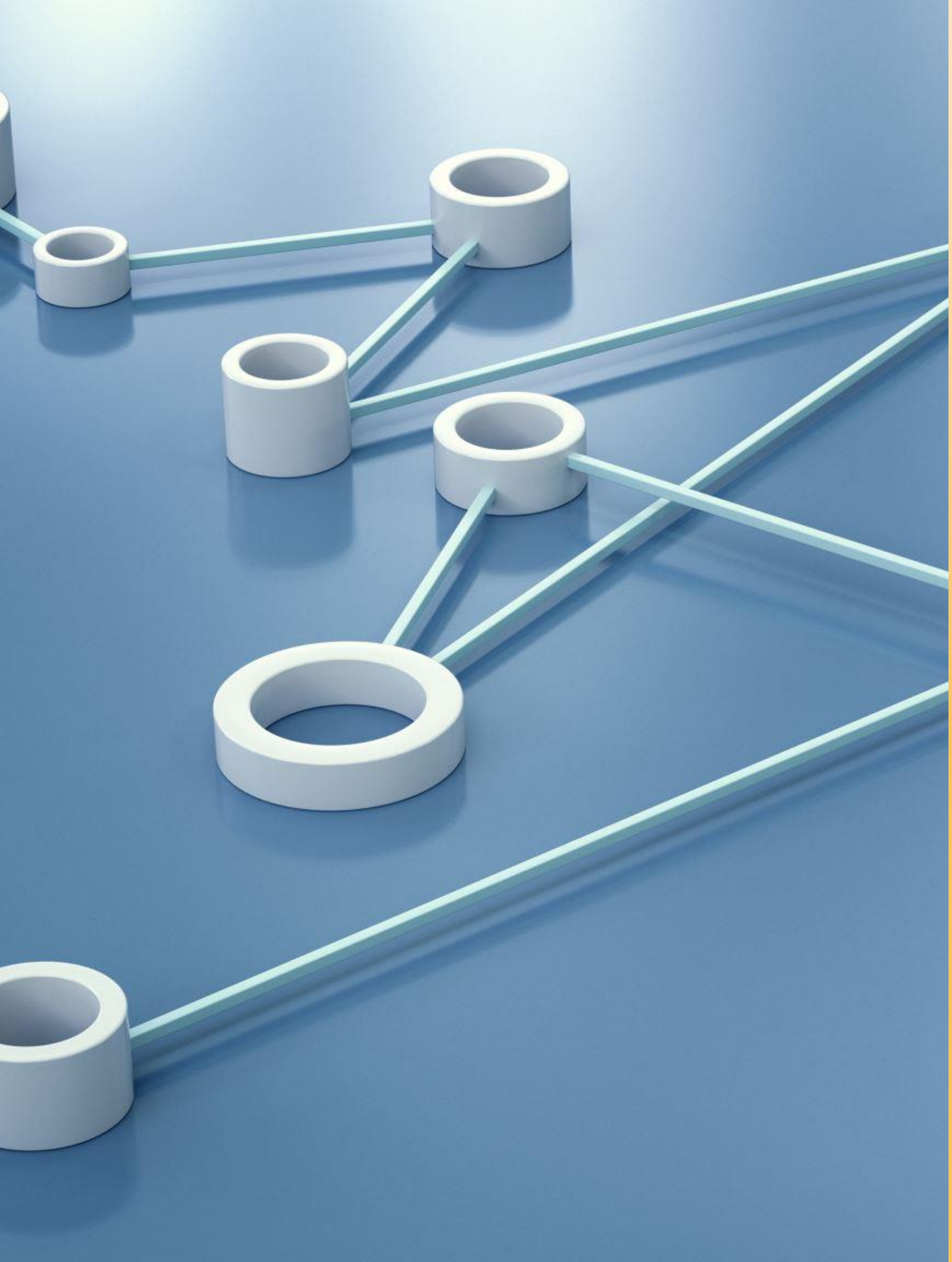
Context is King!

Stronger, Smarter Security with Identity in Context

Image: Harryarts / Freepik

Christen Patterson
CISSP

Christen is a Product Leader specializing in identity. Having worked in security and risk at various companies including Visa, Workday, and IndyKite, she brings together the perspectives of a security practitioner with that of a security solution vendor to apply empathy and innovation to problem solving.



Disclaimer

The views and opinions expressed in this presentation are solely my own and do not necessarily reflect the official policy or position of any current or previous employers.

- Personal Perspective: The content shared here is based on my personal experiences, research, and insights.
- No Endorsement: Any mention of specific companies, products, or services does not imply endorsement or affiliation.
- Independent Thought: This presentation is intended for informational purposes only and should not be construed as professional advice.

Identity-based Knowledge Graphs
are set to change how we
secure our data and our services

Technology Trends

"Identity is the new perimeter"

Rise of knowledge graphs

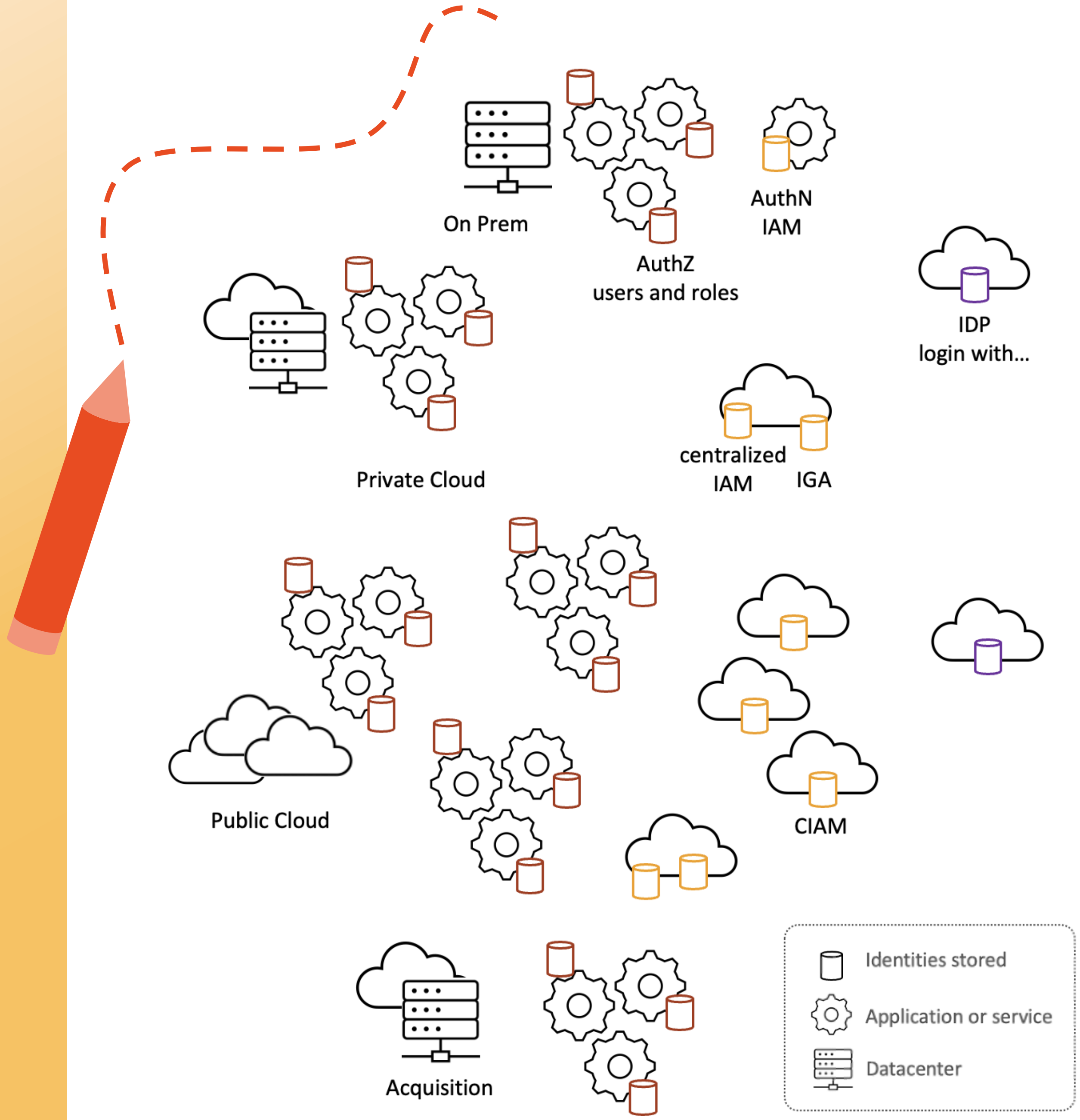
From authN to authZ

Technology Trends

“Identity is the new perimeter”

Why “Identity is the new perimeter”

- Dissolution of traditional network boundaries - Growth of cloud, hybrid cloud, multi-cloud, hybrid multi-cloud enterprises
- Omni-channel customer touchpoints (Web, Mobile, Vehicle, Voice Assistant, POS, Call Center)
- Partner delivered services – B2B2C services
- BYOD policies at work
- Zero trust framework
- Rise of remote work



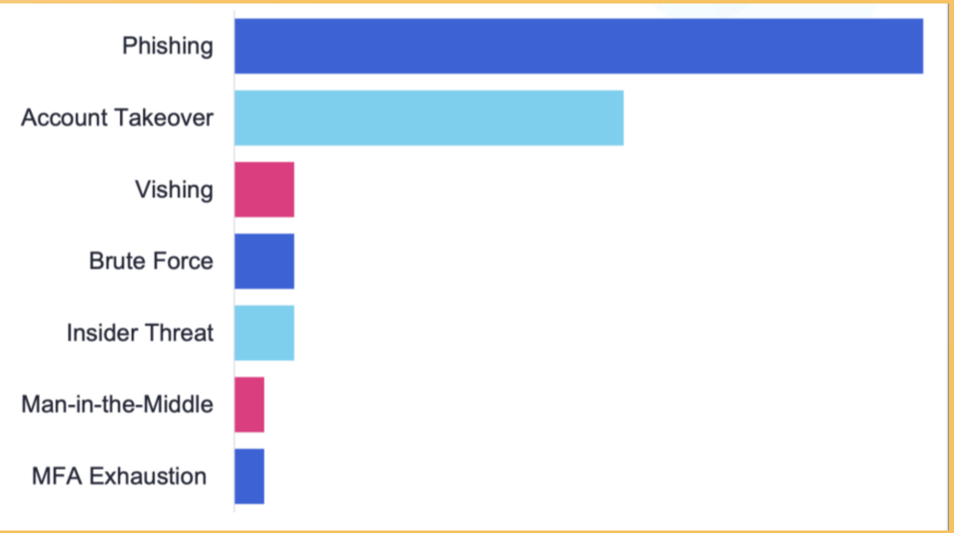
Corollary: Identity is the greatest vulnerability

4/5 breaches involved identity and compromised credentials

75% of breaches are caused by mismanaged identity, access, or privileges

https://pushsecurity.com/blog/identity-attacks-in-the-wild/

Top Identity Attacks 2022

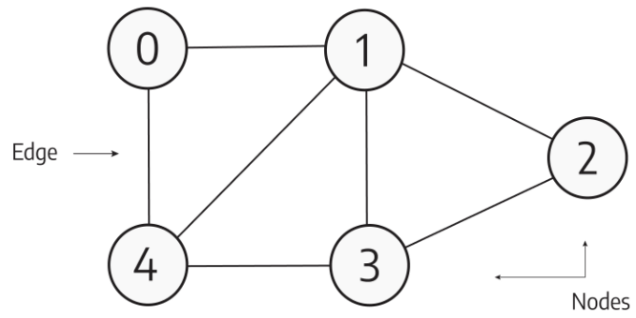


RSAC 2024 session: *Applying Past Lessons for Intel-Driven Identity Threat Detection,* Nicole Hoffman, Cisco Talos

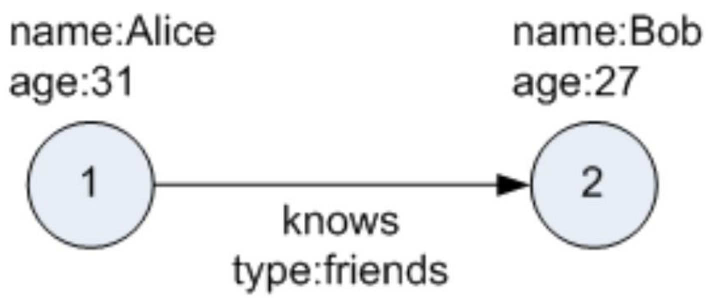
Technology Trends

Rise of Knowledge Graphs

What is a graph?

