Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Web 3.0 and Cybersecurity – Short Paper

Sónia Silva*

ISLA – Polytechnic Institute of Management and Technology, Vila Nova de Gaia, Portugal
Email: silvamanuelasonia@gmail.com

Abstract

The Web 3.0 ecosystem is growing exponentially, which also adds to the cybersecurity concerns it imposes. There is a continuous shift in the Internet architecture, from a read/write model to a newer model known as Web 3.0. Global companies are exploring web 3.0 opportunities in their business processes. Along with opportunities, Web 3.0 poses several cybersecurity risks to organizations that need to detect and mitigate efficiently. Data breaches, computer attacks, and social engineering defined the cybersecurity risk landscape of Web 2.0. This work aims to identify solutions to the problem between the evolution of web 3.0 and companies to evolve their infrastructures promptly to ensure the privacy and security of their data.

Keywords: web 3.0; cybersecurity; security; zero-trust

---

* Corresponding author. Email address: silvamanuelasonia@gmail.com

1. Introduction

The original Web 1.0 was a place to serve static pages built by companies. Over time forums and social networks have emerged, and suddenly we had a Web 2.0 in which users created and added content. Tim Berners-Lee (inventor of Web 1.0) coined the term Web 3.0 to signify a data-based web that not only humans but also machines could process. If Web 1.0 created an encyclopedia, then Web 2.0 was Wikipedia and Web 3.0 would turn everything on the web into a massive database. How canand Web 3.0 be safely performed and managed?

2. Difference between Web 1.0, Web 2.0, and Web 3.0

2.1. Web 1.0

Web 1.0 was the first step of the World Wide Web. It was popularized in the early 1990s and was characterized by static web pages and simple user interactions. Websites are used to share information rather than provide dynamic user experiences. The image below demonstrates how Web 1.0 works:

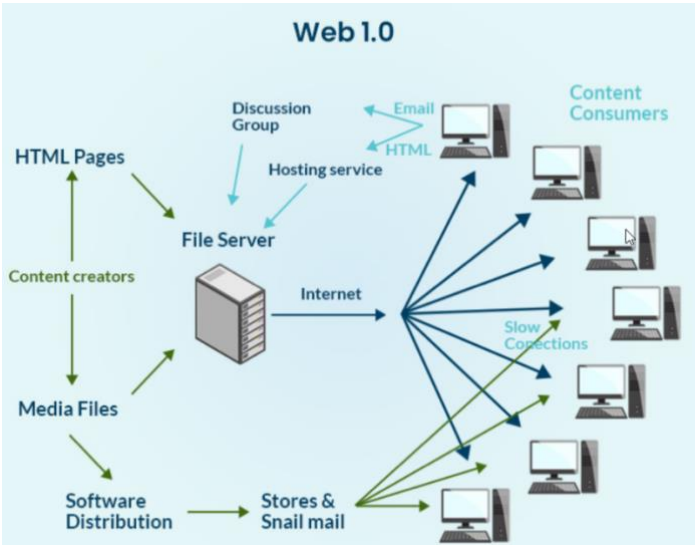

Figure 1: Features of Web 1.0 [1]

Features of Web 1.0

- Static pages.
- Content is served to users from the server's file system.
- Pages built using Server Side Includes or Common Gateway Interface (CGI).
- HTML Tables and Frames are used to position and align the elements on a page.

Web 1.0 had set the groundwork for future iterations of the Web. It allowed users to navigate and access information online easily. However, it lacked features that we now take for granted, such as multimedia and social interaction.

2.2. Web 2.0

Web 2.0 is a term used to describe the second generation of the World Wide Web, characterized by user-generated content, social networking, and participatory media. The image below demonstrates how Web 2.0 works:

