INTEGRATED FRAMEWORK FOR PREDICTIVE AND COLLABORATIVE SECURITY OF FINANCIAL INFRASTRUCTURES

Silvio Ranise – Head of the Security & Trust Research Unit

FONDAZIONE BRUNO KESSLER

ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

ST SECURITY & TRUST

European Commission

FINSEC

https://www.finsec-project.eu/

CENTRI DI RICERCA

FONDAZIONE BRUNO KESSLER

Polo Scientifico e Tecnologico

ICT
Centro per le Tecnologie dell'Informazione e della Comunicazione

CREATE-NET
Centro di Ricerca e Sperimentazione della telecomunicazione per le comunità in rete

CMM
Centro Materiali e Microsistemi

ECT*
Centro Europeo per gli Studi Teorici in Fisica Nucleare e Settori Collegati

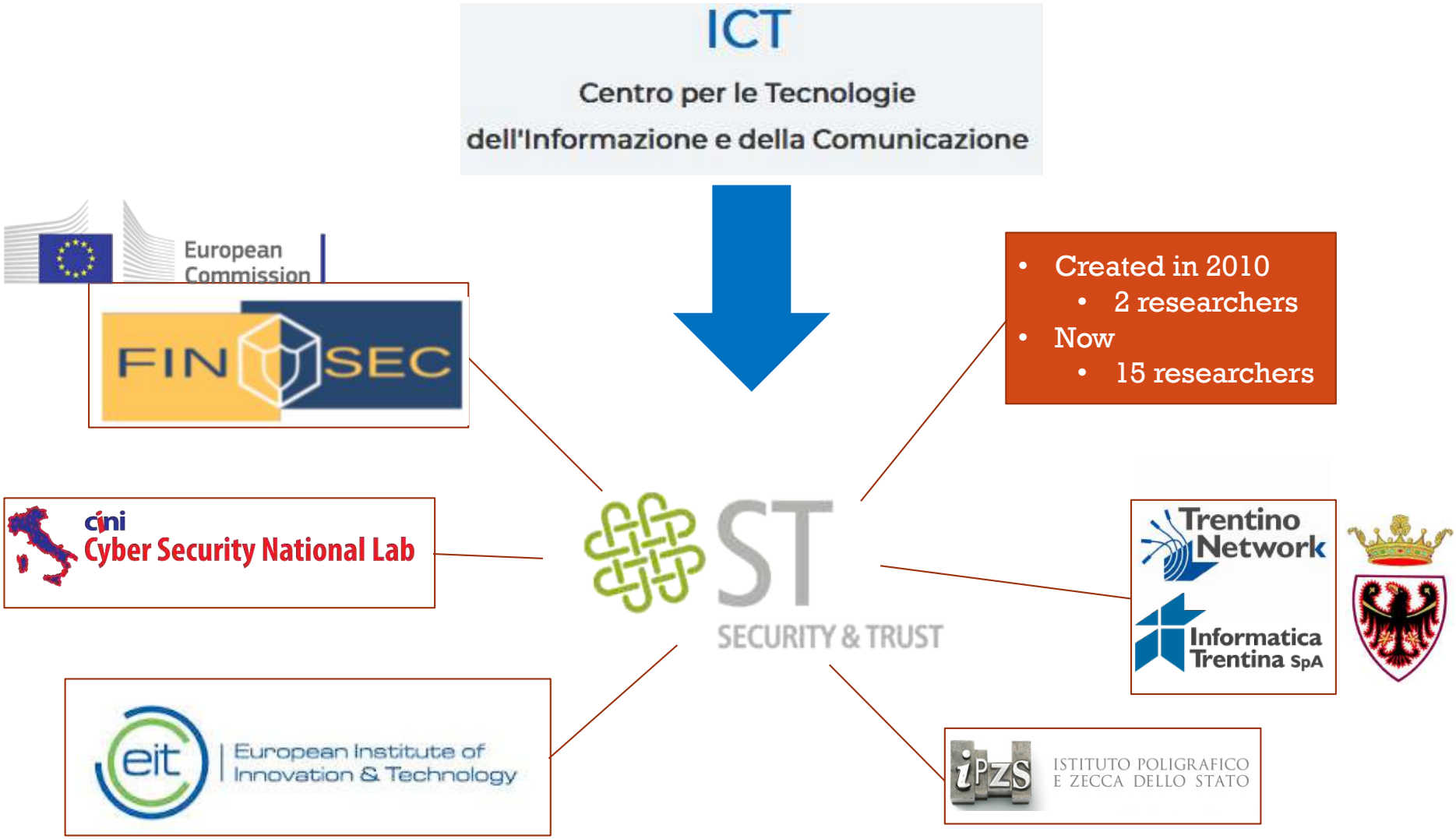
The reason why I am here

Polo delle Scienze Umane e Sociali

ISIG
Istituto Storico Italo-Germanico

IRVAPP
Istituto per la Ricerca Valutativa sulle Politiche Pubbliche

ISR
Centro per le Scienze Religiose


ICT
Centro per le Tecnologie
dell'Informazione e della Comunicazione
European Commission
FIN SEC
cini
Cyber Security National Lab
ST
SECURITY & TRUST
Trentino Network
Informatica Trentina SpA
eit
European Institute of Innovation & Technology
IPZS
ISTITUTO POLIGRAFICO E ZECCA DELLO STATO
• Created in 2010
• 2 researchers
• Now
• 15 researchers

FINSEC

8 MEuros EU project
22 partners
1,000 PMs
May 2018-April 2021

Large industries

Financial organisations

