à accéder à tel site et cette partie-là,
passe en fait en clair dans la négociation TLS.
Je pense qu'il faut préciser, donc l'histoire du virtuallosting, c'est qu'on veut sur un seul serveur physique,
sur une seule adresse IP, en l'occurrence, héberger plusieurs sites web et tant qu'on est en HTTP, c'est simple, on se connecte en TCP, on commence la session HTTP et on dit, je veux me connecter à tel site.
Et le serveur sait quoi répondre.
Le problème, c'est que comme TLS et HTTP sont deux couches indépendantes,
le serveur doit présenter un certificat qui correspond à l'OSNEM, qui est, enfin, OFQDN, qui est accédé,
et qu'avant qu'on lui dise quel est le site que l'on veut accéder, il sait pas quel certificat choisir quand il en a plusieurs.
Et donc SNI, ça permet de dire, dès le début de la session,
bonjour, j'essaye de me connecter sur le site ABC et pas le site DEF et de recevoir le certificat pour le bon site.
C'était déjà une évolution de TLS.
Il est en clair parce que t'as besoin de l'échanger avant d'avoir reçu le certificat et d'avoir vérifié l'identité du serveur
et avant d'avoir fait une négociation des informations cryptographiques de session.
Voilà, c'est ça.
Donc en gros, le problème, c'est que le DNS te permet de trouver l'adresse IP que tu veux me contacter,
mais il manquait le petit bout pour aller un petit peu plus loin pour trouver le serveur que tu voulais vraiment.
Si tu as 10 000 sites qui sont hébergés par 1.2.3.4,
toi, ce que tu veux, c'est établir une connexion avec le serveur 14.
Donc le DNS te permet d'aller sur 1.2.3.4 et le SNI te permet d'aller sur le bon serveur.
Le problème, c'est que quand TLS démarre, il démarre dans le clair.
Il n'y a rien avant.
Quand on veut établir une communication applicative chiffrée,
elle doit être chiffrée de façon symétrique, c'est par exemple HTTPS.
Pour pouvoir avoir ce chiffrement,
si on doit avoir un chiffrement symétrique des deux côtés,
il faut qu'on puisse partager un secret.
Partager un secret, il faut protéger le secret.
C'est pour ça qu'on a TLS.
Donc TLS ne peut pas être symétrique, sinon il faudrait encore quelque chose de symétrique.
Encore quelque chose de symétrique à l'infini, ça ne marche pas.
Donc TLS, il démarre de façon assimétrique.
C'est pour ça qu'on a un PKI, l'infrastructure des publics mondiales,
qui permet d'avoir ce certificat qui permet d'établir cette communication assimétrique.
Seulement pour la démarrer, il vient de démarrer de zéro.
Donc quand TLS démarre, il démarre non chiffré

et comme c'est un protocole poli, il commence par dire bonjour, je suis le tire, clientel.
Et dans ce clientel O, il va passer un certain de paramètres,
dont l'OSMI et dont la LPN et d'autres.
La LPN, c'est l'Application Level Protocole.
Negotiation.
C'est pour que la couche applicative puisse récupérer des informations
sur les paramètres TLS qui ont été négociés dans les couches beaucoup plus basses.
Donc le problème, c'est que comme on part de zéro,
qu'est-ce qu'on va faire pour pouvoir chiffrer ce dernier morceau ?
Alors au départ, ce qu'il faut voir, c'est qu'historiquement,
quand les gens ont fait TLS 1.3, puis l'accès au résolveur des watch, des hotels et des coups,
ils voulaient chiffrer le SMI.
Et donc, pendant très longtemps, le draft qui a été présenté s'appelle E-SMI pour Encrypt d'SMI.
En fait, en faisant, ils sont réperçus qu'il y avait quand même d'autres choses
qui étaient intéressantes de capturer, la LPN et d'autres.
Et en fait, c'est aussi, je pense, marteau pilon pour juste un paramètre.
On va chiffrer tout le clientelot, ce sera plus facile.
Et donc, ils ont appelé Encrypt, par contre.
Dans la littérature, ce qu'il faut voir, c'est que le draft internet,
c'est le nom du document quand le protocole est développé,
il a encore le nom ESNI et pas le nom ECH.
Vous ne verrez pas le nom ESH dans le nom.
Il n'y a plus exactement le nom du draft.
C'est en version 17 aujourd'hui.
Et c'est pour ça qu'il commence par ECH.
En fait, c'est bien Encrypt d'E-SMI.
Mais alors, tu le chiffres de façon assez maitrique,
parce que tu nous as expliqué précédemment que sinon on tombait dans une boucle infinie,
mais tu le chiffres avec quel certificat ?
Alors, justement, c'est là où ça devient très complexe,
parce que comment faire pour démarrer un chiffrement quand on n'a rien ?
Alors, il a fallu l'état d'idée et mettre en place des tas de choses.
Alors, la première chose, c'est qu'on va commencer par dire
que quand le clientelot part du client vers le serveur,
on va faire une poupée russe.
Donc, on va dire, on a bien un clientelot qui passe.
On va l'appeler le clientelot outer, l'extérieur.
C'est un clientelot qui passe.
Il n'y aura rien de vraiment intéressant dedans,
mais il va passer, sauf qu'à l'intérieur,
il a le vrai clientelot, qu'on va appeler le clientelot inner.
Lui, il va être chiffré.
Donc, l'objectif, ça va être comment on fait pour chiffrer quelque chose quand on part de zéro ?
Alors, l'histoire, c'est pas une poudre ici,

mais l'histoire est assez compliquée et colossale.
Franchement colossale, l'effort intellectuel qu'il a fait pour faire ça, il est gigante.
La première chose qu'on va faire, c'est qu'on va commencer par dire,
puisque l'objectif, quand même, c'est de faire en sorte
qu'on ne vaille plus la destination de l'utilisateur.
Donc, si on ne veut plus voir la destination de l'utilisateur,
il faut commencer par cacher tous les serveurs du monde
derrière ce qu'on appelle un client facing server.
Je répète.
C'est gros.
On va prendre tous les serveurs du monde à terme.
Le CH sera complètement déployé et adopté par tout le monde.
Tous les serveurs du monde seront accessibles
qu'à travers un client facing server.
Et pourquoi ?
Parce que ça permet d'avoir un immense ensemble d'anonymités
derrière un frontal.
Excuse-moi, mais là-dessus, est-ce que c'est vraiment réaliste ?
C'est-à-dire qu'avec toutes les stacks legacy,
ou quoi, je veux dire, la mise en place de CH là-dessus, c'est...
Mais en fait, tu l'as, c'est les content distribution network,
c'est les prestataires de cloud.
Ils ont déjà des milliers de sites derrière une adresse IP.
C'est déjà le cas, effectivement, comme dit Christopher.
En fait, c'est...
Il y a des complexités et on verra un petit peu plus tard
où ils en sont vraiment du déploiement,
parce que pendant le début, mais...
Effectivement, je pense que c'est pas là où ça pose un problème,
parce que ça pose un problème, mais ça posera un problème plus tard.
Je pense pas que c'est un problème de scalability,
mais c'est un problème de résidence.
Il faut quand même préciser que c'est TLS 1.3,
ce sont tous les vieux trucs, les machins, les IoT et tout,
et ne supporteront jamais ça.
Tous ceux qui sont en TLS 1.2 ou antérieure, c'est pas...
Alors, il faut bien voir, très bonne remarque.
ECH, c'est une extension du protocole TLS 1.3.
Alors, je vais faire un petit teasing,
mais c'est pas seulement une extension du protocole TLS 1.3,
mais à terme, quand le serveur ne pourra pas honorer ECH,
le TLS 1.3 fera son appel Grease ECH.
Est-ce que Grease ECH, c'est un faux ECH ?
C'est-à-dire que si le navigateur voit que l'autre côté,