DEFINITION	A graph is a structure of a set of objects, in which pairs of objects are "related.” The objects are represented by abstractions called vertices (or nodes), and each of the connections between related pairs of vertices is called an edge.
SIMPLE EXAMPLE	 

What is a property graph?

DEFINITION	Type of graph database that models data as entities and their relationships. It's made up of vertices, or objects, and edges, or arrows, that connect the vertices. Each vertex has a unique identifier and can have multiple properties, which are represented as key-value pairs.
SIMPLE EXAMPLE	

What is knowledge?

DEFINITION	The fact or condition of knowing something with familiarity gained through experience or association.
EXAMPLE	Knowledge in the context of a knowledge base is a collection of information that's organized in a way that helps people find answers to their questions.

What is a knowledge graph?

DEFINITION	*A graph of data intended to accumulate and convey knowledge of the real world, whose nodes represent entities of interest and whose edges represent relations between these entities* Hogan, et al. https://arxiv.org/pdf/2003.02320
	Also known as a **semantic network**, a knowledge graph holds unified, curated data on a **network** of real-world entities such as persons, objects, or events; models the **connections** between the entities, thus capturing **context**; and structures the data in a way that is optimal for deriving inferences

Evolution of Knowledge Graphs

4th Century BC
Aristotle's logic diagrams

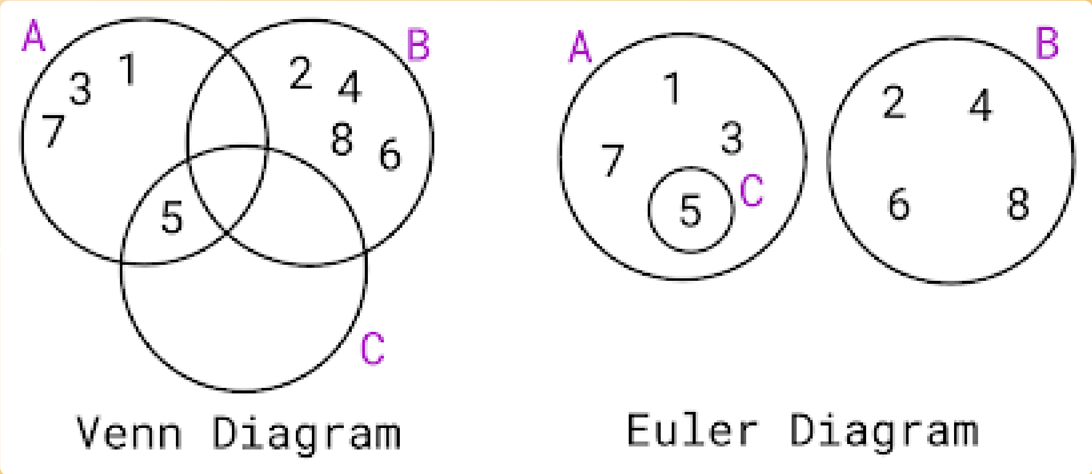
Figure 1. Two classical squares of opposition in (**a**) CPL and (**b**) KD.

Evolution of Knowledge Graphs

4th Century BC
Aristotle's logic diagrams

1768
Euler circles

1880
Venn diagrams



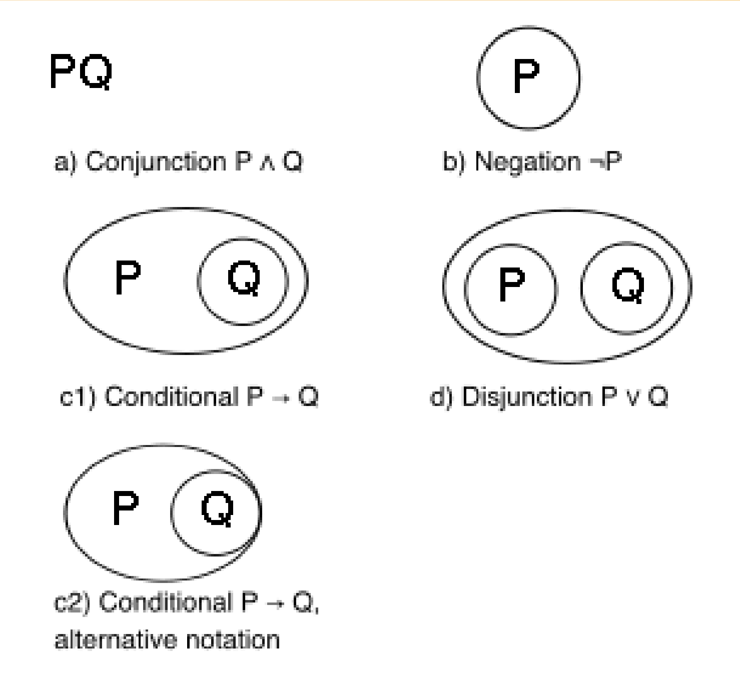
Evolution of Knowledge Graphs

4th Century BC
Aristotle's logic diagrams

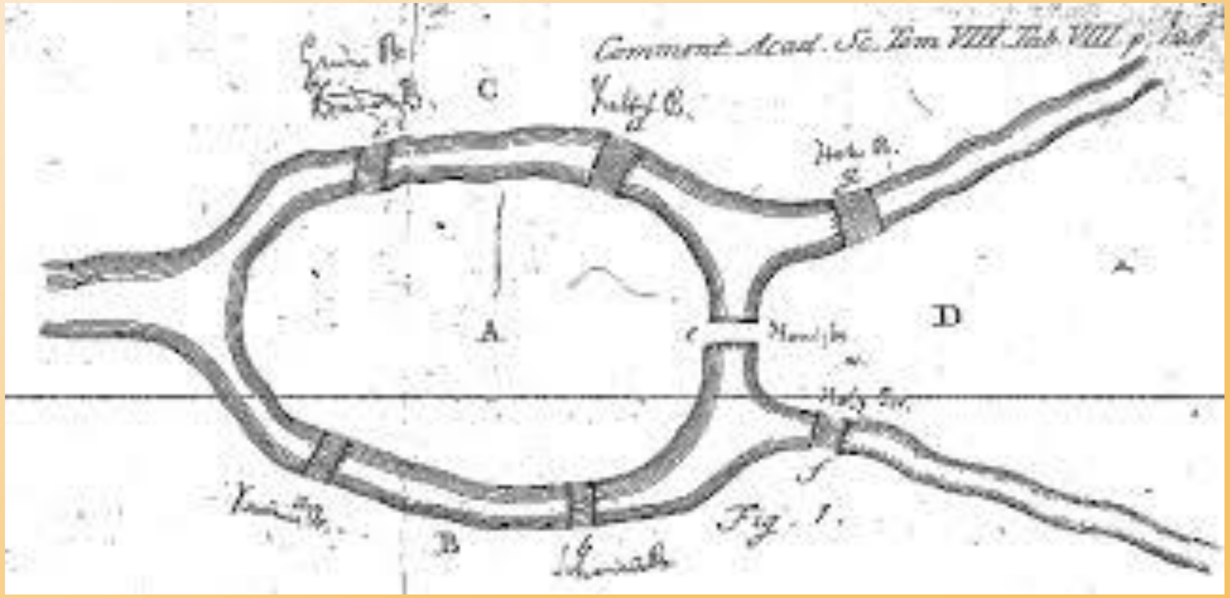
1768
Euler circles

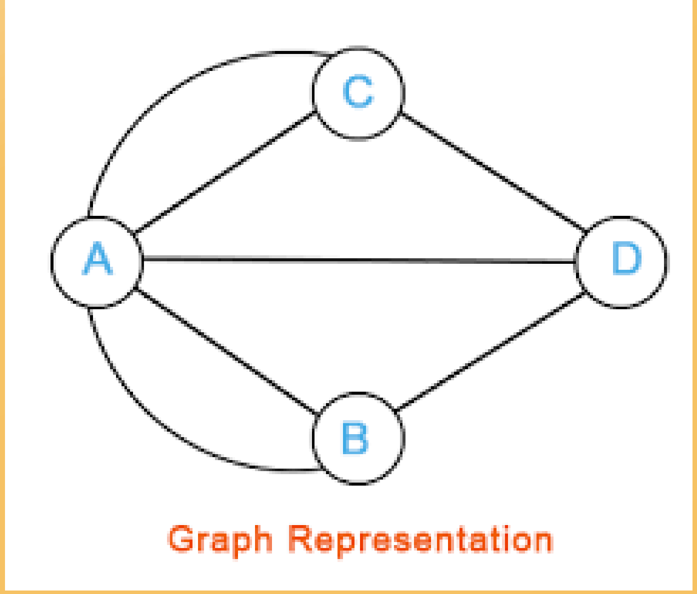
1880
Venn diagrams

1882
Existential graphs



Seven Bridges of Königsberg





Evolution of Knowledge Graphs

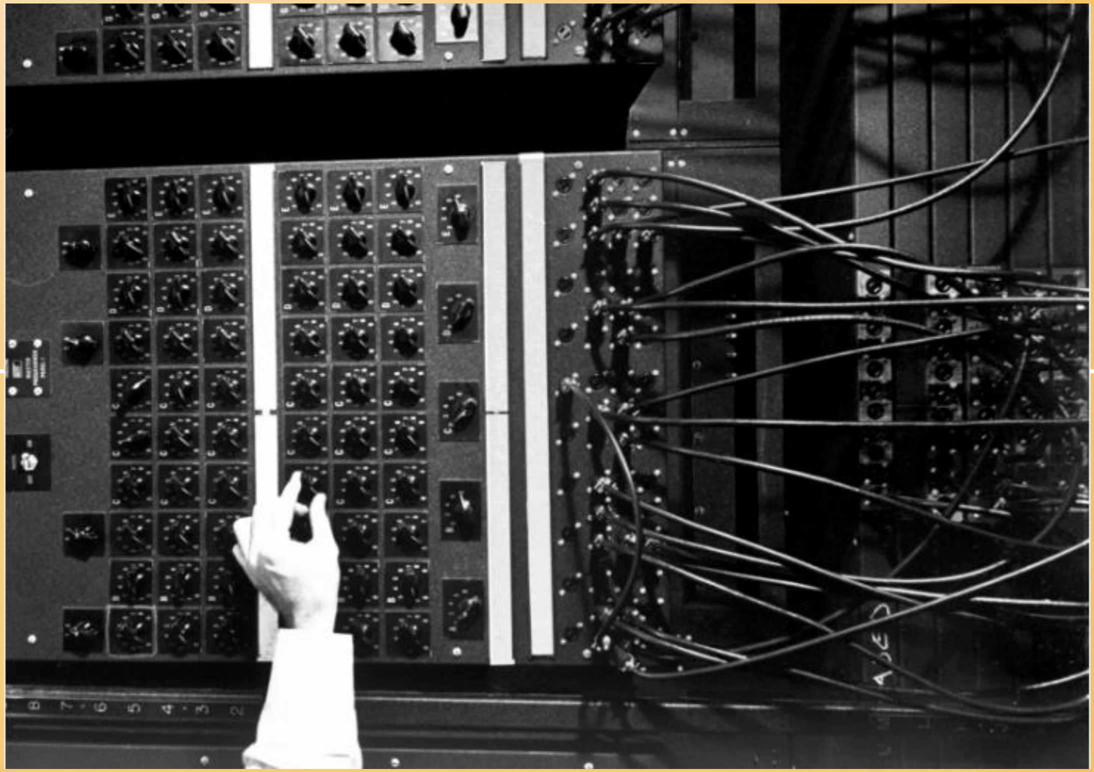
4th Century BC
Aristotle's logic diagrams

