جامعة
حمد بن خليفة
HAMAD BIN KHALIFA
UNIVERSITY
عضو في مؤسسة قطر
Member of Qatar Foundation

Beyond SolarWinds: The Systemic Risks of Critical Infrastructures, State of Play, and Future Directions

SIMONE RAPONI, MAURANTONIO CAPROLU, AND ROBERTO DI PIETRO

SRAPONI@HBKU.EDU.QA, MCAPROLU@HBKU.EDU.QA, RDIPIETRO@HBKU.EDU.QA

INFORMATION AND COMPUTING TECHNOLOGY (ICT) DIVISION,

COLLEGE OF SCIENCE AND ENGINEERING (CSE),

HAMAD BIN KHALIFA UNIVERSITY (HBKU), DOHA, QATAR

Roberto Di Pietro

Vision: To achieve excellence in cybersecurity research addressing both fundamental and applied challenges in the field, as well as to have impact and to generate innovation.

Currently
- Full Professor in Cybersecurity @HBKU-CSE, Doha-Qatar
- Lead of the Cybersecurity Research and Innovation Lab (https://cri-lab.net)

Past
- Global Head Cybersecurity Research @ NOKIA Bell Lab (3 Depts, 50+ HR)
- Professor at University of Padua
- SNE at EUROJUST (DPO)
- United Nations Agencies consultant (cybersecurity)
- ICT Officer Ministry of Defense (10+ years)

Main Research Domain: **Distributed Systems Security**

جامعة حمد بن خليفة
HAMAD BIN KHALIFA UNIVERSITY
كلية العلوم والهندسة
College of Science & Engineering

Cybersecurity @HBKU - People

Full Professor

Prof. Roberto Di Pietro

Associate Professor

Dr. Spiridon Bakiras

Assistant Professor

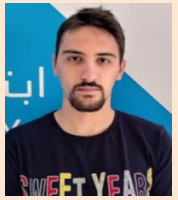
Dr. Gabriele Oligeri

Dr. Saif Al-Kuwari

PostDoc

Dr. Mazhar Rathore

Full Time Ph.D. Student



Simone Raponi

Maurantonio Caprolu

Pietro Tedeschi

Ali Al-Qathani

Elmahdi Bentafat

Omar A. Ibrahim

Saeif Alhazbi

Mouna Rabhi

+ 4 part-time PhD students + 4 MS students

جامعة حمد بن خليفة
HAMAD BIN KHALIFA UNIVERSITY
كلية العلوم والهندسة
College of Science & Engineering

Research Strategy

SCENARIOS

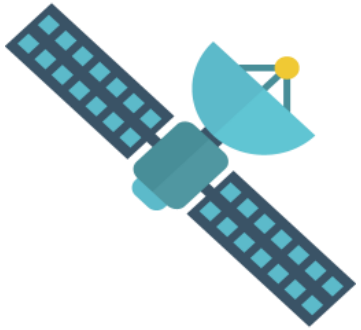
- Cyber-physical systems
- Critical Infrastructure protection

TECHNIQUES

- AI-driven
- Experimental
- Rooted on sound theory

OBJECTIVES:

- Security
- Privacy



Outline

- Automation of Production Processes
  - Examples
- Evolution of Critical Infrastructures
- Supply-Chain and Supply-Chain Attacks
  - SolarWinds Supply-Chain Attack
- First Steps Towards Resolutions
- New Research Directions

Automation of Production Processes

PROs

- More efficiency
- More Reliability
- Optimization of the industrial plants
  - Improved production capacity
  - Reducing management cost
  - Reducing personnel cost

CONS

- Dependence on technological equipment
- Exposure to new vulnerabilities
- Increased attack surface
- Exposure to possible malfunctions
- Security protections are falling behind

Examples

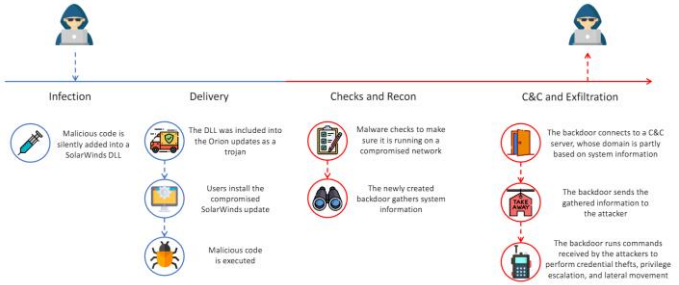
Uranian Power Grid Attack: 2015-2016

Hackers penetrated three Ukrainian power distribution companies, leaving more than 230,000 residents in the dark for one to six hours

WannaCry Ransomware Campaign: 2017

Infected hundreds of thousands of systems.
Showed how malware designed to target generic systems could infect ICSs.

