WOPLLI® Technologies

Architecture Principles & IEEE proposal – Trust over IP Foundation

By Vikas Malhotra

Jan 13th, 2022

Vision


Innovative Work, Play, Learn, Live Experiences
Safe, Fair & Trusted
Trust Fabric for Life Experiences
Experiences

Upcoming website

Digital Trust Statistics

Passwords

- Regular Internet users have an average of 85 passwords for all their accounts. (Cnet, 2020)
- The most commonly used password in the world **remains 123456 followed by 123456789, qwerty, password, and 12345. (Cybernews, 2021)**
- 80% of all hacking incidents are caused by stolen and reused login information. (Verizon, 2020)

Phishing

- As of 2020, phishing is by far the most common attack performed by cyber-criminals, with the U.S. FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime. (FBI Internet Crime Complaint Centre, 2021)
- Google has registered 2,145,013 phishing sites as of Jan 17, 2021. This is up from 1,690,000 on Jan 19, 2020 (up 27% over 12 months). (Tessian, 2021)

Data Breaches

- There were 1,767 publicly reported data breaches in the first six months of 2021, which exposed a total of 18.8 billion records. (Risk Based Security, 2021)
- Over 90% of all healthcare organizations reported at least one security breach in the last three years. 61% acknowledged they don't have effective mechanisms to maintain proper cybersecurity. (Frost Radar, 2020)
- In 2020 the average cost of a corporate data breach was $3.86 million. (Dice.com, 2020)

Privacy Erosion and Surveillance Capitalism

- 82% of web traffic contains Google third-party scripts and almost half of them are tracking users. (WhoTracks.Me, 2019)
- 74% of Internet users feel they have no control over the personal information collected on them. (Ponemon Institute, 2020)
- 72% of Americans report feeling that all, almost all, or most of what they do online or while using their cellphone is being tracked by advertisers, technology firms or other companies. (Pew Research Center, 2019)

Misinformation and Unverified Sources

- In 2020, only 29% of US adults said they mostly trust the news media. (Statista, 2020)
- In Q3 of 2020, there were 1.8 billion fake news engagements on Facebook. (German Marshall Fund, 2020)
- 56% of Facebook users can't recognize fake news when it aligns with their beliefs. (SSRN, 2018)

Artificial Intelligence (AI) Dangers

- 62% of the companies adopting AI are extremely concerned that it will increase their cybersecurity vulnerabilities; 57% are concerned about the consequences of their AI systems using personal data without consent. (Deloitte, State of AI in the Enterprise, 2020)
- 93% of automation technologists feel unprepared or only partially prepared to tackle the challenges associated with smart machine technologies. (Forrester, 2016)
- Only 36% of AI adopters are establishing policies or a board to guide AI ethics. (Harvard Kennedy School, 2019)
- The EU has drafted an Artificial Intelligence Act (AIA) specifically addressing transparency, privacy and security in the use of AI.
- The National Institute of Standards and Technology (NIST) is beginning development of an AI Risk Management Framework (RMF) to guide AI adoption for US federal agencies (where none currently exists).

Causes

It is all about data (& infrastructure)!

- Verification

Problem: There is usually **self-verification** or even if there is 3rd party verification, it may **not be independent**. Verification is also **not continuous**.

- Data (or Information), its access & use without permission of the rightful owner (a person).

Problem: **A person is not considered to be the owner of their data** hence everyone collects and stores. There is a debate on who owns information. Currently, it is usually considered to be the organization one works with or whoever finds (aka harnesses) it.

- Data (or Information), its availability in honey pots.

Problem: Most data is **centrally** stored and managed and is a honey pot that attracts hackers. Has been accelerated with Cloud move over last 15 years.

- Updates & issue Resolution times

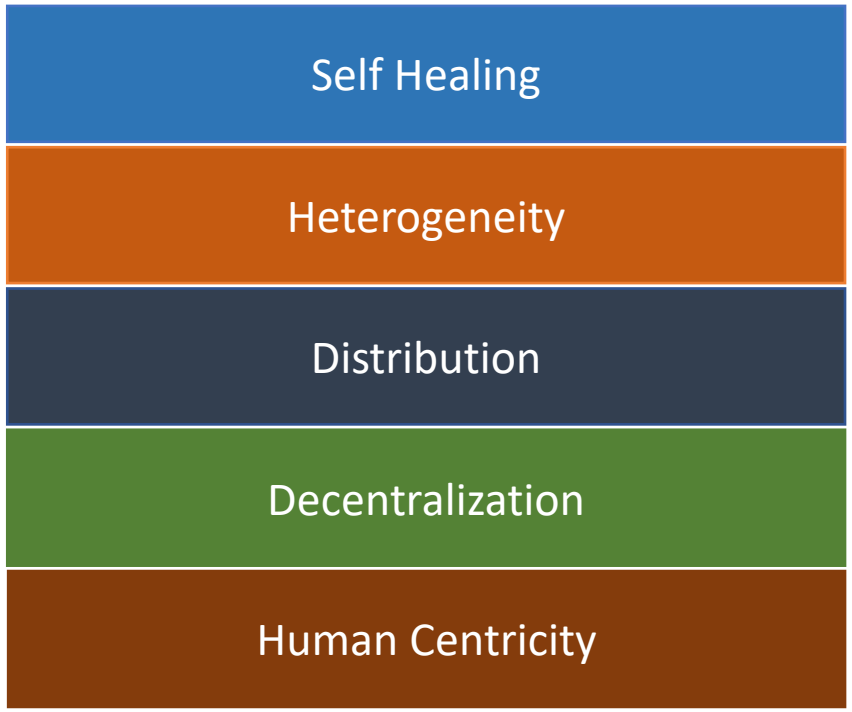
Problem: Need for updates are **not automatically identified**. Updates are **not applied automatically**. **Long resolution times**.

