

RES 212

Network security

Course organization



RES212

v02-2018/04/07

Dario Rossi

<https://res212.telecom-paristech.fr>

Agenda


- Teacher
- Language
- Exam
- Sources
- Syllabus

Teacher

- Dario Rossi
 - dario.rossi@enst.fr LINCS, 23 av. Italie
 - <https://perso.telecom-paristech.fr/drossi> Office hours: Mon 9:00-10:00
- Short CV
 - 2001, MSc @ Politecnico di Torino, Italy
 - 2003, Researcher @ University of California Berkeley, CA
 - 2005, PhD @ Politecnico di Torino, Italy
 - 2006, Associate Professor @ ENST, France
 - 2010, HDR @ UPMC, France
 - 2011, Qualification @ CNU
 - 2012, Professor @ Telecom ParisTech, France
 - 2012, Professor @ Ecole Polytechnique, France
 - 2016, Chair Professor, NewNet@Paris <https://newnet.telecom-paristech.fr>



Exam

- Exam
 - Documents: You can bring any documentation you want
 - Phone: Not allowed (no crowdsourcing)
 - Set-in topic: Slides, Labs (=TP), mandatory readings (if any)
 - Set-out topics (i.e., not in the exam)
 - Extra slides (denoted with )
 - Optional references
- Format
 - Multiple choice questions
 - Many wrong answers, a single correct answer
 - Wrong answers may have a negative weight

Sources: Murphy law

- Website
<https://res212.telecom-paristech.fr>
- RES212: 1st edition this year
- Murphy law: merciless this year
- Consequence: Website will be updated ``just-in-time'' this year

- Thanks to colleagues (alphabetical order)
 - G. Bianchi (Università di Roma 2)
 - G. Boggia (Politecnico di Bari)
 - F. Gringoli (Università di Brescia)
 - G. Piro (Politecnico di Bari)

- **Murphy law**

“If anything can go wrong, it will”

Murphy law for RES212: last month a thief entered the building, cracked the entrance door to the lab, broke into my office, stole my 2 mobile PCs (in sync with each other)

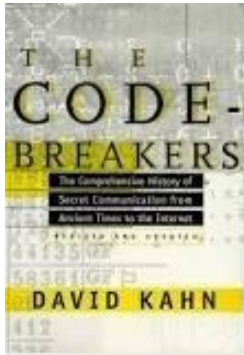
- **Corollary**

“If there is a worse time for something to go wrong, it will happen then”

Corollary for RES212: the disk hosting the *daily* rsnapshot backup suffered physical problems and as a result *all* RES212 material (not public yet) was lost...

Sources: Books (1/2)

- Books (optional readings)



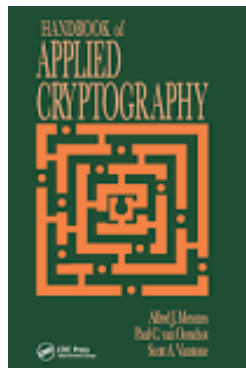
by D. Kahn

Excellent historical perspective (though other books needed)



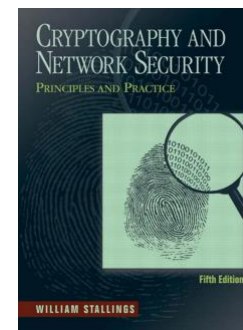
by R. Anderson

Eye opener, holistic approach to security (but remains high level)



by A. Menezes et al.

Very good coverage of crypto (1st chapter suffices for our needs)

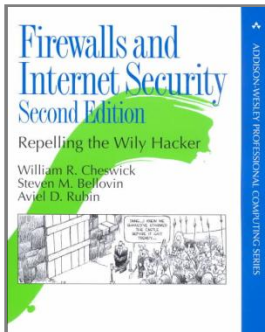


by W. Stallings

Good classic reference, comprehensive for crypto and networking aspects

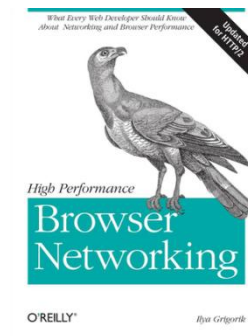
Sources: Books (2/2)

- Books (optional readings)



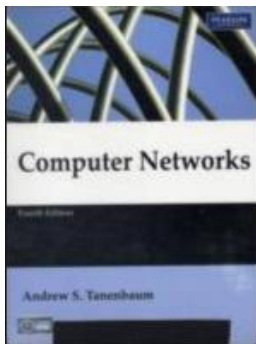
by R. Chenwick et al.

Influential in defining the firewall concept (aged, although like wine...)



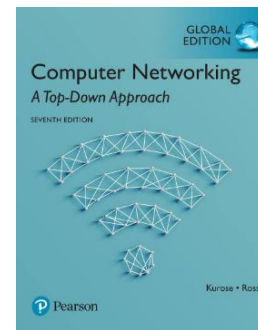
by I. Grigorik

Good coverage of HTTP(S) TLS & certificates (with practice + performance)



by D. Tanenbaum

Network book, security in ~100 pages (chap. 8)



By J.Kurose & K.Ross

Network book, security in ~70 pages (chap. 8)

Syllabus 2017-18/P4

Topic	Room	Date	Type
Introduction (holistic view)	C47	13/4	Cours
Crypto (simplistic view)	C47	14/5	Cours
<i>Top of the stack</i> Web (TLS, Certificates) & VPNs	C47	28/5	Cours
TP#1: Certificates & VPNs	C126	4/6	TP
<i>Bottom of the stack</i> IPsec, VLANs	C47	11/6	Cours
<i>Outside the stack</i> Perimeter security, Firewalls, IDSs	C47	11/6	Cours
TP#2: Firewall	C130	18/6	TP
<i>At large</i> Internet & cyber security; recap	C47	21/6	Cours
Exam	H2	25/6	Exam

?? || //
