The edge of the Internet is becoming the center

OR

The age of the datacenter draws to a close

•••

Stewart Mackenzie
Revuln 19q4

Structure of the talk

1. Where we're going.
2. What's the problem?
3. The road to Internet centralisation
    a. Putting down the wires
    b. Packet switching
    c. Information centric
4. Copernica
    a. Anonymous
    b. Decentralised
    c. State level threat actor
5. Conclusion

Where we're going.

- The edge of the Internet is becoming the center

Where we're going.

- The edge of the Internet is becoming the center
- The truth is currently at the center

Where we're going.

- The edge of the Internet is becoming the center
- The truth is currently at the center
- Data has no provenance

Where we're going.

- The edge of the Internet is becoming the center
- The truth is currently at the center
- Data has no provenance
- GAFAM exploits user's data without consent to make money

Where we're going.

- The edge of the Internet is becoming the center
- The truth is currently at the center
- Data has no provenance
- GAFAM exploits user's data without consent to make money
- Host-centric networking creates monopolies

Where we're going.

- The edge of the Internet is becoming the center
- The truth is currently at the center
- Data has no provenance
- GAFAM exploits user's data without consent to make money
- Host-centric networking creates monopolies
- Centralised monopolies are ripe for exploit by state level threat actors

Where we're going.

- The edge of the Internet is becoming the center
- The truth is currently at the center
- Data has no provenance
- GAFAM exploits user's data without consent to make money
- Host-centric networking creates monopolies
- Centralised monopolies are ripe for exploit by state level threat actors
- Fake news is a result of the center unable to control the edge

Where we're going.

- The edge of the Internet is becoming the center
- The truth is currently at the center
- Data has no provenance
- GAFAM exploits user's data without consent to make money
- Host-centric networking creates monopolies
- Centralised monopolies are ripe for exploit by state level threat actors
- Fake news is a result of the center unable to control the edge
- Edge AI controlled by GAFAM will constantly listen to your voice building psychological models.

Where we're going.

- The edge of the Internet is becoming the center
- The truth is currently at the center
- Data has no provenance
- GAFAM exploits user's data without consent to make money
- Host-centric networking creates monopolies
- Centralised monopolies are ripe for exploit by state level threat actors
- Fake news is a result of the center unable to control the edge
- Edge AI controlled by GAFAM will constantly listen to your voice building psychological models.

This is just symptomatic behaviour of a deeper cause

The core problems

The core problems

- Centralisation of the Internet

The core problems

- Centralisation of the Internet
- Data isn’t secured at the source and has no provenance

The road to Internet centralisation

The road to Internet centralisation

- Phase 1 - putting down the wires for the telephone systems

The road to Internet centralisation

- Phase 1 - putting down the wires for the telephone systems
  - Problems:
    - Intrinsic addresses

