A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan

Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Time

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

“Value-Added Proposition Lab Partner”

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

“Rule of Law”

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

“Percipient Knowledge”

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

“1 Minute”

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

“2 Minutes”

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

“3 Minutes”

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Consensus: “Time Manipulation?”

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Time Manipulator

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

In my world, this is a …

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Cyber Threat

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Bom dia!

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

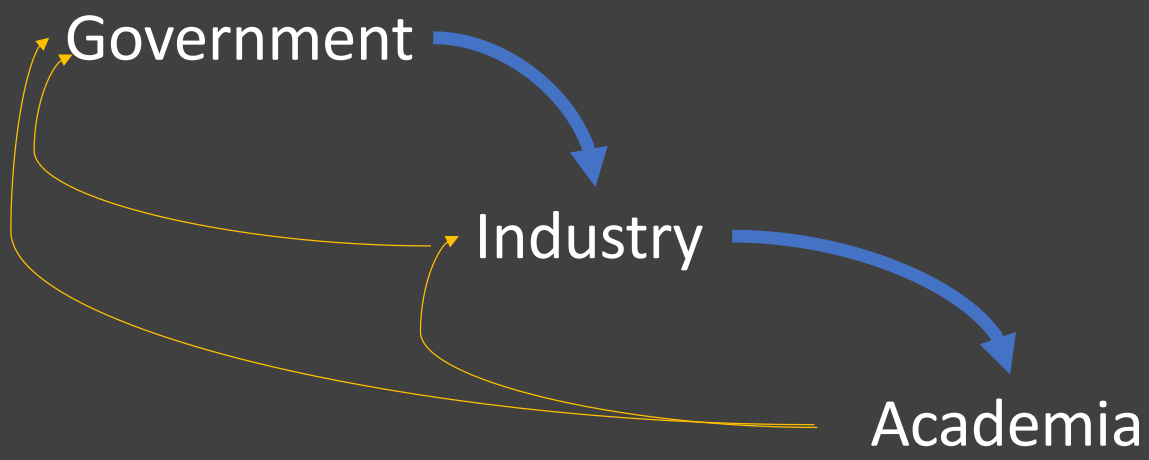
A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Cyber Time

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

Posited Cyber Trend

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan



(1)

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan

Novotel Porto Gaia

Porto, Portugal | 25 September 2019

Prediction Proxies…

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

…for Strategic Infrastructure/Critical Infrastructure

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Case Study:

Outages (Cyber, IT, Power) Affecting Airlines and Airports

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Outages Affecting Airlines:

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Outages Affecting Airports:

5/2013: SAN DIEGO INTERNATIONAL AIRPORT. LET'S GO.

10/2013: london stansted airport — PART OF M.A.G

3/2015: Schiphol Amsterdam Airport

12/2017: Hartsfield-Jackson Atlanta International Airport

MAG The Manchester Airports Group

Schiphol Group

JFK Terminal 4

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

Outages Affecting Airports:

12/2017:

10/2018:

8/2019:

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Timestamping

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

The Cyber-Physical Supply Chain Brittleness Remains…

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

…at the Terminal Substation

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan

Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Digital Twin: Physical and Cyber

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

Physical Domain

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

…back to the Cyber Domain

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Control Group: Time

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Operations Center

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Watch Floor

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Analyst Pool

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Storage Area Network

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

Time Rendering:
Constituent Components

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Time Rendering:
Global Positioning System (GPS)