il ne peut pas faire ECH, il va dire que je prétends que je fais ECH.
Tout a été construit pour faire échouer la défense,
le réseau et les équipements réseaux.
Je pense qu'il faut quand même très largement préciser
que toutes les mesures destinées à anonymiser des consultations,
et en particulier, on pense aux gens qui consultent
depuis des pays dictatoriaux, mais pas seulement,
sont des mesures qui reposent sur le fait de se perdre dans la masse.
Donc, si vous accédez à un serveur qui est hébergé derrière un particulier,
enfin, qui est hébergé chez moi sur ma liaison fibre,
en fait, vous n'êtes pas anonymes du tout,
même si vous avez caché le SNI,
parce que vous devez avoir trois noms de domaines chez moi.
Et en plus, ils sont tous gérés par le même bonhomme.
Ce sont des mesures qui ne protègent les gens qui naviguent
qu'à partir du moment où ils accèdent à des services
qui sont perdus dans la masse d'un prestataire cloud ou d'un CDN.
On peut penser par exemple à Telegram,
qui essaye d'échapper à la censure russe, ce genre de choses.
T'as fait. Donc ça, c'est important.
C'est pour ça que je disais plus l'espace est grand,
plus on est caché, ça le correspond à tout le monde.
Alors, comment on va faire pour y arriver ?
On a un client de facing server, c'est déjà une chose.
Techniquement parlant, on peut mettre le serveur de backend
sur la même machine, on appelle ça le shermode,
ou on les met en split mode, c'est-à-dire qu'on sépare
le client facing server du backend server,
ce qui va être, j'imagine, le cas plus grand de la journée TV.
Donc ça, c'est la première chose.
La deuxième chose, il a bien fallu inventer une nouvelle cryptographie.
Donc il y a une nouvelle crypto qui s'appelle hybrid cryptographie.
Je crois d'ailleurs qu'elle a été faite par Mineria.
Je ne suis plus sûr, mais je pense que c'est Mineria qui l'a faite.
Évidemment, ce qu'elle ne peut pas être symétrique,
c'est l'objectif à la fin.
Elle ne peut pas être asymétrique, c'est ce que TLS doit faire.
Donc on part avec une cryptographie hybrid.
Alors cette cryptographie, le client facing server va la prendre
et va générer un vecteur de configuration
qui inclut la clé publique pour ce site particulier,
maintenant, là, pour les prochaines qui sont en feed-up.
Donc il doit générer tout un vecteur de configuration
avec des paramètres, et il doit faire en sorte

que le client va obtenir cette information-là.
Donc qu'est-ce qu'on avait comme possibilité ?
La possibilité qui a été choisie, qui n'est pas mandatorie,
qui n'est pas obligatoire, c'est le DNS.
Donc la troisième chose qu'on va faire,
après avoir mis en place un client facing server,
après avoir mis en place une nouvelle cryptographie,
c'est qu'on va changer le DNS
pour que le DNS ne soit plus le DNS qu'on connaît
qui nous envoie des braves à récord.
Le DNS va être changé en un directory server mondial.
Ça veut dire que pour chaque entrée, exemple.com,
par exemple, je ne vais pas seulement avoir un point 2.34,
mais je vais avoir l'adresse de son client facing server,
et je vais surtout avoir ce qu'on appelle
quatrième invention, des nouveaux ressources-records
des services binding, qui ne sont pas faits que pour OCH,
il y avait d'autres raisons pour laquelle la communauté
a décidé d'avoir d'autres ressources
pour décrire un domaine particulier.
Mais en particulier, le client facing server
va publier des ressources-records toutes les 48 heures
sur la cible qu'il veut avoir.
Ça commence à faire beaucoup de choses.
Là, on fait un server, une cryptographie Hebride,
des nouveaux services binding,
et on change la nature du DNS.
Donc avec tout ça, comment ça marche ?
Je suis un navigateur.
Je veux faire un OCH.
Qu'est-ce que je fais ?
Je vais sur mon resolver.
Ah oui, on a déjà une cinquième invention,
qui est DOH.
DOH a été inventé dans ce cadre-là.
T'es laissé un point 3, DOH, tout ça,
c'est un ensemble de briques qui ont été construites ensemble.
Donc, le navigateur fait un DOH sur le resolver,
donc personne ne peut le voir en théorie.
Le DOH va sur le DNS pour dire,
pour exemple, le .com, j'ai quoi comme donner ?
Ah ben voilà, tu as ton client facing server,
4.5.6.7.
Tu as ce ressources-records,

tu as publiqué les paramètres dont tu as besoin.
Maintenant, tu peux revenir à la maison,
et avec ça, tu peux construire ta coupérie.
Donc, le navigateur va construire son client HelloInner,
l'on casse sur le client HelloArter,
et il va faire son TLS client Hello normalement.
Il envoie tout ça,
ça arrive bien sûr sur le client facing server,
qui lui a tout ce qu'il faut pour déchiffer ce qu'il y a dedans,
il récupère le SNI,
il fait un TCP forward sur la destination finale.
La destination finale reconnaît que c'est un TLS,
va honorer ce TLS pour revenir dans le client,
et va fermer le handshake correctement.
Et du coup, on a un end-to-end,
depuis le client, vers la destination finale,
sans que personne, à part le client facing server,
ait pu voir où était la destination finale.
C'est un petit peu comme si on avait une sorte de reverse proxy géant
qui va récupérer toutes les sessions HTTPS,
et les forwarder au bon endroit.
On peut voir ça comme ça.
C'est un gros lot de balanceurs,
si tu veux,
ou des reverse proxy,
on peut l'appeler comme on veut.
Mais toujours est-il que c'est quand même,
pourquoi c'est colossal,
c'est pas juste une extension comme ça qui va arriver,
donc c'est colossal,
il a fallu 10 ans de travail, je pense,
un ton de gens pour réussir à faire ce travail-là,
c'est quand même intellectuellement,
c'est incroyable.
Dans le fond, il y a quand même beaucoup d'idées
qui venaient de tort,
il essaie de rendre ça de façon générique pour tout le monde,
effectivement,
avec l'intention de surtout servir les décidents
et communautés discriminées.
Ça résout d'autres problèmes que les aspects privés aussi ?
Alors, c'est déjà un gros truc que ça résout,
après, on peut débattre
si ça résout plus de choses ou moins de choses,