Security specialists

Research centres

- Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures
- GOAL: develop a novel standards-based security reference architecture for **cyber and physical** security dedicated to fintech institutions so to
  - enable timely preparation against attacks and
  - facilitate the sharing of cyber-intelligence information among stakeholders for risk assessment and
  - mitigation of threats in the financial supply chain
- 5 PILOTs: SWIFT, Bank Data-center and ATM, Private block-chain for micro-payments, Insurance, Small and Medium Financial Institutions

The project at a glance

PROBLEM

FIN SEC

Security silos

Cyber Security Systems

Physical Security Systems

An example of a Cyber Security Problem

A DATABREACH IN A EQUIFAX CREDIT REPORTING AGENCY

- Equifax data breach
  - Discovered July 29, 2017
  - Announced Sept. 7, 2017
- 146.6 million Americans were affected
  - Around **half of the American population**!

Not only data, even photos

Driver's License	38,000
Social Security or Taxpayer ID card	12,000
Passport	3,200
Other	3,000

Leaked personal data

Name	146.6 million
Birthdate	146.6 million
Social Security Number	145.5 million
Address	99 million
Gender	27.3 million
Phone Number	20.3 million
Driver's License Number	17.6 million
Email Address	1.8 million
Credit Card information	209,000
Tax ID	97,500
Driver's License State	27,000

