Challenges in Cyber Services

Advances to Protect the Critical Assets

International Academy, Research, and Industry Association (IARIA)

Moderator: Dr. Thomas J. Klemas

20 November 2018 @ 17:45

Facilitating Decision-Making Via Deep Insights

Decision Engineering Analysis Laboratory

San Diego
Cambridge

Panel Details

- Topic: Challenges in Cyber Services, Advances to Protect Critical Assets
- Moderator
  - Thomas Klemas, Decision Engineering Analysis Laboratory, USA
- Panelists
  - Xing Liu, Kwantlen Polytechnic University, Surrey, B.C., Canada
  - Narelle Devine, Department of Human Services, Australia
  - Maria Bada, University of Oxford, Global Cyber Security Capacity Centre, UK
  - Michael Massoth, Hochschule Darmstadt - University of Applied Sciences, Germany
  - Steve Chan, Decision Engineering Analysis Laboratory, USA

Panelist Sub-topics

Panelist Presentations

- Introduce yourself
- Present Subtopic Briefing

1. Xing: "The role of Blockchain in protecting critical assets"
2. Narelle: "The cyber staff shortage that exists world-wide, and developing and growing cyber capabilities."
3. Maria: “Best practices for National level Critical Assets”
4. Michael: “Anomaly Detection in Unsupervised Communication Meta Data of IP-based Internet of Things (IoT) Devices”
5. Steve: Spoofing Attacks: The Exemplar of using Skewing GPS for ICS Attacks.

Panel Summary

- What are the primary challenges facing cybersecurity?
- What advances are needed to protect critical assets?
- How should desired advances be prioritized?

THANK YOU FOR YOUR PARTICIPATION

Facilitating Decision-Making Via Deep Insights

Decision Engineering Analysis Laboratory

San Diego
Cambridge

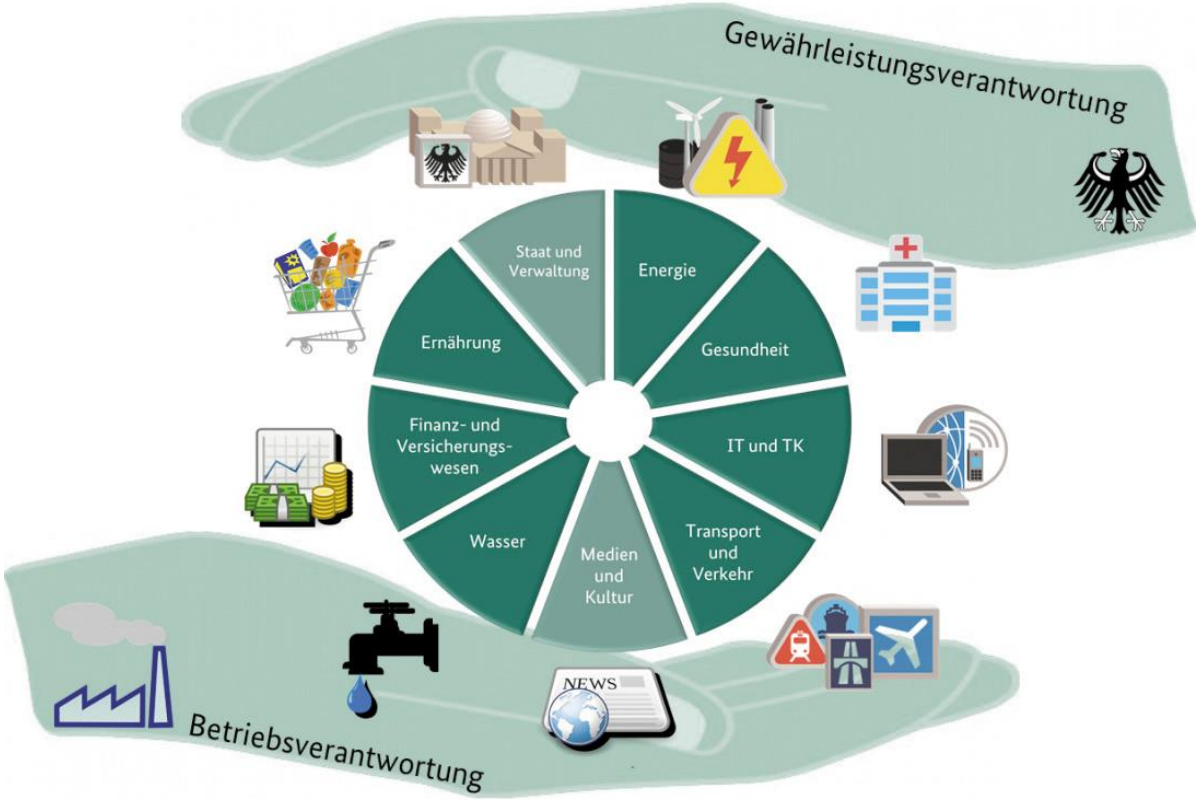
Advances to Protect the Critical Assets:

Anomaly Detection in Unsupervised Communication Meta Data of IP-based Internet of Things (IoT) Devices

Prof. Dr. Michael Massoth

University of Applied Science Darmstadt

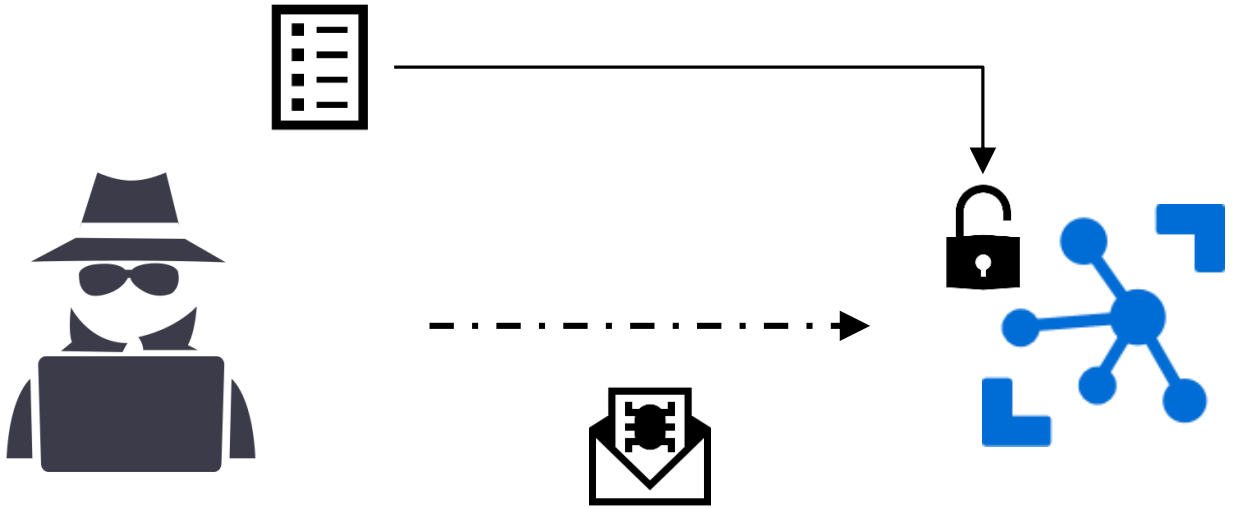
Problem: Protection of our critical infrastructures