The road to Internet centralisation

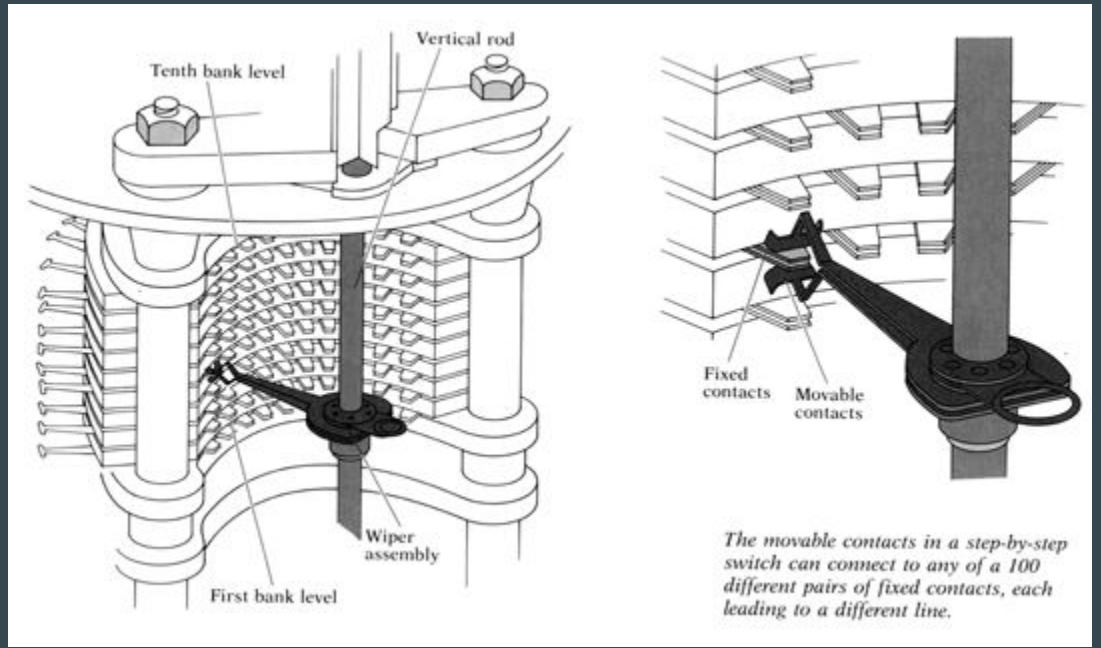
- Intrinsic addresses

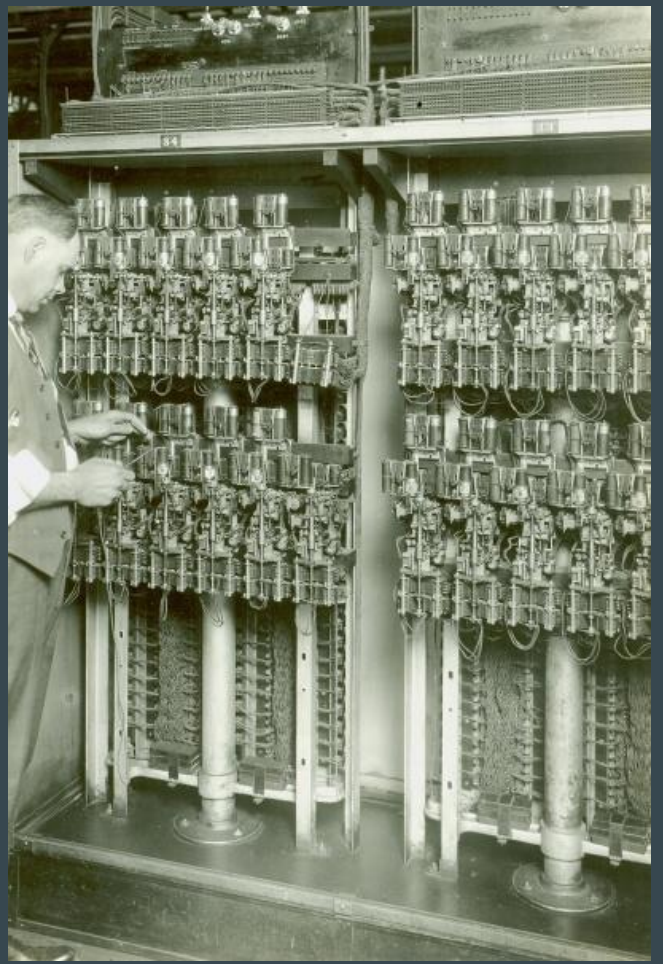
The road to Internet centralisation

- Phase 1 - putting down the wires for the telephone systems
  - Problems:
    - Intrinsic addresses
    - Reliability of connections

The road to Internet centralisation

- Reliability of connections





The road to Internet centralisation

- Reliability of connections

Rf = Connection Reliability Factor
Cpf = Component Failure Probability
Cn = Number of components in connection (count every wire, knob switch etc!)