https://www.wired.com/story/equifax-breach-no-excuse/

Another example of a Cyber Security Problem

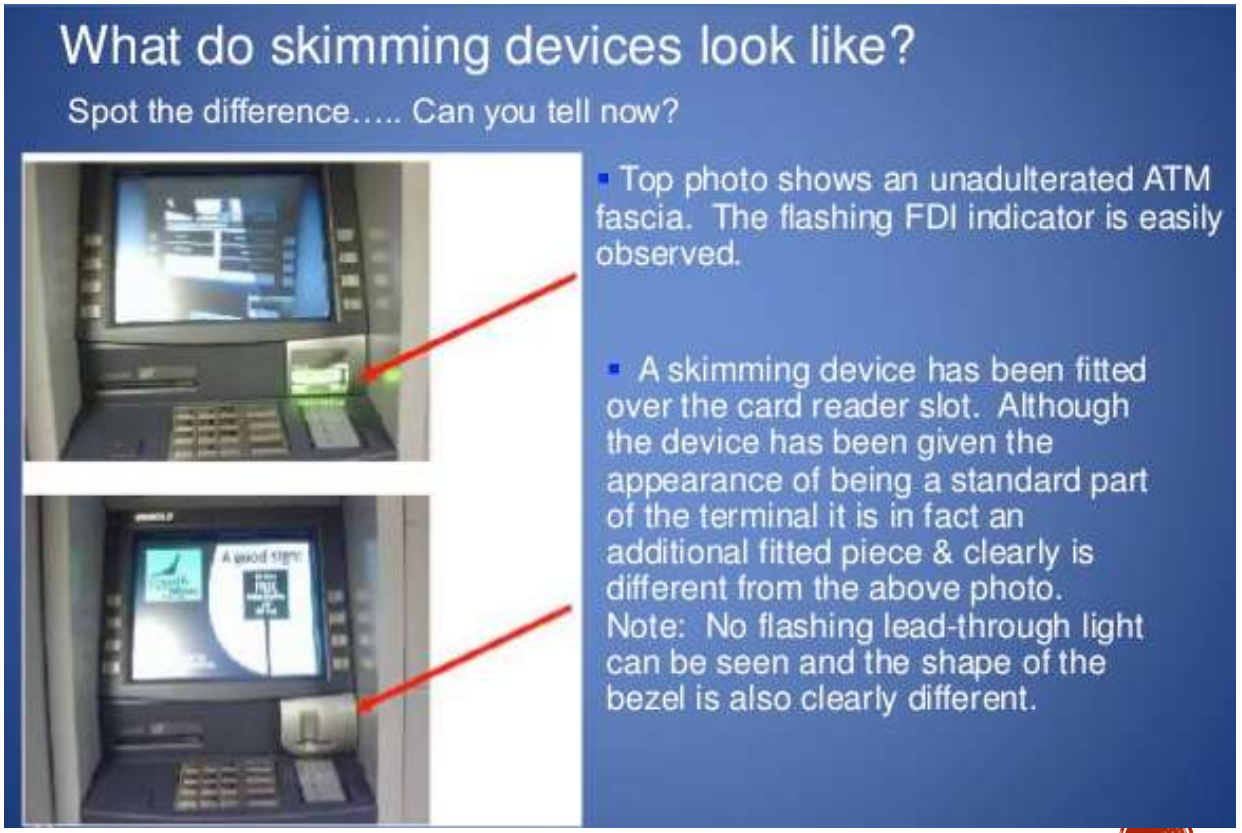
SECURITY VS COMPLIANCE

- Payment Card Industry Data Security Standard (PCI DSS)
- Data breach discovered in Jan 2010
- Intruders had stolen data on **130 million credit and debit cards**
- **Company's insistence that it was certified as fully compliant with PCI DSS**: intrusion occurred even though the company had implemented every single one of the security controls mandated by the PCI standard
- The intrusion highlighted "*very clearly and with no uncertain doubt that companies needed to worry about securing their systems first rather than complying with PCI standards*"
- **Point-in-time certification of a company's readiness to handle security threats**

An example of a Physical Security Problem

ATM SKIMMING ATTACKS

- ATM is compromised by a **skimming** device, i.e. a card reader which can be disguised to look like a part of the machine
- The card reader saves the users' card number and pin code, which is then replicated into a counterfeit copy for theft
- It is a huge problem
  - more than 1.7 million ATMs worldwide
  - every 6 minutes, a new ATM is installed somewhere in the world
  - Annually, there are 40 billion worldwide ATM cash withdrawals
- Impact on banks
  - Negative cash flow but also loss of reputation