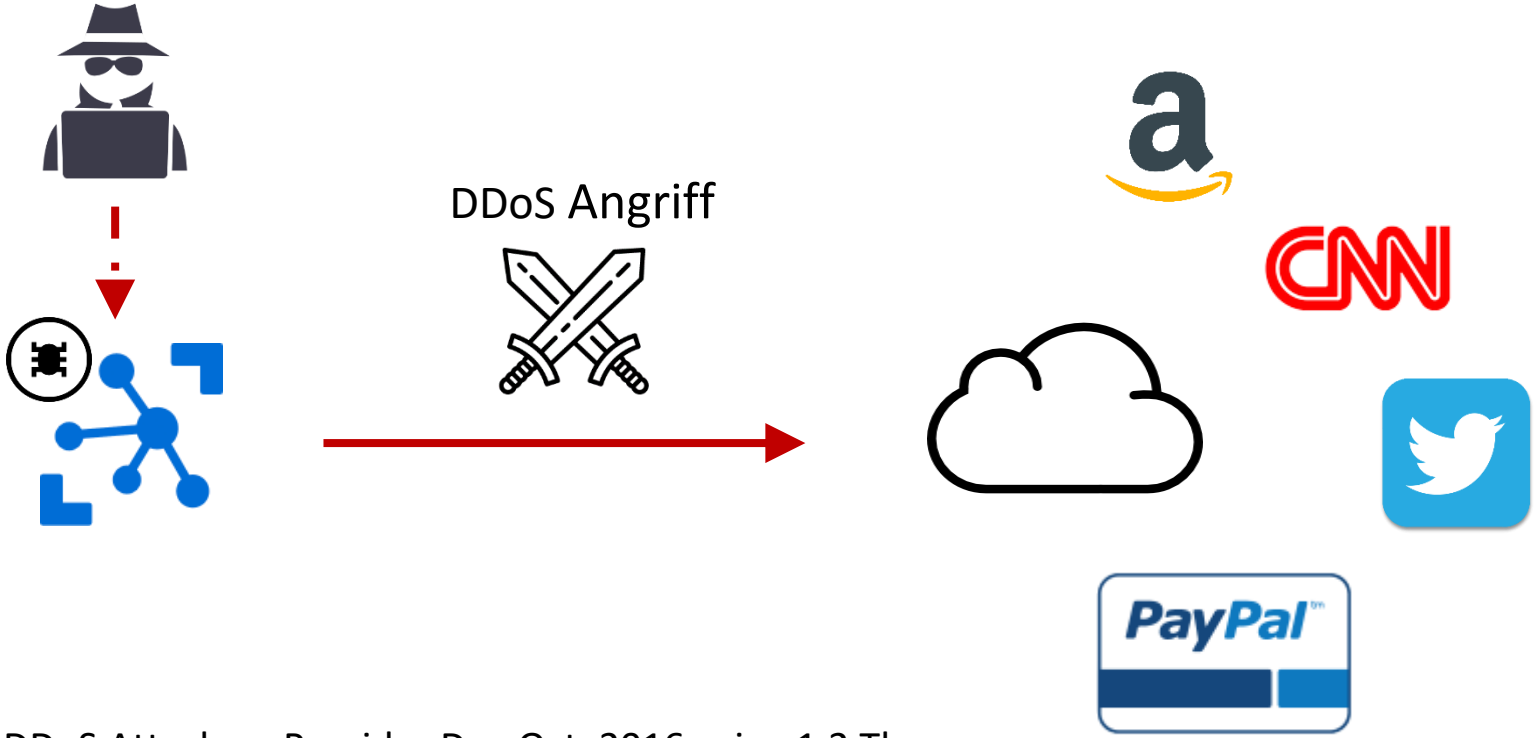
Monitored by millions of

IoT devices

Problem: Many IoT devices are easy to compromise

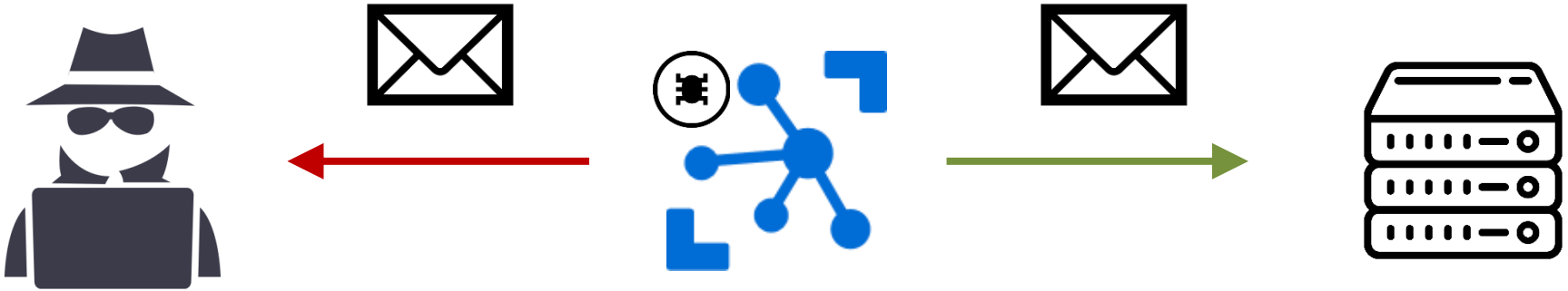


Attack vector (1): Compromised through botnet



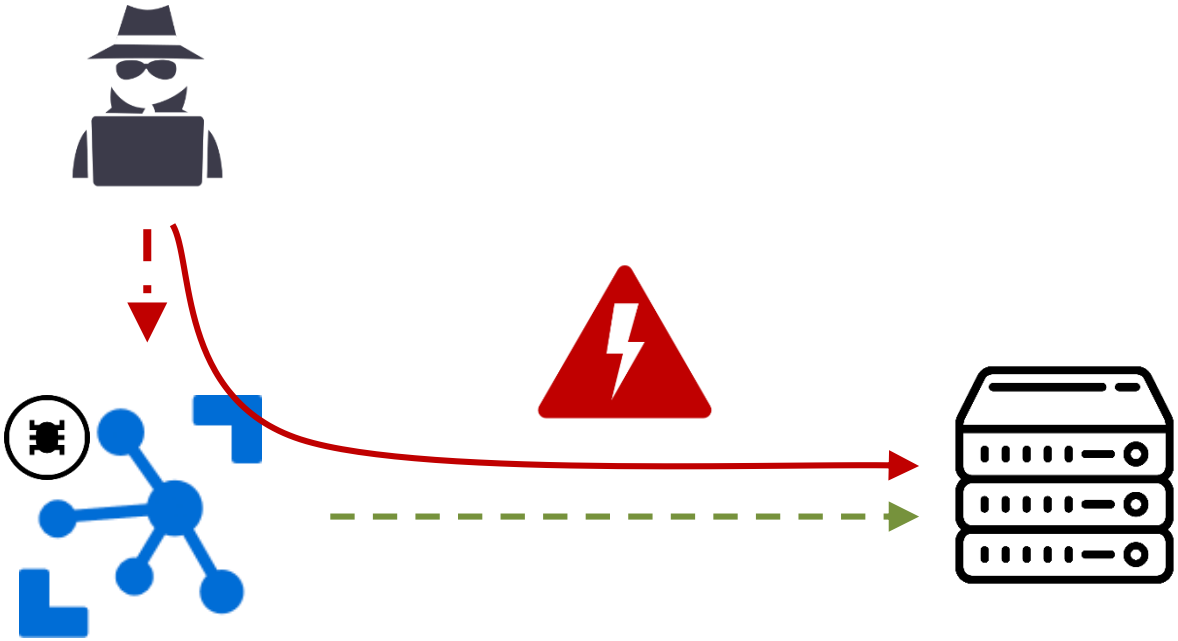
Example: DDoS Attack on Provider Dyn Oct. 2016 using 1.2 Tbps

Attack vector (2): Espionage



Tab data (camera stream, microphones)

Attack vector (3): Sabotage



Sabotage on infrastructure (Utility companies)
or using the IoT device as jumpstation

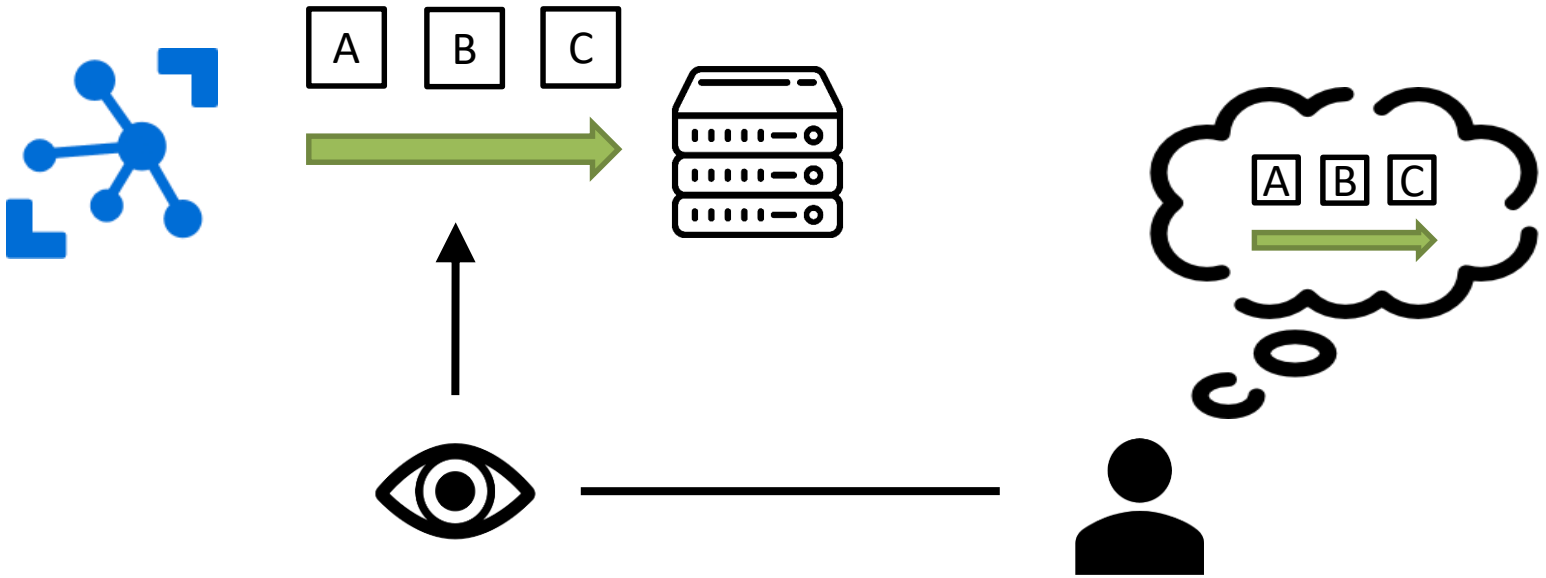
Problem: How to identify a compromised IoT device?