1768
Euler circles

1880
Venn diagrams

1882
Existential graphs

1950s – 1960s
Formal representations for natural language



Evolution of Knowledge Graphs

4th Century BC
Aristotle's logic diagrams

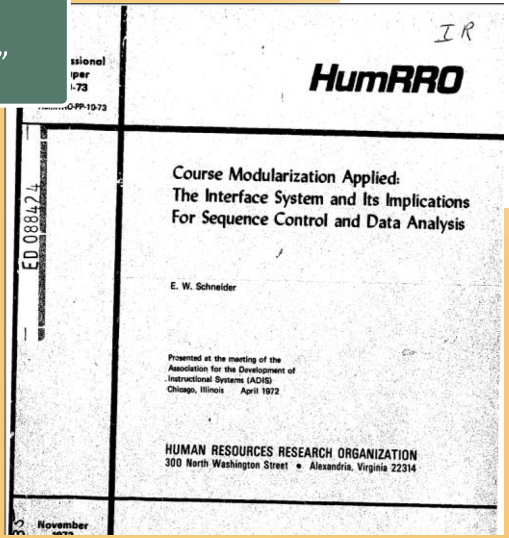
1768
Euler circles

1880
Venn diagrams

1882
Existential graphs

1950s – 1960s
Formal representations for natural language

1972 Term
"Knowledge graphs"



IR

HumRRO

ED 088424

Course Modularization Applied:
The Interface System and Its Implications
For Sequence Control and Data Analysis

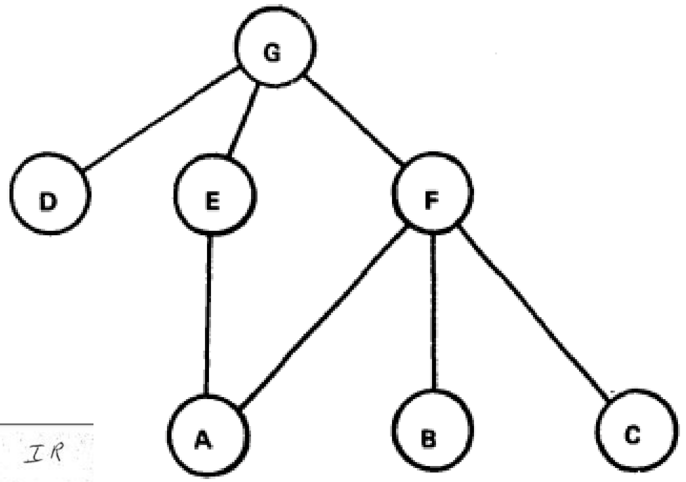
E. W. Schneider

Presented at the meeting of the
Association for the Development of
Instructional Systems (ADIS)
Chicago, Illinois April 1972

HUMAN RESOURCES RESEARCH ORGANIZATION
300 North Washington Street • Alexandria, Virginia 22314

November

A Cluster of Training Objectives



Each objective is an Interface Module.

Figure 13

Evolution of Knowledge Graphs

4th Century BC
Aristotle's logic diagrams

1768
Euler circles

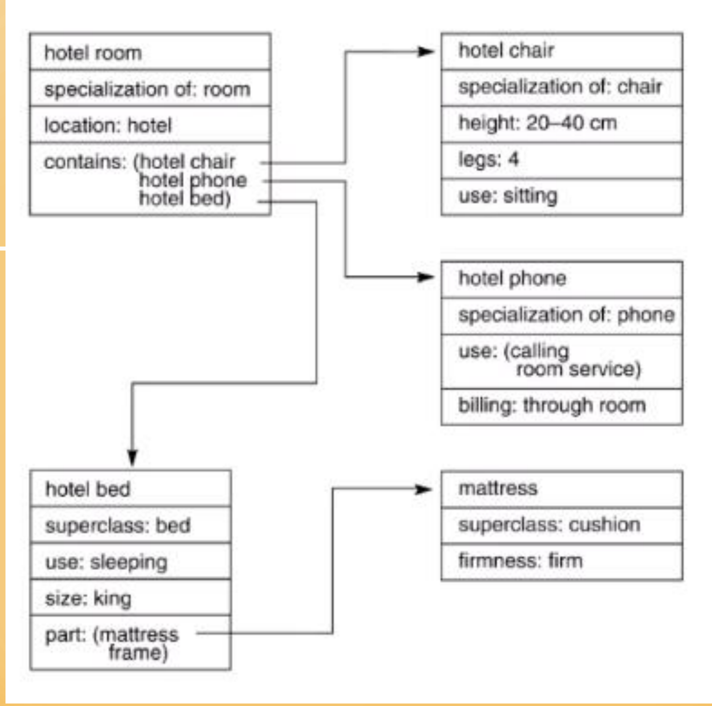
1880
Venn diagrams

1882
Existential graphs

1950s – 1960s
Formal representations for natural language

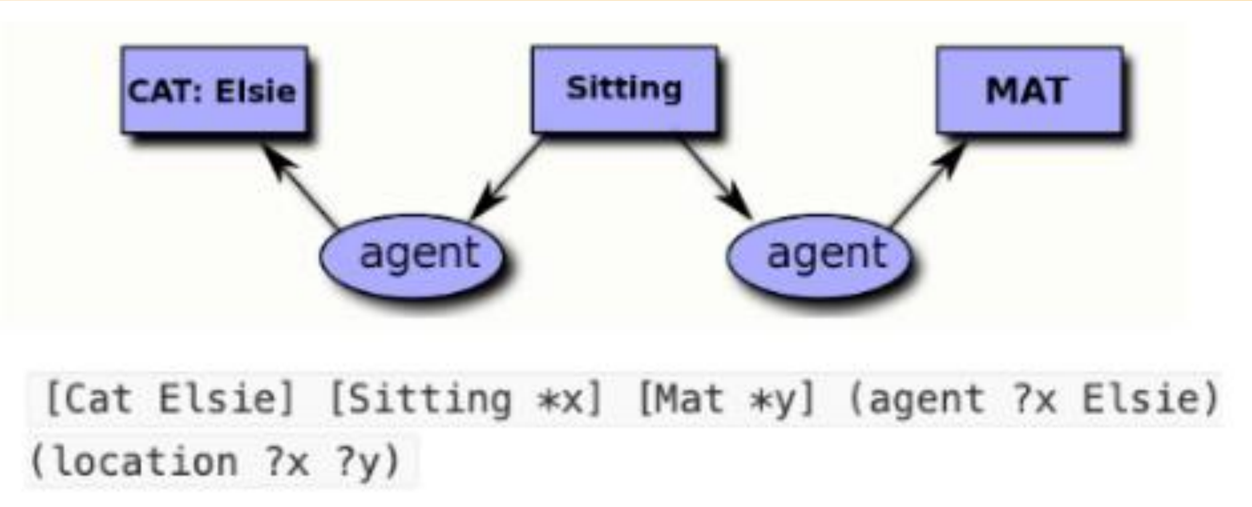
1972 Term
"Knowledge graphs"

1974
Frames



Evolution of Knowledge Graphs

- 4th Century BC
  Aristotle's logic diagrams
- 1768
  Euler circles
- 1880
  Venn diagrams
- 1882
  Existential graphs
- 1950s – 1960s
  Formal representations for natural language
- 1972
  "Knowledge graphs"
- 1974
  Frames
- 1976
  Conceptual graphs



Evolution of Knowledge Graphs

4th Century BC
Aristotle's logic diagrams

1768
Euler circles

1880
Venn diagrams

1882
Existential graphs

1950s – 1960s
Formal representations for natural language

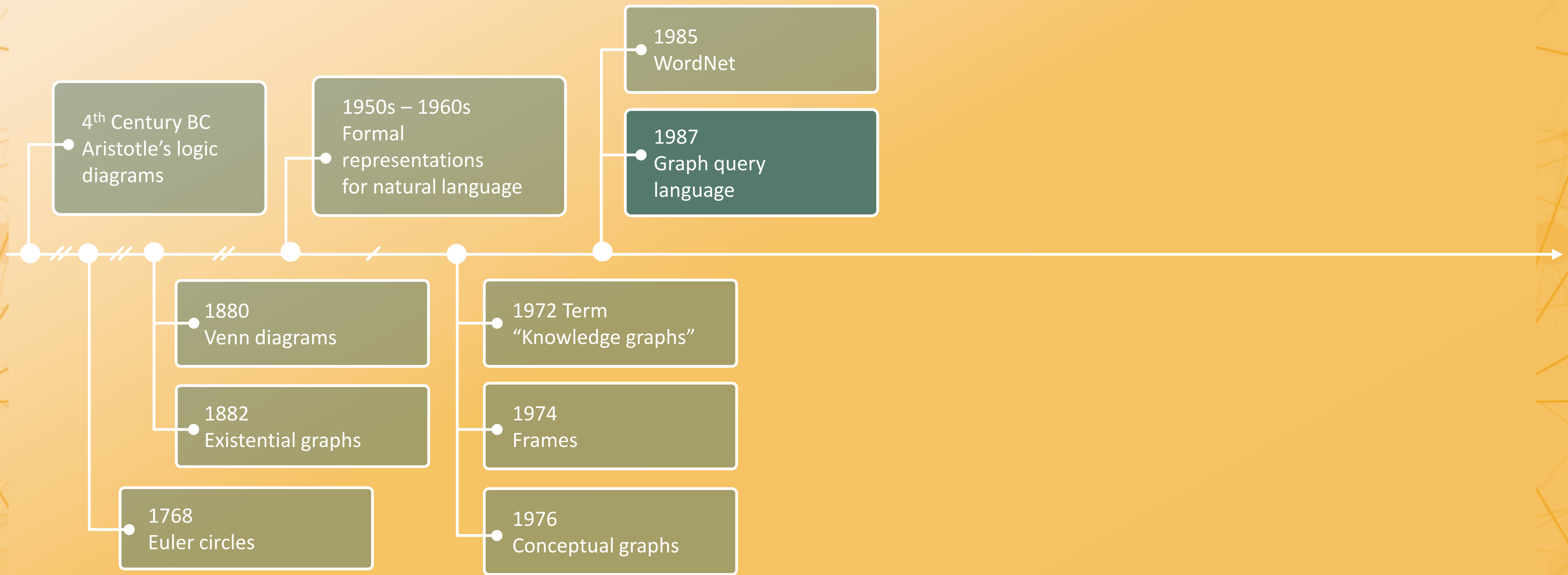
1972 Term
"Knowledge graphs"

1974
Frames

1976
Conceptual graphs

1985
WordNet

Evolution of Knowledge Graphs



Evolution of Knowledge Graphs

- 4th Century BC
  Aristotle's logic diagrams
- 1768
  Euler circles
- 1880
  Venn diagrams
- 1882
  Existential graphs
- 1950s – 1960s
  Formal representations for natural language
- 1972 Term
  "Knowledge graphs"
- 1974
  Frames
- 1976
  Conceptual graphs
- 1985
  WordNet
- 1987
  Graph query language
- 1993
  Ontology
- 1993
  Deductive databases
- 1996
  XML
- 1996
  RDF