$$Rf = Cfp * Cn$$

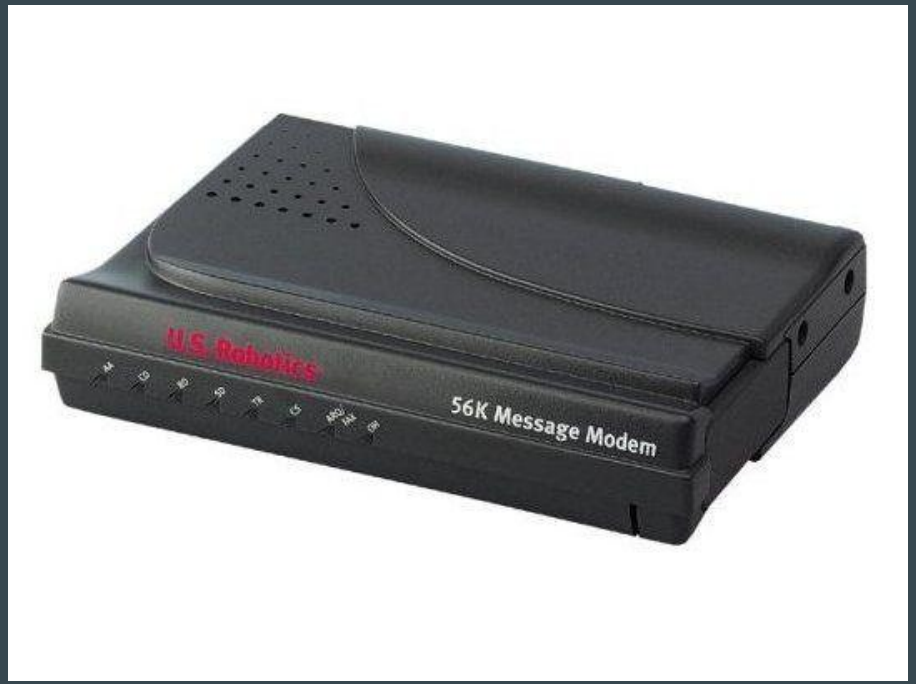
The road to Internet centralisation

- Phase 1 - putting down the wires for the telephone systems
  - Problems:
    - Intrinsic addresses
    - Reliability of connections
    - Very slow connection setup times

The road to Internet centralisation

- Very slow connection setup times

Later



The road to Internet centralisation

- Phase 1 - putting down the wires for the telephone systems
  - Problems:
    - Intrinsic addresses
    - Reliability of connections
    - Very slow connection setup times
    - Topology was critical due to reliability issues

The road to Internet centralisation

- Phase 1 - putting down the wires for the telephone systems
  - Problems:
    - Intrinsic addresses
    - Reliability of connections
    - Very slow connection setup times
    - Topology was critical due to reliability issues
    - Telecom monopolies