not compromised

Idea: Learn normal behavior and monitor

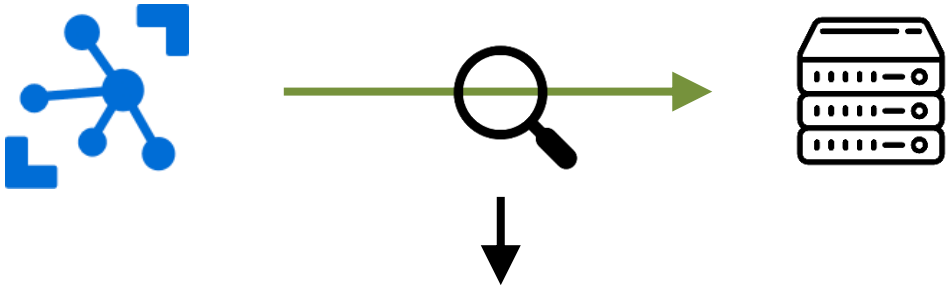
compromised

Idea: Analyzing predictable normal behavior



Observe and learn about **normal network activity** of an IoT device
within a protected environment

Analyzing connection metadata



Step 1
Collect connection
metadata from IoT devices

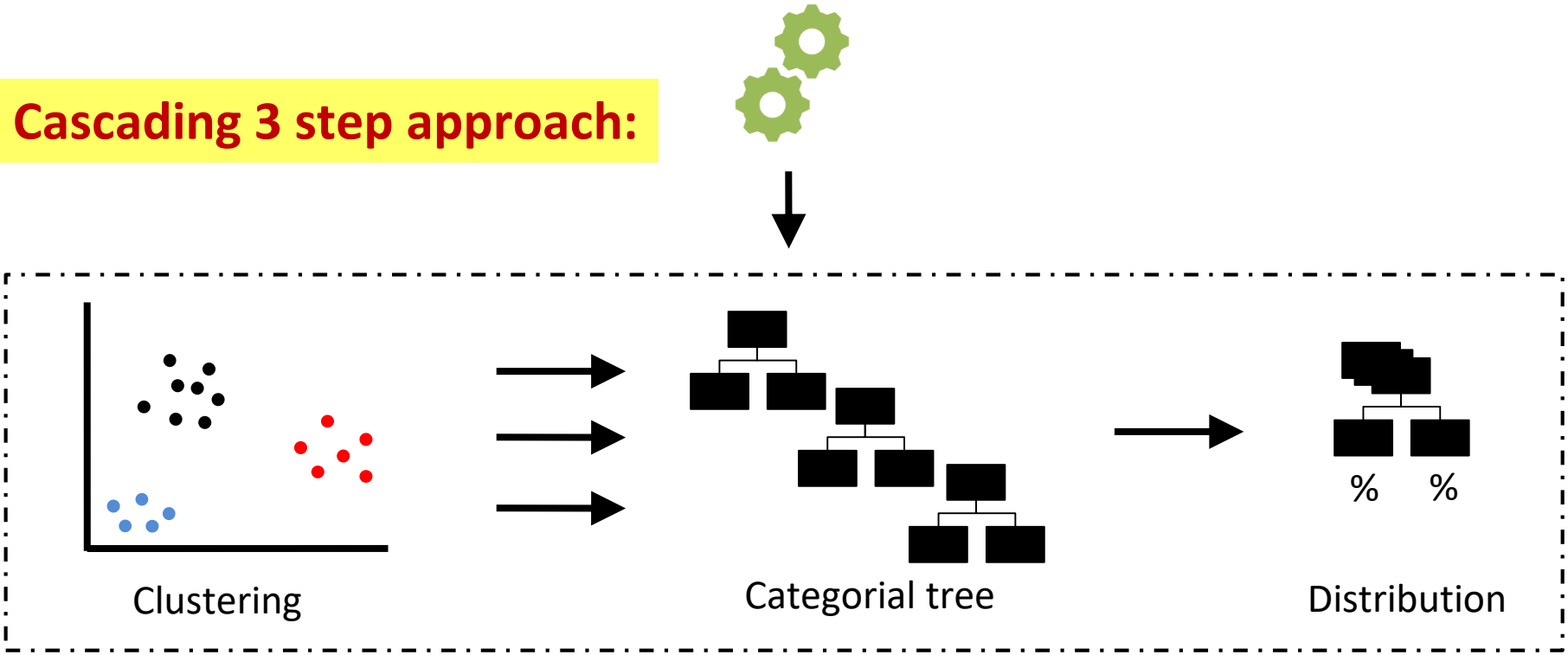
- Source- and Target address
- Duration
- Amount of transferred data
- Used services
- and more....

Analyzing connection metadata

Step 2
Training a communication model

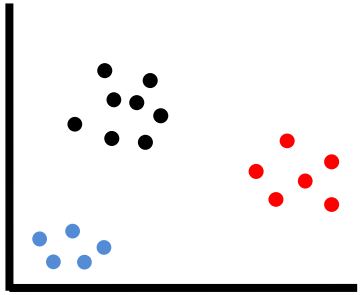
Analyzing connection metadata

Cascading 3 step approach:



Phase 1: Clustering

Duration
# of packets
# of bytes

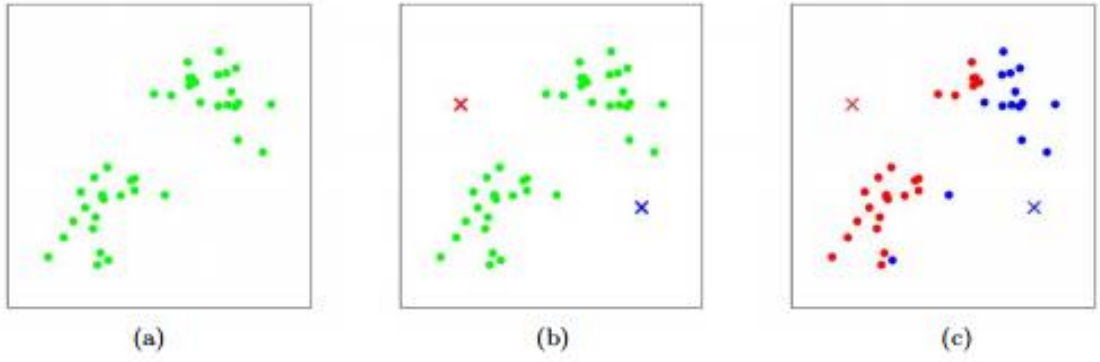


Connection metadata

Numeric parameters

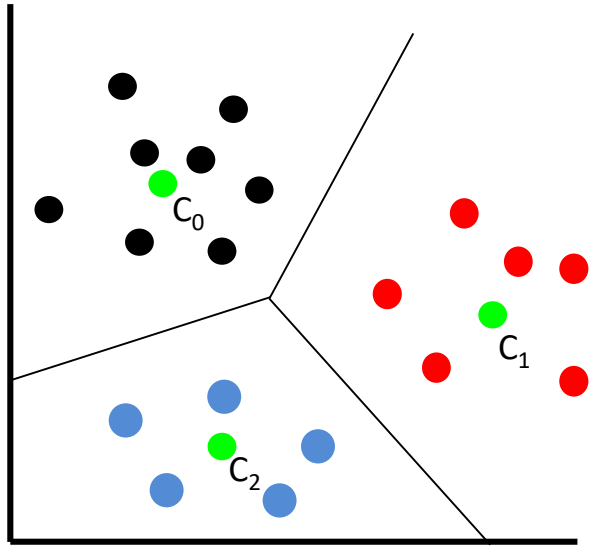
K-means clustering
(with X-means)