moins de choses.
Effectivement, ça pourrait être intéressant,
par exemple,
si je suis une banque et que j'ai des clients,
je n'ai pas du tout envie que quelqu'un
regarde la destination ou mes clients.
Donc ça peut être intéressant pour mes propres clients,
donc il y a des gens qui peuvent le voir positivement
pour leurs organisations.
On peut imaginer aussi les prestataires
non pas de VPN,
mais de proxy anonymisants
sur lesquels on pourrait se connecter
et eux-mêmes, on ne verrait plus rien
une fois que la connexion est faite,
mais on peut déjà le faire avec du TLS aujourd'hui.
Par contre,
il y a une question que ça me pose,
qui était un peu la même qu'on a aujourd'hui
quand on met ces clés publics et ces sages dans le DNS.
L'essentiel du monde ne fait pas de DNS ça.
La plupart du DNS aujourd'hui est pas chiffré signé.
Donc qu'est-ce qu'il va protéger
contre une attaque
ou quelqu'un qui a la main sur les faillis,
je ne sais pas, on peut imaginer dans les circonstances
par exemple dans lesquelles ont été
les gens pendant le printemps arabe en Tunisie
ou les principaux fournisseurs d'accès internet
travaillés avec le régime.
Et donc pour avoir un DNS menteur
qui renverrait des paramètres cryptographiques
truqués pour pouvoir après déchiffrer le SNI,
comment est-ce qu'on s'en protège ?
Alors là pour le moment,
je pense qu'il y a des limites au modèle,
les DNS sages c'est...
En fait, ce qui est assez curieux
c'est que je pense que le taux de succès
de DNS sages a augmenté
avec ce l'âge.
Donc peut-être que l'objectif,
peut-être que l'une des conséquences
sera que DNS sages sera de plus en plus populaire

grâce à cette extension.
Aujourd'hui la principale protection
de l'utilisateur...
On parle toujours dans le cadre
de l'utilisation de TLS dans un navigateur
parce qu'il y a plein d'autres utilisations de TLS.
C'est le fait que les navigateurs récents
font du DNS over TLS
et vont résoudre chez Google
ou Mozilla.
Mais ça ne veut pas dire
que c'est relativement facile
de pousser des extensions qui désactivent ça
pour de bonnes raisons ou de mauvaises,
enfin ça se discute.
Du coup, je ne suis pas certain
qu'utiliser le DNS comme medium
pour diffuser les informations
d'initiation de sessions cryptographiques
soit fiable
tant qu'on n'arrive pas à généraliser DNS sages
et on voit que le gouvernement américain
qui avait donné l'objectif, je crois que c'était 2016,
tous les services fédéraux sont sous DNS sages
apparaissent aussi.
Effectivement, il faut bien voir que
DNS n'est pas obligatoire
dans le protocole.
Le protocole ne dit pas que c'est obligatoire,
je suis de façon de le faire.
Je crois que Meta fait des tests
en ce moment en utilisant pas le DNS
mais on pense que ça reste
quand même temporaire.
Donc après, la communauté
va avancer.
Il faut dire que c'est presque un deuxième problème
dans ce qu'il essaie de faire.
C'est pour ça qu'on n'a pas encore trop regardé
là-dedans pour l'instant.
Je pense qu'il y a déjà tellement de trucs
qu'il faut se rendre compte de l'infrastructure
qu'on est en train d'essayer de faire fonctionner.
Donc pour le moment, je pense qu'il essaie déjà

de mettre ça en place.
Et après, chaque problème ne se trouve pas.
Ça fait grosso modo
dix ans qu'Edward Snowden a publié
les documents de la NSA.
Il y en a eu d'autres qui ne sont peut-être pas
publiés, mais grosso modo
il y a un paquet 2013-2014.
On voit que l'IUTF depuis a
drastiquement poussé
l'évolution de TLS
vers la version 1.3
avec beaucoup
d'attention
au fait que les attaques qui avaient été
documentées soient plus faisables.
Les éditeurs de navigateurs eux-mêmes
les principaux éditeurs de navigateurs
de toute façon, ça va être Google,
Microsoft et Mozilla.
Sachant qu'aujourd'hui, à part Mozilla
quasiment tout le monde utilise WebKit
qui est le même moteur que utilisé par
Chromium à Edge Safari.
À peu près.
Tout le monde a adopté ces évolutions
mais
sur ces dix ans
est-ce que
les questions qui se posaient
à l'époque sont toujours d'actualité
et est-ce que quand l'IUTF aujourd'hui
va standardiser en cryptique
Crilentelo, c'est pour se protéger des mêmes choses
que ce qu'avait documenté Snowden
ou est-ce que c'est pour d'autres préoccupations ?
C'est une très bonne question
parce que les dix ans de Snowden ont été célébrés
il y a même un draft RFC
qui a été produit
pour célébrer ça
donc il y a différentes points de vue
les points de vue de Bruce Mayer
le point de vue de Stephen Farrell

le point de vue d'autres personnes
je voyais les noms maintenant
avec différents points de vue
dessus mais en fait
il n'y a pas de grand chose
moi j'ai pas l'impression qu'il y ait grand chose qui est finalement évolué
à part le fait que l'IUTF
a effectivement cherché
à chiffrer de tout en plus
les raisons profondes de ce monde
n'ont pas changé
voire même empiré
la géopolitique c'est pas l'IUTF que je vais mentionner
mais c'est l'Union international des télécoms
où je peux vraiment voir
la géopolitique mondiale
c'est
je pense que c'est plus intense que il y a 10 ans
alors ce qu'il faut quand même voir
et là je préfère être clair avec tout le monde
c'est que moi je suis pas
en position du groupe qui fait tout ça
pour un certain nombre de raisons
qui sont de ma position
et après je peux expliquer
plusieurs détails pourquoi mais
moi je vois quand même beaucoup de soucis
avec ce qui a été fait
là maintenant
donc je peux expliquer
les conséquences d'implication que ça a
dans d'autres sources
et du coup avec le déploiement de CH
est-ce qu'on est safe
c'est à dire justement je le déploie
alors c'est là où j'ai un gros
une grosse question
alors là il faut voir un petit peu
l'évolution qu'il y a depuis
30 ans entre l'IUTF
et les gens qui essaient de la faire la sécurité
c'est que chaque fois que l'IUTF a fait un
protocole
finalement il y a des gens qui ont trouvé des façons