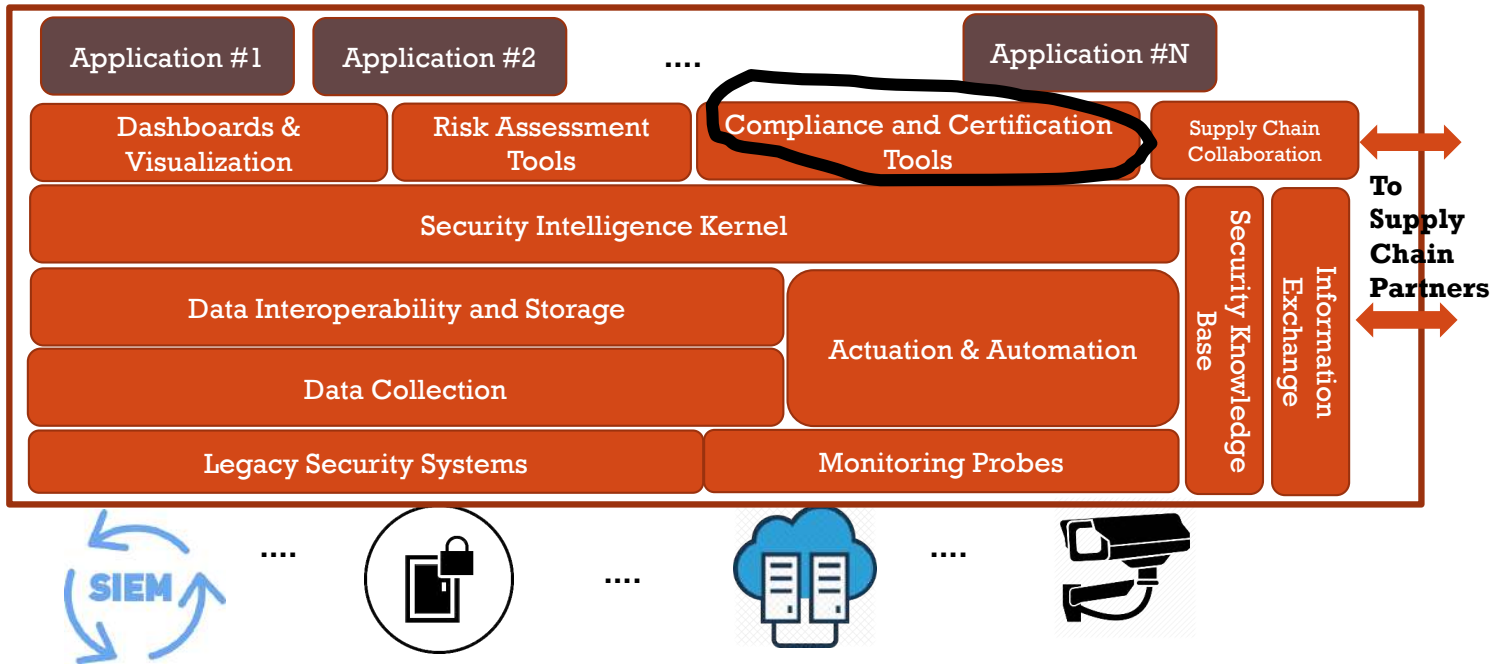


https://krebsonsecurity.com/tag/atm-skimmers/

GOAL


FINSEC
Security
Control
Center
Risk Assessment
Compliance
Auditing
Data Analytics
FINSEC Security
Knowledge Base
FINSEC
System
BANK
ATM
Cyber Security
Systems
Physical Security
Systems

ARCHITECTURE



A BROADER PERSPECTIVE ON SECURITY ISSUES

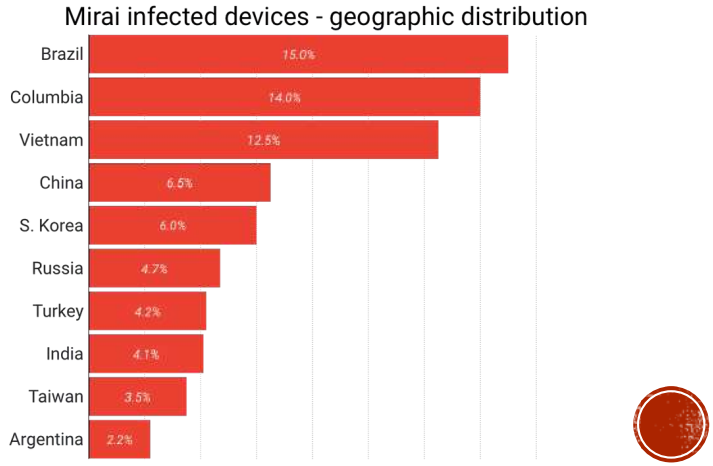
My dynamite will sooner lead to peace than a thousand world conventions. As soon as men will find that in one instant, whole armies can be utterly destroyed, they surely will abide by golden peace.

Attributed to Alfred Nobel

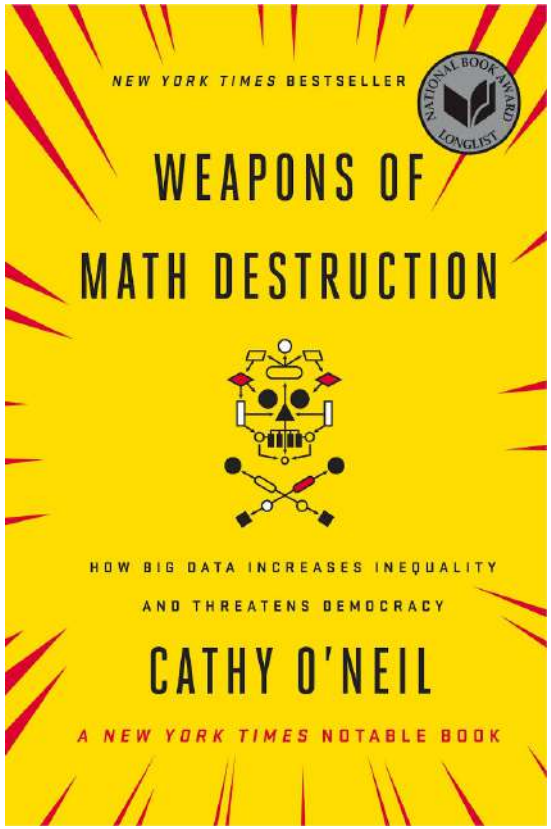
Additional problems

MIRAI WORM (INTERNET OF THINGS)