k-means Clustering

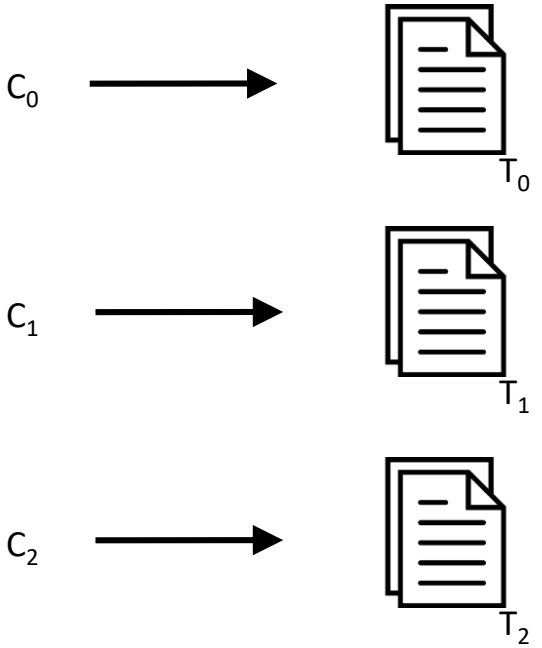


k-means clustering with k=2

Phase 1: Clustering



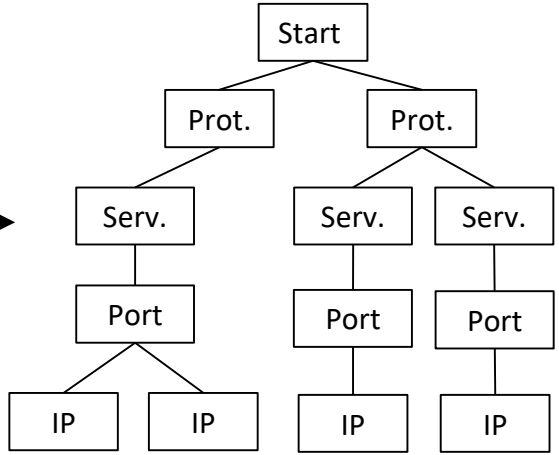
Cluster



k sets of training data with similar numeric parameters

Phase 2: Categorial tree

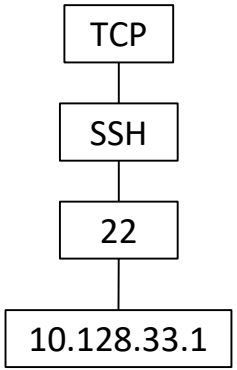
L4 protocol
Service
Port
IP-Address



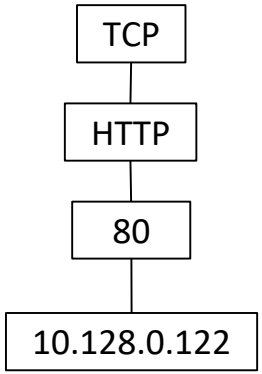
Connection metadata

Categorial parameters

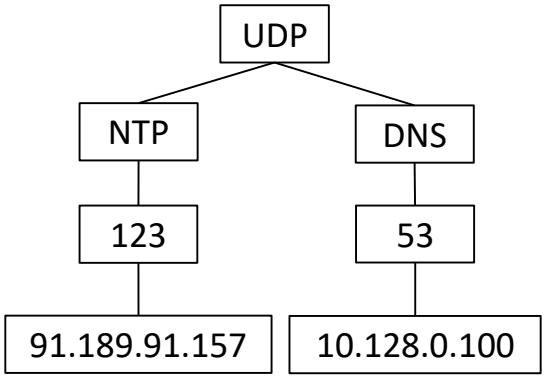
Phase 3: Calculate distribution



2%



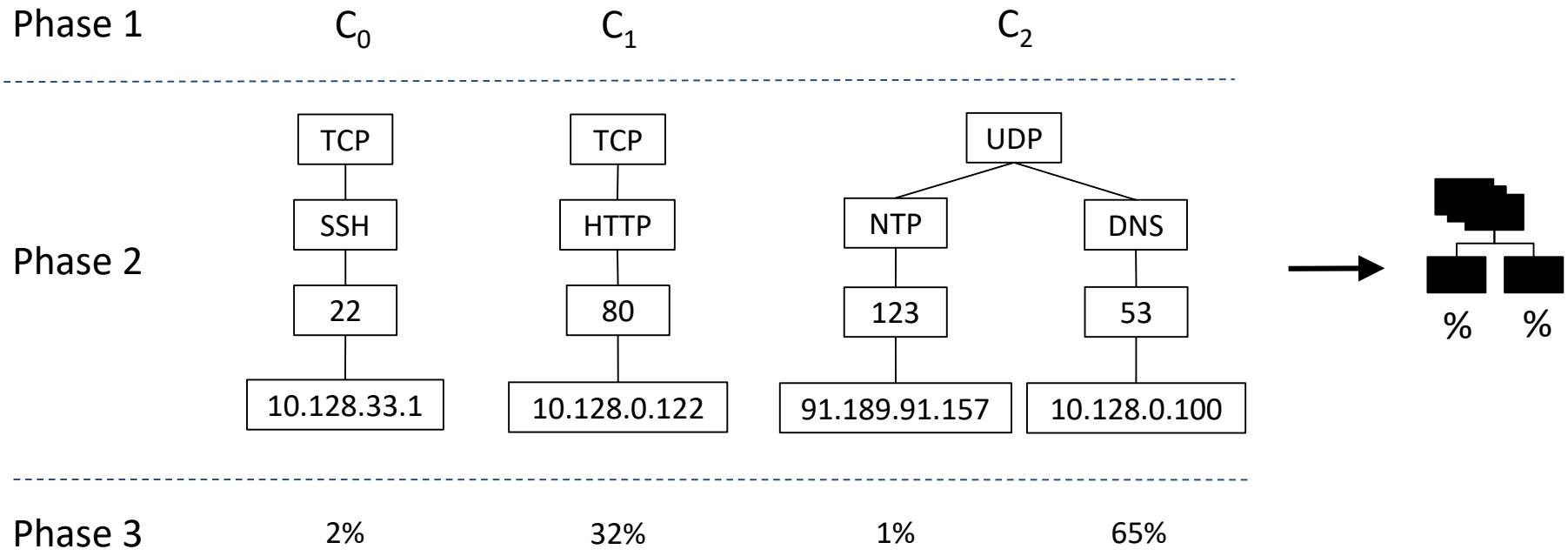
32%



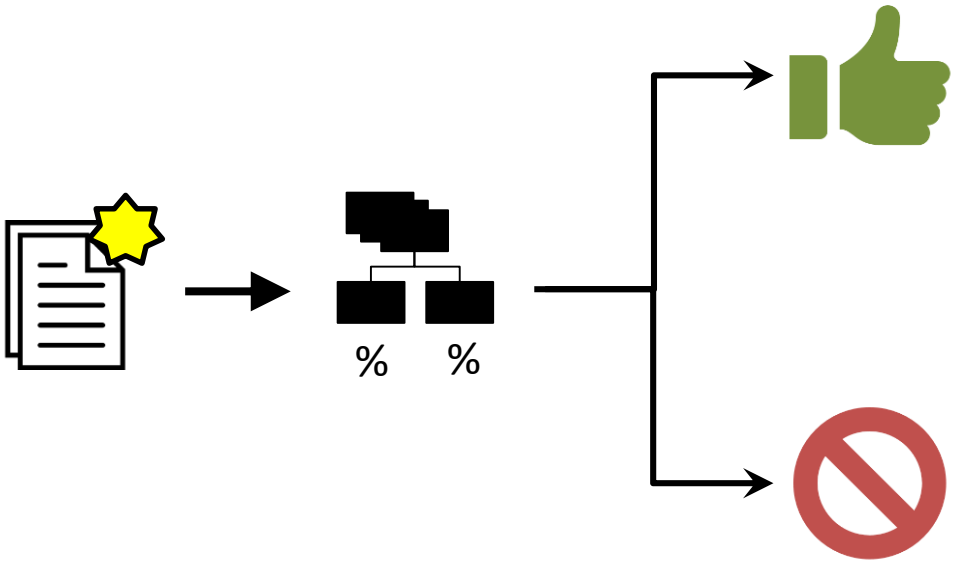
1%

65%

Final communication model

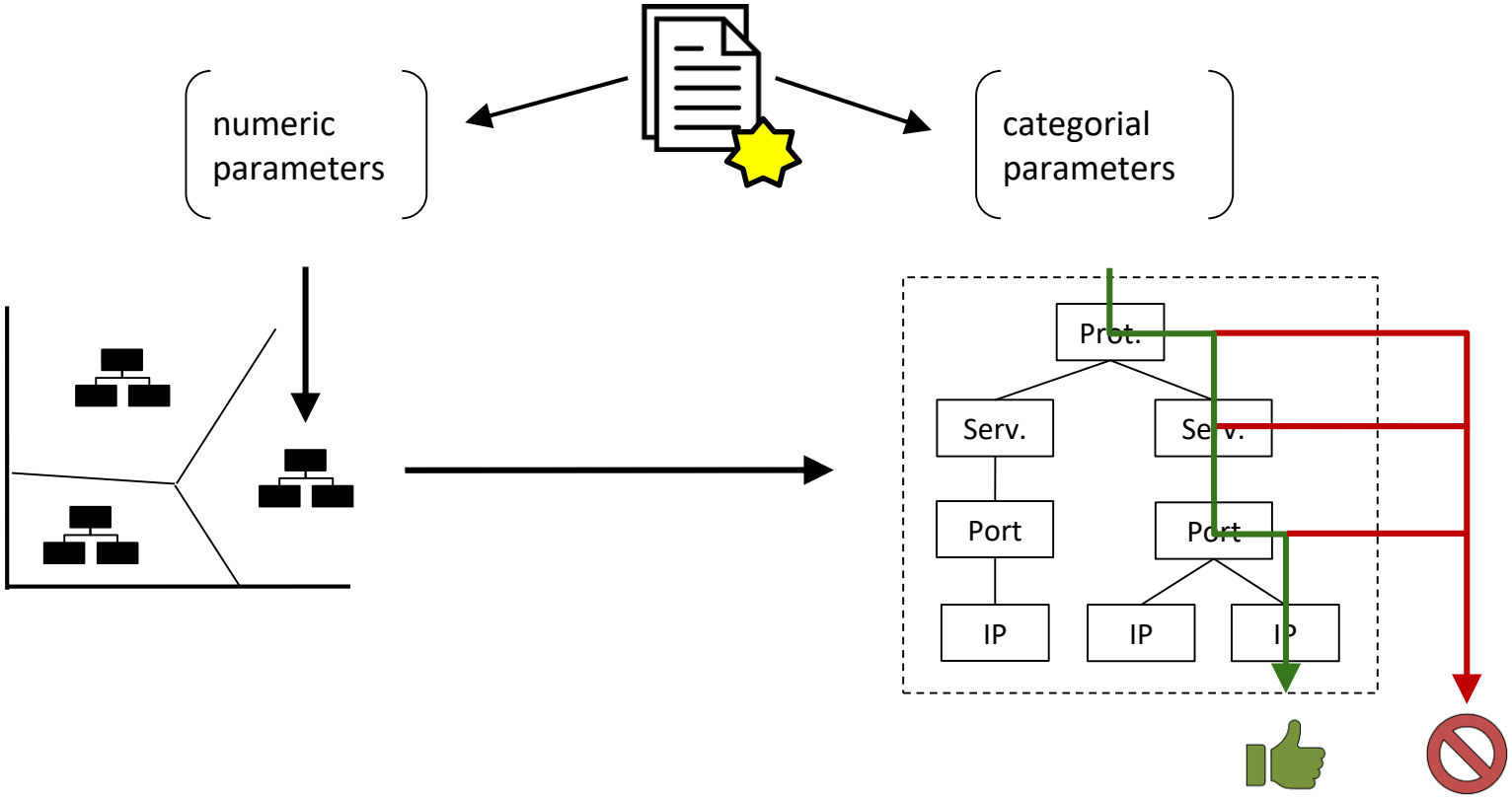


Categorizing connection metadata



Step 3
Apply the communication model to **new connection metadata** and **monitor the distribution** onto the categories.

Monitor connection metadata



Advances to Protect the Critical Assets Policies & Procedures

Dr Maria Bada
Global Cyber Security Capacity Centre
University of Oxford
Academy for Computer Science and Software Engineering
University of Johannesburg
maria.bada@cl.cam.ac.uk
@MariaBadaCC

The Third International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2018
18-22nd November 2018 - Athens, Greece

Global Cyber Security Capacity Centre
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD
DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF JOHANNESBURG

Critical Infrastructure Protection

- While the policies vary around the world, the basic need remains the same:
  - ensure protection of critical assets

- Unfortunately, many organizations do not know what their mission-critical information assets are, where these assets reside or who is responsible for them.

- A higher level of cyber resilience and CI protection can be achieved:
  - International standards such as ISO 27001 and ISO 27035
  - The implementation of business continuity management, penetration testing and cyber incident response management

The NIS Directive

The NIS Directive

- The NIS Directive stipulates that affected operators of essential services (OESs) and digital service providers (DSPs) must have in place:
  - An understanding of their assets and a mechanism to identify unknown devices
  - A mature vulnerability management program
  - Mature threat detection systems, including detecting, identifying, and reporting capabilities
  - Effective incident reporting mechanisms, including systems to record and report incidents within 72 hours of detection
  - Mature incident management
  - Response and recovery plans

The NIS Directive
Key Organisational Requirements

- ***Governance:*** Appropriate management policies and processes in place to govern the security of network and information systems.

- ***Risk management process:*** Take appropriate steps to identify, assess, and understand security risks to the network and information systems.

- ***Supply chain:*** Understand and manage security risks to networks and information systems which arise because of dependencies on external suppliers, including ensuring that appropriate measures are employed where third party services are used.

- ***Staff Awareness & Training:*** Awareness, knowledge, and skills to carry out roles effectively supporting the delivery of services.

The NIS Directive
Requirements on Cross-border Cooperation

- ***EU Security Network:*** Creation of a network of Computer Security Incident Response Teams (CSIRTs) in each Member State.
- ***Member State Strategy:*** Implementation of a national cybersecurity strategy.
- ***Cooperation Group:*** Creation of a Cooperation Group whose purpose is to facilitate collaboration around cybersecurity between Member States.
- ***Incident Reporting:*** Implementation of a range of risk management measures both technical and operational.

The Capacity Maturity Model CMM

The CMM

D 1.3: Critical Infrastructure (CI) Protection

This factor studies the government's capacity to:

- identify CI assets and the risks associated with them
- engage in response planning and critical assets protection
- facilitate quality interaction with CI asset owners
- enable comprehensive general risk management practice including response planning

https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

The CMM