The road to Internet centralisation

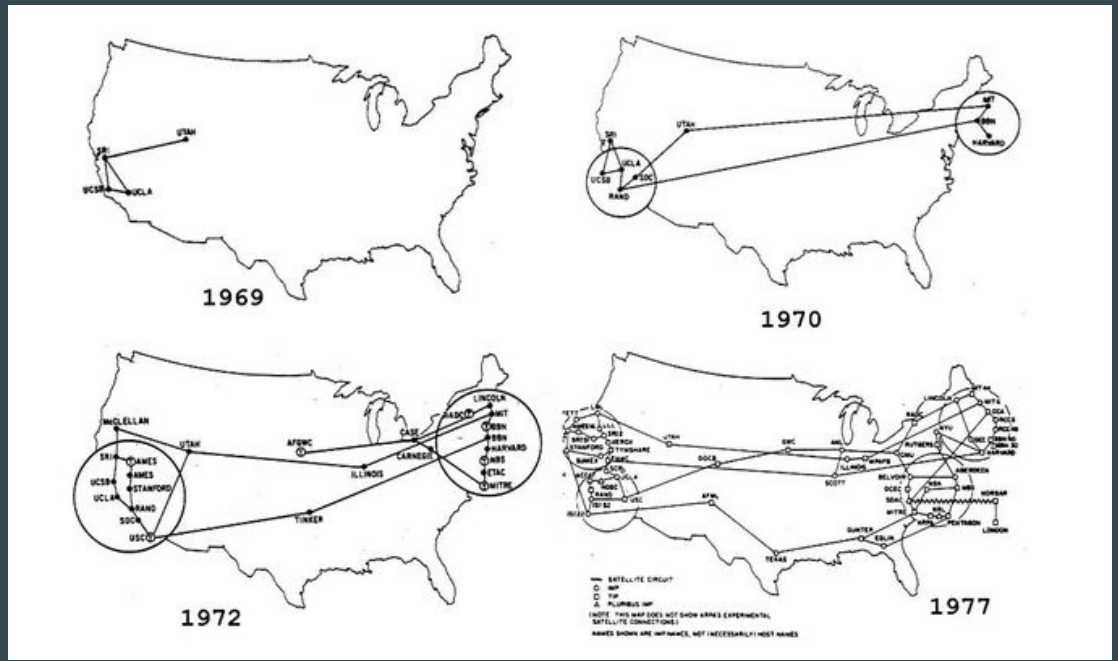
- Phase 1 - putting down the wires for the telephone systems
  - Problems:
    - Intrinsic addresses
    - Reliability of connections
    - Very slow connection setup times
    - Topology was critical due to reliability issues
    - Telecom monopolies
  - Solution:
    - Wires are put down - the backbone is formed

The road to Internet centralisation

- Phase 2 - The Internet as we know it or Packet Switching or End Points
  - Solutions
    - Intrinsic addresses

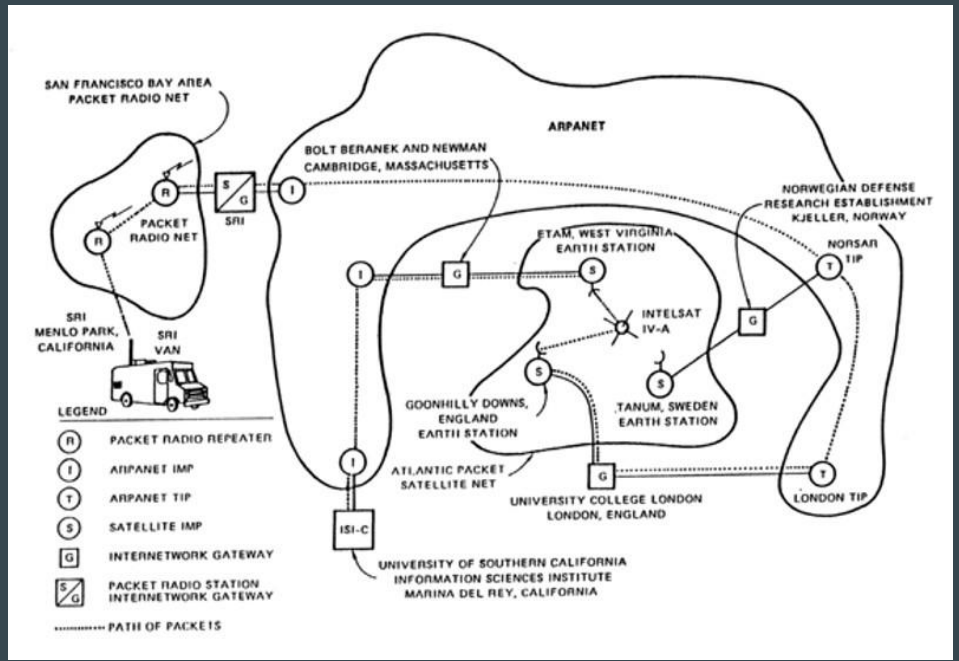
The road to Internet centralisation

- Intrinsic addresses



The road to Internet centralisation

- Intrinsic addresses



The road to Internet centralisation

- Phase 2 - The Internet as we know it or Packet Switching or End Points
  - Solutions
    - Intrinsic addresses
    - Connection setup times disappeared totally as you're always connected