Evolution of Knowledge Graphs

4th Century BC
Aristotle's logic diagrams

1768
Euler circles

1880
Venn diagra

1882
Existential gr

1993
Ontology

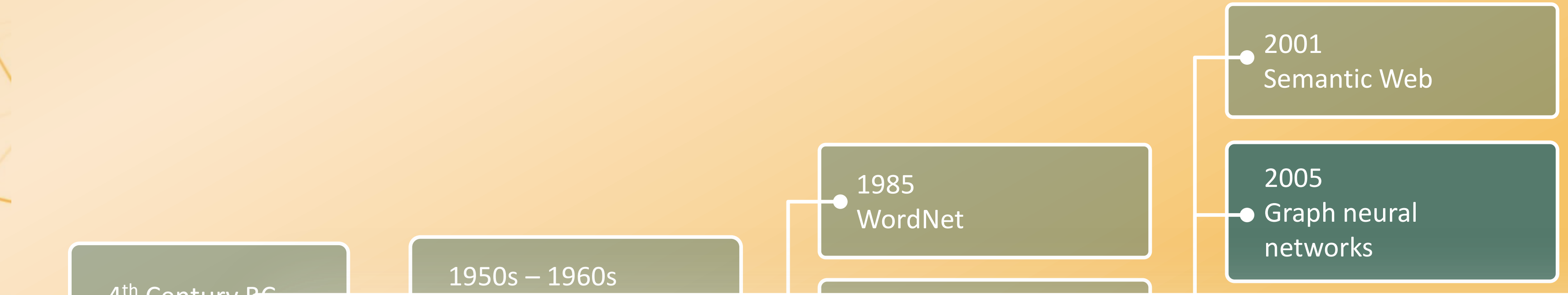
1993
Deductive databases

1996
XML

1996
RDF

2001
Semantic Web

Evolution of Knowledge Graphs



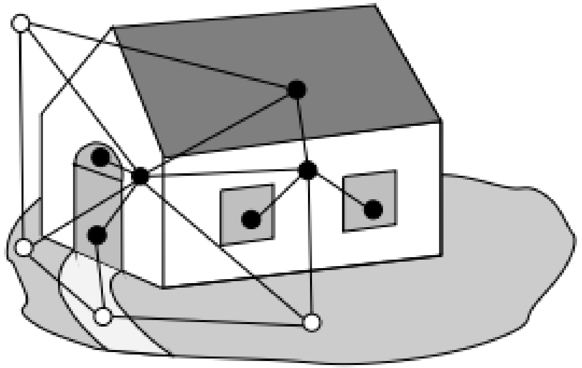
A New Model for Learning in Graph Domains

Marco Gori
Dipartimento di Ingegneria
dell'Informazione
Università di Siena, Italy
E-mail: marco@dii.unisi.it

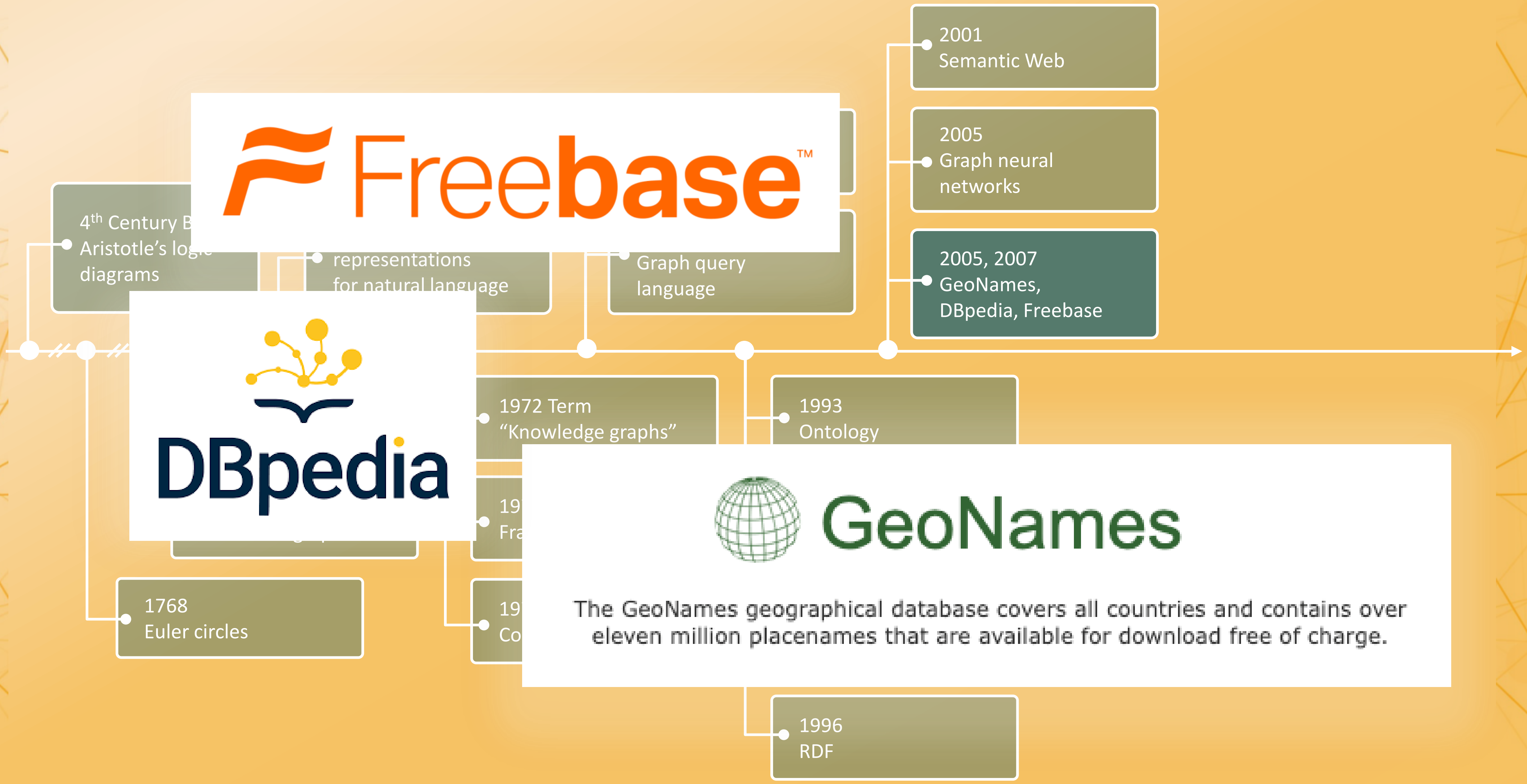
Gabriele Monfardini
Dipartimento di Ingegneria
dell'Informazione
Università di Siena, Italy
E-mail: monfardini@dii.unisi.it

Franco Scarselli
Dipartimento di Ingegneria
dell'Informazione
Università di Siena, Italy
E-mail: franco@dii.unisi.it

***Abstract*— In several applications the information is naturally represented by graphs. Traditional approaches cope with graphical data structures using a preprocessing phase which transforms the graphs into a set of flat vectors. However, in this way, important topological information may be lost and the achieved results may heavily depend on the preprocessing stage. This paper presents a new neural model, called graph neural network (GNN), capable of directly processing graphs. GNNs extends recursive neural networks and can be applied on most of the practically useful kinds of graphs, including directed, undirected, labelled and cyclic graphs. A learning algorithm for GNNs is proposed and some experiments are discussed which assess the properties of the model.**