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

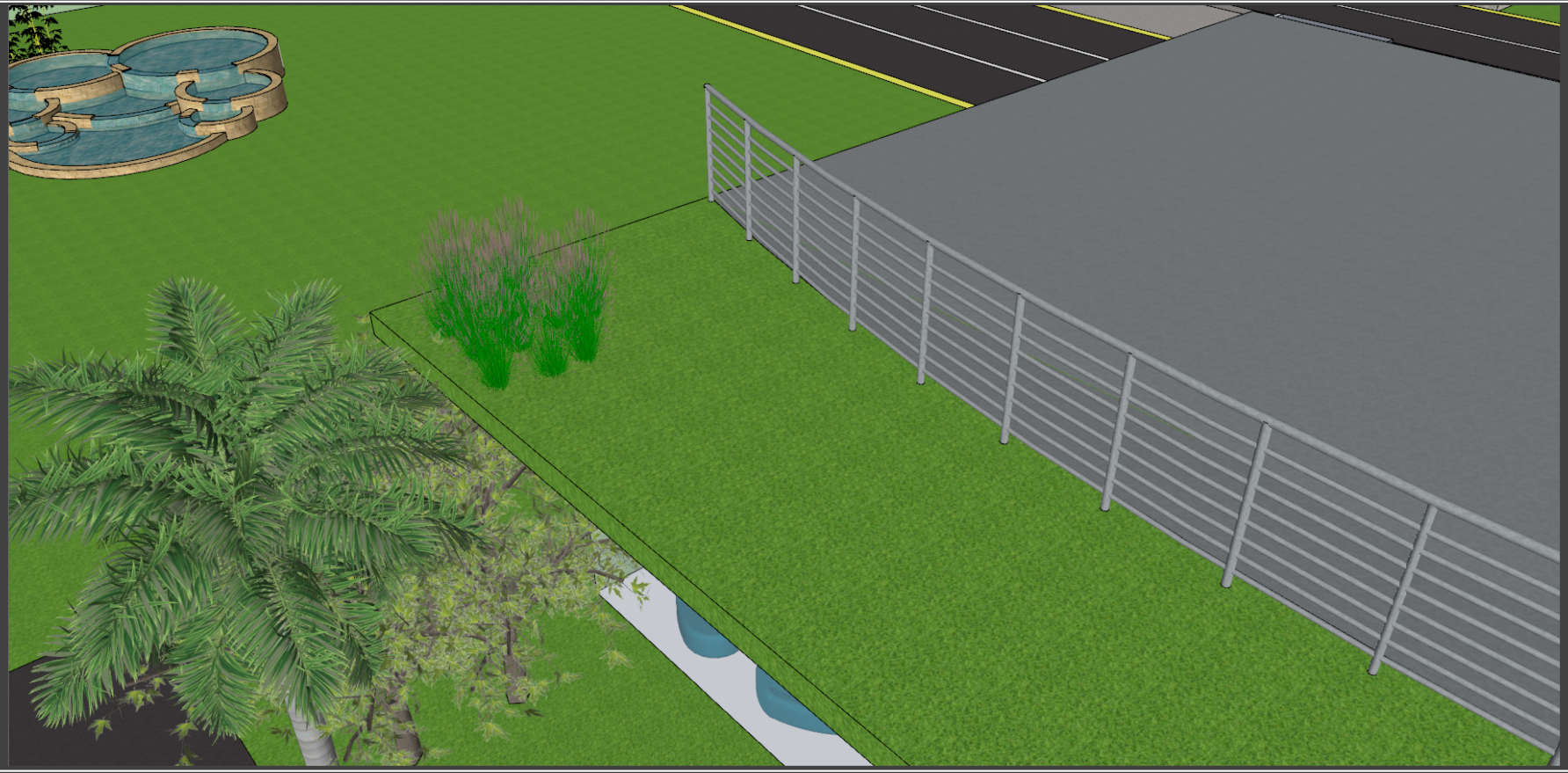
Experimental Group: Time

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan



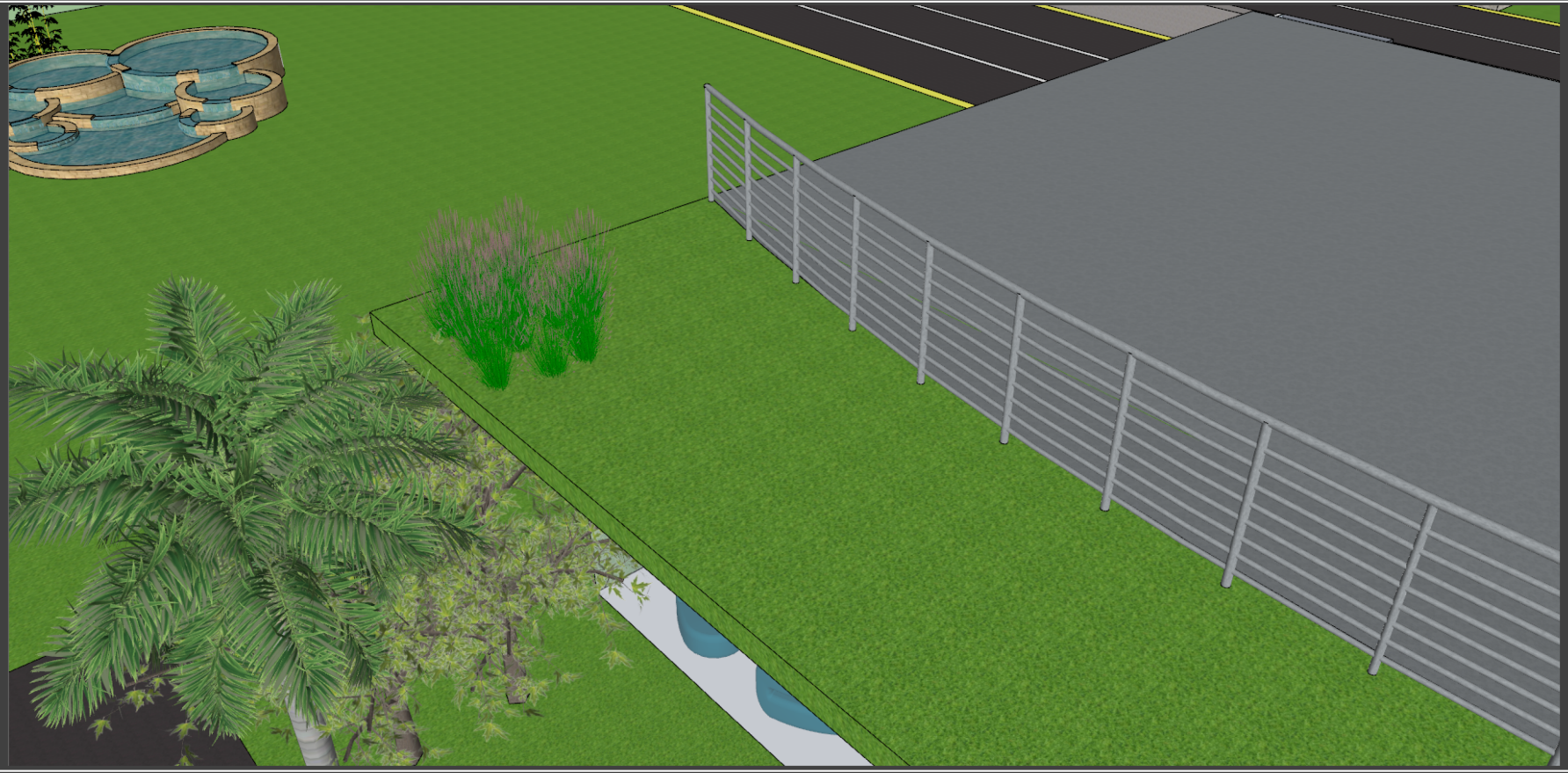
Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan



Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan

Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan

Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Cyber:
Which Int?

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Cyber:
GEOINT?

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan

Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Cyber: DIGINT?

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Cyber:
OSINT?

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan

Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Cyber:
WEBINT?

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan

Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Cyber:
MASINT?