de faire des procès dessus
donc il y a une sorte de course à l'armement
depuis 30 ans
où on n'arrive pas à mettre d'accord
ou au moins à faire en sorte que les gens
ont la sécurité de la vie privée se part
donc il y a un problème de fond
qui est que
la vie privée
si je suis jamais comme une jauge
elle doit être privée mais pour ça elle a besoin
de sécurité
donc la sécurité
quand la vie privée
n'aime pas la sécurité
elle doit donner quelque chose de sensible
à un parti tiers dont elle ne peut pas lui faire confiance
et elle a raison
elle ne peut pas faire confiance à la sécurité
et de l'autre côté
la vie privée a besoin de la sécurité
pour prouver qu'elle est privée
donc on est dans un espèce de chat
de Schrodinger quantique
où on a les deux états en même temps
malheureusement on est dans un mode
où on n'a pas
l'expérience pour les physiciens
ça fait que les physiciens ont vu ce paradoxe
et en même temps ils en ont fait quelque chose
mais nous on n'est pas dans cet état
donc on est dans un état dogmatique
où on a des gens qui ont cassé cette complexité
on a les zélotes de la vie privée d'un côté
et les zélotes de la sécurité de l'autre
on a deux camps qui ne se parlent pas
et malheureusement on n'arrive pas
donc il y a des gens comme moi qui auraient bien voulu
qui est un modèle différent
qu'on appellerait de respectful inspection
dans lequel
premièrement on a une ontologie
de l'interception
qui permettrait de séparer

tout ce qui est au-delà d'interception légale
censure
etc. qui sont des choses différentes
je ne mets pas à l'égal
mais qui sont des interceptions qui veulent être invisibles
d'une interception
qui veut être visible
parce qu'elle a ce chose qui a dit
je n'en ai rien à faire de où vous allez
ce chose que je veux c'est pouvoir vous sécuriser
il n'y a pas de conneries qui vous arrivent
il n'y a pas de mauvaises choses qui sont
donc comme on n'arrive pas à même entrer en matière
parce que moi en tout cas j'ai perdu le consensus
en 2018
sur une sans-histoire que je ne vais pas faire maintenant
on ne peut pas revenir dessus
c'est très difficile de revenir dessus
donc là on a un modèle de sécurité
qui est uniquement un modèle
où on a les éléments de sécurité
sur les deux endpoints
je ne suis pas d'accord avec ce modèle
je peux expliquer pourquoi mais
je n'ai pas gagné cette date
il faut peut-être placer le modèle de menace
grosso modo quand on considère
le modèle de menace sur une connexion
TLS
on a d'abord le SIGINT
l'observation passive
qui est un état ou un adversaire
qui observe la communication et qui en déduit
ce que vous faites et qui va l'utiliser
contre vous
donc ça depuis SSL.3
quelque chose
il n'y a plus vraiment de gros attaques qui permettent
de déchiffrer le contenu des communications
mais en revanche il y a la capacité
de savoir ce que
vous visitez
pas le détail du chemin mais le site que vous visitez
et c'était à cause du SNI

il y a un modèle d'interception
silencieuse
pardon qui était tous les procs si invisibles
en fait qui est
ce qu'on pouvait faire sur son réseau
et qui marche de moins en moins avec TLS 1.3
enfin plus avec TLS 1.3
qui est de rediriger silencieusement toutes les connexions
HTTPS vers un proxy
et que le proxy
termine la connexion SSL
qui l'établisse pour vous vers le serveur destination
et du coup
voit le contenu de la connexion TLS
et soit capable d'analyser ce contenu
et éventuellement faire du filtrage antiviral
du DLP
et toute forme de protection
alors que ce soit vous utilisateurs
ou votre organisation qui soit protégée
pardon
il y a la protection contre l'injection
quelque chose qui est important
et qui en particulier a été documenté
d'abord dans les leaks nodens
mais on a pas mal d'attaquants qui utilisent ce genre de choses
je sais pas, un des plus connus
c'était Mosquito
de Turla donc un attaquant suposé russe
qui injecte des réponses malveillantes
dans un trafic légitime
il y a aussi tout un tas d'attaques
en particulier qu'on voit
peu en France mais qu'on voit chez les fournisseurs
d'accès internet aux Etats-Unis
qui est de l'injection de publicité dans du trafic légitime non chiffré
et puis
il y a
l'usage
de l'analyse de vos communications
pour essayer de déterminer
en aveugle ce que vous faites
et puis de l'autre côté
le côté protection c'est se protéger

contre une infection qui arrive sur le poste de travail
ou une attaque
qui peut être fichine aussi
depuis une adresse illégitime
et qui nécessite
d'inspecter le trafic enfin
en tout cas de savoir ce à quoi vous vous connectez
pour le comparer à soit des motifs
soit des bases
d'homènes ou de sites
ou des motifs du RL malveillant
qui
permettent de déduire que vous êtes en train de vous faire avoir
et que votre poste va se faire compromettre
et clairement
si on chiffre la connue question de bout en bout
la sécurité elle est entièrement
dans le navigateur parce que tous les intermédiaires
sur le réseau peuvent plus le voir
il y a quand même une exception
c'est si je positionne explicitement une configuration
de proxy dans mon navigateur
jusqu'à présent même en TLS 1.3
je peux faire de l'inspection de trafic
sur le proxy qui est configuré
donc qu'est ce que ça change ?
alors
ça me fait que j'ai pas fini la réponse
à Paul mais d'abord
répondre à ça
alors la différence c'est
qu'il y a le mode transparent
et le mode explicit
le mode explicit
il faut bien comprendre parce que les gens me disent
effectivement mais non on s'en fiche
on a un proxy explicit donc on peut continuer à se défendre
mais vous ne pouvez plus
alors pourquoi vous ne pouvez plus c'est que quand on est
en mode explicit sans CAH
qu'est ce qui se passe ?
j'ai mon navigateur qui va dire
au proxy j'aimerais que toi tu te connectes
pour moi à l'autre bout donc