SolarWinds Supply Chain Attack: 2020



A hacker group gained access to computer systems belonging to multiple US government agencies, big tech companies, and government agencies networks

Evolution of Critical Infrastructures

Presidential Policy Directive 21
(PPD-21)

Identification of 16 critical infrastructure sectors

High-level directions

lacked some concrete definitions that could have helped in addressing the subsequent implementation plans

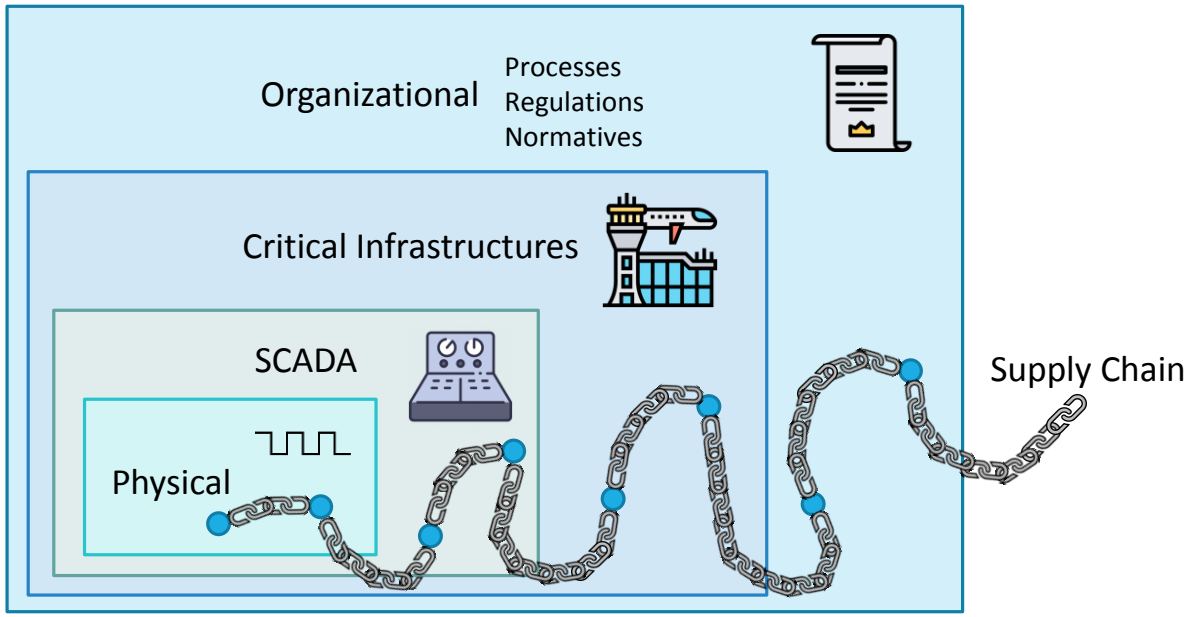
Decreto del Presidente del Consiglio dei Ministri
(DPCM 30 Luglio 2020)

- Defined the methods for identifying the subjects included in the National Cybersecurity Perimeter
- Crucial step towards securing the ICT infrastructures
- Among the first to start including the supply chain as a fundamental component

