White Paper on Existence Technology Security Breakthrough
A Complete Explanation

Why the Current Cyber Crisis

The current cyber crisis is the result of a misapplication of technology based on a misunderstanding applying security protocols. Much of the current cyber crisis was created by a choice made last century. ANY path forward requires analysis of past decisions. Why were the choices made? Were those decisions correct? Are they still valid?

When secure activity entered the Internet, the digital security theorists fell into three major camps:

1. Create a parallel Internet for secure activity. *This was rejected*
2. Require a second Factor in addition to data for authentication
3. Place a portal to secure services in a public environment

The overwhelming choice was option 3. Once the choice was made, billions of dollars were spent to mitigate the damage created by this choice. The result of this choice is an environment where data is secure until an attacker arrives. Then security fails.

In order to justify choosing option three, marketing was applied making scientifically unsupported claims and falsely claiming functionality. This has exacerbated the problem by giving people unversed in computer science a false sense of security.

Multi-Factor Authentication (MFA) is an example of weakened security passed off as an improvement. It was introduced to harden access control in a public environment. In reality MFA is a multiple-step process in which data is gathered. Multi-Factor means two or more unique factors. Data is one factor and no MFA solution on the market today can name their alleged Non-Data Factor.

In science, words have defined meanings. Marketing may confuse people, but it doesn't change the definition of terms. MFA is conceptually and scientifically invalid. Yet "Experts" continue to explain how gathering data in multiple steps equates to two or more factors.

Two-Factor Authentication (2FA), as deployed, merged options 2 and 3. The organizations that chose this path were driven by the need to join the digital world and understood that data-only authentication was inadequate in any access control protocol. They acted responsibly and should be applauded.

However, there are three problems with existing 2FA solutions. First, public access was retained. Second, the solution is deployed at the endpoint while at the server, 2FA remained data-only authentication. Thirdly, 2FA failed to evolve with the Internet.

Correct Solution Gone Wrong

The correct solution was to merge options 1 and 2. The digital security theorists were correct, a parallel method for secure activity and hardware are required. However, they were also wrong. What was needed was a hardware-based factor to create a parallel Internet access method rather than an entire second set of cables, routers, switches: hardware. (Really, these were valid discussions in their day!)

A parallel private environment that is hardware based, created Existence as a Non-Data Factor. If the 2FA providers focused as much effort on analysis as they did on marketing, they would have evolved to Existence Technology. However, they choose to stagnate. Worse yet, the assumptions from their past became given facts today. Those decisions are invalid and have yet to be reviewed.

Token Proves Existence

A correctly-executed option 1 and 2 solution's parallel-access-environment has been patented and integrated into a token. The token must exist and be present to:

- Create a private portal
- Authenticate the environment BEFORE granting portal access
- Be part of a secondary credential authentication *and*
- Maintain the environment

An Existence model uses and requires an Existence-Factor throughout activity and any current data factor, such as a password, to authenticate access. This process limits access to a single individual with a single uniquely serialized token that can be identified prior to loading a login page with a single related data credential.

An Existence model focuses on creating security through the use of an independent parallel Internet created through secure environments on each end. Each authorized individual maintains the *only* token that will create their own uniquely serialized private portal, and that portal exists only when they are conducting secure activity.

Underlying Premise

There are three major classes of Data on the Internet: “Public” (self-explanatory), “Classified” (secure data that is created by public access) and “Corporate Secure” (data with a known audience).

Segregation of Corporate Secure data is an essential first step. Public and Classified data are part of public activity.

Corporate Secure data is a special class with a requirement for special access. There is nothing public about secure data.

The most basic security protocol is restricting access to authorized entities only. Therefore, placing a portal on a public website is a correctable mistake. How? Remove the portal.

Once the website portal is removed, there is no longer a valid reason to retain browser-based access. Remove it as well.

Loading any secure data and conducting any secure activity via an environment that is built on content-mining was completely illogical in the first place. The fact that so many plugins also content-mine, further compromises this environment.