D 1.3: Critical Infrastructure (CI) Protection					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Identification	Some understanding of what comprises CI assets is acknowledged, but no formal categorisation of assets has been produced.	A list of general CI assets has been created.	A detailed audit of CI assets as it relates to cybersecurity is performed on a regular basis. CI asset audit lists are disseminated to relevant stakeholders.	CI risks and assets have been prioritised according to vulnerability and impact, which guides strategic investment. Vulnerability/asset management processes are in place so that incremental security improvements can be made.	Priority listing of CI assets is regularly re-appraised to capture changes in the threat environment.
Organisation	There is little or no interaction between government ministries and owners of CI assets. No mechanism for collaboration exists.	There is informal and ad-hoc threat and vulnerability disclosure among CI owners as well as between CI and the government, but the scope of reporting requirements has not been specified.	A mechanism is established for regular vulnerability disclosure with defined scope for reporting incidents (either mandatory or voluntary) between CI asset owners and the government. Formal internal and external CI communication strategies have been defined and are consistent across sectors, with clear points of contact. Strategic engagement between government and CI is agreed and promoted.	There is a clear understanding of which threats to CI are managed centrally, and which are managed locally. A public awareness campaign to facilitate the CI communication strategy is established with a point of contact for this information. Cybersecurity requirements and vulnerabilities in CI supply chains are clearly identified, mapped and managed.	Owners of critical infrastructure and assets are able to rapidly respond to the changing threat landscape. Trust has been established between the government and CIs with respect to cybersecurity and exchange of threat information, which is fed into the strategic decision-making process.

The CMM

Risk Management and Response	Risk management skills and understanding may be incorporated into business practices, but cybersecurity, if recognised, is subsumed into IT and data protection risk and is not recognised as a priority. Response planning and threat awareness may have been broadly discussed, but no formal plan exists.	Physical and virtual access control is implemented. CI has basic capacity to detect, identify, respond to and recover from cyber threats, but such capabilities are uncoordinated and vary in quality. Protection of CI assets includes basic level cybersecurity awareness and data security policies, but no protection processes have been agreed.	Best practices in security measures, guidelines, and standards for CI cybersecurity have been established and adopted. Cybersecurity risk management processes have been established, supported by adequate technical security solutions, communication links, and harm mitigation measures. CI risk management procedures are used to create a national response plan including the participation of all vital entities.	Cybersecurity is firmly embedded into general risk management practice. Assessment of the breadth and severity of harm incurred by CI assets is regularly conducted and response planning is tailored to that assessment to ensure business continuity. Resources are allocated in proportion to the assessed impact of an incident to ensure rapid and effective incident response. Insider threat detection is accounted for.	Audit practices to assess network and system dependencies and vulnerabilities (i.e. unmitigated dependencies) are implemented on a regular basis and inform continuous reassessment of CI risk portfolio, technologies, policies and processes. The impact of cybersecurity risk on the business operations of CI, including direct and opportunity costs, impact on revenue, and hindrance to innovation, are understood and incorporated into future planning and executive decision making.

Recommendations

Recommendations for Critical Infrastructure Security

- **Create better information sharing strategies with private sector:** promote information sharing between the government and the private sector.
- **Roll out a cyber education strategy:** It is necessary for cyber education to become a bigger priority within the government.
- **Carry out crisis scenario exercises:** Such preparation needs to take place in advance, in crisis scenario exercises that simulate how a response team would handle a sudden incident.