Evolution of Knowledge Graphs



Evolution of Knowledge Graphs

4th Century BC
Aristotle's logic diagrams

1768
Euler circles

1880
Venn diagrams

1882
Existential graphs

1950s – 1960s
Formal representations for natural language

1972 Term
"Knowledge grap

1974
Frames

1976
Conceptual graphs

1996
XML

1996
RDF

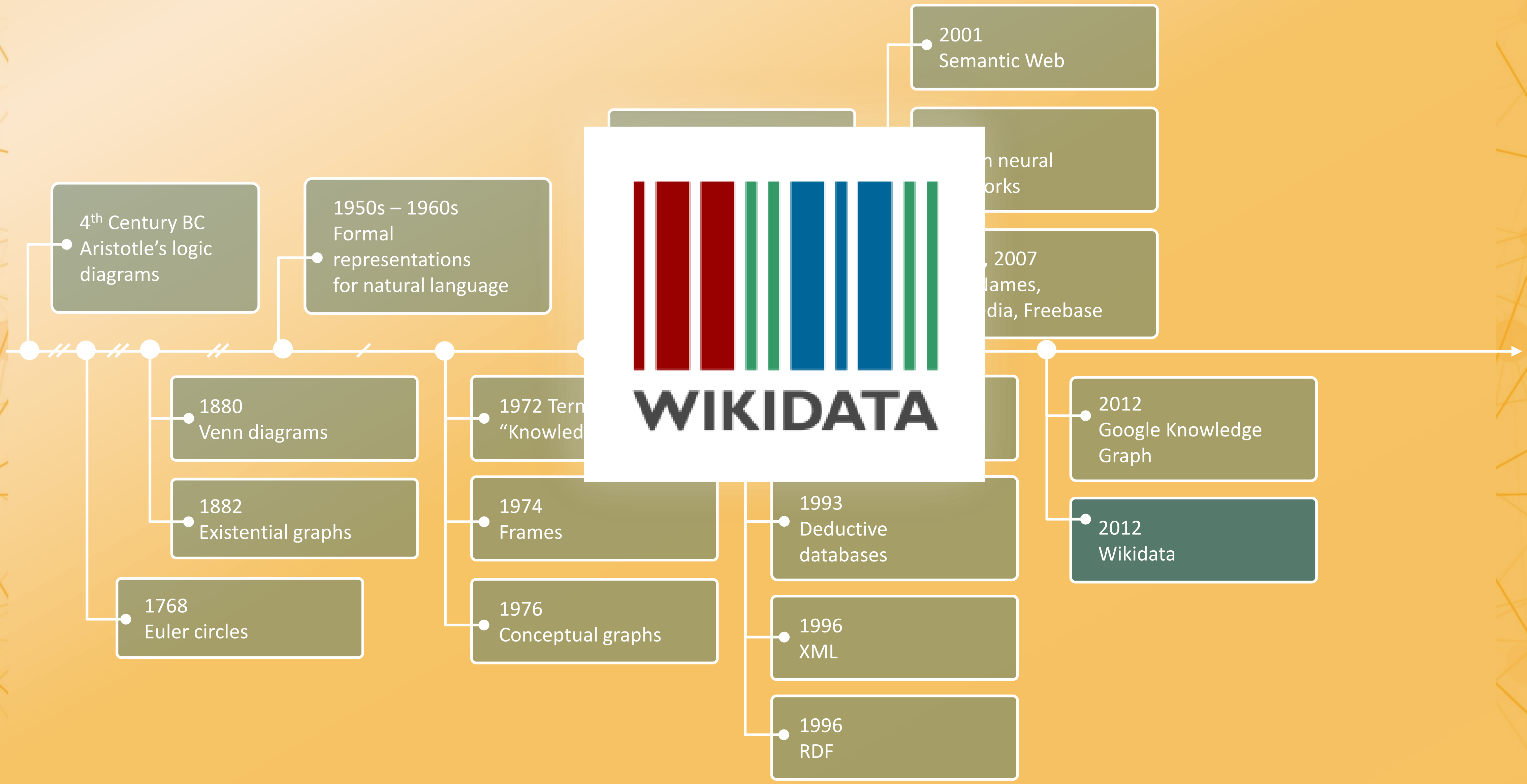
2001
antic Web

h neural
orks

, 2007
Names,
edia, Freebase

2012
Google Knowledge Graph

Evolution of Knowledge Graphs



Evolution of Knowledge Graphs

4th Century B
Aristotle's log
diagrams

1768
Euler circles

Existential graphs

Frames

1976
Conceptual graphs

1985

Deductive
databases

1996
XML

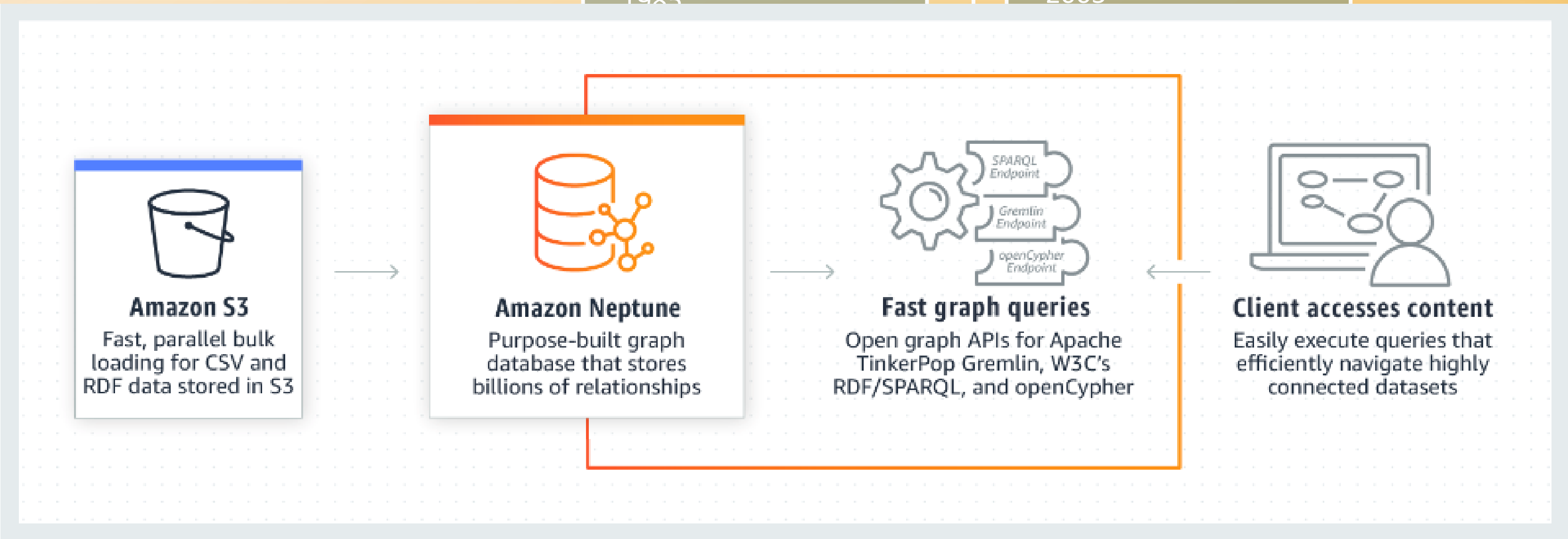
1996
RDF

2001
Semantic Web

2005

2012
Wikidata

2017
Amazon Neptune



Evolution of Knowledge Graphs

- 4th Century BC Aristotle's logic diagrams
- 1768 Euler circles
- 1880 Venn diagrams
- 1882 Existential graphs
- 1950s – 1960s Formal representations for natural language
- 1972 Term "Knowledge graphs"
- 1974 Frames
- 1976 Conceptual graphs
- 1985 WordNet
- 1987 Graph query language
- 1993 Ontology
- 1993 Deductive databases
- 1996 XML
- 1996 RDF
- 2001 Semantic Web
- 2005 Graph neural networks
- 2005, 2007 GeoNames, DBpedia, Freebase
- 2012 Google Knowledge Graph
- 2012 Wikidata
- 2017 Amazon Neptune
- 2020 Google KG 500B+ facts

Evolution of Knowledge Graphs

4th Century BC
Aristotle's logic diagrams

1768
Euler circles

1880
Venn di

1882
Existen

1976
Conceptual graphs

1985
WordNet

1996
XML

1996
RDF

2001
Semantic Web

2005
Graph neural

ebase

2012
Google Knowledge Graph

2012
Wikidata

2017
Amazon Neptune

2020
Google KG 500B+ facts

2024
Microsoft GraphRAG

Evolution of Knowledge Graphs

- 4th Century BC
  Aristotle's logic diagrams
- 1768
  Euler circles
- 1880
  Venn diagrams
- 1882
  Existential graphs
- 1950s – 1960s
  Formal representations for natural language
- 1972 Term
  "Knowledge graphs"
- 1974
  Frames
- 1976
  Conceptual graphs
- 1985
  WordNet
- 1987
  Graph query language
- 1993
  Ontology
- 1993
  Deductive databases
- 1996
  XML
- 1996
  RDF
- 2001
  Semantic Web
- 2005
  Graph neural networks
- 2005, 2007
  GeoNames, DBpedia, Freebase
- 2012
  Google Knowledge Graph
- 2012
  Wikidata
- 2017
  Amazon Neptune
- 2020
  Google KG 500B+ facts
- 2024
  Microsoft GraphRAG