entre mon navigateur
et le proxy quelque part on s'en fiche
en TLS 1.2
c'est pas grave et après
le proxy lui va faire les choses comme il faut
bien l'extérieur
alors ce qu'il faut bien comprendre c'est que quand on commence
tu te connectes
avec la destination
exemple.com qu'on passe
au serveur donc le serveur après s'en fiche de ce qu'il y a derrière
lui il sait qu'il doit aller sur exemple.com
le petit problème c'est que
quand maintenant on passe en le CAH
c'est une navigateur
il veut faire un TLS 1.3 avec le CAH
mais évidemment pour rester cohérent
il ne va plus passer
exemple.com dans le HTTP connect
ce chose qu'il peut passer c'est
le client facing server
donc le proxy
qu'est-ce qu'il fait il voit arriver
pas sur client facing server
mais je peux rien en faire du client facing server
et c'est là où ça dérape
donc c'est bien pensé parce que là
effectivement
tous les gens qui imaginent qu'ils vont pouvoir encore faire
la défense avec un client facing server
avec un explicit proxy
non ça ne marchera plus
votre défense se fera percer
de bout en bout
et est-ce qu'il y a un moyen
ou est-ce qu'il y aura plutôt un moyen
de dire aux navigateurs
de ne pas utiliser le CAH
mais de rester sur un mode
traditionnel
c'est une bonne question
mais je n'ouvre pas la question de Paul
je vais d'abord répondre à Paul
et je vais revenir après nos yeux

donc Paul tu disais mais est-ce qu'on est protégé finalement
moi je pense que la réponse est non
dans cette course
à l'armement
à chaque fois un parti a réussi
à brêcher le protopole
je pense qu'il y a des armées
qui sont suffisamment fortes
qui vont réussir
à brêcher le protopole
je ne demande pas comment
c'est purement spéculatif
mais je suis convaincu qu'il y en a qui vont réussir à le faire
je connais un petit peu le monde de l'interception légale
parce que j'ai dû implémenter d'interception légale
dans des pays responsables
comme la Suisse et l'Allemagne
je sais comment ça marche
je sais la puissance de feu de ces communautés
c'est quand est-ce que ça arrive
ce qui veut dire que
les gens qui pensent qu'en faisant OCH
ils vont réussir à protéger les gens
non, ils leur montrent
je pense qu'à un moment donné
les gens vont croire qu'ils sont protégés avec OCH
mais ils ne le seront pas
c'est mon opinion personnellement
pour revenir à ce que disait Joanne
qu'est-ce qu'il y a comme possibilité
la possibilité il faut remettre dans le contexte
pourquoi est-ce qu'on pose la possibilité
est-ce qu'on peut mettre au sel ou pas
alors, avant que je réponde à ça
il faut que j'explique qu'il y a effectivement un problème
parce qu'on a des gens
les droits de l'homme qui quand même
contrôlent l'IOTF
pratiquement tous les éléments de l'IOTF
il faut quand même voir qu'il y a un point de contrôle important
à l'IOTF par les gens
par une partie des gens les droits de l'homme
c'est pas ma partie
je suis très pro

droits de l'homme mais pas comme ça
et c'est des gens qui ont une approche
les seuls qu'il faut protéger c'est les dissidents
et les groupes fortement discriminés
parce que je comprends qu'il faut les protéger
mais en revanche
ce qu'ils ont beaucoup de problèmes
à considérer c'est que
il n'y a pas que ces gens
on a les enfants
qui se connaissent en ligne
on a le système éducatif
qui a besoin de protection
on a les entreprises qui ont besoin de se protéger
et là aujourd'hui c'est des communautés
il y en a d'autres
qui aussi ont des droits
et aujourd'hui le problème c'est que
ces gens là si on leur met au CH
ils ne peuvent plus faire la défense comme une fois
aujourd'hui en Royaume-Uni
par exemple
les gens qui font du chaine de protection
c'est pratiquement obligatoire de le faire par le réseau
il y a des
grosses incitations pour que
les opérateurs mettent en place
des systèmes de protection
qui disent oui on peut le faire aussi
sur l'on point c'est aussi possible
j'étais chez Norton avant donc je sais très bien
qu'on peut le faire sur l'on point mais je sais aussi les limites que ça
donc tout est-il que
là on est en train de retirer un moyen
donc le problème c'est que
on a
des gens qui sont les droits de l'homme qui ont une vision
très particulière en disant
c'est
le prix éthique
à payer est tellement fort
qu'on doit faire un sacrifice
donc ils n'ont pas peur
de ne pas fournir de solutions

et de s'attendre d'autres communautés
les systèmes des écoles aujourd'hui
par exemple s'ils ne montrent pas qu'ils ont une défense
contre les sites
c'est pas que les expériences de sites pornographiques
ça peut être des sites par exemple
d'humiliation, de suicide
d'harcèlement etc
c'est un certain nombre de choses et bien
dans certains pays les écoles n'ont pas les subsides
de l'état donc ils ne peuvent pas payer pour pouvoir
faire avancer parce qu'ils ont besoin
donc c'est pas que je ne dis pas qu'il n'y a pas des alternatives à tout ça
mais
on est en train de prendre en étranglement un certain nombre
de groupes
qui elles
d'abord ne sont pas au courant
le premier problème c'est que personne n'est au courant
j'expliquerai après le rôle
des mauvais acteurs là-dedans
mais donc déjà là on a un certain nombre
de problèmes, il faut quand même faire quelque chose
alors en plus
on a les bad guys
alors voilà le problème que moi j'ai
ça ça me chagrille beaucoup plus
c'est que je suis un agent
qui minait, l'IOTM vous êtes en train
de me dire, vous êtes en train de faire un protocole
qui permet de cacher la destination
et quand le protocole n'est pas là
vous envoyez des écrans de fumée pour faire croire
qu'on comprend
de me cacher mais on a un deal
on a un deal
moi je se fais du ransomware
tout mais quand on a le contrôle je les passe
par au search, garantie
donc
le petit problème qu'on a c'est qu'il faut
quand même voir que le chiffrement
n'est pas égal à la sécurité
ça c'est une illusion

les gens qui sont en IOTF
ont très peu de connaissances de
ce qu'on appelle la sécurité opérationnelle
donc ils ne comprennent pas ça
ils veulent pas l'entendre parler parce que pour eux le filtrage
est mauvais
alors quand on est en train d'effondre c'est quand on a un ransomware
il n'y a plus que sur un lien parce que c'est arrivé
à certains de mes clients
ils ont failli perdre
leurs subsidiaires pour un vieil de 3 milliards d'euros
à 30 ans d'existence
et que vous avez un seul lien qui tient pour le backup
qui est en train de nous attaquer
je vous jure que là
IOTF peut IOTF filtrage pas filtrage
il va falloir faire quelque chose
donc on a un gros problème entre
des communautés qui ne veulent pas se comprendre
aujourd'hui mais là effectivement
il y a un souci
si je suis dans le monde entreprise
je peux faire plusieurs choses
d'abord je peux essayer
de désactiver les options OCA
dans les navigateurs si je les contrôle
je suppose qu'on peut trop c'est une point
parce que là je peux le faire
c'est une première chose
ça a plein de limites parce que ça ne marche pas
pour le bring your own device
ça ne marche pas non plus
comme le disait Paul je crois
parce qu'il n'y a pas que
les navigateurs en TLS
il est utilisé par des applications
et vous êtes sûrs que les gens qui vont écrire des applications
ils vont embarquer les librairies TLS
avec OCA sans même s'en rendre compte
ça ne sera pas optionnel
et puis troisièmement
il y a les navigateurs c'est pas dit
qui vont le laisser
en mode optionnel