The road to Internet centralisation

- Phase 2 - The Internet as we know it or Packet Switching or End Points
  - Solutions
    - Intrinsic addresses
    - Connection setup times disappeared totally as you're always connected
    - Combinatorics of failure flipped on its head, more nodes less probability of failure

The road to Internet centralisation

- Phase 2 - The Internet as we know it or Packet Switching or End Points
  - Solutions
    - Intrinsic addresses
    - Connection setup times disappeared totally as you're always connected
    - Combinatorics of failure flipped on its head, more nodes less probability of failure
  - Problems
    - GAFAM - data dissemination monopolies AND telecom monopolies

The road to Internet centralisation

- Phase 2 - The Internet as we know it or Packet Switching or End Points
  - Solutions
    - Intrinsic addresses
    - Connection setup times disappeared totally as you're always connected
    - Combinatorics of failure flipped on its head, more nodes less probability of failure
  - Problems
    - GAFAM - data dissemination monopolies AND telecom monopolies
    - Content dissemination over host-centric networking is insanely expensive

The road to Internet centralisation

- Phase 2 - The Internet as we know it or Packet Switching or End Points
  - Solutions
    - Intrinsic addresses
    - Connection setup times disappeared totally as you're always connected
    - Combinatorics of failure flipped on its head, more nodes less probability of failure
  - Problems
    - GAFAM - data dissemination monopolies AND telecom monopolies
    - Content dissemination over host-centric networking is insanely expensive
    - Edge AI deployed constantly monitors your digital actions building psychological profiles phoning home to GAFAM clouds.

The road to Internet centralisation

- Phase 2 - The Internet as we know it or Packet Switching or End Points
  - Solutions
    - Intrinsic addresses
    - Connection setup times disappeared totally as you're always connected
    - Combinatorics of failure flipped on its head, more nodes less probability of failure
  - Problems
    - GAFAM - data dissemination monopolies AND telecom monopolies
    - Content dissemination over host-centric networking is insanely expensive
    - Edge AI deployed constantly monitors your digital actions building psychological profiles phoning home to GAFAM clouds.
    - Data has no provenance and isn't secure

We're at a fork now

Path A: Continue using the centralised Internet

- As the edge is growing exponentially, GAFAM can't keep up
- GAFAM desperate to control the edge will use edge AI to monitor, surveil, profile then curate edge data independently to be sent home to GAFAM servers later.
- Of course this AI will be packaged as some digital assistant like Siri on Apple, it's even reaching into developing countries via feature phones and Google Assistant on KaiOS - Google paid 22 mill USD to get GA + Gapps on KaiOS.
- This path isn't possible in the long run because of data dissemination over a host-centric network costs a lot.
- Edge processing power and storage capacity will dwarf GAFAM centralised servers

We’re at a fork now

Path B: Start growing a decentralised Internet

We’re at a fork now

Information-centric network, the natural progression of the Internet

- Solutions
  - Centralisation of the Internet

We’re at a fork now

Information-centric network, the natural progression of the Internet

- Solutions
  - Centralisation of the Internet
  - Secure signed data (provenance of data) with optional encryption

We’re at a fork now

Information-centric network, the natural progression of the Internet

- Solutions
  - Centralisation of the Internet
  - Secure signed data (provenance of data) with optional encryption

