ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité »
Lundi 13 Janvier 2025

La distribution de l'heure exacte, un sujet crucial mais méconnu

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 2 Cybersécurité et E-santé U. Paris Cité

SOMMAIRE

Introduction

Le temps est une ressource stratégique fondamentale, souvent sous-estimée mais essentielle à de nombreux secteurs clés comme les transports, la finance, les télécommunications et la défense. Pourtant, les moyens actuels de mesure et de distribution du temps sont confrontés à des vulnérabilités grandissantes qui peuvent avoir des conséquences majeures sur la sécurité et le bon fonctionnement de nos infrastructures critiques.

Lors de cette édition des « **Lundi » de la cybersécurité »**, organisée par l'Université Paris Cité en partenariat avec l'ARCSI, Gérard Berry, professeur émérite au Collège de France, a proposé une analyse approfondie de ce sujet à travers l'histoire, en mettant en lumière les avancées scientifiques majeures, les défis liés à la distribution du temps et les menaces spécifiques à notre époque. De plus, cette conférence a abordé les réponses françaises, notamment avec la solution **SCPTime**, visant à renforcer la souveraineté et la résilience de notre système temporel face aux attaques potentielles.

Cette session a également inclus une intervention du **Cercle des Femmes de la Cybersécurité (CEFCYS)**, mettant en avant l'importance de la diversité et de l'inclusion dans le domaine de la cybersécurité. Le CEFCYS a présenté ses initiatives pour promouvoir les carrières dans cette filière, notamment à travers des programmes de mentorat, des événements de sensibilisation et des actions concrètes pour attirer davantage de talents féminins.

En rassemblant experts, professionnels et étudiants, cette édition des « Lundi~~s~~ de la cybersécurité » a permis non seulement d'éclairer un enjeu technique et stratégique souvent méconnu, mais aussi de promouvoir une vision inclusive et collaborative pour relever les défis actuels et futurs de la cybersécurité

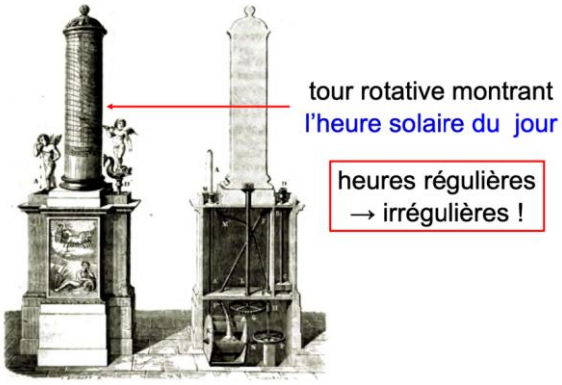
I. Bref survol de la mesure du temps à travers les âges

Gérard Berry a débuté son intervention en retraçant l'évolution historique de la mesure du temps, qu'il a décrite comme un enjeu scientifique et pratique qui a marqué toutes les civilisations.

Il a expliqué que dans l'Antiquité, les premières méthodes de mesure du temps reposaient sur l'observation directe de phénomènes naturels, comme les cadrans solaires, qui utilisaient l'ombre projetée par le soleil pour indiquer l'heure. Cependant, il a souligné que ces instruments, bien qu'ingénieux, souffraient de nombreuses limitations, notamment leur dépendance aux conditions météorologiques et leur manque de précision.

Le Professeur Berry a poursuivi en expliquant que la clepsydre, une horloge à eau utilisée à la même époque, représentait une tentative d'introduire une régularité dans la mesure du temps. Cependant, cette technologie restait limitée à des usages locaux et ne permettait pas de synchroniser des activités à grande échelle. Il a insisté sur le fait que le temps, à cette époque, était essentiellement une notion locale, suffisante tant que les activités humaines restaient confinées à de petits périmètres géographiques.

La clepsydre de Ctésibios, Athènes, −270



Le Professeur Gërard Berry a ensuite abordé l'ère des grandes découvertes maritimes au XVII^{e} siècle, où il a expliqué que la mesure du temps est devenue cruciale pour résoudre le problème de la longitude. Selon lui, il était impossible de déterminer avec précision la position d'un navire en mer sans une horloge fiable capable de maintenir une précision à la seconde près. Il a évoqué les travaux de John Harrison, qui a conçu des horloges marines révolutionnaires, et a expliqué comment ces inventions ont permis de transformer la navigation et d'accroître la sécurité en mer.