nous quand on a démarré cette histoire
chez nous c'est parce que je me suis réveillé un jour
l'année dernière en janvier
2022 en réalisant
que Chrome allait partir avec CH
en force
j'ai eu de la chance j'ai pu contacter Kenji Bae
qui est le product manager
de Google
de Chrome
qui était français on a discuté
une très bonne discussion et puis
il y a d'autres forces qui ont fait qu'ils ont rendu ça optionnel
mais c'est temporaire
les navigateurs un jour vont peut-être le changer
c'est obligatoire
et quatrièmement
on a le malware
qui lui il ne va pas jouer par ses règles
ça c'est la première chose
la deuxième chose qu'on peut faire
c'est
si on contrôle son DOH server
et là c'est un petit peu plus puissant
on peut faire des ressources et corp
si je coupe les ressources et corp
je désactive
ECH par force
et du coup s'il n'y a pas les ressources et corp
les navigateurs ou autres ne peuvent pas engager
en fait on voit bien
il y a clairement une question
en qui j'ai confiance
est-ce que j'ai confiance dans mon organisation
qui m'a fourni un poste de travail avec sa configuration de proxy
est-ce que j'ai confiance de mon fournisseur
d'accès internet à sujet T
à mes lois locales
j'ai confiance en fait dans un GAFAM
qui fournit le gros de l'hébergement sur internet
et dans les gros CDN
qui sont tous américains
qui plus est aujourd'hui
les organisations de droit de l'homme

se reposent sur le fait que les Etats-Unis
est un des pays les plus libéraux le monde
mais rien de garantit que le gouvernement américain
n'évolue pas dans les prochaines années
dans quelque chose d'un petit peu plus
fondamentaliste chrétien par exemple
du coup
est-ce qu'on n'a pas déjà perdu cette bataille
d'acteurs qui fournissent des navigateurs
et qui ont franchement décidé que contrôler
le navigateur et le serveur c'était plutôt leur truc
Très bonne question
et
là pour expliquer un petit peu
il faut redonner un peu de
d'écosystème
il n'y a pas que les fournisseurs de navigation
ce qui me pose beaucoup plus de problèmes
c'est les CDN
alors les CDN
d'abord il faut voir que c'est une population
très particulière
il faut voir que c'est une population
qui a
quand même
réalisé un coup
qui est de pratiquement créer
ce qu'on pourrait appeler le layer 9
donc on avait le layer 7, on connaissait bien
le layer 8
c'est un petit peu tous ces gens
qui ont réussi à sortir du layer 7
vers un nouveau monde
il y a Google
d'autres
et
le problème c'est que tout ça c'était dans un modèle d'internet
qui était N2N
sauf qu'il y a des petits malins qui s'appellent les CDN
qui ont changé ce paradigme
dans un paradigme H2H
et par effet de gravitation
ils ont commencé à déformer le champ
de gravitation d'internet

donc ce layer 9
les CDN, le problème c'est que
quand on regarde
on s'est posé la question, il y a un universitaire
très brillant, il y a l'OTF de San Francisco
qui a fait une très belle plantation sur la fragmentation
mais en finant
je comprends pas ce que c'est que la fragmentation
parce que mes données me disent que le monde n'est pas fragmenté
le monde est essentiellement US
et quand ils montent
toutes les capacités qui sont offertes
aujourd'hui, elles sont essentiellement
à plus de 60% jusqu'à 90%
offertes par des boîtes américaines
ça veut dire que aujourd'hui ce défaite de gravitation
il est essentiellement centralisé
sur les CDN et dans les CDN
sur un acteur
donc la vraie question qui se pose
d'abord, c'est pourquoi on a aussi peu de diversité
qui pose la question
alors, ce que je vois
c'est qu'on a un phénomène de centralisation
qui est aussi un phénomène
qui est un effet perverte
de la standardisation
dans les standards, quand on les écrit
on peut permettre
plus de choses pour certains groupes
que d'autres
j'ai qu'un certain standard, tu prends iMap par exemple
iMap a permis beaucoup de centralisation
c'était un effet de voir
d'autres standards, c'est pour ça que les droits de l'homme sont là
ils ont compris que certains standards
peuvent être plus favorables
à certaines idées des droits de l'homme
par rapport à d'autres
avec l'objectif, il ne faut pas oublier
la standardisation
elle est derrière la réglementation
je ne peux pas acquier de réglementation
si je n'ai pas de standard technique derrière

les deux sont deux roues
qui se lient
parce qu'on appelle l'harmonisation
je suis dans la réglementation X
je le fais par le processus d'harmonisation
une européenne, je crois que ça s'appelle l'OL5
c'est le processus qui permet
de faire cette harmonisation
donc il y a des gros effets qui se passent
donc le problème pour en venir, la question c'est que
les gens qui font les navigateurs
je comprends très bien pourquoi ils le font
mais les gens qui font les cdn
ils ont un intérêt beaucoup plus important
parce que quelque part
ils permettent de changer
le marché d'un point vers l'autre
si je suis cdn
et que je vois le sni
je peux appliquer
toute une sac de sécurité
mais je ne permets plus aux autres de le faire
là on va avoir un problème
de dominance de marché
de dominance de marché
il se gère par d'autres
pour le moment c'est de dire attention
c'est pas que les navigateurs qui font ça
c'est d'abord
je pense que c'est les plus puissants
sur ce sujet c'est les cdn
je ne suis pas sûr d'avoir bien saisi
ça veut dire que les cdn
qui sont essentiellement américains
ils pensent qu'ils vont être les seuls
à pouvoir faire une analyse du contenu
que ne pourront pas faire
tous les acteurs actuels
bien connus en diverse sécurité
ça montre
ça met en évidence ce point
mais en évidence en fait une lutte qui a
commencé il y a quasiment une décennie
et d'ailleurs qui est intéressante parce qu'on la voit