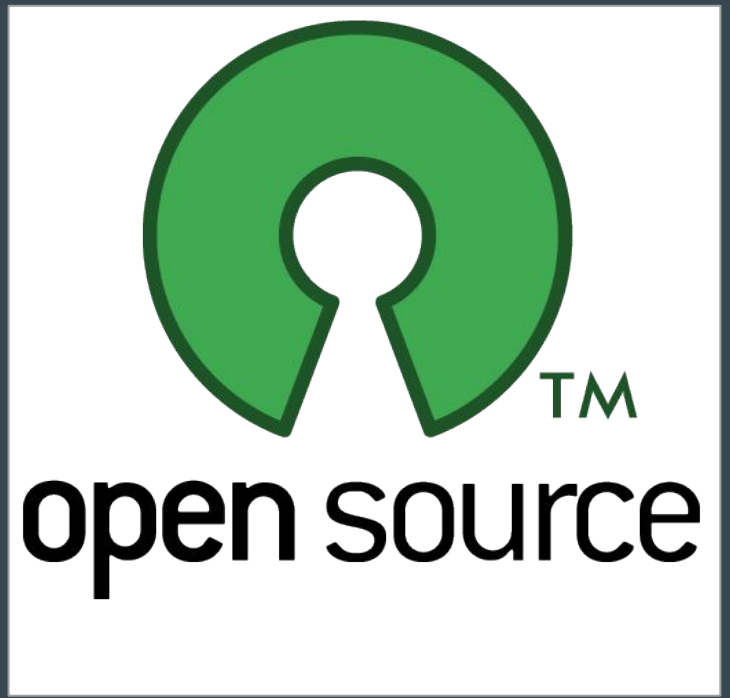
Enter Copernica

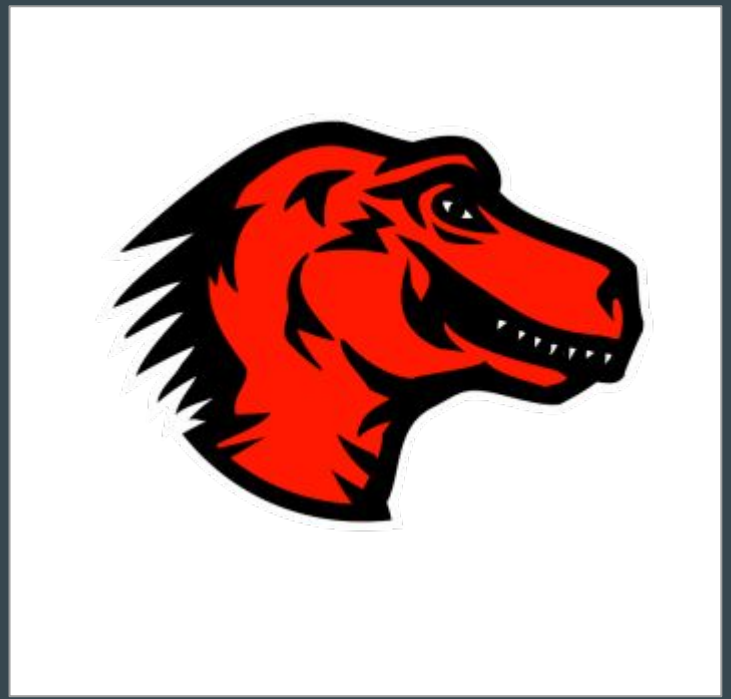
Copernica

Named after Copernicus, who realised the Earth isn't the center of the Universe just as the IP host isn't the center of networking, instead the Sun or Named Data should be the center of the networking world.

Copernica

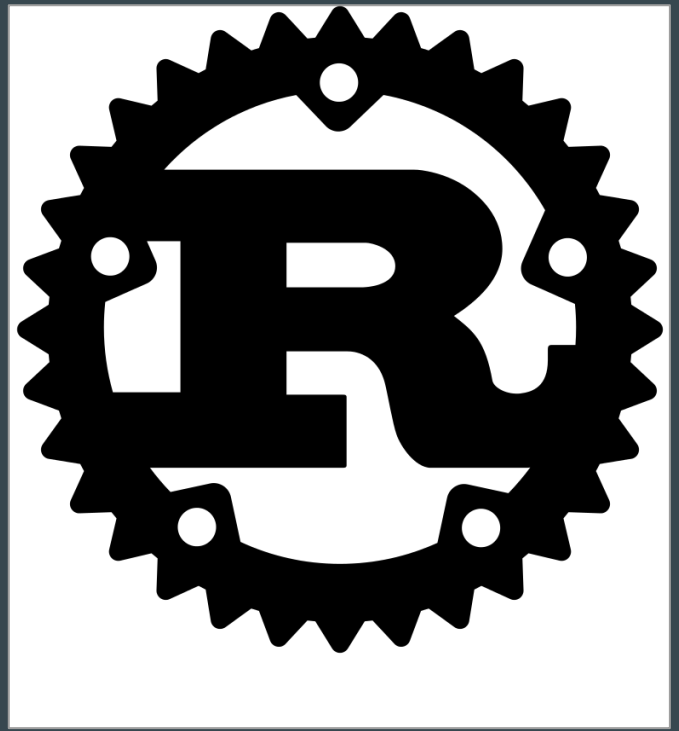
- Free software / Open source using MPLv2 License (you own your contributions)





