sciendo

MARKETING OF SCIENTIFIC AND RESEARCH ORGANIZATIONS, 2021, Vol. 42, Issue 4, p. 97–109
pISSN 2353-8503
eISSN 2353-8414

ZERO IDENTITY — THE NEW CYBERSECURITY PARADIGM

ZERO IDENTITY — NOWY PARADYGMAT CYBERBEZPIECZEŃSTWA

Wayne Ronhaar
Pepperdine University CEO-Cylentium
24255 Pacific Coast Highway, Malibu, CA 90263
Wayne@Cylentium.com ● ORCID 0000-0002-8107-5666

William Bradley Zehner II
St. Edward's University
3001 South Congress Ave, Austin, TX 78704
wbzehner@gmail.com ● ORCID 0000-0003-3203-5382

Robert Langhorne
VP & CTO — Cylentium
2002 Brushfire Court, Arlington, Tx 76001
Rob@Cylentium.com ● ORCID 0000-0002-0891-5091

DOI: 10.2478/minib-2021-0023

ABSTRACT

Global cybercrime is exploding geometrically. The traditional methods of securing cyber systems via complex passwords frequently fail, exposing the computer systems to many types of cybercrimes. Cybercrime of all kinds is a growing concern for individuals, government and business organizations, and society. Zero Identity is a new technology that "bubbles, cloaks, and hides" computers and their contents from cybercriminals. Zero Identity is a mature and proven military-based technology with over a 20-year history. Cylentium, a cybersecurity startup, is adapting Zero Identity technology to consumers and civilian organizations. Market and technological acceptance of Zero Identity may lead to a cybersecurity paradigm shift in the next decade. This paper explores the history of Zero Identity, what it does, how it works, and its future prognosis. One of the original developers (Rob Langhorne) of the Zero Identity concept was interviewed, as was the concurrent entrepreneur (Wayne Ronhaar). Both Langhorne and Ronhaar became coauthors of this article to contribute their first-hand historical perspectives, challenges, and insights to transform technology into a commercial product in a series of articles.

Key words: Cybersecurity, Cyber Invisibility, Cylentium, Hacking, Paradigm Shift, Passwords, Quantum Computing, Wireless Wall, Zero Identity

ABSTRAKT

Zjawisko cyberprzestępczości rośnie w zawrotnym tempie na całym świecie. Tradycyjne metody zabezpieczania systemów cybernetycznych za pomocą złożonych haseł często zawodzą, narażając systemy komputerowe na różnorodne formy cyberprzestępczości. Cyberprzestępczość stanowi zatem coraz większy problem dla osób prywatnych, organizacji rządowych i biznesowych oraz społeczeństwa. Zero Identity to nowa technologia, która maskuje komputery, odizolowuje je w tzw. „bańkach" i tym samem ukrywa ich zawartość przed cyberprzestępcami. Zero Identity to dojrzała i sprawdzona technologia o pochodzeniu wojskowym z ponad 20-letnią historią. Cylentium, firma typu „startup" działająca w dziedzinie cyberbezpieczeństwa, dostosowuje technologię Zero Identity do konsumentów i organizacji cywilnych. Rosnąca akceptacja rynkowa dla technologii Zero Identity może doprowadzić do zmiany paradygmatu cyberbezpieczeństwa w następnej dekadzie. W niniejszym artykule, na podstawie wywiadów z Robem Langhornem, jednym z pierwotnych twórców koncepcji Zero Identity oraz z Waynem Ronhaarem, przedsiębiorcą-współtwórcą, opisano historię systemu Zero Identity, jego sposób działania oraz jego perspektywy na przyszłość. Zarówno Langhorne, jaki Ronhaar przedstawili swoje własne perspektywy na proces przekształcania nowej technologii w produkt komercyjny oraz na różne wyzwania napotkane na tej drodze. Tym samym stali oni współautorami tego artykułu.