entre l'ITU et l'UTF
qui est la force des pays
des nations
contre la force
de ce qu'a représenté l'internet
qui est de droit américain quasiment depuis le début
et où il y a une très forte
prévalence des acteurs américains
ça fait quelques années
que des pays
dont on n'aime pas
en Europe et aux Etats-Unis
la relation au droit de l'homme
comme le son, la Chine, la Russie,
l'Arabie Saoudite etc
on découvre qu'à travers
que l'ITU qui est une agence
des Nations Unies, il pouvait avoir une influence
sur des standards
l'UTF
c'est avant tout quelque chose de plus ouvert
mais qui est dominé par les acteurs qui peuvent faire
et les américains ont été très dominants
là dessus et les entreprises américaines
ont été très dominantes historiquement dans ce domaine
et en particulier aujourd'hui
les acteurs, clairement les acteurs du cloud
je veux dire il y a des standards comme
HTTP2 et HTTP3 qui ont essentiellement
d'intérêt si on a des millions de sites
si vous hébergez 10 sites
ça n'a aucun intérêt
cette évolution aujourd'hui
elle fait qu'il y a un clash et qu'il y a
les tentatives de restructurer
ce que c'est que le réseau international
et ce que c'est l'internet entre ces deux optiques
la force des nations
et la force de l'UTF
et des standards qui sont essentiellement
basés aux Etats-Unis
on a bénéficié pendant
ces 30 ou 40 dernières années
le fait qu'on bénéficie

d'un accord
grosso modo sur les valeurs
avec les américains
à quelques détails prêts par exemple
les américains ne considèrent pas que censurer
les publications nazies c'est une bonne chose
alors qu'en France ou en Allemagne
c'est complètement interdit
mais globalement sur les valeurs humaines
protection des minorités etc on a partagé
la même vue et le fait que
les principaux acteurs de l'internet soient américains
a bénéficié à nos vues
aujourd'hui on a la Chine, on a la Russie
on a tout un acteur dont on parle moins
qui ont des milliards d'utilisateurs
mis bout à bout
si vous regardez ce qui est censuré en Inde
ce n'est pas forcément votre vision
de ce que l'internet devrait être non plus
on n'en parle pas
parce qu'on parle beaucoup de la Chine
et des pays du golf mais ça reste problématique
et on se retrouve dans
une tension qui descend
aujourd'hui dans la technique
je crois que c'est Borts-Mayors qui a publié
un livre qui défend l'idée que les choix techniques
sont des choix politiques
et là on est typiquement là dedans
ou en fait si on a un tunnel
opaque entre le navigateur
et les ressources web
eh bien on a
une force énorme
sur ce que vous voyez, sur ce que vous choisissez
sur ce que vous ne voyez pas
des gens qui opèrent les sites web
ou du moins le point auquel vous vous connectez
l'internet Facing
Server
sur ce que vous voyez et aujourd'hui
ils sont tous à sujet
la loi américaine

et si la loi américaine évolue
eh bien on peut imaginer une divergence
entre les valeurs européennes
françaises
mais globalement européennes
et les valeurs américaines
et dans ce cas là on va avoir
des questions à se poser
sur qui est légitime
ou pas dans ce que l'on a fait
on peut le voir directement aujourd'hui
à la France qui décide de bloquer
l'accès à certains sites
mais si votre navigateur se connecte
fait du DNS
aujourd'hui c'est essentiellement par du masquage
du site DNS, de la redirection du black oling
si votre DNS va directement chercher
sur 8888 qui est chez Google
ce filtrage est inopérant
alors
le problème que ça pose
c'est que c'est pas seulement l'UIT
parce que l'UIT j'ai un rôle
j'ai des rôles extrêmement forts
l'UIT dont je connais très bien
le truc c'est
c'est un problème d'état mais ça a bien au-delà de l'UIT
prends par exemple la réglementation
d'ORA
c'est la réglementation de l'UE
qui
va forcer tout le monde
financier
à appliquer un
risk-management et d'autres choses
c'est très intelligent
d'ORA et c'est très bien fait je pense
c'est une très grosse réglementation qui va arriver
le 17 janvier
et qui est sur la Digital Operational Resiliency Act
donc c'est un problème de résilience
en gros une européenne veut faire en sorte que
tout son

secteur financier
européen ou ceux qui opèrent en Europe
soit extrêmement résilient
et l'article 1.1
il parle de quoi
sécurité des réseaux
et des systèmes d'information
or le problème qu'il y a
avec ça c'est que
le CH empêche de faire c'est ce qu'on appelle
du déchiffrement sélectif
c'est quoi le déchiffrement sélectif
c'est de dire aujourd'hui
quand je suis dans une entreprise
ben quand je
voie passer mon trafic je veux pas tout intercepter
si l'utilisateur va sur game.com
je m'en fiche
sur sa banque je m'en fiche
par contre ce qui est dans la politique
je vais pouvoir faire deux choses
tout ce qui est bien un site
qui est douteux
c'est au scanner
et tout ce qui est en data loss prevention
si j'en vois que sur box.com
je veux faire en sorte que
il n'y ait pas de bêtises qui sortent
souvent c'est des bêtises
on met un fichier qu'on ne devrait pas
sur box.com ou sur d'autres sites
donc quand on s'est acheté en place tout ça c'est mort
ça veut dire que
si je suis une banque ou une entreprise
et que je dois faire ça pour des caissons
de conformité je ne peux plus le faire
donc imagine
le problème que moi j'ai avec mes clients
c'est que je ne vais pas jouer au dé
avec leur sécurité
je ne veux pas me permettre
que tout d'un coup il y ait tout des flux qui partent
ils ne peuvent pas les contrôler
pendant leur sécurité ou ils vont se taper

des amores d'énormes parce qu'ils ne peuvent pas
accomplir l'RGDP
ou les droits
ou toutes les choses qu'ils vont devoir faire
la NIST, la DIS2 etc etc
je ne parle pas de CRA et des autres choses qui sont en train
donc on a quand même un gros clash
on reprend ce que disait Christophe entre effectivement
une vision gouvernementale des choses
et une vision IETF des choses
derrière c'est quand même une vision très fortement liée
au droit de l'homme parce que les CDN
ils bénéficient quand même d'une rhétorique
fantastique
ils n'ont pas besoin de se justifier
pour pouvoir faire les choses
moi par contre quand je prends le micro à IETF
j'en prends plein la tranche mais ça c'est autre chose
et finalement on en revient sur la remarque de Christophe
derrière
Cuit de l'adoption qui va y avoir
6 mois, 1 an, 3 ans, 5 ans
c'est à dire que vu finalement
je veux dire des risques
potentiellement pris avec la mise en place de
je veux dire de CH
peut-être que l'adoption va être
complètement minime voire inexistante
dans les prochains mois
alors je pense
c'est ça aussi Paul parce que je ne pouvais pas y croire
quand j'ai vu de CH arriver
pas comme ça, pas dans ce modèle-là
non je pense que l'adoption va être
très forte
ce qu'il faut voir c'est
on va reprendre les jeunes titres de données historiques
quand TS1.3 est arrivé
il était à 0% en 2018
le décollage
c'est une ligne constante
sur 4 ans
en 3 ans il dépassait TS1.2
et en 4 ans il domine complètement