Copernica

- Implemented in the Rust programming language



Copernica

- Free software / Open source using MPLv2 License
- Implemented in the Rust programming language
- Overlay on UDP, as every box on the current Internet supports UDP.
- Aspires to use raw (no IP) broadcast over Wifi 5G connecting Hong Kong homes together.

Copernica Objectives

- Be a viable secure networking protocol for the a new content-centric Internet that actively promotes decentralisation

Copernica Hard Design Constraints

- Routing information must be anonymous with no addressing information
- Must not make use of global knowledge (trusted third parties are security holes)
- The threat actor for this network is a highly organised wealthy totalitarian government

What is Copernica’s Secret Sauce?

Copernica - Secret Sauce is Sparse Distributed Representation

Each interface has a 2048 bit vector where F = False, T = True

F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	...

Copernica - Secret Sauce is Sparse Distributed Representation

You as the publisher of data need to convert the name of your data into a Sparse Distributed Representation Index (SDRI):

“My-Excel-Document.xls” => 10, 45, 67

F	F	F	F	F	F	F	F	F	F	T	F	F	F	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F	T	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
F	F	F	T	F	F	F	F	F	F	F	F	F	F	F	F
F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	...

Copernica - Secret Sauce is Sparse Distributed Representation

“My-Excel-Document.xls” => 10, 45, 67

So how do we do the conversion in a deterministic manner such that different parties can arrive at the same result?

Every data name consists of two components: **your unique id + the data name**

Copernica - Secret Sauce is Sparse Distributed Representation

Your unique ID looks like this:

ceo1q0te4aj3u2llwl4mxuxnjm9skj897hncanvgcnz0gf3x57ap6h7gk4dw8nv

Your data name looks like this:

“my-excel-file.xls”

The ID is a Bech32 address derived from Ed25519 (Edwards-curve Digital Signature Algorithm)

“ceo1q0te4aj3u2llwl4mxuxnjm9skj897hncanvgcnz0gf3x57ap6h7gk4dw8nv::my-excel-file.xls”

Copernica - Secret Sauce is Sparse Distributed Representation

Next we take the below name and pass it through a SHA3_512 hashing algorithm:

SHA3_512(“ceo1q0te4aj3u2llwl4mxuxnjm9skj897hncanvgcnz0gf3x57ap6h7gk4dw8nv”)

=>

768ade3da083187a1028dccea3fe7e738c76be4c2ef3fd54bfcfd63f67b34fd588698057a3165b941bbe77355541120c7933efc854ffea0dbb80fcfd7f068a4c

Copernica - Secret Sauce is Sparse Distributed Representation

We then calculate the positions of the least frequent occurring character in the hash

lowest_occurring_character("768ade3da083187a1028dccea3fe7e738c76be4c2ef3fd54bfcfd63f67b34fd588698057a3165b941bbe7735554112 0c7933efc854ffea0dbb80fcfd7f068a4c")

=>

[(18, "2"), (40, "2"), (93, "2")]