2 Novembre 1707, naufrage massif : mauvaise estimation de longitude

Dans son exposé, Gérard Berry a également mis en lumière l'impact de l'industrialisation au XIX^{e} siècle sur la standardisation de la mesure du temps. Il a rappelé que, jusqu'à cette époque, chaque ville fonctionnait selon son heure locale, mais que l'apparition des chemins de fer a rendu cette fragmentation temporelle intenable. Il a expliqué que la nécessité de coordonner les horaires des trains pour éviter les accidents a conduit à l'adoption des fuseaux horaires et au temps moyen de Greenwich (GMT) comme référence internationale. Cette période a marqué un tournant majeur dans l'uniformisation de la mesure du temps.

Enfin, le Professeur Gërard Berry a évoqué le XX^{e} siècle comme l'époque où le temps est devenu une ressource économique et stratégique. Il a décrit comment les horloges ont été utilisées pour organiser le travail dans les usines et mesurer la productivité des ouvriers, une pratique qui a profondément influencé les sociétés industrielles. Il a souligné que cette obsession pour la précision et la synchronisation s'est intensifiée avec l'émergence de technologies comme les télécommunications et l'informatique.

II. Les méthodes modernes de distribution du temps

Lors de son intervention, Gérard Berry a présenté les principales méthodes modernes utilisées pour mesurer et distribuer le temps, tout en soulignant leurs forces et leurs limites. Selon lui, ces systèmes jouent un rôle fondamental dans le fonctionnement des infrastructures critiques et des technologies qui façonnent notre quotidien.

Il a commencé par expliquer que la méthode la plus répandue est l'utilisation des **systèmes de navigation par satellites**, tels que le GPS, Galileo ou encore Glonass. Ces systèmes, extrêmement précis grâce à leurs **horloges atomiques embarquées**, permettent de synchroniser des milliards d'appareils dans le monde. Cependant, Gérard Berry a mis en garde contre leur **vulnérabilité au brouillage et au leurrage**. Ces attaques, de plus en plus fréquentes, consistent soit à bloquer les signaux pour empêcher leur réception, soit à manipuler ces signaux pour induire des erreurs de localisation et de synchronisation. Il a mentionné des exemples récents où des aéroports et des infrastructures critiques ont été perturbés par ces techniques.

Formatted: Font: Bold

Horloges atomiques

En complément des satellites, Gérard Berry a détaillé l'utilisation du **protocole NTP** (Network Time Protocol), un système largement utilisé pour distribuer l'heure via Internet. Bien que pratique et accessible, il a souligné que ce protocole est moins précis que les GNSS et présente également des failles de sécurité. Selon lui, le NTP peut être compromis par des attaques qui altèrent les données transmises, ce qui peut avoir des conséquences graves, en particulier dans les environnements où la précision temporelle est essentielle, comme les data centers ou les systèmes financiers.

Gérard Berry a ensuite abordé des technologies plus résilientes, comme **la distribution du temps via des fibres optiques dédiées**. Ces infrastructures permettent de transmettre des signaux temporels avec une précision exceptionnelle et une meilleure protection contre les interférences extérieures. Cependant, il a noté que leur déploiement reste limité à des cas spécifiques, en raison de leur coût élevé et de leur complexité d'installation.

Il a également évoqué les **émetteurs radio longue portée**, qui étaient autrefois largement utilisés pour diffuser l'heure. Bien qu'ils soient moins répandus aujourd'hui, ces systèmes offrent encore une alternative viable dans certains contextes, mais ils sont énergivores et sensibles aux perturbations.

Pour conclure cette partie, Gérard Berry a insisté sur **l'importance de combiner plusieurs méthodes pour renforcer la résilience des systèmes de distribution du temps**. Il a expliqué que la dépendance excessive à un seul système, comme les **GNSS**, expose les infrastructures critiques à des risques importants, et que des solutions hybrides, intégrant fibres optiques, satellites et technologies locales, doivent être développées pour garantir une synchronisation fiable et sécurisée.

Cette réflexion a ouvert la voie à une discussion plus approfondie sur les **enjeux de cybersécurité liés à la distribution du temps**, qui seront explorés dans les parties suivantes.