Technology Trends

Fine-Grain Authorization

Access management technologies

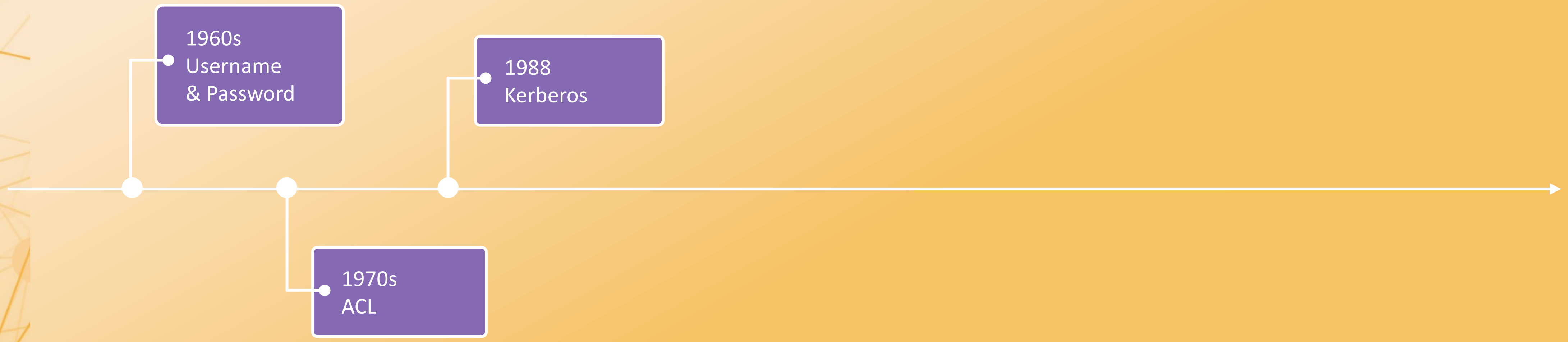
1960s
Username
& Password

Access management technologies

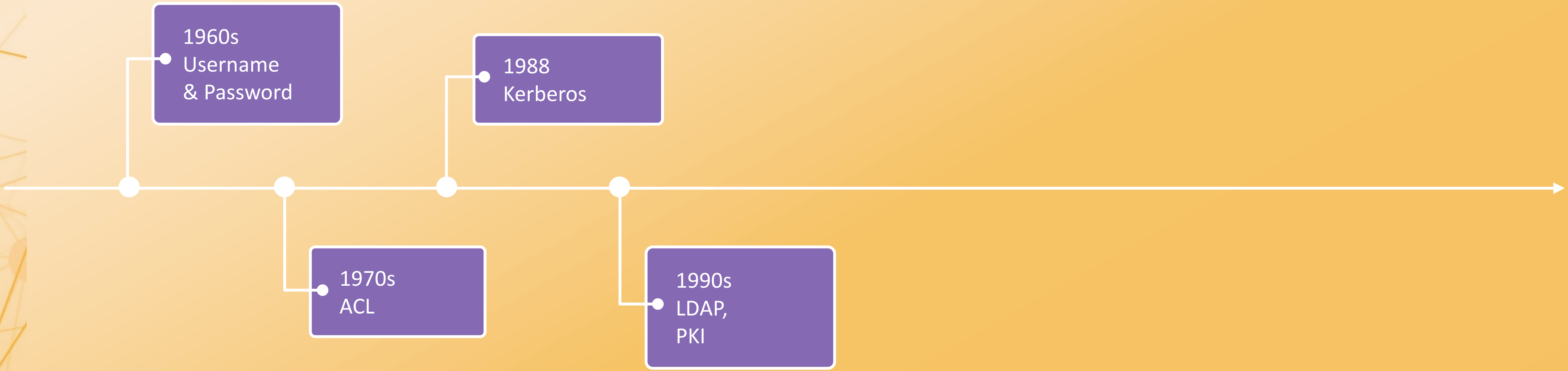
1960s
Username
& Password

1970s
ACL

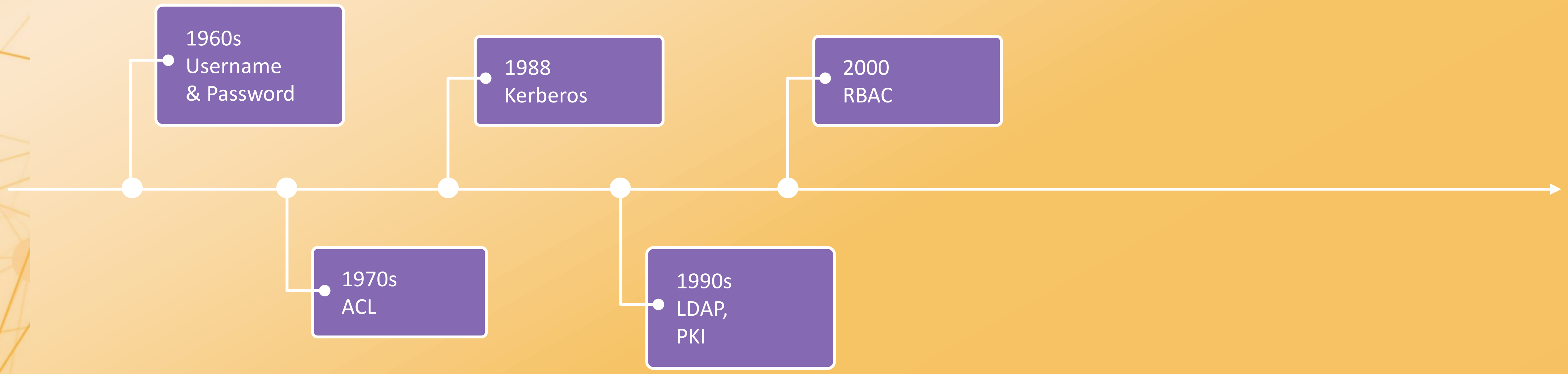
Access management technologies



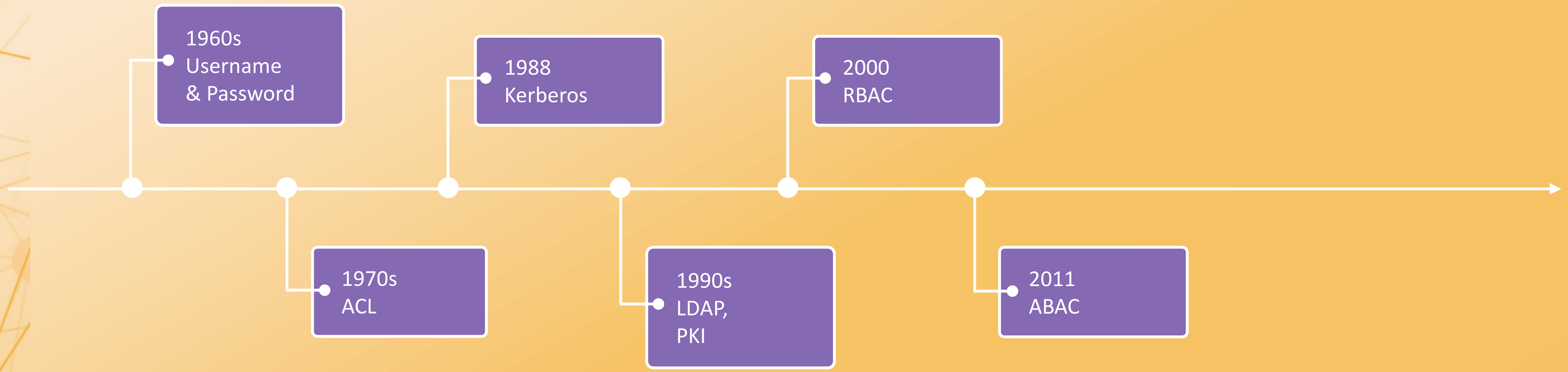
Access management technologies



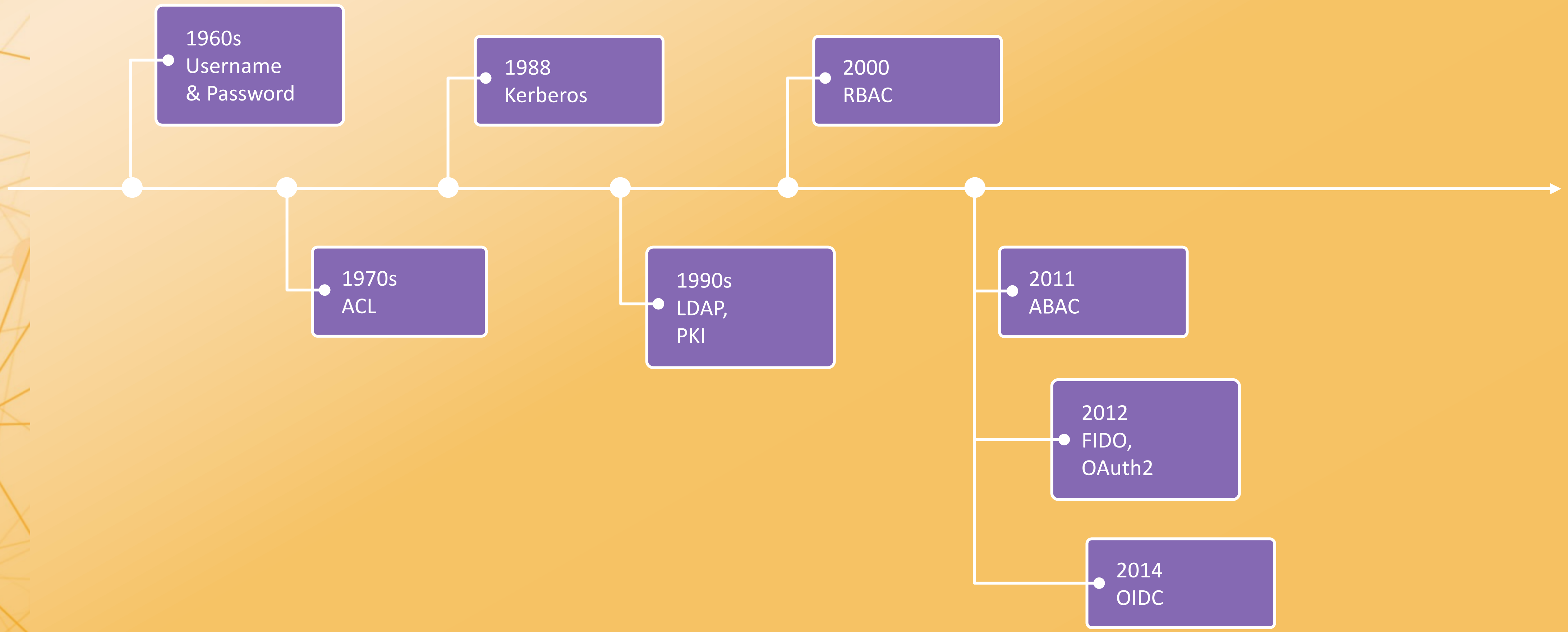
Access management technologies



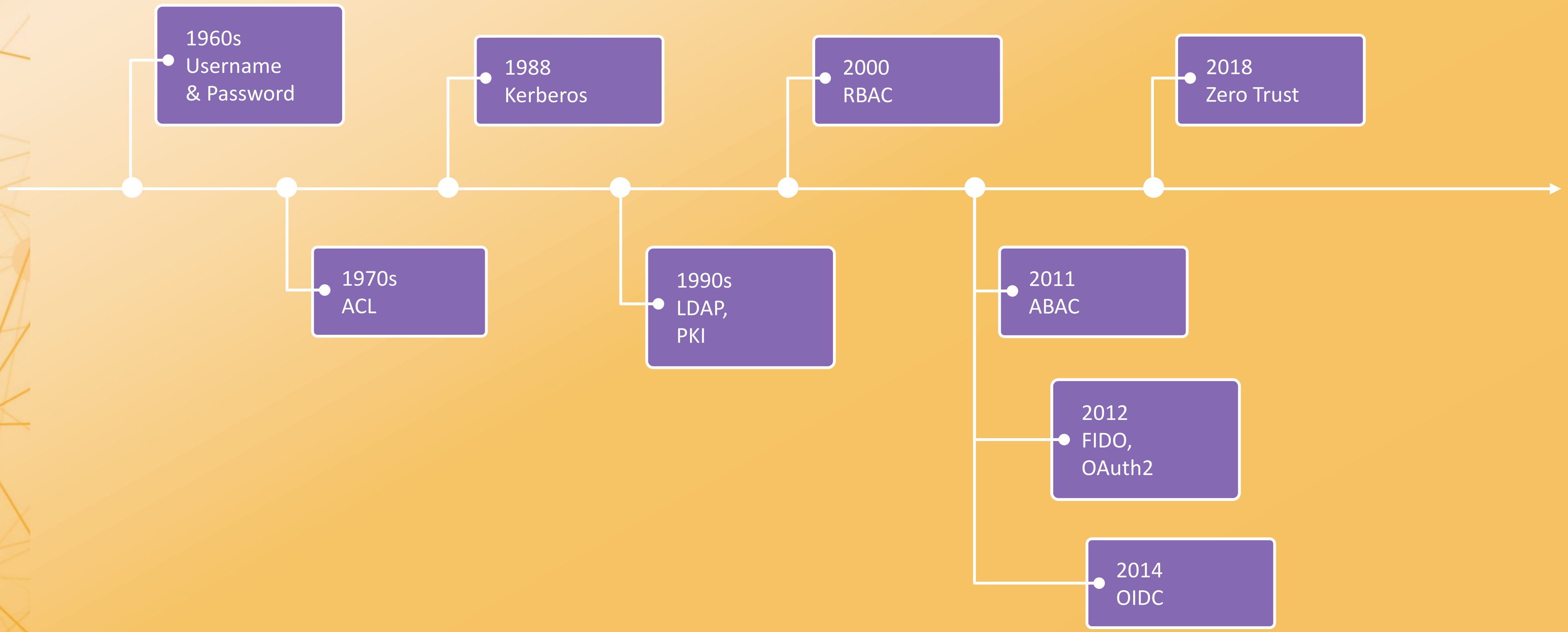
Access management technologies



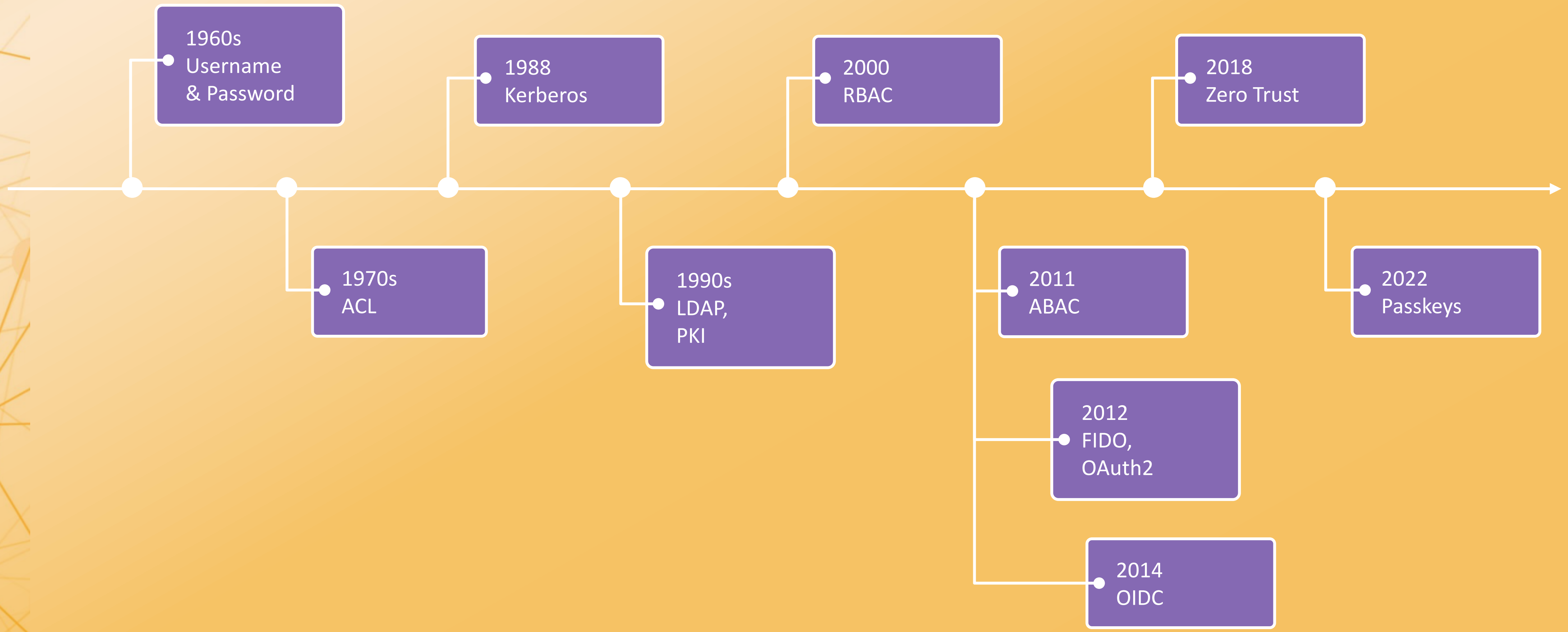
Access management technologies

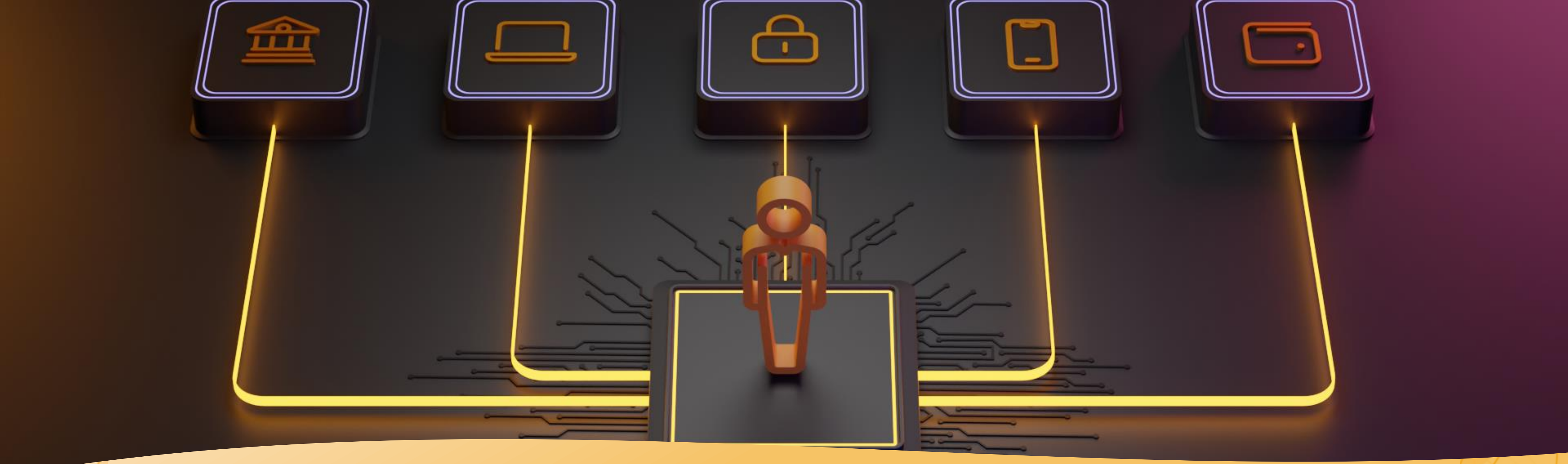


Access management technologies



Access management technologies





Credit: Lenart Lipovsek, IndyKite

Focus shift from authentication to authorization

“The shift from authentication to authorization standards is a crucial evolution in cybersecurity to address the challenges posed by cloud-native architectures and the explosion of apps, remote users, and devices.”

Case for storing that context in a graph: Identity is a graph

A person's identity is a collection of connections to devices, persons, companies and services, and thus a holistic picture of a digital identity is optimally captured in a graph.

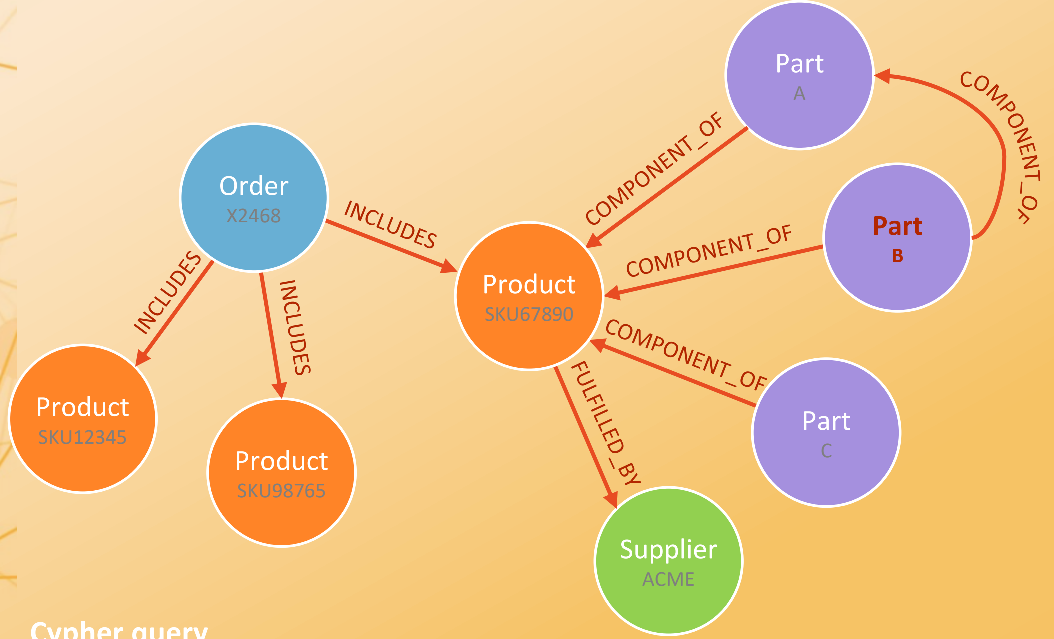
In the digital world, people, services, and devices have an identity, sometimes even more than one, and those identities are becoming increasingly interconnected with rich and deep relationships. (Memgraph)

An identity graph provides a single unified view of customers and prospects based on their interactions with a product or website across a set of devices and identifiers. (AWS)

We love graph because it gives us the means to turn identity data into identity knowledge. (IndyKite)

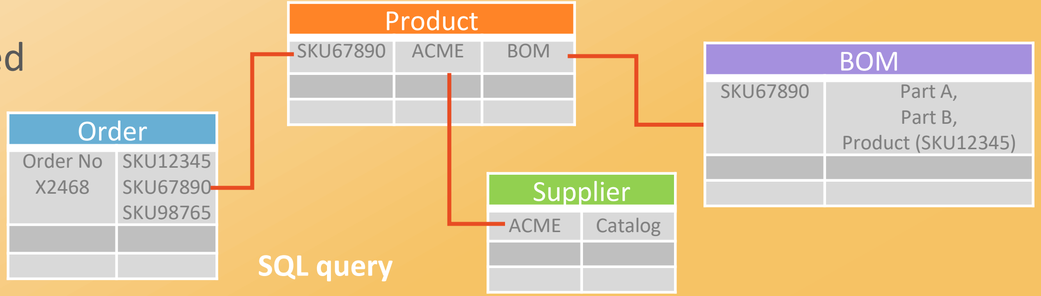
Why use graphs? **Performance**

Find all orders and suppliers impacted by Part B, which was recalled



Cypher query

