Course 25: Networks security

Professional Bachelor's Degree

Réseaux Informatiques, Mobilité, Sécurité (RIMS)

Computer Networks, Mobility, Security (CNMS)

Jean-Marc THIRIET, Cyril BRAS,
Denis LUBINEAU, Olivier BRIZARD
jean-marc.thiriet@univ-grenoble-alpes.fr
http://www.gipsa-lab.grenoble-inp.fr/

~jean-marc.thiriet/lpro/cnms_en.html

……./lpro/rims_fr.html

Condensed CV

- Docteur Université Henri Poincaré Nancy 1: February 1993
- Associate Pr. Nancy-IUT Dépt. Réseaux & Télécoms 1993-2005
- Habilitation à Diriger des Recherches December 2004
- Full Professor UGA 2005
  - Teaching in networks, network security, industrial networks, signal processing, Programmable Logic Controllers (DUT, bachelor, master)
  - Responsible for the CNMS programme from 2007 to 2015
  - Head of the Dept « Réseaux et Telecom » from 2016-2018

  - Research in the dependability of automation systems which integrates communication networks, cyber-security of cyber-physical systems
  - Presently Responsible for International Relationships, IUT1, UGA
  - 2011-2015 : Head of GIPSA-Lab (Research Laboratory in Automatic and Signal Processing)

  - 2005-2009 Responsible for a European project EIE-Surveyor www.eie-surveyor.org which concerns the evolution of Higher Education in Europe in our disciplines (110 universities are partners)

Convergence between IT and cyber-physical systems (CPS)

US Black-out, 2003

INFRASTRUCTURE

Industrial
Control
Systems (ICS)

Smart grids

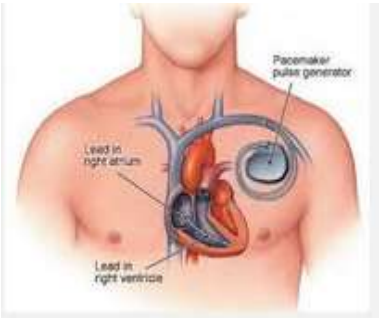
Cyber attack ukrainian power network, Dec. 2015

- Integrity of the information and communication infrastructure

→ Challenge: DEPENDABILITY (RAMS Reliability, Availability, Security & Safety, Maintainability)

EMBEDDED SYSTEMS

Drones
Autonomous vehicles
Connected objects



Maroochy shire, Stuxnet, CrashOverride

Overview of cyber attacks against ICS systems (from HdR Peter Matousek)

Year	Attack	Place
1982	Explosion of Siberian gas pipeline caused by a trojan which reset pump speeds and valve settings	Soviet Union
1997	Knock out of Worcester air traffic control communication	MA, USA
2000	Maroochy shire sewage spill	Australia
2003	Crash of the Safety Parameter Display System in Davis-Bess nuclear power plant by Slammer worm	OH, USA
2003	Shutting down of CSX train signaling system by Sobig virus	FL, USA
2005	Zotob virus knocked 13 of Daimler-Chrysler's manufacturing plants	USA
2010	Stuxnet virus damaged Iranian centrifuges by increasing and decreasing their speed and pressure beyond normal levels	Iran
2014	Disrupted control system in German steel mill	Germany
2015	Power outage off Ukrainian power plant distribution caused by BlackEnergy malware	Ukraine
2016	Industroyer malware attack on Ukrainian power grid	Ukraine
2017	Cyber-espionage attack against aerospace and energy industry by APT33 group	USA
2019	Cyber attack against chemical giant Bayer	Germany
2019	Intrusion attack against U.S. Energy sector by KAMACITE group	USA
2019	Cyber attack against Kudankulam nuclear power plant	India
2020	Compromising supply chain of Solarwinds software used in industrial environment	USA
2021	Ransomware attack against oil distribution company Colonial Pipeline	USA

Cyber-security

- **Cybernetics** from Greek κῠβερνήτης (*kubernêtês*) => Used 19th and 20 century => ideas of control and communication
- **Cyber** : Greek *kubernân,* to govern
- Today used for everything relative to the « digital » world (internet, web…)
- **Cyber-security**:
  - Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber attacks. Effective cyber security reduces the risk of cyber attacks, and protects organisations and individuals from the unauthorised exploitation of systems, networks and technologies (https://www.itgovernance.co.uk/what-is-cybersecurity)
  - État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. (ANSSI, https://www.ssi.gouv.fr/entreprise/glossaire/c/)

Memoir

- Objectives
  - To "cultivate" oneself to security (technology watch)
  - Write a professional document that can complement a CV
- How do you do it?
  - Read articles, websites, make an "analysis" of them (list, your relative notes, etc.).
  - Write a personal "synthesis", your vision based on what you have read.
- Deadlines
  - For Monday, September 25, 2023, 8.00 pm : Send me
    - The choice of your subject
  - For Thursday, December 7, 2023, 8:00 p.m.: Send me
    - The title of your memoir, the proposed plan...
    - The current status of your "analysis": "commented" list of references and links you have read, used
  - By Thursday, 8 February 2024, 8 p.m., latest deadline
    - 1 electronic version of the full report (and annexes) to be sent to me
    - jean-marc.thiriet@univ-grenoble-alpes.fr
- We place ourselves in a professional framework: no delay will be allowed

Organization of the memoir

- The memoir should contain the following parts:
- Title
- Table of Contents
- Main part (synthesis) composed of ten to fifteen pages written by YOU (not copy-pasted !) (30 lines, 1500 signs per page)
  - Alternatively it may be a 4 to 6 page report respecting the IEEE format
- Bibliographical and “webographic” references (**classified** and **commented**)
- Appendices (interesting documents you may have found)

- Each one will have to carry out this « synthesis work » on the basis of readings (books, journals, Internet) and/or from her/his own experience, gained during the practical part of the academic project, for instance, or from past experiences (training periods…)

Subjects

1. Proposal for a network/computer security policy for a company
2. Security protocols, secure architecture through VPN
3. Secure IoTs?
4. Telecom, Mobile phone protocoles, security aspects
5. Cloud environment, security challenges
6. Industrial networks, safety networks, state of the art about security
7. Wireless networks (Wi-Fi, LoRA, ZigBee, 6lowPAN), security problematics
8. Other idea?

Deontology

- Students

  => signing of a computer use agreement (charte informatique)
- Administrator Network/Systems

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

Internships

- Possibilities in Europe or outside Europe
- Typically from 11th March to 24th June 2024 (15-16 weeks)
- For everybody (16th October 2023 8pm, by e-mail)
  - List of companies with links if relevant (means you used it) (Table sent by JMT)
  - CV and letter (after evaluation by Mrs Royer and/or Mrs Dupont-Belrhali, English and/or French), if possible
  - List of previous students to contact
  - Half a page to one page sheet explaining your strategy to look for an internship, the web-sites you consulted (like KOMPASS, and other)
- Other information
  - I will send you a letter explaining our programme

Organisation course M25

- Chap. 1: Basic codes (JMT), 2H
- Chap. 2: Firewall (CB) 4H
- Chap. 3: Crypto (JMT) 6H
- Chap. 4: Protocoles, VPN (JMT) 3H
- Exam (JMT)
- 2 labs (OB & JMT)