THANK YOU!

Dr Maria Bada
Global Cyber Security Capacity Centre
University of Oxford
Maria.Bada@cl.cam.ac.uk
@MariaBadaCC

Australian Government
Department of Human Services

The cyber staff shortage that exists worldwide and developing and growing cyber capabilities

Narelle Devine
Chief Information Security Officer
Department of Human Services


AUSTRALIA
Australian Government
Department of Human Services
CYBER SECURITY BRANCH

“Only thing worse than training your employees and having them leave is not training your employees and having them stay”

- Henry Ford

OPERATION: SHELL BREAKER 2014

CYBER WAR GAMES

10-14 SEPTEMBER 2018

CANBERRA, AUSTRALIAN CAPITAL TERRITORY

“The current and projected workforce needs must be met, not only by training more cybersecurity personnel, but also raising the bar on their skills, aptitude and ability to collate”

- NIST

@narelle_devine

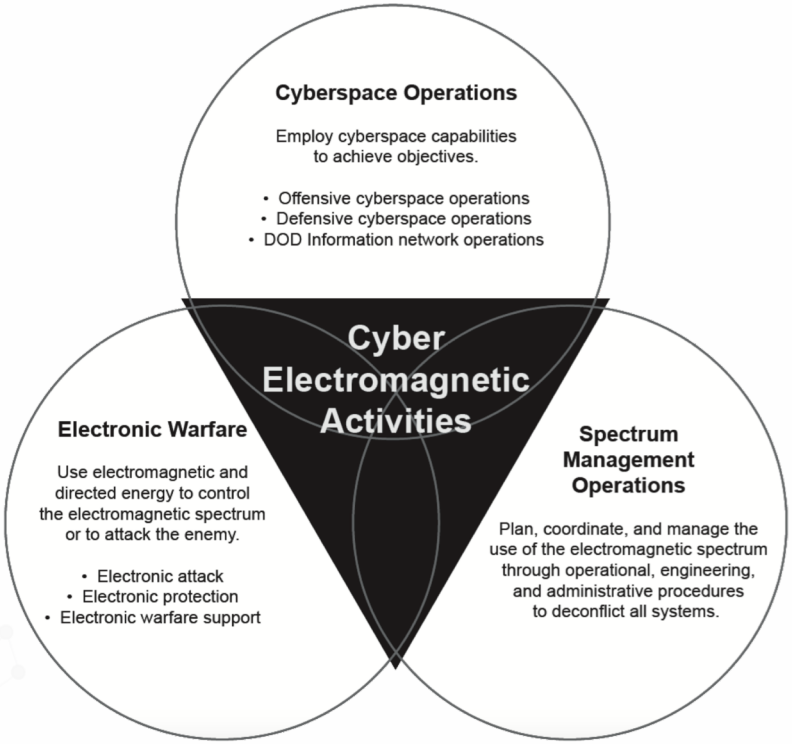
Narelle Devine

Facilitating Decision-Making Via Deep Insights

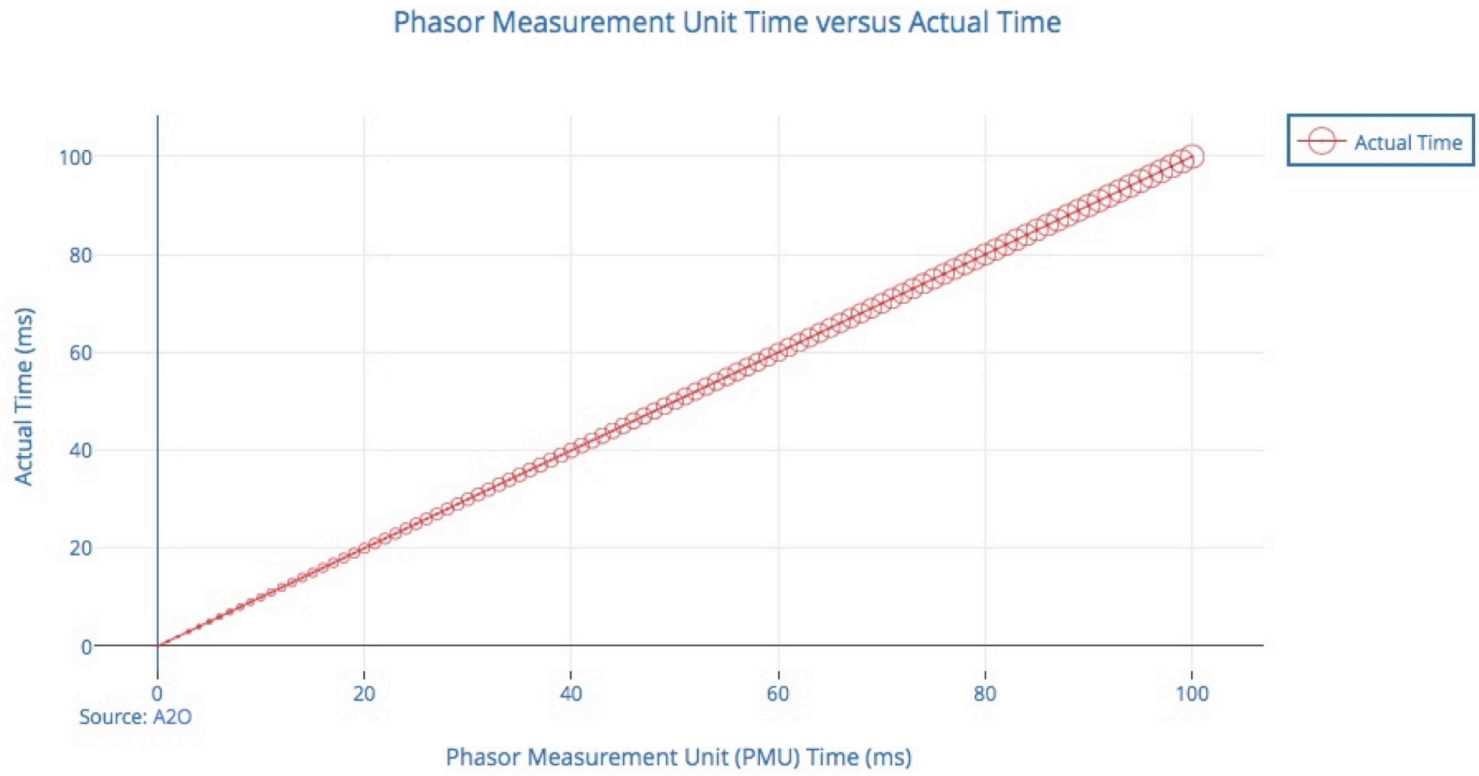
Panel on
Challenges in Cyber Services:
Advances to Protect Critical Assets.
Tuesday 20 November 2018

Dr. Steve Chan
Decision Engineering Analysis Laboratory

”Normal Time” versus Anomalous Time for Global Positioning System (GPS) Timestamps