Słowa kluczowe: cyberbezpieczeństwo, cyberniewidzialność, Cylentium, włamanie komputerowe, zmiana paradygmatu, hasła, komputery kwantowe, Zero Identity

JEL: K24, L26, M13, O00, O31, O33

Introduction

In 1969, the US Department of Defense awarded the initial contracts to develop ARPANET, which connected four computing sites at universities and research centers in the Western United States and eventually morphed into today's Internet. In 1973, the University College of London (England) and Royal Radar Establishment (Norway) connected to ARPANET, and today's worldwide Internet was born. The government-funded Internet research project eventually transformed how societies live, work, and play in almost every corner of the globe (Cohen-Almagor, April 2011).

So, H.K., Kwok, S.H.M., Lam, E.Y., and Lui, K. (2010) of the University of Hong Kong point out the need for robust electronic cyber security like Zero Identify in end-to-end networks. This article explores another US

government-funded technology with the potential to transform societies, Zero Identity aka Wireless Wall — a technology that can provide strong security in end-to-end networks.

The Cybersecurity Challenge

Nearly a decade ago, in 2012, Leon Panetta, former director of the US Central Intelligence Agency and the US Secretary of Defense, warned the world of the societal dangers from cyber threats (Perlroth, N., 2021). Jang-Jaccard, J. and Nepal, S. (2014) explored the increasing frequency and devastating impact of the exploding number of cybersecurity threats and possible defenses.

More recently, on May 7, 2021, the Colonial Pipeline, which supplies nearly half of the diesel, gas, and jet fuel to the Eastern Region of the US, was hacked using a compromised password (Turton W. and Mehrotra, K., 2021). Colonial Pipeline paid the hackers approximately $4.5 million in ransom. The U.S. Justice Department recovered about $2.4 million of the ransom.

Later in May 2021, JBS–USA, the US's largest meatpacker responsible for processing about 25% of the US beef while employing approximately 50,000 individuals, was hacked for ransom (AP, 2021). JBS–USA paid the cybercriminals an $11.5 million ransom.

Cybersecurity is a global issue. Cybercriminals have twice dropped Ukraine's electrical power (Krigman, A. 2020) as well as disabling the data on nearly 35,000 of Saudi Aramco's computers (Pagliery, J. 2015). Saudi Aramco accounts for approximately 10% of the world's hydrocarbon production.

There are no accurate estimates of the exact scope of cybersecurity crime and related challenges. There is no single source for collating the cybercrime data. Additionally, many ransomware crimes are not reported. Consequently, it is difficult to quantify the number of attacks, ransoms paid, and massive incremental economic investments by individuals and organizations in cybersecurity protective software and technologies. More broadly, by 2021, global cybercrime damages are predicted to reach $6 Billion /year (Morgan, 2020). In terms of human time lost, the numbers

are similarly astronomical. The Norton LifeLock report for 2020 estimates that 330 million people in 10 countries experienced cybercrime in the last 12 months, spending 2.7 billion hours dealing with the aftermath (Norton, 2020).

Additionally, the growth of cybercrime is rapidly accelerating. Ransomware attacks strike the American government, businesses, and nonprofit organizations every *eight minutes* (Perlroth, N., 2021). In their fourth report on cybercrime, *The Center for Strategic and International Studies* and the computer security company McAfee estimated the monetary loss from cybercrime at $500 billion in 2018, which exploded to $945 billion in 2020 — almost doubling in two years (Riley, T., 2020).

Organizations tend to underestimate the costs of ransomware attacks. In 2019, the *Washington Post* estimated the average cost to the organization of a ransomware attack to be approximately $762,000. Riley (2020) reported that the impact of business interruption costs "can be five to 100 times larger than the cost of the ransom itself". A 2017 cyberattack on the Danish shipping company Maersk "disrupted operations for two weeks which cost the company $300 million," according to Riley (2020). From a management perspective, it is quicker and cheaper to pay the ransom to restore the organization's system than rebuild it since most ransom demands are minor compared to the economic impact.

With an even more pessimistic outlook for cybercrime, *Cybersecurity Ventures* predicts damages from cybercrime to "total $6 trillion globally in 2021... up from $3 trillion in 2015". Unfortunately, the same organization is already predicting that those totals will hit $10.5 trillion by 2025. Between the staggering economic costs, the time spent resolving the aftermath of attacks, and the rapid growth rate we already see, we desperately need new technology to protect our digital presence.