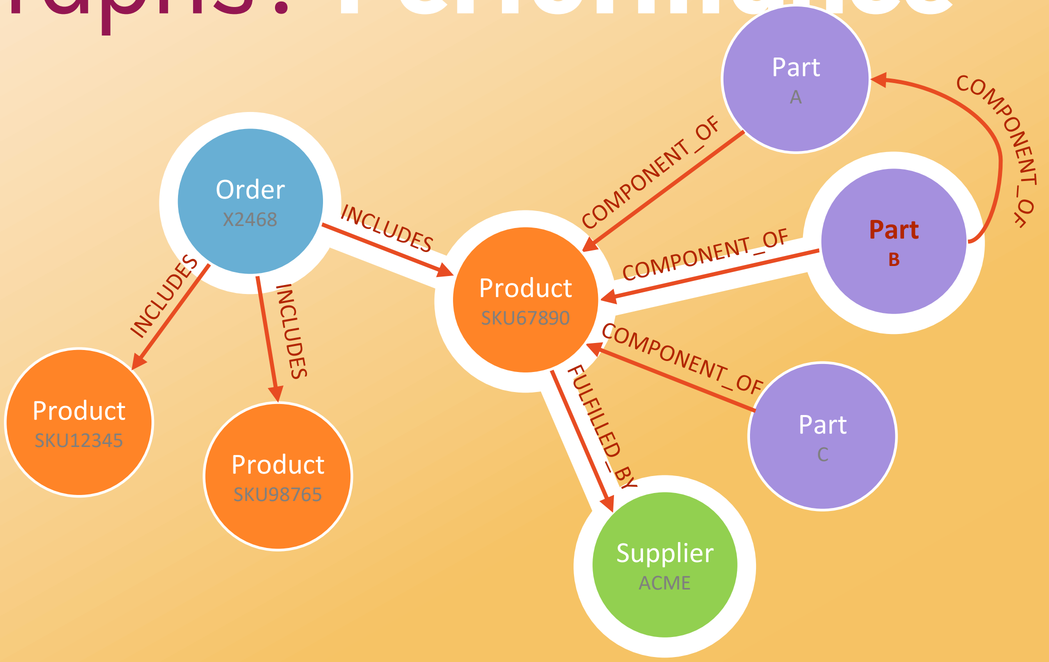
```
MATCH (order:Order)-[:INCLUDES]->(product:Product)-[*]-> (part:Part
{name: 'Part B'})

MATCH (product)-[:FULFILLED_BY]->(supplier:Supplier)

RETURN order, supplier
```



SQL query

```
WITH RECURSIVE bom_hierarchy AS (
    SELECT
        b.product_id,
        b.component_id
    FROM
        bom b
    WHERE
        b.component_id IN (SELECT product_id FROM products WHERE
product_name = 'Part B')
    UNION ALL
    SELECT
        b.product_id,
        bh.component_id
    FROM
        bom b
    JOIN
        bom_hierarchy bh ON b.component_id = bh.product_id
)
SELECT
    o.order_id,
    s.supplier_id,
    s.supplier_name
FROM
    orders o
JOIN
    bom_hierarchy bh ON o.product_id = bh.product_id
JOIN
    catalog c ON bh.product_id = c.product_id
JOIN
    suppliers s ON c.supplier_id = s.supplier_id;
```

Why use graphs? **Performance**



Index-free adjacency allows the system to traverse between related entities. As graph databases store relationships as references or pointers between nodes, a database can follow a memory pointer and rapidly navigate between entities. In this case, the database doesn't need need indexes or mapping tables.

AWS: What's the Difference Between a Graph Database and a Relational Database?

Why use graphs? **Flexibility**

- Data model with frequent changes
- Customers, employees, partners have different data models
- Not all entities share the same set of attributes
- Attribute types are not strictly defined
- Additional attributes added later

Graph database-backed access control systems allows for easy rule creation in fast response to such changes and complexities

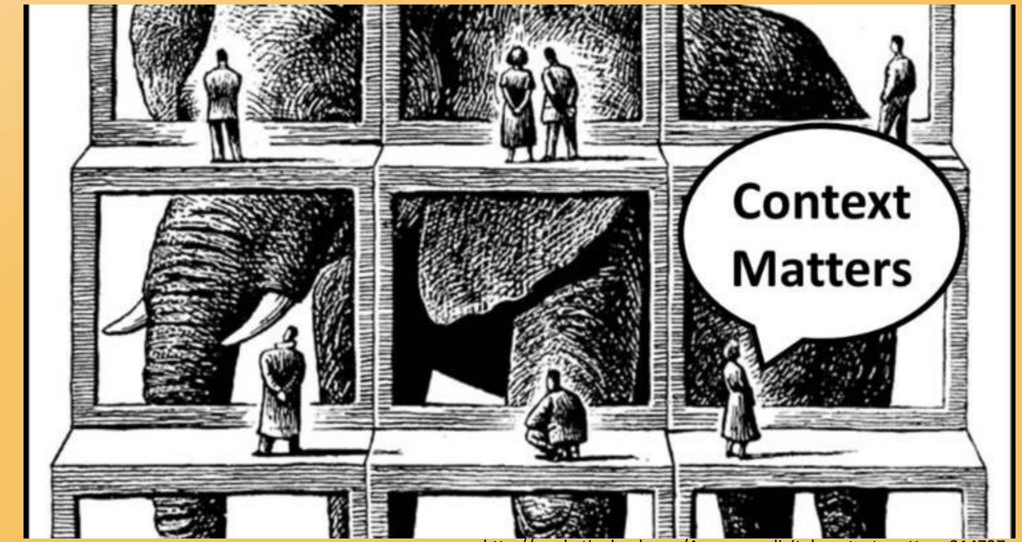
Base authorization decisions on rich context

Unify your identity data into a knowledge graph

- Data from systems hold data germane to your business domain

Add in resource context

- Salient attributes about the protected assets important enough to be used in determining access