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

Testing Results

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Some Thematics from IARIA 2019

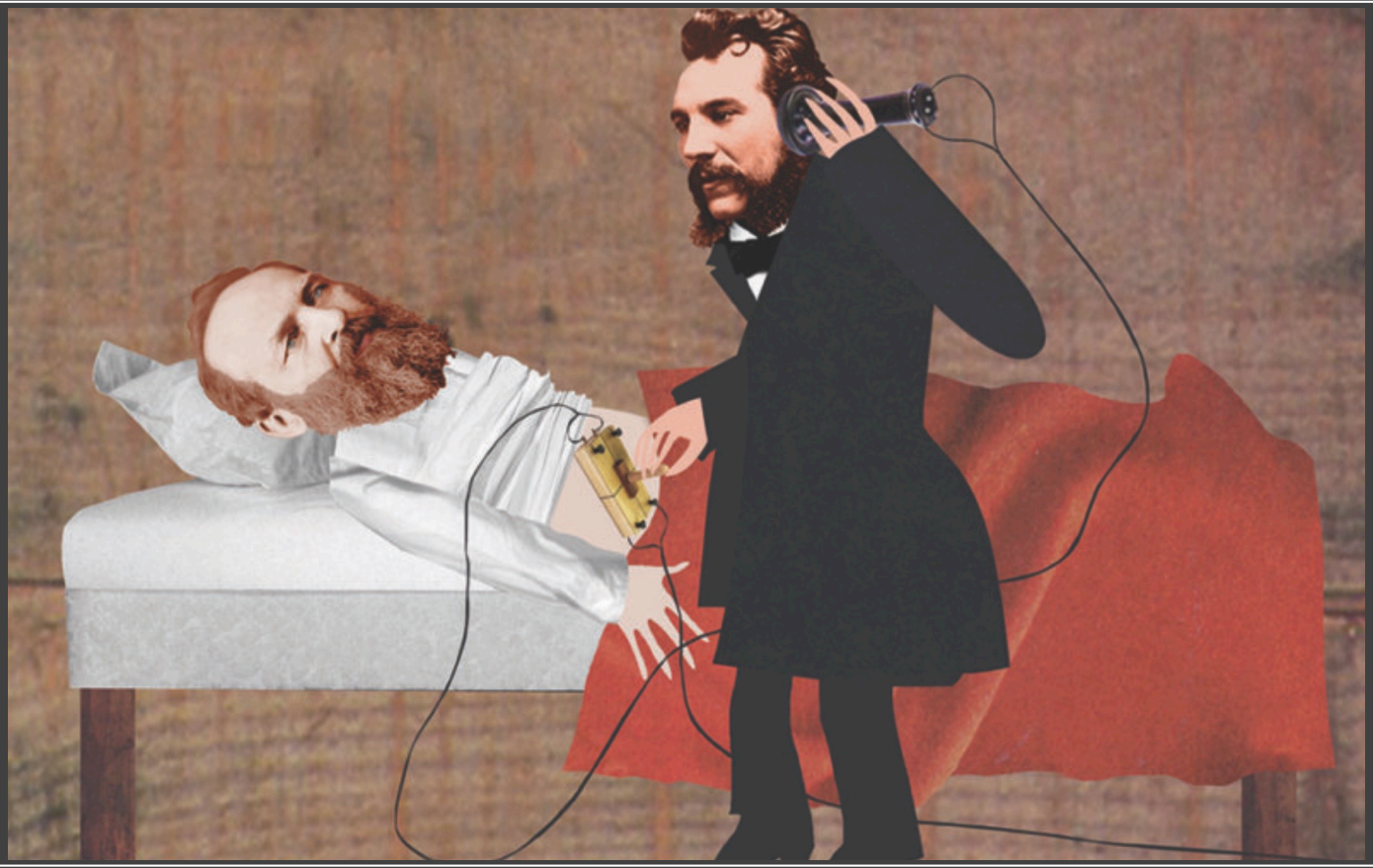
Novotel Porto Gaia
Porto, Portugal | 25 September 2019

Thematic #1: Context Matters

A Cyber Key to Log Analysis

Robust Timestamping Paradigm

Dr. S Chan



Novotel Porto Gaia

Porto, Portugal | 25 September 2019

A Cyber Key to Log Analysis
Robust Timestamping Paradigm
Dr. S Chan

Thematic #2: Multi-Domain Collaboration

Novotel Porto Gaia
Porto, Portugal | 25 September 2019

Thank you!
Questions?

schan@dengineering.org