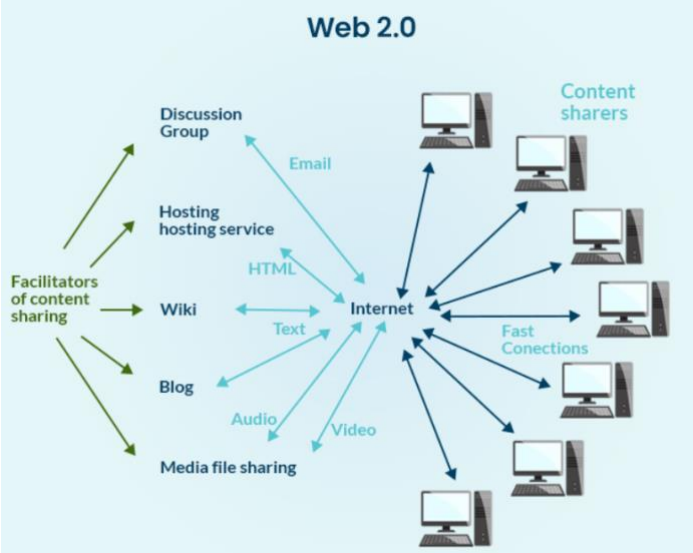

Figure 2: Features of Web 2.0 [1]

The first generation of the World Wide Web, created in the early 1990s, was static and consisted mainly of HTML pages read by web browsers. Web 2.0 brought about a new era of websites that allowed users to interact with the website itself. This was made possible by new technologies like AJAX.

- Features of Web 2.0
- Second-generation Web era
- They have Read-write only content.
- Consumers can consume and contribute content.
- Responsive and Dynamic content
- Information flows between the site owner and site users through evaluation & online commenting.
- Software applications based on APIs allow self-usage
- Web access leads to different concerns, from the traditional Internet user base to a broader variety of users.
- It includes CMS(WordPress), Portal, social media (Orkut, Facebook, Twitter, etc.), wikis (Wikipedia), messenger (Yahoo mail, MSN), etc.

The most significant challenge is Data security. Current Web 2.0 companies are centralized, so their decisions can be influential and harmful to a specific person, or country.

2.3. Web 3.0

Web 3.0 is an umbrella term for a new generation of internet-based applications and services that facilitate the exchange of value between participants in a decentralized network. It builds on the principles of Web 2.0. It

considers the advances of blockchain technology, which underpins many of the new applications and services.

Web 3.0 is referred to by experts as a "semantic web" because computers rather than humans can read the pages. It also includes artificial intelligence (AI) and computers not needing to go through centralized databases to process data.

It is an evolution of the current Web. It has been developing for over a decade and is still in its early stages.

The goal of Web 3.0 is to create a more intelligent and interconnected internet by using semantic markup and artificial intelligence.

It will allow users to interact with the Internet more naturally and make it easier to find and use the available information. Web 3.0 will also make creating intelligent applications that understand and respond to user requests easier.

Whereas web 2.0 was primarily driven by the introduction of mobile, social, and cloud technologies, web 3.0 is powered by four new layers of technological innovation:

- Edge computing
- Decentralization
- Artificial Intelligence & Machine Learning
- Blockchain

Features of Web 3.0

- **Semantic Web**

The next evolution of the Web affects the Semantic Web. The semantic Web enhances web technologies in demand to create, share and connect content through search and analysis based on understanding the meaning of words rather than on keywords or numbers.

- **Artificial Intelligence**

Web 3.0, computers will be able to understand information likewise to humans through technologies based upon Semantic Web concepts and natural language processing

In Web 3.0, computers can provide different information like humans to provide faster and more relevant results. They become more intelligent to fulfill users' requirements.

- **3D Graphics**

The 3D design is being used widely in websites and services in Web 3.0. e-commerce, Museum guides, computer games, and geospatial contexts are examples of 3D graphics.

- **Connectivity**

With Web 3.0, information is more connected to semantic metadata. As a result, the user experience develops to another level of connectivity that leverages all the available knowledge.

- **Ubiquity**

Ubiquity means presence everywhere. With Web 3.0, information & content are more connected and ubiquitous, accessed by multiple applications and with a growing number of everyday devices connected to the web. Example: The Internet of Things.

