UGA
Université
Grenoble Alpes

9. Synthesis

Jean-Marc THIRIET

Balance on what has been done

- Chapter 1 - *Networks*
- Chapter 2 - *Error detections and corrections*
  - *Abstract*
  - *Exercises* on parity, CRC, checksum (security layer 2)
- Chapter 3 - *Introduction to security of information systems*
  - *Abstract*
  - *Exercises* on risk analysis (risk analysis for the definition of a security policy)
- Chapter 4 - Attacks
  - *Abstract*
  - *Exercises* (examples of attacks)
- Chapter 5 - Technologies
  - *Abstract*
  - *Exercises* on firewall
  - Lab on the firewall (NAT, filtering)

Balance on what has been done

- Chapter 6 - *Cryptology*
  - *Abstract*
  - *Exercises*
  - Lab on cryptography
- Chapter 7 - *Protocols* (IPSec)
  - *Abstract*
  - *1 Exercise on IPSec* (not done)
- Chapter 8 - *Intrusion detection*

Conclusion

It is possible to protect systems and networks

- Multiple protection technics, but each solution gets some weaknesses
  - Problems of configuration
  - Software security holes
- Pirating is more and more easy if there are no protection
  - Hacking a Wi-Fi network with a smartphone
- More and more risks
  - Remote working
  - Communicating tools
- Vital/strategic data for companies

A "good” security

The network administrator should

- know everything about configurations
  - Servers
  - Network devices
  - Client computer
- know about other communicating devices
  - Smart phones
  - Embedded systems, IoT
  - WIFI
- Use of probes
- Use of logs

Certainty?

- We won’t avoid hacking
  - But we will protect data
    - Saving policy
    - Recovery plan after an incident
  - We should know when the system is hacked…
    - Log
    - Real-time alarms
- Train the users about
  - Risks
  - Consequences
- Managing security requires to remain curious and open-minded, but not to be paranoid

- The use of the methods described in this course engages the responsibility of the users!

References (1/2)

- J.F. Aubry – Cours de Sûreté de Fonctionnement, INPL Lorraine, 2005.
- E. Cole, R. Krutz, JW Conley - Network security bible – Wiley, 2005.
- A. Fernandez-Toro, management de la sécurité de l'information, implémentation ISO 27001 et 27002
- C. Davis, M. Schiller, K. Wheeler – IT auditing : using controls to protect information assets
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013.
- Security for industrial communication systems, Dacfey Dzung, Martin Naedele, Thomas P. Von Hoff, Mario Crevatin, pp. 1152-1177, Proceedings of the IEEE, Vol. 93, n° 6 "Industrial Communication Systems", June 2005
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Course of Jean-Luc Noizette, ESSTIN, Nancy.
- G. Avoine, P. Junod, P. Oechslin – Sécurité informatique, exercices corrigés – Vuibert, Paris, 2006
- Presentation of Eric WIESS
- VPN, mise en œuvre sous Windows Server 2003, P. Mathon, 2004

References (2/2)

- Compression et cryptage des données multimedia, X. Marsault, Hermès, 1995
- SSL VPN, Understanding, evaluating and planning secure, web-based remote access – J. Steinberg & T. Speed, 2005.
- P. H. Oechlin, LASEC/EPFL
- http://sebsauvage.net/comprendre/encryptage/crypto_rsa.html
- F. Halsall – Computer networking and the internet – Addison Welseley, 2005 + additional student support at www.pearsoned.co.uk/halsall
- SSH, le shell sécurisé, D. J. Barrett et R.E. Silverman, O'Reilly, 2001
- Hacking interdit, IIème édition, Micro Applications, 2007
- D. Vergnaud – Exercices et problèmes de cryptographie, Dunod, 2015
- CEH, Certified Ethical Hacker, Matt Walker, McGrawHill, 2017
- L. Bloch & al. – Sécurité informatique pour les DSI, RSSI et administrateurs, Eyrolles, 2016.
- Sécurité et espionnage informatique : connaissance de la menace APT, Cédric Pernet, Eyrolles
- Guide d'autodéfense numérique, éditions Tahin Party
- Cybertactique : Conduire la guerre numérique, Bertrand Boyer, Nuvis
- Learn Social Engineering, Dr E. Orzkaya, 2018, Packt
- Preventing Ransomware, A. Mohanta M. Hahad K. Velmurugan, 2018 Packt
- Collectif sous la Direction de Y. Fouratier & L. Petre-Cambacedes – Cybersécurité des installations industrielles – Cepadues, 2015.