c'est à dire qu'on est sur une adoption
qui prend à peine quelques années
il faut voir qu'il y a
quand même un grand nombre de parties
des gros partis qui ont fait un investissement
qui sont gigantesques
mais colossales
et donc ils vont
voir ce qu'on appelle
le retour sur investissement
donc où on en est aujourd'hui
d'abord le protocole
je pense qu'il va bientôt être ratifié
il sera ratifié à mon avis avant l'été prochain
pourquoi je dis ça c'est parce que
en Champlain d'An je vois très bien
les activités qu'il y a sur le GitHub
qui gère le draft CH
là j'ai été bombardé
de notifications
sur les derniers jours
mais je vois beaucoup
d'activités comme l'IETF 118
va se passer à Prague
début novembre
à mon avis on va voir
une demande pour faire un last call
donc la communauté va dire on veut faire un last call
ils vont voter
la réponse sera oui
et donc ils vont lancer le last call
ça veut dire que c'est une procédure
où ils vont commencer à faire la fin
du développement
ils vont être en last call
et après le last call il y a ce qu'on appelle usg
donc usg c'est l'ensemble
des areas directeurs
de l'IETF qui vont commencer
à regarder tout ça
et le problème c'est qu'ils doivent
quand même aligner un certain nombre de textes
parce qu'il n'y a pas qu'och
il y en a plusieurs textes qui sont interdépendants

entre eux c'est ça leur complication
ça c'est une chose
donc à mon avis je pense que
en parlant avec les présidents
du groupe tls
on est un peu pressur
que si ils lancent maintenant
si toutes les lunes étaient alignées
il leur faudrait 5 mois
donc 5 mois on va se retrouver au mois de mars
on va leur donner jusqu'à l'été
par contre
comme ils contrôlent tout
ils savent que le moment où ils appuient sur le bouton
ils sont sûrs d'arriver au bout
donc qu'est ce qu'on voit
par contre au niveau de l'implémentation
c'était en prod
ça c'était il y a 15 juin
4 flair a annoncé qu'ils partent en prod
ils ont essayé
ils ont lancé ça a merdé
ils vont revenir mais peu importe
ils sont pratiquement
faut quand même voir aujourd'hui que les russes
les chinois et les iraniens
bloquent déjà des flux le ch
crohn nous a annoncé
qu'ils sont déjà à plus de 1% d'utilisation
de ch
et ça c'était au mois de juillet
on va être déjà à plus
donc ce qu'il faut voir c'est que
tous ces acteurs ne vont pas attendre la ratification
pour que ce soit implémenté
c'est déjà implémenté
et ce que je comprends pas c'est
ce que je comprends pas c'est que
moi je connais l'ITF
d'une autre époque parce que j'ai
j'ai fait tous les ITF
de 98 à 2002
et à l'époque
j'avais vu une forte évolution

avec une participation asiatique
avec les chinoises en pleine explosion
et là tu me décris un ITF
comme si on était au début
des années 90
ou 2000
donc je...
mais je comprends pas
les chinois ils jouent
quel rôle
ou aucun rôle
parce que
parce que qu'est ce qu'ils
pensent de cette évolution
protocolaire
alors c'est aussi une très bonne question
les chinois sont très présents à l'ITF
mais ils ont entre guillemets d'autres chats à fouetter
les chinois ils ont un autre gros problème
c'est de positionner new IP
un new IP c'est...
ça viendra plus tard
dans toutes les évolutions qu'on a en ce moment
il y a un très gros changement qui est prévu
qui s'appelle new IP
que les chinois ont poussé en regardant
ce que les eurequois avaient fait avec
une résolution
et ils ont essayé de le pousser
en 2019
à l'UIT
et on l'a repoussé
ils ont essayé de le passer en force
d'une façon très bizarre à l'ETI
et ça a été repoussé on s'en a aperçu la dernière minute
et ils ont essayé de le pousser à l'UTF
et on l'a repoussé aussi
finalement ils sont arrivés à l'UTF
avec ce qu'on appelle le working group 4
donc tout ça c'est quoi
c'est sympa d'essayer de vouloir fixer BGPA
et de changer
il y a un grand nombre de choses sur internet
avec l'identification de devices

avec tincements sur deux choses
on va pas faire le sujet maintenant
ça peut être le sujet dans notre podcast
mais les chinois ils sont très occupés par rapport à ça
alors maintenant si on est cynique
moi je serai chinois au russe
j'attends qu'une seule chose c'est que
tout ça ça se termine
quand je voudrais faire mon propre CDL
mon propre affaire
j'ai tout ce qu'il faut pour centraliser et contrôler ensemble
ah non on a probablement pas fait le tour de la question
mais est-ce que tu voudras porter le mot de la fin ?
alors le mot de la fin que j'ai
c'est
moi j'espère qu'un jour on arrivera
à
faire se rejoindre les deux communautés
de la vie privée et de la privacy
de la sécurité parce que je pense qu'on en a absolument besoin
et je pense que
les gens qui reprochent aux gens de la sécurité
d'être man in the middle
moi je peux dire aux gens qui vont faire
ce monde là
mais qu'allez vous faire quand vous aurez man in the browser
vous ne pouvez pas
avoir le navigateur comme jugé parti
donc si je prenais une analogie
avec le corps humain
les gens
qui sont dans mon opposition ils rêvent
d'un modèle qui soit purement lié à une sécurité
qui ressemble au système immunitaire
ils voudraient ne plus avoir
en gros ne plus avoir de médecins
de médicaments etc.
c'est vrai ou pas leur faire confiance
c'est ça qui t'entendu
moi ce qui me gêne dans tout ça c'est que
le CH va trop vite
les gens ne sont pas au courant
les gens qui font du malware
passons par le CH

ça c'est garanti je peux vous le prouver
pour faire des commandes contrôles
et le problème c'est qu'on va arriver
dans un modèle dans lequel
on va tuer un modèle de défense
petit à petit
et donc c'est assez bizarre
parce que le corps humain a mis
des millions d'années pour se faire
nous on joue au modéus
et en 50 ans on a fait un Frankenstein
donc comment est ce qu'on va faire
pour pouvoir s'occuper de ce Frankenstein
sans médecins, sans médicaments
et sans psychanalyste
c'est ce qu'on veut de la sorte
l'image est intéressante
en tout cas le sujet est passionnant
merci beaucoup Arnaud d'avoir accepté
notre invitation
merci aux contributeurs
nous espérons que cet épisode vous aura intéressé
et nous vous donnez rendez-vous la semaine prochaine
pour un nouveau podcast
au revoir