III. Enjeux de la cybersécurité temporelle

Dans son intervention, Gérard Berry a mis en évidence les nombreux **défis liés à la sécurité de la distribution du temps**, un enjeu souvent sous-estimé mais critique pour les infrastructures modernes. Selon lui, la dépendance croissante de notre société à des systèmes de synchronisation temporelle, comme les satellites GNSS ou les protocoles NTP, expose nos infrastructures à des **menaces cybernétiques graves**.

Il a commencé par expliquer que les **systèmes GNSS**, utilisés pour fournir une synchronisation précise à l'échelle mondiale, sont particulièrement vulnérables. Ces systèmes peuvent être perturbés par des attaques de **brouillage**, où les signaux satellites sont bloqués ou masqués, rendant les récepteurs incapables de déterminer l'heure ou la position. Il a également évoqué les attaques par **leurrage**, où des signaux falsifiés induisent volontairement des erreurs de localisation ou de synchronisation. Gérard Berry a souligné que de telles attaques peuvent avoir des conséquences dramatiques, notamment dans des secteurs critiques comme l'aviation, les réseaux électriques ou les infrastructures portuaires. Par exemple, il a mentionné l'augmentation de 500 % des brouillages signalés dans l'aviation civile en 2024, impactant jusqu'à 1 500 vols par jour.

Il a poursuivi en détaillant les failles du **protocole NTP**, utilisé pour synchroniser les serveurs et systèmes via Internet. Ce protocole, bien que largement adopté, reste vulnérable aux **attaques par interception ou altération des données transmises**. Gérard Berry a expliqué que ces attaques peuvent désynchroniser des réseaux critiques, fausser des transactions financières ou provoquer des interruptions de service dans les data centers, soulignant ainsi l'impact potentiel sur l'économie et la sécurité nationale.

Un autre aspect qu'il a abordé est la **désynchronisation des réseaux distribués**, comme ceux utilisés dans les data centers ou les systèmes de cloud computing. Une synchronisation incorrecte peut provoquer des incohérences dans les bases de données, des erreurs dans les calculs distribués, ou même des pertes de données. Gérard Berry a insisté sur le fait que, bien que ces problèmes soient moins visibles pour le grand public, ils peuvent entraîner des pertes financières considérables et des atteintes à la réputation des entreprises.

Il a également évoqué les implications stratégiques de la **dépendance aux technologies étrangères**, en particulier aux systèmes GNSS comme le GPS (américain) ou Galileo (européen). Selon lui, cette dépendance pose des questions de souveraineté, car la capacité d'un pays à fonctionner de manière autonome peut être compromise si ces systèmes sont perturbés ou manipulés par des puissances étrangères.

Pour conclure cette partie, Gérard Berry a insisté sur l'urgence de renforcer la **cybersécurité des systèmes temporels**. Il a évoqué la nécessité de développer des solutions résilientes, comme des systèmes de redondance utilisant des horloges atomiques locales ou des réseaux de fibres optiques, pour pallier les failles des technologies existantes. Il a également souligné l'importance de sensibiliser les décideurs et les ingénieurs à ces enjeux pour intégrer la sécurité temporelle dès la conception des systèmes.

Selon le Professeur Gérard Berry, ces défis doivent être traités rapidement pour protéger les infrastructures critiques et garantir la fiabilité des technologies sur lesquelles repose notre

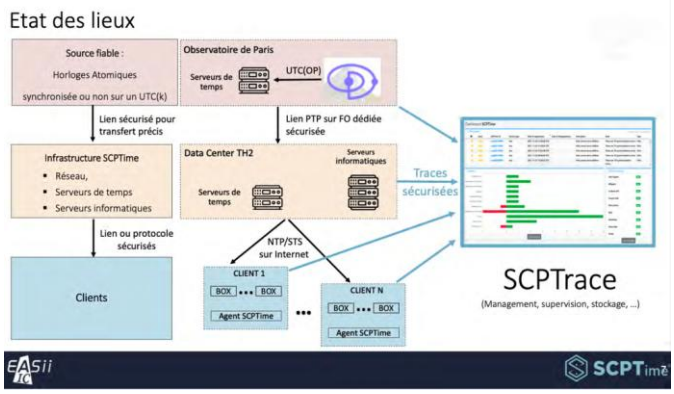
société moderne. Ces enjeux, bien que complexes, nécessitent une approche collective impliquant les gouvernements, les entreprises et les institutions de recherche.