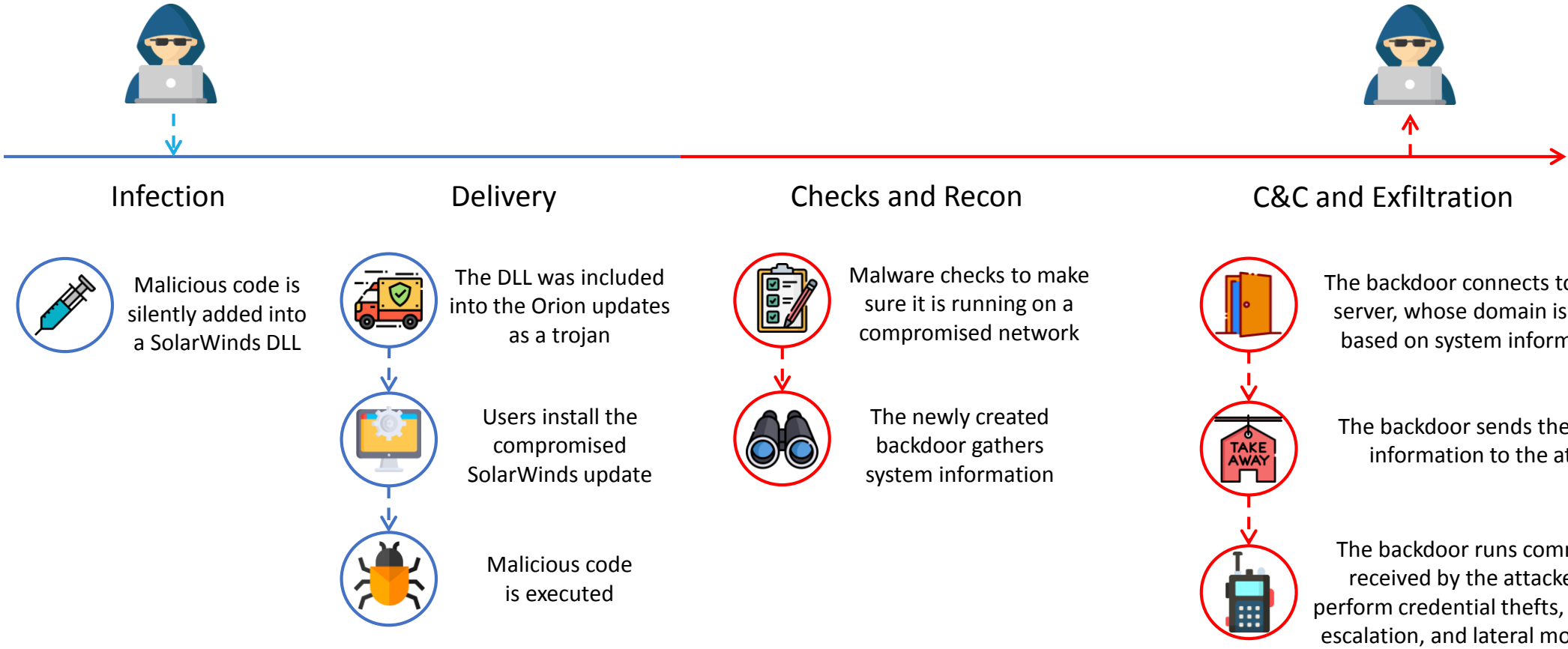
Supply-Chain and Supply-Chain Attacks

> A supply chain is the network of all the individuals, resources, organizations, and activities involved in the creation and distribution of specific products to the final buyer.

> A supply chain attack, also known as third-party attack or value-chain attack, refers to a type of cyber attack that exploits third-party vendors, such as software providers. to target larger organizations



SolarWinds Supply-Chain Attack



First steps towards resolution

The complexity of the supply chain calls for manageable solutions providing strong guarantees

1st Solution

Resort to Cybersecurity Certifications

issued by

- Trusted third parties (e.g., private companies)
- Government Agencies

Limitation

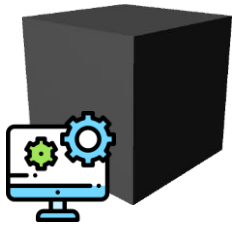
The composition of products and processes individually certified does not necessarily lead to a certified final product or process

New Research Directions

Goal

Automatic verification of the integrability of individually certified solutions

Possible Solution



Definition (or exposure) of the software components' interfaces that identify, in a verifiable way, the functionalities provided, as in a black-box approach

+

AI-driven

Static Analysis
Dynamic Analysis
IDS
IPS

Image Copyrights

- https://indico.esa.int/event/323/contributions/5041/attachments/3743/5197/11.30a_-_ADS_-_Ethernet_for_Space_with_TSN.pdf
- https://pngio.com/images/png-a2516892.html
- https://www.melodylinhart.com/picture/ddccd6ff3ac697fccb61b10428a64e71/
- https://www.pngitem.com/middle/JRJbRw_padlock-clipart-privacy-online-privacy-icon-hd-png/
- https://www.administratieondercontrole.nl/
- https://pngio.com/images/png-a2411981.html
- https://russiabusinesstoday.com/energy/ukraine-must-take-control-of-its-power-grid-banish-russian-oligarchs-expert-says/
- https://cofense.com/category/ransomware/
- https://www.iconspedia.com/icon/usa-flag--48.html
- https://en.m.wikipedia.org/wiki/File:Google_Chrome_icon_(2011).svg
- https://www.iconfinder.com/icons/856358/halt_hand_red_sign_stop_adblock_block_icon
- https://www.freeiconspng.com/images/3d-cube-png
- https://www.vidabox.com/kiosks/inforcenter-informetrics-itting-detailed-inspection-per-kit.html
- https://www.flaticon.com/free-icon/chip_897066?term=artificial%20intelligence&page=1&position=9&page=1&position=9&related_id=897066&origin=search

جامعة
حمد بن خليفة
HAMAD BIN KHALIFA
UNIVERSITY
عضو في مؤسسة قطر
Member of Qatar Foundation

Dr. Roberto Di Pietro

Full Professor in Cybersecurity
ACM Distinguished Scientist
Jean-Claude Laprie Award recipient

Cybersecurity Research and Innovation Lab https://cri-lab.net/
Hamad Bin Khalifa University
College of Science & Engineering
rdipietro@hbku.edu.qa