The number 2 occurs in positions 18, 40 and 93

Copernica - Secret Sauce is Sparse Distributed Representation

We then calculate the bit position of each character using this algorithm

768ade3da083187a1028dccea3fe7e738c76be4c2ef3fd54bfcfd63f67b34fd588698057a3165b941bbe7735554112 0c7933efc854ffea0dbb80fcfd7f068a4c

2048_bitvector_position = position_in_hash * 16 + decimal(hexadecimal_character)

[(18, "2"), (40, "2"), (93, "2")]

[290 <= 18 * 16 + 2, 642 <= 40 * 16 + 2, 1490 <= 93 * 16 + 2]

=>

[290, 642, 1490]

Copernica - Secret Sauce is Sparse Distributed Representation

We then calculate the bit position for the ID and ID+DATA_NAME

[2048_bitvector_position(“ceo1q0te4aj3u2l...57ap6h7gk4dw8nv”),
2048_bitvector_position(“ceo1q0te4aj3u2l...57ap6h7gk4dw8nv::my-excel-file.xls”)]

=>

This is our SDRI, a unique anonymous identifier of information.

[[290, 642, 1490][17, 481, 593]]

Copernica - Secret Sauce is Sparse Distributed Representation

[[290, 642, 1490][17, 481, 593]] [[351, 573, 2031][21, 373, 351]]

Copernica Packet Structure - Simple Request/Response Model

```
struct Sdri {
    id: Vec<u16>,
    name: Vec<u16>,
}

enum Packet {
    Request     { sdri: Sdri },
    Response    { sdri: Sdri, data: Data },
}
```

Copernica Packet Structure - Simple Request/Response Model

If a state threat actor intercepts a Request Packet all they'll see is:

[[290, 642, 1490], [17, 481, 593]]

If a state threat actor intercepts a Response Packet all they'll see is:

[[[290, 642, 1490], [17, 481, 593]]
[EnCt2d5f14f76c5e5c3d6d5c6be14487c509ad5702bc0d5f14f76c5e5c3d6d5c6be14I+vuDw9yVgG0HbBR7l28RJT
VIhIIIBPIQK1x+OOxOZpCrlQFWClEI/9mNC8/LYxvOowGYEmPN3IYlwgoZpk/4ub5YJEbpeYg8LdkHGUfsL
yqedNTSKTFe4+tvRfc3wi5oroltf32CVkIlQ==IwEmS]]

Copernica

This type of communications can traverse over insecure channels, it can go into the NSA, Huawei and come out again and they will have an extremely hard time extracting information from this.

[[[290, 642, 1490], [17, 481, 593]]
[EnCt2d5f14f76c5e5c3d6d5c6be14487c509ad5702bc0d5f14f76c5e5c3d6d5c6be14I+vuDw9yVgG0HbBR7l28RJT
VIhIIIBPIQK1x+OOxOZpCrlQFWClEI/9mNC8/LYxvOowGYEmPN3IYlwgoZpk/4ub5YJEbpeYg8LdkHGUfsL
yqedNTSKTFe4+tvRfc3wi5oroltf32CVkIlQ==IwEmS]]

You can put the above data on a usb drive, stick it in your sock, walk across the North Korean border and this data can be copied everywhere.

Copernica

- No Global Routing Information
  - No Single Point of Failure
- Totally Anonymous
- Mandatory Signing of Data to prove Provenance
  - Unsigned data isn't moved on the network
- Encryption by default, opt-out for non-encrypted packets
- Very easy to build Web of Trust
- Totally Decentralised / Distributed
  - Breaking the backbone of data dissemination monopolies

Conclusion

As the edge of the Internet is becoming the new center, GAFAM and totalitarian governments are going to have an increasingly hard time controlling the edge from the centre. Fake News is but a symptom of this loss of control in combination with untrusted data. Unsigned information is mis-information.

Specialist AI in tracking, monitoring and reporting will curate edge data on your machines and phone home to GAFAM clouds. If GAFAM built your phone is that AI malware?

Copernica let's you own your own data and trust others. CCP will not be able to control this network.

Stewart Mackenzie - sjm@fractalide.com