IV. La solution française : SCPTime

Lors de son intervention, Gérard Berry a présenté **SCPTime**, une initiative française innovante visant à répondre aux défis critiques liés à la sécurisation de la mesure et de la distribution du temps. Selon lui, cette solution illustre l'excellence française dans ce domaine et constitue une avancée stratégique majeure pour garantir l'autonomie et la résilience des infrastructures.

Gérard Berry et Jacques Thimonier, architecte des solutions SCPTime chez Gorgy Timing puis chez EASii IC ont commencé par expliquer que **SCPTime** repose sur l'utilisation d'**horloges atomiques locales**, qui permettent de générer une synchronisation précise et indépendante des systèmes de navigation par satellites (GNSS). Contrairement à ces derniers, SCPTime n'est pas exposé aux menaces de brouillage ou de leurrage, car il fonctionne via des infrastructures terrestres dédiées. Cette indépendance vis-à-vis des GNSS, souvent contrôlés par des puissances étrangères, renforce la souveraineté technologique de la France.

Jacques Thimonier a ensuite détaillé le fonctionnement de SCPTime, qui s'appuie sur un réseau de **fibres optiques sécurisées** pour distribuer le temps avec une précision et une fiabilité inégalées. Cette infrastructure permet de synchroniser des équipements critiques dans des secteurs aussi variés que les télécommunications, les transports, l'énergie ou encore la finance. En complément, SCPTime intègre des mécanismes de redondance, garantissant une continuité de service même en cas de perturbation locale.



Jacques Thimonier a également mis en avant l'implication de grandes institutions françaises, comme le **LNE-SYRTE (Laboratoire National de Métrologie et d'Essais - Systèmes de Référence Temps-Espace)**, basé à l'Observatoire de Paris. Ce laboratoire, reconnu mondialement pour son expertise dans les horloges atomiques, joue un rôle clé dans le développement et la mise en œuvre de SCPTime. Il a souligné que ces collaborations entre le secteur public, les entreprises privées et les institutions scientifiques renforcent l'impact et la crédibilité de cette solution.

SCPTime propose également des **protocoles de synchronisation sécurisés**, conçus pour répondre aux besoins spécifiques de divers secteurs. Par exemple, il est particulièrement adapté aux environnements exigeant une précision absolue, comme les transactions financières, où une erreur de quelques millisecondes pourrait avoir des conséquences majeures, ou encore les réseaux électriques, où une désynchronisation pourrait entraîner des coupures massives.

Jacques Thimonier a également souligné les **bénéfices stratégiques** de SCPTime pour la France. En plus de réduire la dépendance aux infrastructures étrangères, cette solution positionne le pays comme un leader mondial dans la distribution sécurisée du temps. Elle ouvre également des opportunités économiques, en offrant une alternative fiable et souveraine à des clients internationaux préoccupés par les vulnérabilités des systèmes actuels.

V. Présentation du Cercle des Femmes de la Cybersécurité (CEFCYS)

Le **Cercle des Femmes de la Cybersécurité (CEFCYS)**, fondé en 2016, a été présenté lors de l'événement comme une association clé pour promouvoir la diversité et l'inclusion dans le domaine de la cybersécurité. Avec près de 600 membres, dont 15 hommes, le CEFCYS agit à travers la France pour sensibiliser et valoriser les métiers de la cybersécurité auprès des femmes et des hommes.

L'association se distingue par ses nombreuses initiatives : programmes de mentorat, organisation d'événements comme les **Trophées des Femmes Cyber**, masterclasses, webinaires et job dating, dont le prochain aura lieu le 7 mars 2025 à l'Université Paris Cité. Le CEFCYS met aussi l'accent sur la sensibilisation auprès des jeunes et du grand public pour encourager un usage sécurisé du numérique.

Son objectif principal est de **faire progresser la représentation des femmes**, actuellement minoritaires (14 à 17 %), dans une filière dynamique qui offre une grande diversité de métiers au-delà des compétences techniques, comme la gouvernance et la gestion de projets. Grâce à des partenariats avec des entreprises, institutions et écoles, le CEFCYS œuvre pour une cybersécurité plus inclusive et collaborative.