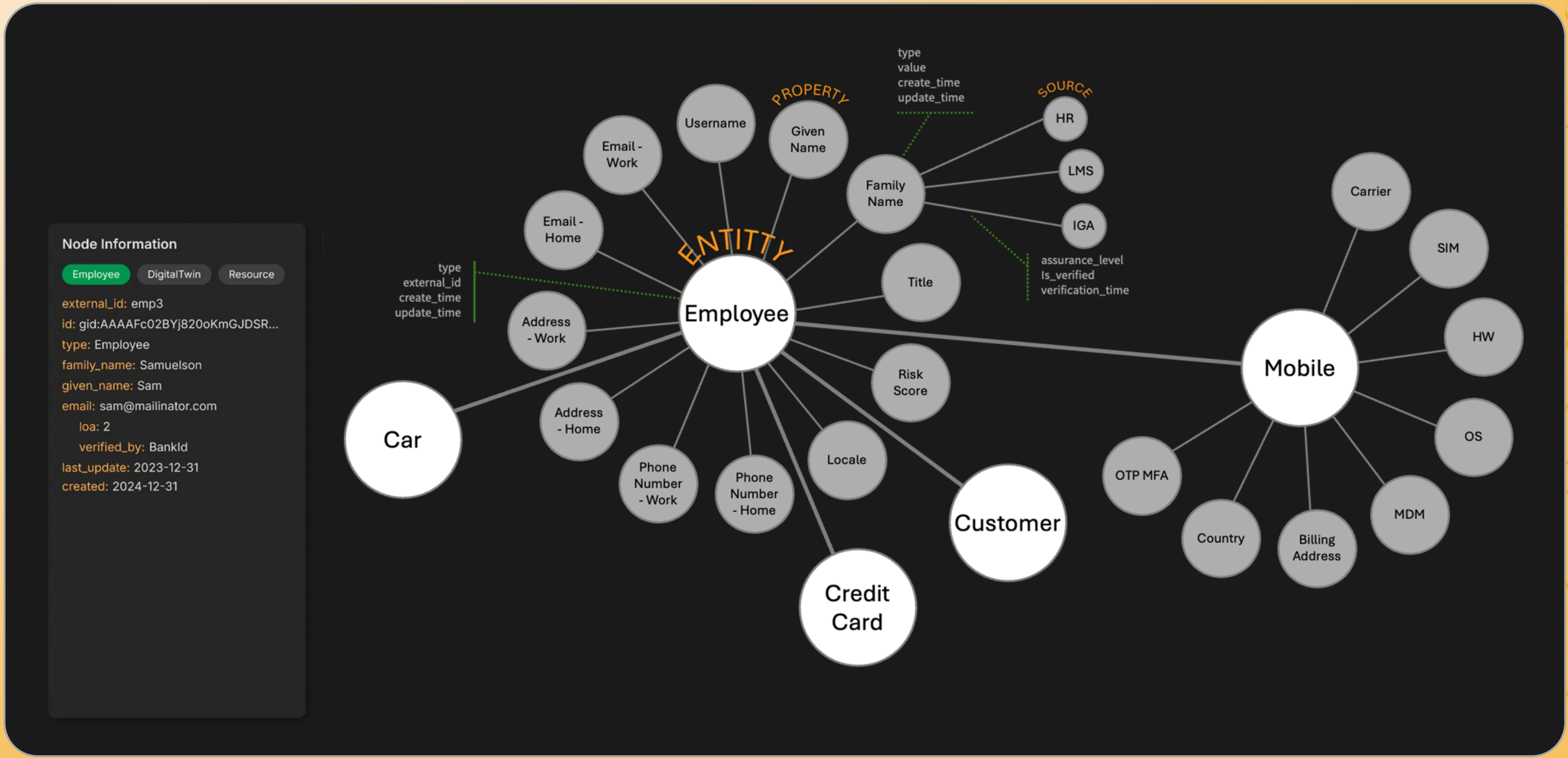


http://marketingland.com/4-reasons-digital-context-matters-214727

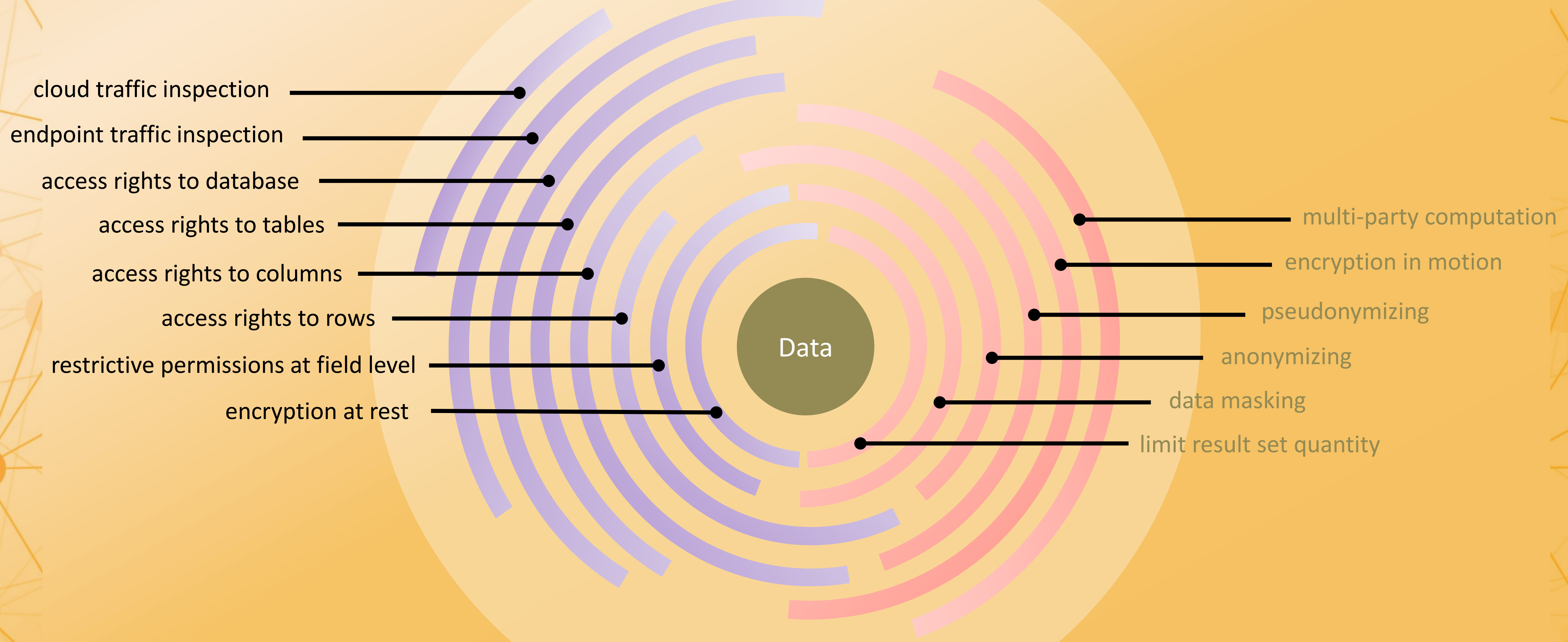
Enrich your data

- With inferences made using mapped relationships and graph analytics (e.g., centrality, connectivity, and community detection)

Context-rich Identity knowledge



Fine-Grained Authorization at each layer...



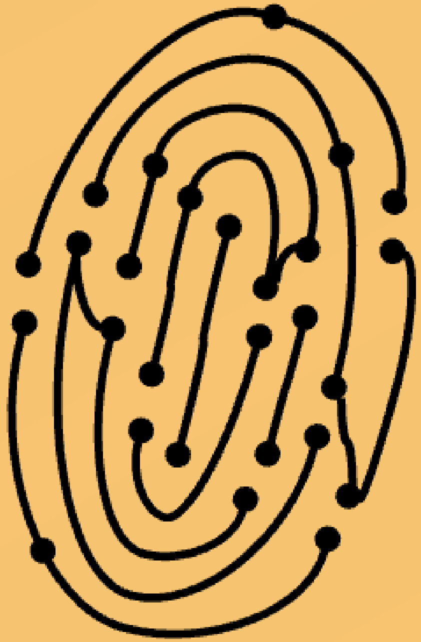
...with rich context aware access policies

Identity context for semantic fingerprinting

Semantic information in an identity-based knowledge graph can be analyzed to form an access *fingerprint*

Once a semantic fingerprint is established, it can be used detect attention shifts

Any such anomalous activity can be used in risk models and inform adaptive authentication and authorization



Other use cases for context-rich identity data

- Entity resolution
- Link analysis
- Recommendations
- Personalization
- Community detection
- Influencer detection
- Data quality monitoring

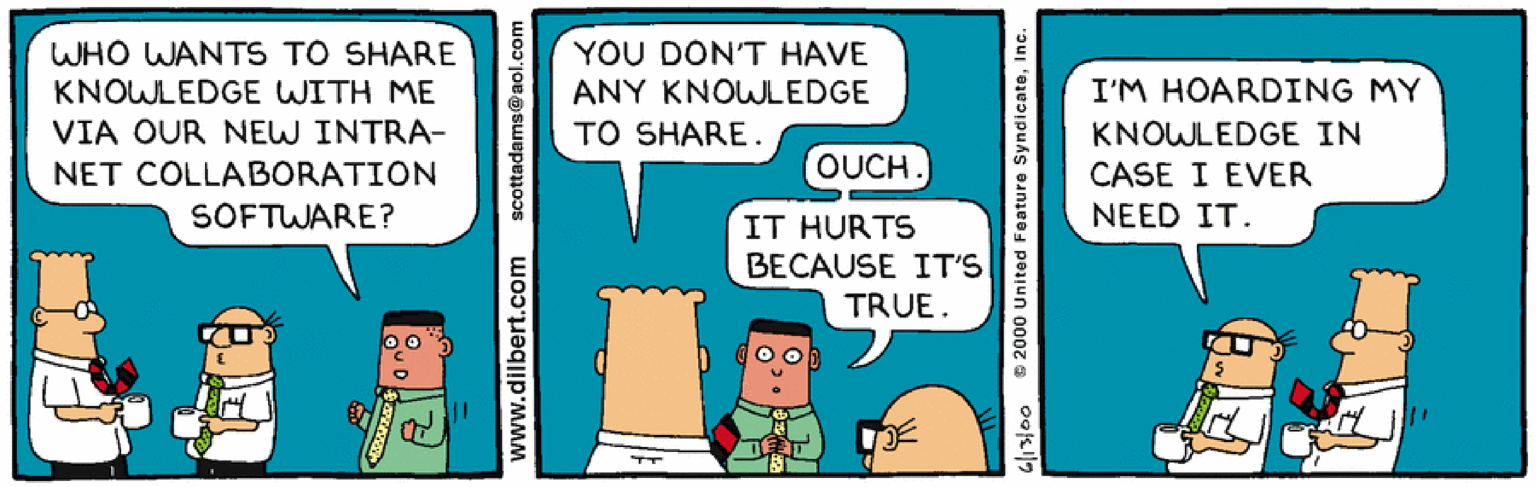
Conclusion

Identity Knowledge Graph = context context context

In summary, as traditional network perimeters dissolve, identity has become the new frontier in cybersecurity, necessitating robust identity management, continuous monitoring, and integration with modern security frameworks like Zero Trust and XDR to mitigate identity-based threats effectively.

Call to Action

Let's connect:
www.linkedin.com/in/christenpatterson



appendix


TO THE UNTRAINED EYE IT MIGHT LOOK AS IF I DO NO WORK.
scottadams@aol.com
www.dilbert.com
BUT INSIDE HERE IS A RAGING SEA OF KNOWLEDGE MANAGEMENT AND STRATEGIC THINKING.
© 2000 United Feature Syndicate, Inc.
5/12/00
DID YOU HEAR THAT GURGLING SOUND?