Passwords — The Current Protective Paradigm

Cybersecurity attacks are increasing as increasing numbers of individuals work remotely due to covid. None one is safe — including high profile individuals such as Bill Gates and Elon Musk. In a 2020 cyber-

attack on Twitter, "Hackers compromised the accounts of 130 high-profile users and were able to reset the passwords of 45 of those accounts (Okereafor, K. and Adelaiye, O., July 2020)".

The current paradigm to protect computer systems from attack is passwords to identify the user via identification and double authentication systems. The passwords are increasingly complex. The drill is familiar: "Your password must have a minimum of 8 to 12 separate characters including capital and lowercase letters and numbers and special characters".

Steward and Strausbaugh (2017) point out that passwords have been "computer security's "first and last line of defense for decades" — especially 8-character passwords.

Without going into the math, the typical 8-character password of uppercase and lowercase letters can be "brute-forced" cracked by a computer "guessing" the number of combinations and permutations in about 7 minutes. Adding special characters lengthens the time to crack an 8-character password to about 96 hours.

However, the "cracking and hacking programs" and computers used by the bad actors are becoming increasingly powerful and quick. More letters, numbers, and special characters lengthen the password's complexity and strength. The newest programs and computers that breach passwords can "crack" more complex passwords in even less time, rendering password barriers alone passe.

Unfortunately, new technology also aids hackers and bad actors. Brute force solutions will become easier as computers and hacking programs improve and exceptionally high-powered computers become accessible. The decade of the 2020s will herald the arrival of practical quantum computers, which are millions of times faster than current computers. Google's quantum computer is 100 million times faster than traditional "bit and byte" personal computers (Nield, D. 2015). Quantum computers will accelerate the demise of traditional passwords.

Backdoor Hacking

Another way bad actors "attack and hack" computers and acquire

information is through other devices controlled by the computer system. The devices can be a mobile phone-controlled thermostat, a television, a printer, or any number of devices. A 2021 survey by *Statista* (January 22, 2021) reported that the typical American home contains a minimum of 10 devices which are entry points for hackers.

Adding another device to the computer and network system creates another potential entry point for hackers to steal data. So, what can individuals do to protect themselves, and more importantly, their families? What actions can close the back doors to a computer system?

Zero Identity — The New Paradigm

A new technology called Zero Identity, or Cyber Invisibility, adds a new layer of protection to the individual's current password. The system authenticates who is allowed into the network. The idea behind the innovative Zero Identity technology is both simple and proven. The technology is simple since its "cloaks" or "bubbles" your location. The Cylentium user cannot be seen electronically under and inside the "bubble," cannot be identified electronically. Thus, the individual's computer and back door entry points cannot be found and attacked by hackers and bad actors.

The electronic technology that "bubbles" your computer and related devices from cyber predators was developed as military technology. Wayne Ronhaar, the founder of Cylentium, an organization adapting the military-grade "bubble" technology to protect consumers, families, and small enterprises, describes Zero Identity in the following mantra: "If you cannot be seen, you cannot be found; if you cannot be found, you cannot be hacked; if you cannot be hacked, you are safe and secure."

What Does Zero Identity Do?

Zero Identity makes the computer network electronically invisible by surrounding it with a protective "bubble." Cylentium technology is

sophisticated enough to allow a specific computer or individual to be "bubbled" to a large organization or geographical site. Integrating repeater and concentrator technologies into the network potentially extends the geographic "bubble" to hundreds of square kilometers.

A bubble can be extended through mesh networking to remote computers and devices when traveling, other networks, or even to a unique set of friends and colleagues. An individual or organization may belong to multiple bubbles with different rules and permissions applying to each bubble.

Zero Identify secures individuals and organizations from bad actors and hackers by making computers and systems electronically invisible unless authenticated. The Zero Identity "bubbles" allow authenticated communications such as email to operate both normally and securely.

How Zero Identify Works

Cylentium's Zero Identify technologies work to cloak and protect the individual by combining multiple security technologies into a robust, technologically protective barrier without going into a deep technical dive. The technologies include:

- Zero Identity technology masks and hides the unique computer identification number that identifies every computer. If bad actors look for this identification number as an entry point to hack the network, Zero Identify prevents detecting the device's ID.
- A VPN (Virtual Private Network) embedded in the Zero Identity technology hides a computer's physical location and IP address while encrypting the internet traffic. The VPN secures network communications, hiding a computer from bad actors.
- Zero Identity uses proven "frequency-hopping spread spectrum" technology to rapidly change the sending and receiving frequencies to secure communication between devices.