In the image below is a summary of the differences between Web 1.0, Web 2.0, and Web 3.0:

Figure 3: Difference between Web 1.0, Web 2.0, and Web 3.0 [1]

3.0. Challenges of Web Evolution 3.0

Companies have witnessed many transformations and opportunities for the digital revolution as they embrace Web 3.0 in their workflow. But at the same time, it has become profitable for cybercriminals to hack into the computer infrastructure to create disruption. Due to the decentralization of the Internet and the anonymity that Web 3.0 will provide, DevSecOps teams should consider developing a new robust ecosystem in Web 3.0 to keep sensitive data secure. Next, some cybersecurity challenges are presented in Web 3.0 that companies need to be aware of:

- **Date Authenticity**

One of the significant challenges with Web 3.0 is ensuring the authenticity of your data. It is a challenging task for companies to maintain data authenticity due to data management through the latest technologies and decentralized data management. The Chief Information Security Officers (CISOs) should consider designing and

implementing an evaluation mechanism to analyze the accuracy and security of data in Web 3.0. CISOs should consider answers to the following questions: "How will the security and accuracy verification mechanism work?", "Who will confirm the validity of the data?", "How to calculate and prevent data manipulation?". In addition to the authenticity of the data, it is also important to ensure the availability of data.

- **Social engineering attacks**

Because Blockchain is a foundation of Web 3.0, transactions stored in Blockchain are tamper-proof. However, it is a difficult task to ensure that tamper-proof data is protected from being compromised. Cybercriminals use phishing attacks impersonating a legitimate third party as a vector to steal sensitive information from users or companies in the Web 3.0 ecosystem. Cybercriminals are exploiting other social engineering attacks to exploit authentication mechanisms to gain access to users' data.

- **Identity threats**

Web 3.0 banks on its own identity to provide sets of portable credentials, complaints, and permissions to users involved with websites, other users, and other Web applications. Self-sovereign identity based on blockchains allows users to control aspects of their identity that they share based on the parts they engage with. But the implementation of an identity of self-sovereignty has some challenges inherent to identity risk. For example, cybercriminals may collect sensitive data about a user from the same identifier used to interact with specific websites or applications. It becomes a significant risk of identity theft due to unsafe authentication mechanisms.

- **Increased spam**

Web 3.0 makes up a vast library of integrated and interconnected metadata. These vast libraries can become dangerous channels that cybercriminals can exploit to infiltrate the computer infrastructure. The Web 3.0 ecosystem uses entire Internet resources as databases to respond to users. Cybercriminals can target, exploit and pollute certain assets or resources to prevent spam. Such spam attacks can be hidden malicious JavaScript code or a rescue attack that infiltrates the IT network and is sent to all network users. While the web 3.0 ecosystem has robust tools to protect databases, there will be a constant risk of content placement data leakage. CISOs should consider designing and implementing effective strategies to prevent data leakage.

- **Confidentiality concerns**

Web 3.0 also imposes the challenge of data breaches and makes it difficult to maintain confidentiality. While the Web 3.0 ecosystem has robust tools to protect databases, there will be a constant risk of data leakage. CISOs should consider designing and implementing effective strategies to prevent data leakage.

3.1. New Cyber Attacks

Web 3.0 will have to struggle with new attacks based on the underlying technologies and less oversight. Web 3.0 is still emerging, and cyberattacks will evolve with it, but for now, there are several new types of attacks that users

and organizations should be aware of, including:

- **Cryptojacking**

This attack involves a cyber attacker who installs mine encryption software on a victim's computer and networks without their knowledge or consent.

- **Smart contract hacks**

Smart contract hacks are probably the most important attack to avoid since smart contracts are responsible for executing cryptograms and other transactions in the lock chain. Smart contract hacks can disrupt the functionality of cryptographic wallets, disrupt project governance, and interfere with cryptographic loans and other FinTech transactions in the lock chain. An additional issue with the smart contract is the lack of legal protection. Many jurisdictions do not have adequate protections for smart contracts or the means to enforce the limited regulations they have.

- **Ice phishing**

An ice phishing attack involves a cyber attacker who convinces an unsuspecting victim to sign a transaction that transfers his cryptographic files to the attacker.

- **Rug pulls**

A Rug pulls typically involves social media influencers or minor celebrities, building interest and advertising for a particular currency and then taking the funds before the currency devalues. Some also know this attack in the cryptographic investment community as "pump and dump". Rug pulls fall into a legal gray area, and currently, there are few protections for investors.