VI. Questions / Réponses

Question 1 : Quel est le rapport entre le temps en physique et en informatique ?

Gérard Berry a expliqué que, bien que le temps soit une question fondamentale en physique (avec des débats sur son existence ou sa nature), ce raisonnement ne s'applique pas directement à l'informatique. Il a précisé que, dans la vie courante et les systèmes actuels, les considérations liées au temps quantique ne jouent pas encore un rôle significatif.

Question 2 : Les cyberattaques visant la distribution du temps sont-elles techniquement réalisables et fréquentes ?

Gérard Berry a indiqué que des cyberattaques ciblant la distribution du temps ont déjà été réalisées, mais elles restent rares, car elles sont plus complexes à exécuter que d'autres types d'attaques plus accessibles. Cependant, il a souligné que la "guerre du temps" entre États pourrait devenir une menace sérieuse dans l'avenir.

Question 3 : Quels sont les standards pour la synchronisation précise des horloges dans les réseaux ?

Un intervenant a mentionné le protocole PTP (Precision Time Protocol), norme IEEE 1588, qui permet une synchronisation précise. Cependant, ce protocole est coûteux à mettre en œuvre à grande échelle car il nécessite des équipements spécifiques. Il a également été noté que ce protocole manque de mécanismes de sécurité intégrés, ce qui constitue un problème.

Question 4 : Comment sécuriser les signaux GPS contre le brouillage ou le spoofing ?

Les discussions ont mis en avant l'importance des solutions de redondance et de résilience. Par exemple, l'utilisation combinée de réseaux terrestres (fibres optiques) et de systèmes satellitaires permettrait de réduire les risques. Galileo, en particulier, offre des services authentifiés pour garantir la provenance des signaux.

Question 5 : Pourquoi utilise-t-on trois horloges dans un système critique comme un bateau ?

Gérard Berry a expliqué que si deux horloges affichent des temps différents, il est impossible de déterminer laquelle est correcte. Avec trois horloges, un système peut détecter et écarter celle qui est défaillante, rendant le système plus fiable.

Question 6 : Comment sensibiliser le grand public et les professionnels à la fiabilité du temps dans les systèmes critiques ?

L'intervenant a insisté sur l'importance de la formation et de la sensibilisation, notamment via des guides et des recommandations. Il a cité des initiatives comme un guide récemment publié

pour sensibiliser les secteurs maritimes et portuaires aux risques liés à la perte de synchronisation GPS.

Question 7 : Quels progrès pour Galileo par rapport au GPS ?

Galileo est déjà opérationnel mais possède moins de satellites que le GPS. Il a été conçu en tenant compte des erreurs du GPS et propose des services supplémentaires, notamment l'authentification des signaux pour garantir leur origine et renforcer la sécurité.

Question 8 : Le sextant est-il encore utilisé dans la navigation maritime ou aérienne ?

Il a été mentionné que les sextants sont toujours utilisés dans certaines formations de pilotes ou pour la navigation de secours sur des bateaux. Cependant, leur utilisation reste marginale face à l'omniprésence des systèmes GPS modernes.

Question 9 : Pourquoi le GPS civil a-t-il été rendu plus précis ?

Initialement, le GPS civil était volontairement imprécis pour des raisons de sécurité militaire. Toutefois, il a été ouvert après des besoins militaires urgents (par exemple, lors de la guerre du Golfe) et pour des raisons économiques et sociales, notamment après des accidents liés à son imprécision.

Question 10 : Quel est le rôle des signaux GPS et Galileo dans les blockchains ?

Les blockchains dépendent de l'horodatage précis fourni par ces systèmes. Une attaque sur les signaux GPS ou Galileo pourrait compromettre la fiabilité de la blockchain. Bien que ce risque reste théorique, il nécessite une attention particulière dans la sécurisation de ces technologies.

Question 11 : Que peut-on faire pour améliorer l'éducation scientifique liée au temps ?

Gérard Berry a plaidé pour une vulgarisation scientifique accrue, expliquant que de nombreuses personnes ignorent des concepts fondamentaux comme le fonctionnement des ondes ou du GPS. Il a mentionné son livre grand public pour sensibiliser davantage sur ces questions complexes mais accessibles.