A Brief History of Zero Identity Technological Development

Cylentium's technology foundation is military-grade cybersecurity. Twenty years ago, the computer scientists at the US Naval Postgraduate School in Monterey, California, conceived and developed the "bubbling" technology. The original impetus behind the technology was to secure all communications of US Naval vessels in foreign waters or threat environments from external cybersecurity threats and attacks.

The concept was to create an "invisible cloak" on all communications, electronic traffic, wireless, ethernet, satellite, radio, and related electronic signals by making a ship's electronic signals invisible to others. The Zero Identity technology creates a safe "bubble" that allows electronic communications to function freely within the bubble, making the ship effectively electronically undetectable and untraceable to others.

Shortly after developing the concept and prototype, the US Naval Postgraduate School ceased its support for the project due to a lack of research funds. However, the US Naval Postgraduate School formally allowed Dr. Dennis Volpano, a civilian Ph.D. computer science instructor, to develop the technology independently.

In 2000 and 2001, Dr. Dennis Volpano sold the cybersecurity concept to a Silicon Valley technology startup company, Cranite Systems, Inc ("Cranite"), which he co-founded and was Chief Technology Officer. Angel investors initially funded Cranite Systems. In subsequent years, an American venture capital fund named Kleiner Perkins financed Cranite Systems. Investments in Cranite Systems exceeded $30 million.

Cranite developed a working prototype of Cylentium technology, then called 'Wireless Wall", and sold primarily to government clients and business organizations. Many of the early adopters of the Wireless Wall technology were US government agencies. Others were civilian aerospace companies such as Lockheed Martin and Rockwell International.

These organizations scrutinized the Zero Identity Wireless Wall technology, extensively testing it before purchasing. After testing, these security-focused organizations' purchase shows the technology is robust, met stringent cybersecurity requirements, and works.

Exhibit 1. Presents a partial representative list of early adopters of the Wireless Wall Technology

Representative Early Adopters of Wireless Wall Technology	
Booz Allen Hamilton Technology Consultants	US Army Medical Command
Canadian Air Force Tactical Forces	US Army Mobile Handsets
Canon Information Systems Research — Australia	US Bureau of Resource Reclamation
City of Renton, Washington	U.S. Joint Forces Command
City of Savannah, Georgia	U.S. Marine Corps
First Responders — New York City	US Medical & Disease Research
First Responders — Snohomish County, Washington	U.S. National Security Agency
Lawrence Livermore National Lab	US Naval Academy — Annapolis
Lockheed Martin	U.S. Naval-Marine Corps Intranet
Rockwell International — Space Division	US Naval Research Center
Sandia National Labs	US Naval Weapons Support Center
University of Texas Medical Branch	US Office of Secretary of Defense
Walter Reed Medical Center	U.S. Space and Naval Warfare Systems Command
US Army Inspector General School	U.S. Special Operations Command
US Army Madigan Medical Centers	U.S. State Department
US Army Military Academy — West Point	White Sands Missile Range

In 2008, Cranite pivoted the focus of Wireless Wall to target the then-new rapidly growing VPN (virtual private network) market. Warburg Pinkus, a global equity fund, invested $20 million in additional development funds to refocus the Cranite and the Wireless Wall technology on the rapidly emerging VPN market. As a result of the 2008/2009 financial and technology crisis, Kleiner Perkins and Warburg Pinkus abandoned Cranite, the Wireless Wall technology, and VPN market targeting. The sudden loss of financial resources from venture funds and resulting lack of cash flow forced Cranite to cease operations and dissolve the company.

Due to the lack of ongoing technical support and updates, the existing Wireless Wall customers slowly phased out, except for the US Department of Energy (DOE), which had bubbled a critical US nuclear reactor site.