4.0. Web 3.0 Security Issues

In the 2022 CISO Research Report prepared by Dynatrace [4], they interviewed 1,300 CISOs on the state of application security and DevSecOps in their organizations. Here are the answers:

- 75% of CISOs are worried too many application vulnerabilities leak into production, despite a multi-layered security approach.
- 69% of CISOs say vulnerability management has become more difficult as the need to accelerate digital transformation has increased.
- More than three-quarters (79%) of CISOs say that automatic, continuous runtime vulnerability management is key to filling the gap in the capabilities of existing security solutions.

One of the best defenses for businesses and people is to create a Zero Trust Policy when it comes to data security.

4.1. Zero Trust Security Model [5]

Gone are the days of cybersecurity measures that only involved firewalls and anti-viruses. With today's cloud-forward architectures and remote endpoints, protecting the network perimeter isn't just impractical – it's impossible. Threats can now come from anywhere, both externally and internally.

A paradigm shift is needed to protect users and data effectively. Enter zero trust. How does zero trust work, and what makes it different from the traditional cybersecurity approaches?

4.1.1. What is Zero Trust Security?

As the name suggests, zero trust is a framework in which anyone accessing your network, internally or externally, must be constantly authenticated for continued access. This contrasts with traditional network security, where connections inside the network are always deemed "safe." This approach becomes problematic with modern networks that often lack an "edge." Thanks to cloud infrastructures and remote access, it's nearly impossible to screen connections at the network perimeter. Thus, everyone is considered not trusted, and constant validation is required to weed out security threats and ransomware.

Zero trust is a relatively new concept, which means software providers typically have liberal interpretations when implementing it.

However, the NIST and National Cyber Security Center of Excellence (NCCoE) have attempted to develop a standard called NIST 800-207. It describes a zero-trust architecture that outlines best practices and techniques for implementing this approach.

Specifically, NIST 800-207 outlines three important guidelines for an effective zero-trust framework: continuous verification, automated context collection, and minimizing the impact of a breach.

4.1.2. How Does Zero Trust Security Work?

A zero-trust network operates on a simple principle: assumes everyone is a threat unless proven otherwise. Therefore, it requires a more comprehensive protocol than perimeter-based defenses like firewalls. In addition, its technologies involve constantly monitoring, verifying, and updating user access privileges when necessary.

To do this, network administrators must always have complete visibility over all user accounts. There also needs to be granular control over which data and applications individual users have access to on the network. This can be done through authorization and authentication methods.

However, doing so can become problematic in larger organizations with thousands of users and events. That's why zero-trust networks often use artificial intelligence (AI) and machine learning to flag suspicious behavior and rapidly mount a response.

Speaking of response, a crucial part of a zero-trust approach is to try and limit the impact of a breach. This can be

achieved by segmenting the network or utilizing zero-trust network access (ZTNA), which connects users to apps and resources directly and never through the network.

4.1.3. Benefits of a Zero Trust Model

- **Comprehensive security**

Zero trust provides much more adequate protection against external and internal attacks, with the latter being the hardest to defend against. What's more, one-to-one access based on an "as-needed" basis reduces the attack surface and prevents hackers from moving laterally through the network.

- **Better visibility**

A big benefit of zero trust is that it gives complete visibility into every connection on their network. This allows administrators to detect and react to suspicious behavior immediately. Additionally, it can log details of a breach for future improvement.

- **Simplified network management**

Zero trust systems greatly simplify network administration by streamlining and (in some cases) automating access protocols. There's no need for admins to approve access for every user individually.

- **Skips unreliable endpoint security**

Endpoints, like user devices and servers, are often the entry point for most hackers. Unfortunately, sophisticated attacks can often bypass even the tightest security on these endpoints. But with zero trust, you can maintain protection even if an insecure endpoint device connects to your network.

4.1.4. How to Implement Zero Trust Security

- **Mapping and segmenting data**

The first step to a zero-trust network is to classify which data is sensitive. This allows you to isolate them into more secure sections, away from other parts of the network that regular users can access. Part of this also involves knowing which applications are using the data. With this knowledge, you can map out how the data flows throughout your network to identify vulnerabilities.

- **Setting up the architecture**

Once you have your data "map" on hand, you can now design policies and boundaries around them. This step is crucial since you'll decide which users can access which data.