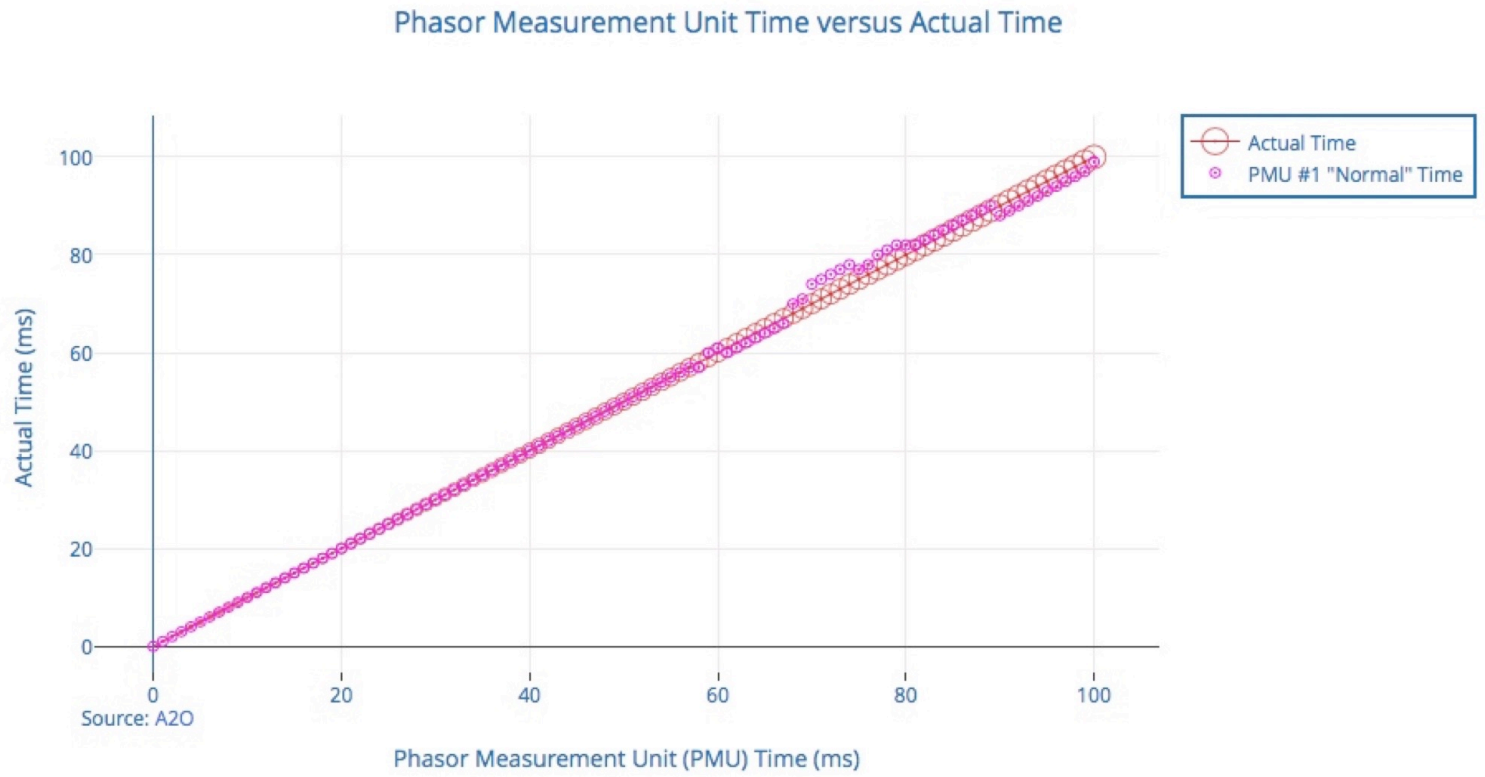
Facilitating Decision-Making Via Deep Insights



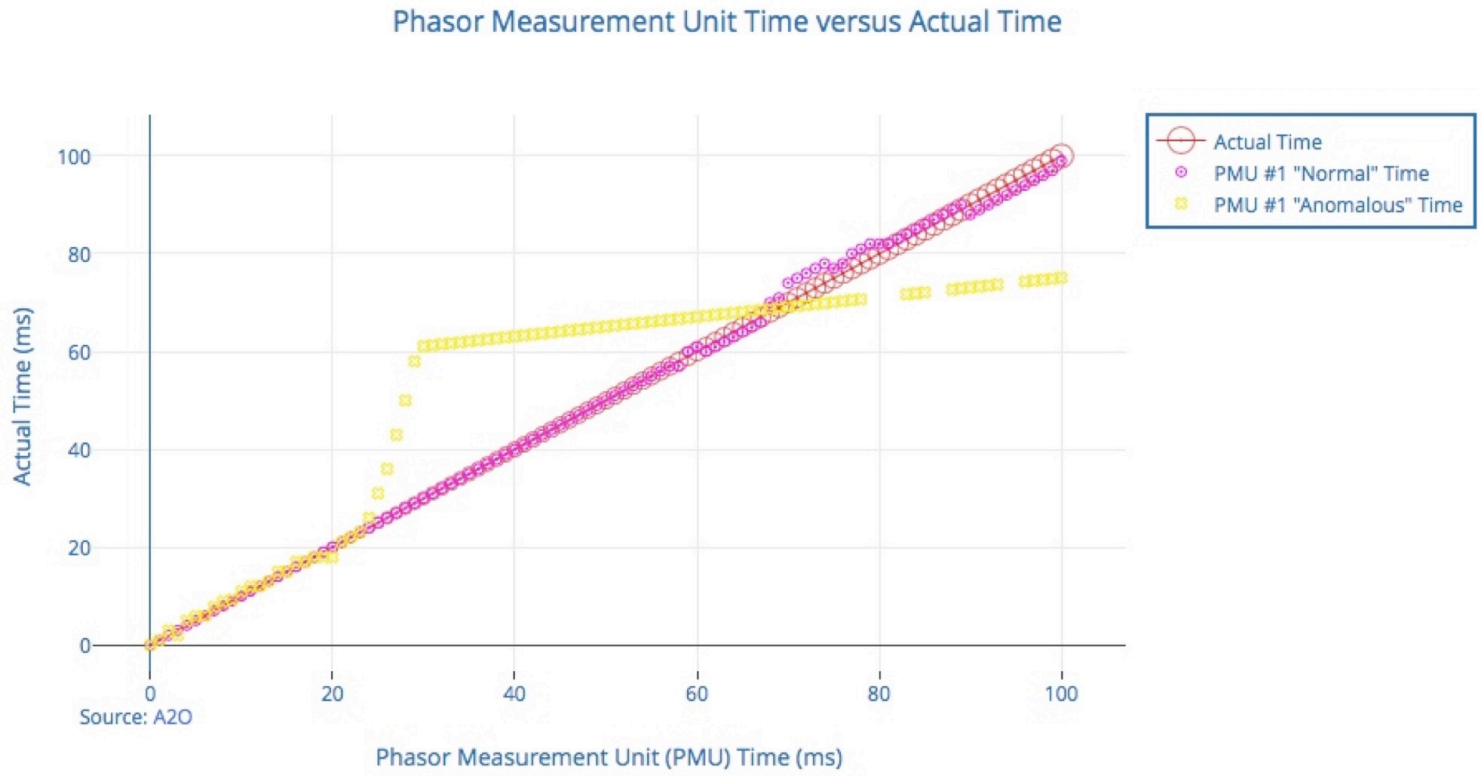
Decision Engineering Analysis Laboratory

San Diego
Cambridge

Facilitating Decision-Making Via Deep Insights



Facilitating Decision-Making Via Deep Insights



Decision Engineering Analysis Laboratory

San Diego
Cambridge

Facilitating Decision-Making Via Deep Insights

Thank you to IARIA and all the participants of Cyber 2018.

The Third International Conference on Cyber-Technologies and Cyber-Systems

November 18, 2018 to November 22, 2018 - Athens, Greece

Decision Engineering Analysis Laboratory

San Diego
Cambridge

Using Blockchain to Protect Critical Assets

XING LIU
KWANTLEN POLYTECHNIC UNIVERSITY
CANADA

“Natural” Questions

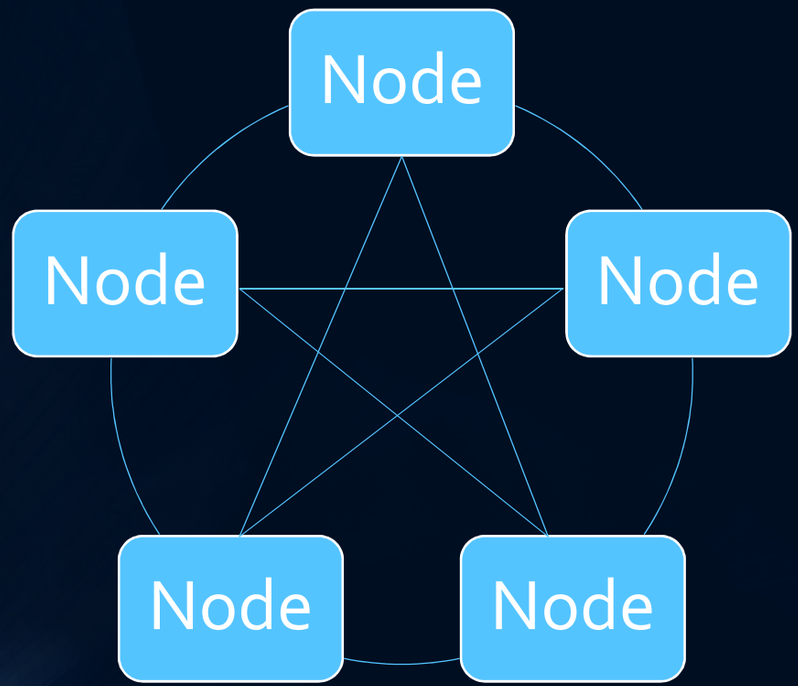
- What is a blockchain
- What is special
- What can it do for us

What Is A Blockchain (NIST)

- Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority
- Can be considered to be a spreadsheet that is duplicated thousands of times across a network of computers.