Ed Smith, CEO of TLC- Chamonix, acquired Cranite's Wireless Wall physical assets and intellectual property in June 2010. Mr. Smith

attempted to focus on the VPN market, believing he could capture the VPN market with the Wireless Wall Technology. Because Mr. Smith, as a one-person company, was too small and lacked the critical technical expertise to capture and service global customers — especially significant government contracts, he exhausted all fiscal resources.

In 2017, to revive and relaunch Wireless Wall, Ed Smith reached out to Robert Langhorne, the original team leader and developer of Wireless Wall for Cranite. Ed Smith and Robert Langhorne agreed to form a new company INP — Intelligent Net Protection, Inc., and relaunch Wireless Wall technology under the INP company banner. Late in 2017, INP bid on a NATO Global Wireless Cybersecurity Contract and won against formidable competitors, including Cisco, based on the superiority of Wireless Wall technology. Shortly after the awarding of the contract, NATO canceled the awarded contract due to INP's lack of infrastructure and inability to meet NATO's global support requirements.

As a result of the cancelation of the NATO contract and a desire to press ahead with INP, in 2018, Ed Smith and Robert Langhorne reached out to Wayne Ronhaar, CEO of Snowy River International, to help unlock the potential of the technology by developing a global business strategy and related action programs. A new company, named Cylentium, was created to update the proven Wireless Wall technology and rebrand the technology in cybersecurity organizational and consumer marketplaces.

Zero Identity Today

Today, Cylentium is aggressively and successfully raising funds to convert the technology to civilian use and create the necessary global structure to support all potential clients. Cylentium has identified four major market segments, each with unique needs. (1) Governments that need data security and secure communications; (2) the business market with similar requirements to the government sector; (3) the rapidly growing IoT (the Internet of Things) market focused on complex manufacturing processes that need protection from ransomware; (4) and the consumer which market needs protection from hackers.

Cylentium, Inc. is currently focused on the consumer market as the Zero Identity technology protects home networks, which are otherwise open to data breaches by hackers. The expanding world of working remotely due to Covid-19 and the increasing proliferation of home devices connected to the network (such as smart appliances, televisions, et al.) has driven consumer cybersecurity needs to new levels.

The typical home in the US has 10 to 17 IoT devices — each one representing an unprotected back door. Additionally, the expansion of digital banking and financial transactions makes the consumer more vulnerable to cybercrime. As a result, consumer ransomware attacks have increased. The consumer's limited current defense against bad actors uses increasingly complex passwords and multi-step authentication.

Cylentium, Inc. focuses primarily on the consumer market with brand-new, improved products designed to bring proven military-grade cybersecurity protection to "bubble" the consumers' homes.

Summary

Zero Identity technology supersedes the password and multi-step authentication challenges, which frequently fail to protect the network systems and create opportunities for cybercrimes. The Zero Identity technology is robust, proven effective in rigorous environments at military and government sites such as the State Department and the US Secretary of Defense and in practical civilian business applications such as at Lockheed Martin and Rockwell International.

Several organizations have attempted to commercialize the Zero Identity technology by forcing its application to large and complex organizations. Today, Cylentium focuses on addressing the technology's consumer and small business applications.

The Zero Identity technology has the possibility of becoming the new paradigm for cybersecurity. Zero Identity "bubbling" protects individuals and organizations by increasing the difficulty of hacking computers, homes, and organizations by "hiding" the computers and network. Zero Identity may impact global society, as did the Internet, by creating an entirely new cybersecurity paradigm: protecting the systems from hackers to save consumers an estimated $10 trillion in losses due to cybersecurity crime annually.