- **Monitoring everything**

You also need a way to monitor your architecture 24/7; to see if the policies and safeguards you set are doing their job.

- **Automation**

Finally, to get everything up and running, you need a system to orchestrate your zero-trust policies. This will allow you to enforce zero-trust rules without doing it manually.

5. Conclusion

The world and digital connections have become much more complex than previously thought. Businesses and society have structured themselves around the Internet in such a way that it is impossible to exist for one them.

The truth is even with the many advances made in the last two decades, the problem of digital security becomes increasingly critical for organizations. As more "things" became more connected, threats also grew and diversified.

Money is no longer the only target of cybercriminals. In the 21st century data and privacy have become the most precious assets of companies and the most tied. In a reality where data traffic has grown exponentially, moving through billions of devices, possibilities for cyberattacks have become endless.

While technology increases are associated with the increasing complexity and sophistication of cyberattacks, it is important not to forget that cybercriminals exploit how the weaknesses already exist in companies, especially as they are associated with the human factor - which is nothing more than the initial level of security of a company.

A recent adoption by companies of the telework model has increased the volume of online work and the exchange of confidential information in unprotected environments. Expanding and democratizing cybersecurity knowledge is important to create a new generation of users prepared to deal with threats and loopholes that become more complex day after day. We should not consider that only those who work in IT environments should have digital education.

Whether it's the CEO, the sales commercial, or the cleaning lady, more users have access to digital security training, understand the most vulnerable habits and how to avoid them, and the safer our digital environment and, consequently, our life will be. That is, it is of no use to implement a zero-trust policy, among other security policies, and invest in cybersecurity solutions (hardware and software) if before that it does not develop the mentality of employees for the basics of cybersecurity.

For example, an open phishing email and clicking a link can quickly become a window of opportunity for a cybercriminal causing serious graves for companies.

References

[1] Vinod Luhar " Evolution of Web – 1.0, 2.0, and 3.0" Internet: https://aspiresoftware.in/blog/the-evolution-of-web-1-0-2-0-and-3-0/, Apr. 6, 2022 [Dec. 15, 2022].

[2] Nikhil S "Implications of Web 3.0 on Cyber Security" Internet: itsecuritywire.com/featured/implications-of-web-3-0-on-cyber-security/, Jul. 12, 2022 [Dec. 19, 2022].

[3] Jonathan Tarud "Overcoming Web 3.0 Security Issues" Internet: https://www.koombea.com/blog/web-3-0-security-issues/, Jun.28, 2022 [Dec. 20, 2022].

[4] Dynatrace "2022 CISO Research Report" Internet: https://assets.dynatrace.com/en/docs/report/17322-rp-2022-global-ciso-report.pdf?_ga=2.173300963.1736076590.1671807550-1942815419.1671807550&_gac=1.18168267.1671807550.Cj0KCQiAwJWdBhCYARIsAJc4idCd8yF5haB4Rfgj84NIRHaMowBlszZgsXoQE-yliawig_dDy3GBxbIaAqnTEALw_wcB, 2022 [Dec. 23, 2022].

[5] TOKENEX "What is the Zero Trust Security Model?" Internet: https://www.tokenex.com/blog/zero-trust/, Feb.04, 2022 [Dec. 23, 2022].

[6] Duarte, N., Coelho, N., Guarda, T. (2021). Social Engineering: The Art of Attacks. In: Guarda, T., Portela, F., Santos, M.F. (eds) Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2021. Communications in Computer and Information Science, vol 1485. Springer, Cham. https://doi.org/10.1007/978-3-030-90241-4_36

[7] F. Alves, N. Mateus-Coelho and M. Cruz-Cunha, "ChevroCrypto – Security & Cryptography Broker," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-5, doi: 10.1109/ISDFS55398.2022.9800797.

[8] N. Mateus-Coelho and M. Cruz-Cunha, "Serverless Service Architectures and Security Minimals," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800779.

[9] Nuno Mateus-Coelho, A New Methodology for the Development of Secure and Paranoid Operating Systems, Procedia Computer Science, Volume 181, 2021, Pages 1207-1215, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.01.318.