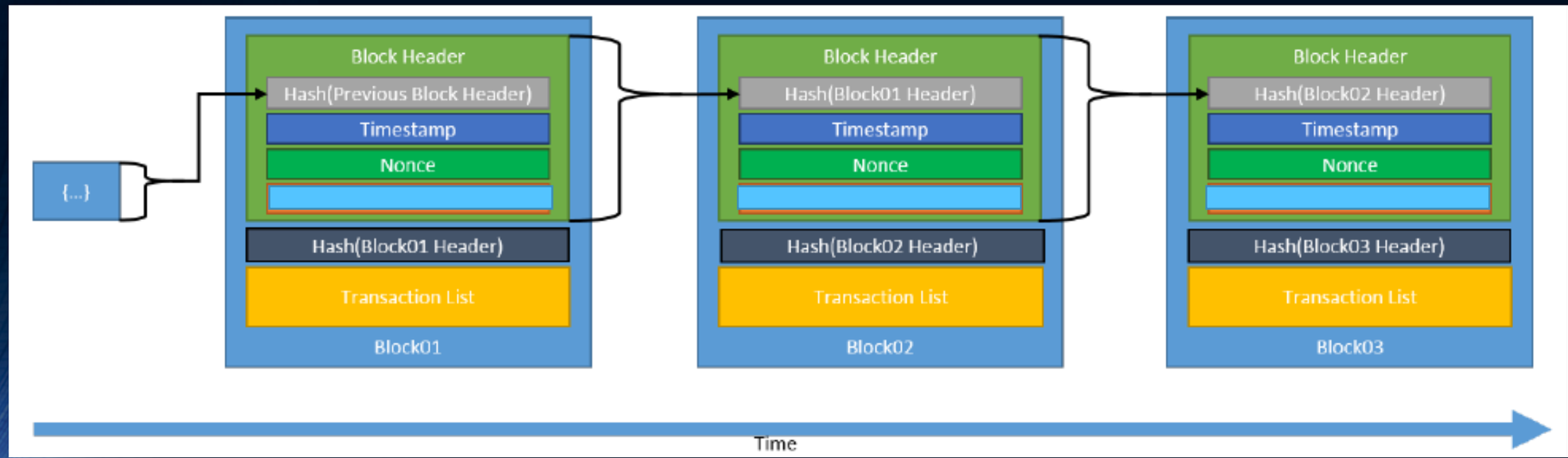
Source:
D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview", Draft NISTIR 8202, NIST, January 2018

A Live Blockchain: A Distributed System as a Network of Nodes



Each node keeps a copy of the blockchain (the ledger)

A Blockchain (the Ledger)



Source:
D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview", Draft NISTIR 8202, NIST, January 2018

What Is Special about A Blockchain

- Transactions are signed and can be verified
- The ledger is duplicated and distributed
- Transactions are added to the blockchain after being verified
- Blockchains are maintained through a consensus mechanism

What Is New about Blockchain

- Distributed → No need for central agent
- Growing-only chain → Permanent records
- Duplicated copies → No single point of failure
- Chained structure → No modifications of history allowed
- Consensus mechanism → Stop bad transactions and blocks
- Smart contracts → Immutable processing of complex transactions
- Transparency → All participants can see the transactions (for public chains)
- Traceability → Transactions made when and by whom

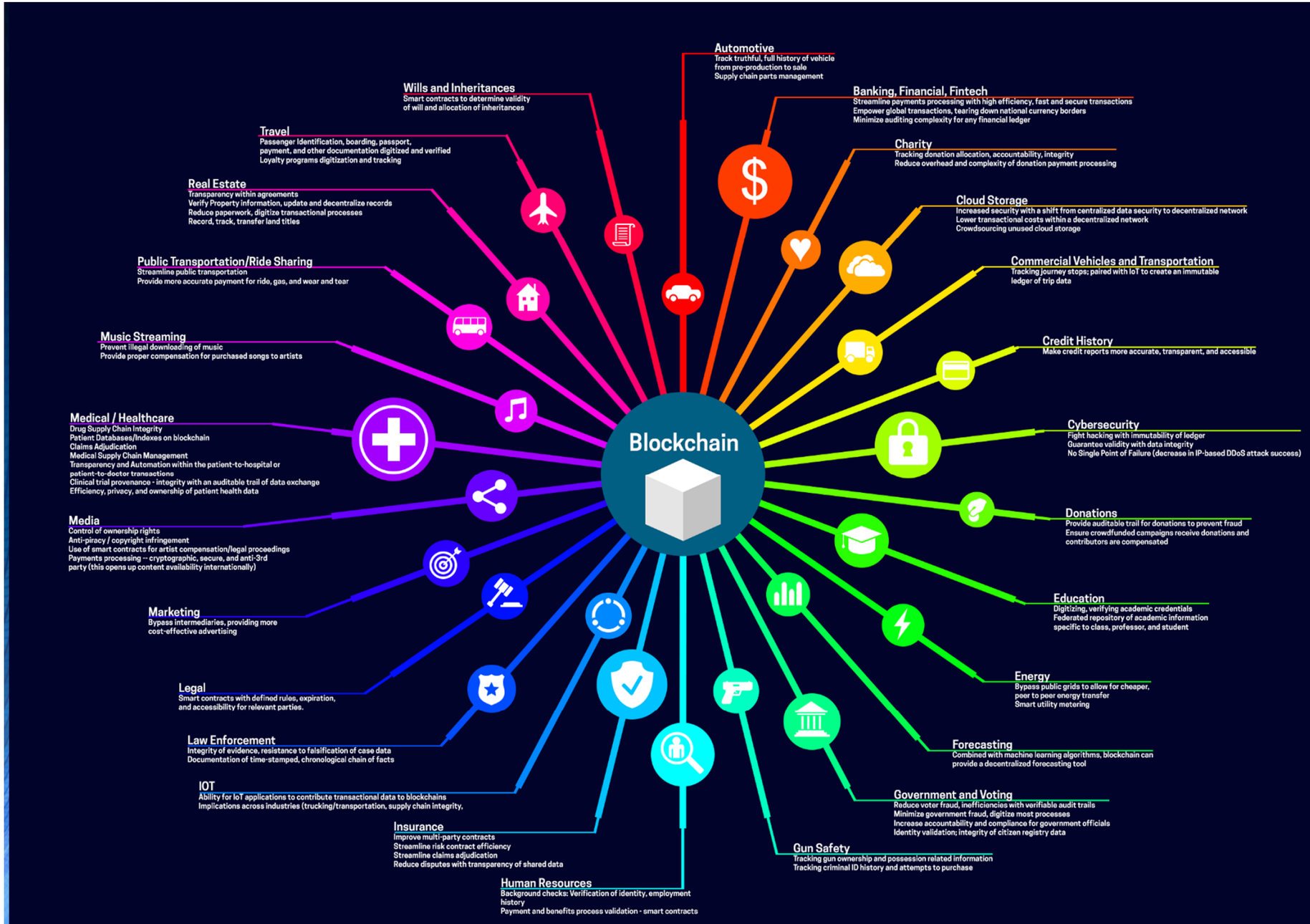
- Comparing to current centralized data storage → Much higher security

To make it short:

- Cryptography makes data harder to read
- Blockchain makes data harder to corrupt

Applications

Lots of attempts are underway



Source: medium.com

Supply Chain Management as An Example

With blockchain:

- Companies gain a real-time digital ledger of transactions and movements for all participants in their supply chain network
- Companies can see the total volume all relevant partners
- Procurement: more visibility and potentially more savings
- Ability to track and manage resources at the ecosystem level
- Much greater accuracy, better forecasts, less inventory to maintain service

Paul Brody: How blockchain is revolutionizing supply chain management, ey.com

Supply Chain Management as An Example

- (Smart contracts) Immediate and automatic digital invoicing and payments
- Reduced working capital requirements
- Simplified finance operations
- Prevent fraud
- More accurate inventory control
- Product transaction status updated for everyone, everywhere, within minutes, with full traceability back to the point of origin

Identity Management: Another Example

Digital identities Problems:

- Where is all that information located?
- What purpose does it get used for and by whom?
- How secure is it?
- Who has seen it?
- How up-to-date is it?
- Nobody really knows – neither do the individuals who generate the data, nor do the governments and industries that own the databases - it is totally out of our control
- Servers can be hacked, and personal data in the hands of a small group of companies

https://www.accenture-insights.nl/en-us/articles/how-blockchain-will-revolutionize-identity-management

Identity Management Using Blockchain

With blockchain:

- Single source of truth
- Individuals control of their identities
- Improved interactions with public and private service providers
- Trusted source of information for every interaction with all stakeholders
- You are the owner of your identity data

Healthcare Applications of Blockchain

Data managed by medical organizations includes:

- Patient health information (PHI)
- Electronic health records
- Data collected from IoT devices (Internet of Things) or monitoring systems
- Medical insurance claims

- Similar to identity management, blockchain brings in enhanced security to the data

Other Applications

- Insurance
- Student records
- IoT device ID management
- IoT sensor data management
- ……

Is Blockchain Perfect?

Not really ….

- Vulnerabilities in the consensus mechanisms
- Vulnerabilities due to attacks on computer networks
- ……

- More research needed to make blockchains more secure

Thank you very much