Architecture Principles

While verification (with VC) has progressed well in past 2 years,

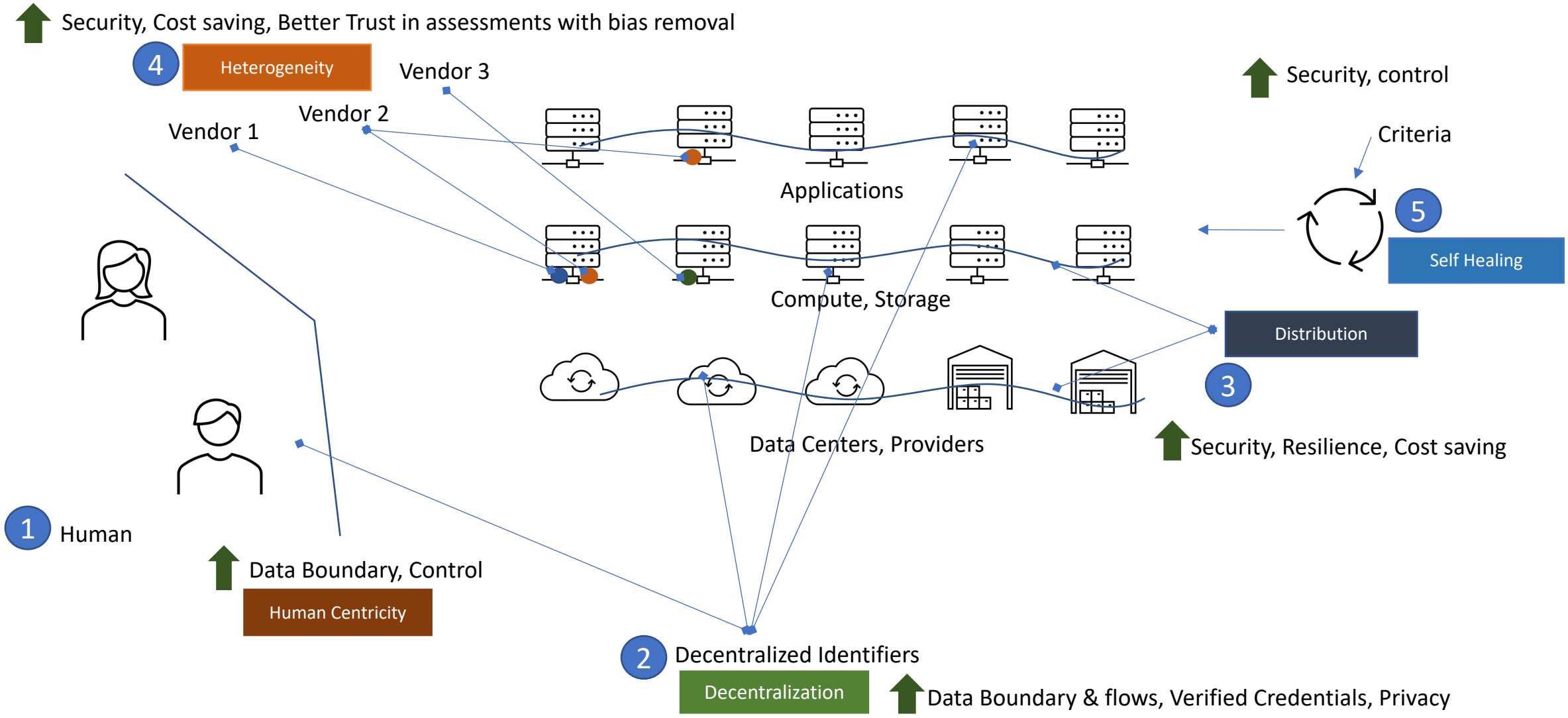
WOPLLI wants to Rethink architecture for data, its ownership, how infrastructures are secured & managed etc.

Architecture Principles (Data & Cyber security context)



- Controls & architecture adjust based on criteria
- Similar controls sourced from different places and applied at different places. Assessment of different controls done heterogeneously.
- Distribution of information & processing at various digital layers
- Decentralized & Sovereign identity, data flows along with verified credentials
- Control on information, human becomes the data boundary, build for human

Cloud / Services - PoV



IEEE workgroup proposal

Seeking support for “Cyber Security for Next Generation Systems” workgroup

- Explore architecture based on 5 principles
- Explore architecture & needs for specific technology areas
  - Artificial Intelligence & Autonomous Systems
  - Web 3.0
  - Quantum Computing

Proposed Output: (1) Considerations & guidance for Cyber Security for next generation systems.

Reach Vikas Malhotra (vikasmal@woplli.com) to enlist support and join.

Thank you!

Vikas Malhotra, Founder & CEO, WOPLLI Technologies

vikasmal@woplli.com