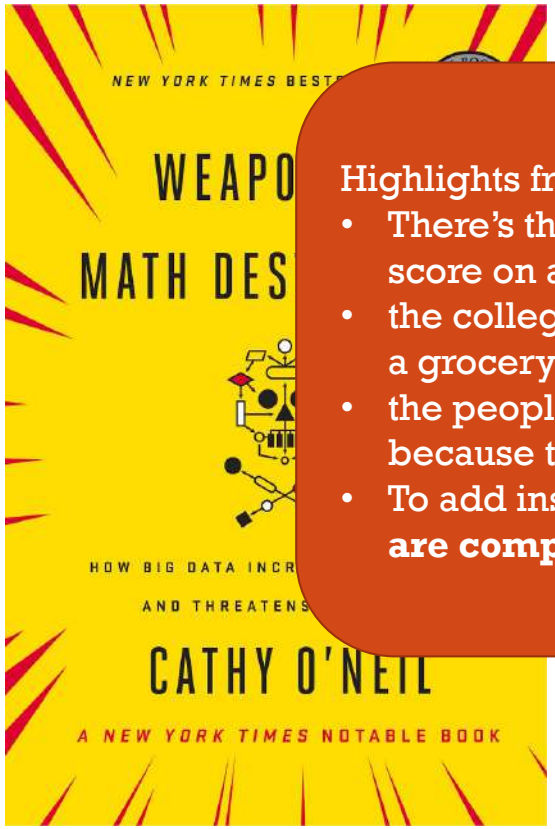
- Impact of attacks
  - Krebs on security: "**The Democratization of Censorship**"
  - DYN (DNS provider): impossible to access popular web sites such as Amazon, Twitter, Paypal, …
  - Lonestar (telco): shutting down Internet for an entire country (Liberia)



IMPACT OF ML ON PEOPLE

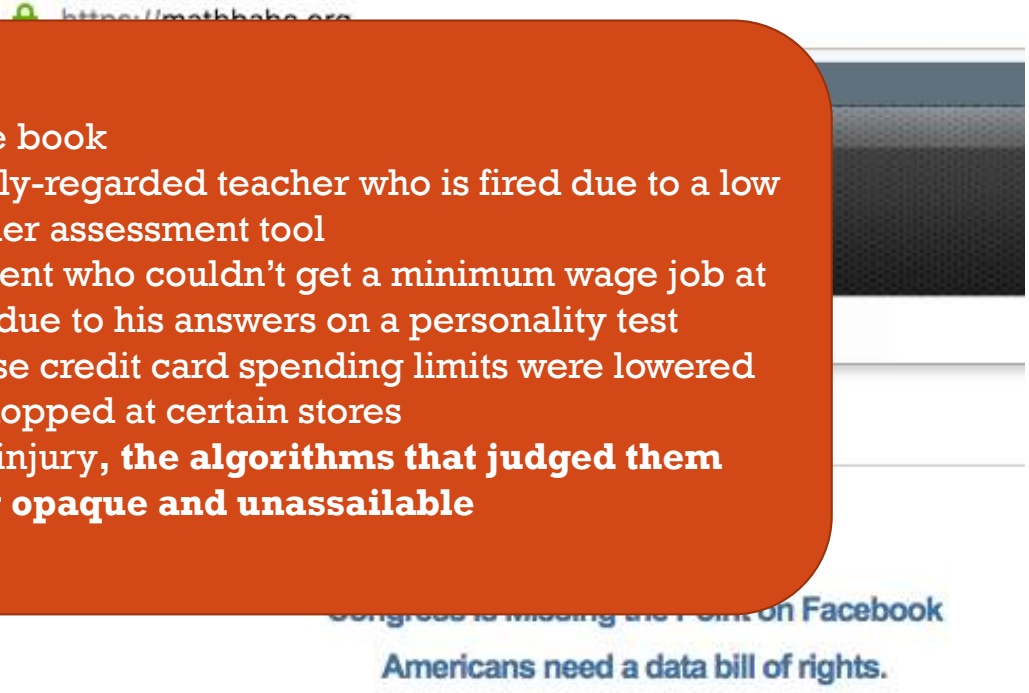


IMPACT OF ML ON PEOPLE



Highlights from the book

- There's the highly-regarded teacher who is fired due to a low score on a teacher assessment tool
- the college student who couldn't get a minimum wage job at a grocery store due to his answers on a personality test
- the people whose credit card spending limits were lowered because they shopped at certain stores
- To add insult to injury**, the algorithms that judged them are completely opaque and unassailable**



Interplay among problems!

WORLD ECONOMIC FORUM

The Global Risks Report 2018