INSTITUT Mines-Télécom

Journée du Conseil scientifique de l'Afnic 2016

#JCSA16

Lundi 11 juillet 2016, 9h30-18h30

Institut Mines-Télécom, 46 rue Barrault

Paris 13ème

afnic

La cryptographie en support aux infrastructures et services Internet

9h30-12h30 Matinée Tutoriel

La blockchain, des principes de base aux contrats Ethereum

Par Stéphane Bortzmeyer (Afnic)

Le tutoriel se déroulera en deux parties :

- un rappel de l'architecture de la chaîne de blocs, ses principes, et ses mécanismes de sécurité. Pourquoi avoir confiance dans une blockchain ? On parlera des différents types de blockchain, de Bitcoin et de ses clones (comme Litecoin) pour arriver à Ethereum, qui stocke dans la chaîne des programmes (appelés contrats) et pas seulement des échanges d'argent ;
- l'écriture de contrats Ethereum en Solidity. Le langage machine d'Ethereum, le langage Solidity, le compilateur solc, des contrats simples (stocker et récupérer une variable), jusqu'à un contrat plus complexe et fournissant un service réel (contrat dont on vous laisse deviner la fonction).

11h00-11h20 Pause-Café

12h30-14h00 Cocktail déjeunatoire

14h00-18h30 Après-midi Séminaire

14h00 – 14h45 Session d'ouverture

Allocutions d'ouverture et présentation du Conseil scientifique de l'Afnic
(Afnic, Institut Mines-Télécom)

Introduction du Séminaire
Laurent Toutain (Maître de conférence, Télécom Bretagne - Président du Conseil scientifique de l'Afnic)

Points saillants de l'enquête de toile de fond technologique Afnic 2016
Alexandre Clame (INIT Merketing) & **Mohsen Souissi** (Afnic)

14h45 – 16h00 Session « Cryptographie pour des infrastructures émergentes

The GNU Name System : A clean-slate solution to DNS security and privacy nightmare
Christian Grothoff (Inria)

Tor et ses .onion, un système d'adressage « privacy by design »
Lunar (TorProject)

16h00 – 16h30 Pause-café

16h30 – 18h00 Session « Cryptographie pour des infrastructures essentielles de l'Internet

From the Ground Up Security : DNS-based Security of the Internet Infrastructure
Benno Overeinder (NLnet Labs)

Mesures HTTPS par l'Observatoire de la résilience de l'Internet français : compatibilité TLS et conformité des certificats
Guillaume Valadon et **Maxence Tury** (ANSSI)

Public Notary Transparency : des registres publics en ajout seul et leurs usages avec TLS
Florian Maury (ANSSI)

Synthèse & conclusion

Suivez et commentez cet événement en direct sur Twitter avec le hashtag #JCSA16

Biographie des orateurs (dans l'ordre de déroulement du programme)

Stéphane Bortzmeyer *est ingénieur à Afnic Labs, où il s'occupe de normalisation (IETF), de vie privée (projet « DNS privacy »), de DNS, de sécurité et de veille technologique, ce qui inclut la chaîne de blocs. Il utilise Bitcoin depuis 2013, Ethereum depuis 2015 et programme des contrats en Solidity. Il a une réputation de 285 sur https://ethereum.stackexchange.com/ :-)*

Christian Grothoff *est chercheur à l'INRIA Rennes où il a monté l'équipe "décentralise". Il est l'un des principaux auteurs et architectes du projet GNUnet qui vise à proposer des alternatives et axes de recherches autour des mécanismes de vie privée, de sécurité, et de nommage. GNUnet propose en effet son propre mécanisme de résolution de Nom: GNS (Gnu Name System) et a fait l'objet de nombreuses recherches et publications.*

Lunar *a fait ses premiers pas dans la télécommunication avec un minitel à l'âge de 10 ans, et n'a jamais arrêté de bricoler des morceaux de réseau numérique depuis lors. Il porte un regard profondément critique sur l'impact social du monde numérique. Cela ne l'empêche pas de persister à voir entre les mailles du filet de la surveillance des possibilités de prises de pouvoir collectives. Depuis ses premières contribution au projet Tor en 2009, il participe activement à promouvoir son usage et expliquer les questions techniques et politiques qui y sont liées.*

Benno Overeinder *is managing director of NLnet Labs. NLnet Labs is a non-profit research lab whose mission is to build a bridge between academic results and practical deployment of new technology in our networks. In this context, Benno is particularly interested how results from research have practical and operational implications on how we run our networks.*

Before joining NLnet Labs in 2007, Benno obtained his MSc. and PhD. in Computer Science from the University of Amsterdam, the Netherlands. Until 2001, he was a researcher at the University of Amsterdam, and from 2001 to 2007, he worked as an assistant professor at the VU University Amsterdam.

At NLnet Labs, Benno's topics of interest are Internet infrastructure stability and security, and the interplay between (open) standards, software development, operational practices, and policies and governance. The main focus is on two key components that turn a network of networks into and open Internet for all, namely DNS and BGP.

Guillaume Valadon *dirige le laboratoire sécurité des réseaux et des protocoles de l'ANSSI. Il contribue régulièrement à l'Observatoire de la résilience de l'Internet Français. Ses recherches portent sur les protocoles, notamment BGP, IPv6 et TLS.*

Maxence Tury *Maxence Tury est ingénieur sécurité des réseaux à l'ANSSI. Ses travaux portent principalement sur le protocole TLS et les IGCs afférentes, depuis les conventions d'encodage de bitstrings ASN.1 jusqu'à la prévention haut niveau des compromissions HTTPS. Récemment, il a contribué Scapy sous la forme d'un parseur de certificats X.509, et prépare une prise en charge du protocole TLS.*

Florian Maury *est spécialiste en sécurité des réseaux et des protocoles, pour l'ANSSI. Il travaille sur les problématiques de sécurité du DNS, sur les dénis de service distribués, sur les infrastructures de gestion de clés et la cryptographie appliquée en général, et sur le développement sécurisé d'applications web. Ses recherches ont notamment mené à la découverte de plusieurs vulnérabilités DNS et OpenPGP. Il est l'auteur principal du guide de l'ANSSI traitant de bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine.*