References

1. AP (June 2, 2021). *Getting Back online After Cyberattack*. https://www.cnbc.com/2021/06/02/jbs-worlds-largest-meat-producer-getting-back-online-after-cyberattack.html
2. Cohen-Almagor (April 2011). Internet History. *International Journal of Techno ethics*. https://ieeexplore.ieee.org/abstract/document/5622061
3. Jang-Jaccard, J. and Nepal, S. (August 2014). A survey of emerging threats in cybersecurity. *Journal of Computer and Systems Sciences*, *80*, 5, pp. 973–993. https://doi.org/10.1016/j.jcss.2014.02.005
4. Krigman, A. (October 22, 2020). *Cyber Autopsy Series: Ukraine Power Grid Attack Makes History*. https://www.globalsign.com/en/blog/cyber-autopsy-series-ukranian-power-grid-attack-makes-history
5. Morgan, S. (November 13, 2020). Cybercrime to Cost the World $10.5 Trillion Annually by 2025. *Cybersecurity Ventures*. https://cybersecurityventures.com/cybercrime-will-cost-the-world-16-4-billion-a-day-in-2021
6. Nield, D. (December 10, 2015). Google's Quantum Computer is 100 million Times Faster Than Your Laptop. *Science Alert*. https://www.sciencealert.com/google-s-quantum-computer-is-100-million-times-faster-than-your-laptop
7. Norton (2020). *Norton Cyber Security Insights Report: Global Results, Symantec*. https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/
8. Okereafor, K. and Adelaiye, O. (July 2020). Randomized Cyber Attacks Simulation Model: A Cyber Security Mitigation Proposal for Post Covid-19 Digital Era. *International Journal of Recent Engineering Research and Development*, *5*, 7, pp. 61–72.
9. Pagliery, J. (August 5, 2015). *The Inside Story of the Biggest Hack in History*. https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html
10. Perlroth, N. (June 6, 2021). *Are We Waiting for Everyone to Get Hacked?* New York Times.
11. Riley, T. (December 7, 2020). Cybersecurity 202: Global Losses from Cybercrime Skyrocketed to nearly $1 Trillion in 2020. *The Washington Post*.
12. Stewart, T. and Strausbaugh, S. (September 26, 2017). *The 8 Character Password is Dead. Protiviti*, https://tcblog.protiviti.com/2017/09/26/the-8-character-password-is-dead
13. Turton, W. and Mehrotra, K. (June 4, 2021). Hackers Breach Colonial Pipeline Using Compromised Password. *Bloomberg*, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
14. So, H.K., Kwok, S.H.M., Lam, E.Y., and Lui, K. (2010). *Zero-Configuration Identity-Based Signcryption Scheme for Smart Grid*. 2010 First IEEE International Conference on Smart Grid Communications, pp. 321–326. Doi: 10.1109/SMARTGRID.2010.5622061.
15. Vailshery, L. (January 22, 2021). Average Number of Devices in the Typical American Home. *Statista*, https://www.statista.com/statistics/1107206/average-number-of-connected-devices-us-house

Wayne Ronhaar, — BS, MS Technology Management. Wayne earned bachelor's and master's degrees in business and technology from Western Washington University and Pepperdine University respectfully, is working on his Doctor of Business Administration, DBA, at Pepperdine University. With 40+ years of experience as an American entrepreneur and technology executive, Wayne has previously served as National Strategy Executive Microsoft Canada, CIO in Silicon Valley, Chief Innovation Officer Finance & Banking, and Chief Enterprise Architect Oil & Gas, Banking, Consumer Loyalty. Wayne has extensive international experience, including North & South America, Europe, the Middle East, and Africa.

Brad Zehner — Ph.D. Executive Management and Leadership — Peter F. Drucker School — The Claremont Graduate University and master's degrees in business, marketing, and psychology. Dr. Zehner was Associate Professor of Marketing and Strategy at Pepperdine University, Associate Director of the IC2 Institute — a "think and do" tank focused on wealth creation and Director of the MS in Technology Commercialization program at the University of Texas at Austin. Dr. Zehner was Associate Professor of Management and International Business at St. Edward's University in Austin, Texas. Formerly, he was a global executive responsible for Worldwide Marketing and Sales for 12 machinery companies and simultaneously Managing Chairman of 4 small companies located in the US, England, France, and Hong Kong. And Vice President — Strategic and Business Planning for 26 Industrial Products in 13 nations.

Rob Langhorne — BS in computer science — College of William and Mary. Rob has over 20+ years of experience in building complex software and leading diverse technological teams. Today, Rob is Cylentium's Chief Technology Officer and was one of the original developers of the Wireless Wall and Cylentium technologies. Before joining Cranite, Rob was vice president of engineering at fusion One, a pioneer developer of Web-based synchronization and mobility solutions. Rob's career has included management positions at Apple Computer, Spyglass, and Rocket Mobile. He also has led teams and developed products for Philips, Oracle, Software AG, and the US Air Force.