Security Systeme Information Administration
Lecture 0

Pascal Lafourcade

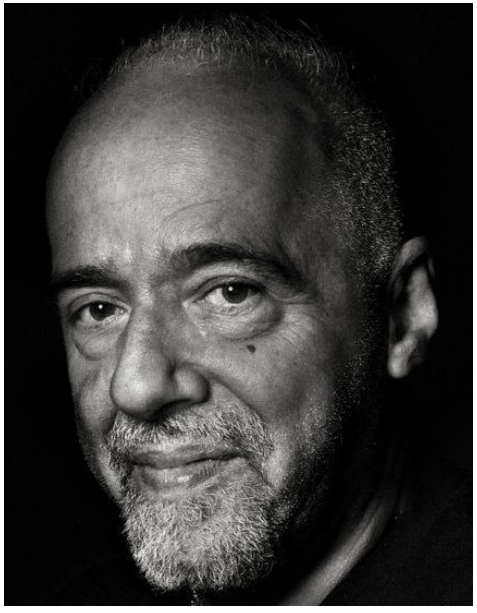
UNIVERSITÉ Clermont Auvergne

LIMOS

2023-2024

“To teach is to show what is possible.”

“To learn is to make yourself possible.”

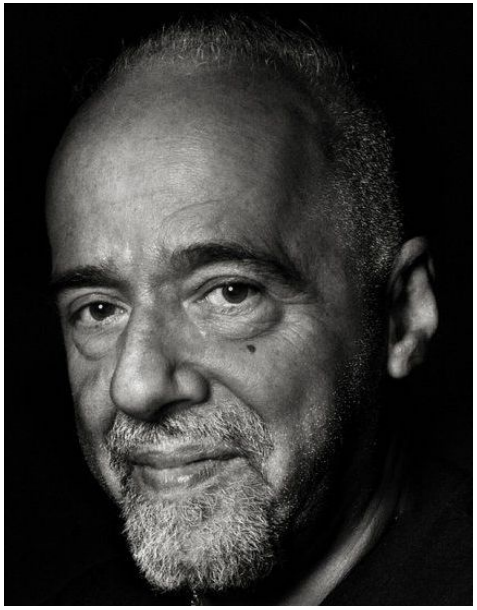


Paulo Coelho

Le Pélerin de Compostelle

“To teach is to show what is possible.”

“To learn is to make yourself possible.”



Paulo Coelho

Le Pélerin de Compostelle

The students learn, the teacher promotes learning!

Organisation du cours : 12 Sessions

Planning

- Lecture 1: Friday 22 September 13h30 - 15h30
- Exercice Session 1: Friday 29 September 13h30 - 15h30
- Lecture 2: Friday 6 October 13h30 - 15h30
- Exercice Session 2: Friday 13 October 13h30 - 15h30
- Lecture 3: Friday 20 October 13h30 - 15h30
- Lecture 4: Friday 27 October 13h30 - 15h30
- Exercice Session 3: Friday 10 November 13h30 - 15h30
- Exercice Session 4: Friday 17 November 13h20 - 15h30
- **Presentation Session 1**: Friday 24 November 13h30 - 15h30
- **Presentation Session 2**: Friday 1 December 13h30
- Lecture 5: Friday 8 December 13h30 - 15h30
- Practical Session: Friday 15 December 13h30 - 15h30

I hear, I forget.

I see, I remember.

I do, I understand.

Confucius

Grading

- Présentations : 25'+ 10' Q
- Exam 2h in january

$$Final = 60\% Exam + 40\% \max(CC, Exam)$$

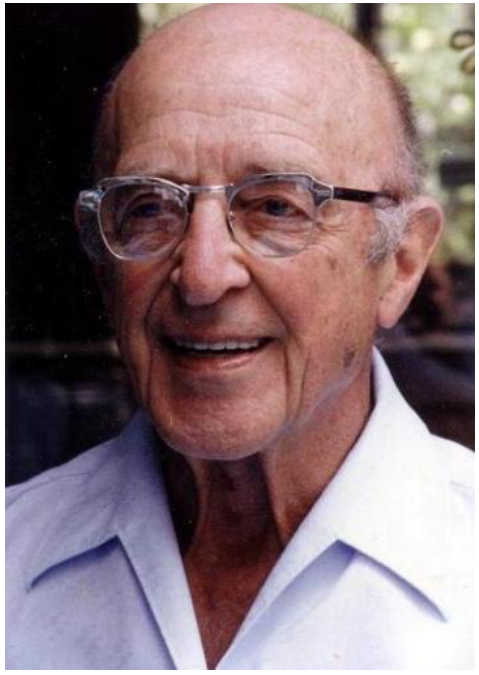
$$CC = 60\% Presentation + 40\% TP$$

pascal.lafourcade@uca.fr
leo.robert@uca.fr

Topics

1. TLS/ALPACA
2. TLS/CRIME
3. Same Origin Method Execution (SOME) Attack
4. Spectre and Meldown
5. RowHammer
6. Petya/NotPetya Ransomware

The only knowledge that really influences behaviour is that which one has discovered and appropriated oneself.



Carl Rogers

How does lecture work

- Lecture available, at least one week before.
- Exercice session available also before.

Answer YOUR questions during the lecture

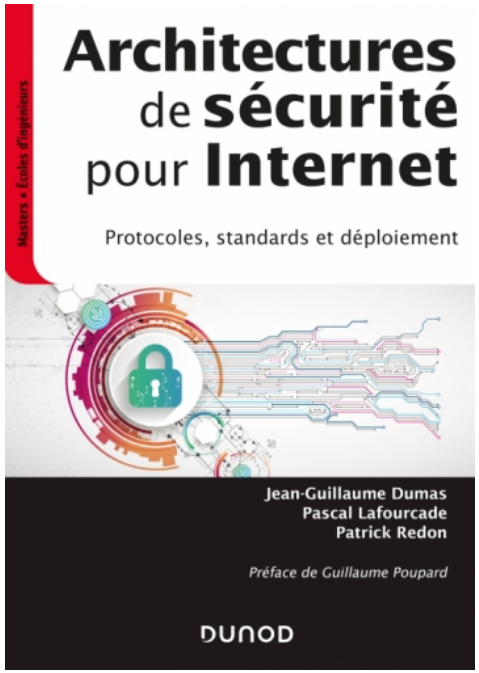
- Read the material of the lecture before
- Understand and prepare questions

Content of the Lectures

1. Introduction to cybersecurity
2. Public Key Cryptography
3. Symmetric Cryptography
4. Main ATTACKS (Presentation)
5. PKI, TLS, Malwares ...
6. TOR, ZKP, Bitcoin ...

Questions?


Les
BLOCK
CHAINS
EN 50 QUESTIONS
Comprendre le fonctionnement et les enjeux
de cette technologie innovante
Jean-Guillaume DUMAS
Pascal LAFOURCADE
Ariane TICHIT
Sébastien VARRETTE
DUNOD


Masters • Écoles d'ingénieurs
Architectures
de sécurité
pour Internet
Protocoles, standards et déploiement
Jean-Guillaume Dumas
Pascal Lafourcade
Patrick Redon
Préface de Guillaume Poupard
DUNOD

Bruce Schneier

“Security is a process, not a product.”