A Existence model is as much a mindset as it is a methodology and system. Secure access begins by requiring as state-of-existence created by their Existence Token. An individual is forced to recognize that they are performing secure activity and the individual is responsible for their actions. Mitigating irresponsible behavior perpetuates that behavior. Existence requires every party to act responsibly.

Security Requires Buy-in from Everyone or Security Fails

The current cybersecurity model places responsibility and liability on a secure-environment owner while requiring little, or nothing from, authorized individuals. Again, half a solution; both parties must participate and be responsible for security to be effective!

Designing access to secure activity to the lowest common denominator has driven cybersecurity to an ever increasing failure. The only way to fix this problem is educating people to use proper security protocols, raising the level of the lowest common denominator rather than compromising critical security protocols.

Seatbelt usage in vehicles is a result of educating the public about auto safety. People can also be taught to act responsibly online; it just requires the business community to decide the damage is unsustainable. Then to apply validly configured technology to meet, objectively real, security protocols. **Guessing identity is not valid for any form of security!**

The Technology

Skipping the technical explanation for now, at its essence, deploying Existence Technology is a very simple five-step process:

1) Identify authorized individuals
2) Distribute Existence Tokens
3) Add a field to the user database for the public key associated with the individual's token and ship the correct token to the correct individual (a process already accomplished with credit and debit cards)
4) Remove portal from website and place proxy (reverse proxy) for access
5) Block all connections other than pre-authenticated Existence private portals.

Contrast this with the current access-control model:

Figure 1

The current access-control model for a secure environment can best be represented in Figure 1. Today, you have 17 billion plus potential connections to a single public portal where every set of valid *data* credentials are accepted. Filtering unlimited uncontrolled access to only authorized individuals is next to impossible.

Yet the mistake in this model is even worse. Every bit of secure data for *every* authorized individual is available at the exact same uncontrolled public portal. A breach at the public portal has the potential of compromising every authorized user and all data they have access to.

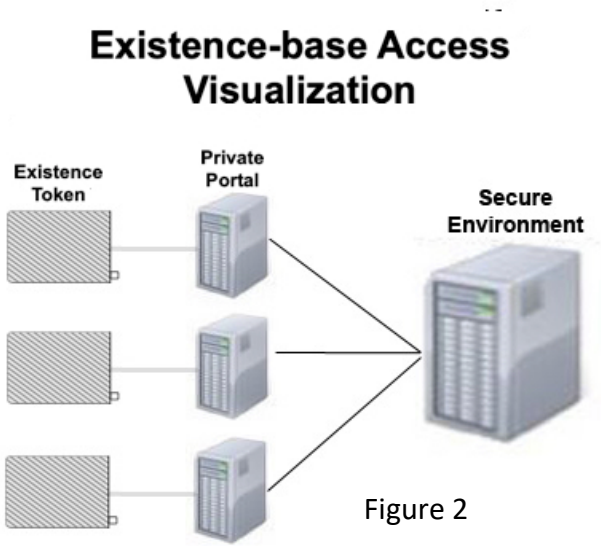

Figure 2

Existence Technology changes the approach to securing an environment. An Existence Token is distributed to authorized individuals, website portals are removed, and browser-based access is blocked. Analysis for individual environments must start here.

An Existence Token is connected to a local device. The token initiates a session that creates a uniquely serialized private portal. At the secure environment, role-based security must be initiated prior to presenting portal access, rather than after data credentials are received.

A token-based directly-asserted identity solution removes the need for public access to secure activity. No matter how nuanced the conversation is, at its core a website portal is a path into a secure environment that can be exploited. The only solution is to remove this attack vector.

Public access to a secure environment is a known, persistent, exploited weakness. If everything else around a secure environment stays exactly the same, how much better would every security product perform when access is limited to only known entities?

The path to security never ends. But it also never begins until the first step is taken. Once public access is removed, security experts can focus on the next step. In a binary environment, after every decision there is always another decision to make. Everything on the wrong fork in a binary environment will wither and die. Perceptive tech companies will evolve quickly to take advantage of the non-public access fork.

The ripple effect from every step forward in a binary environment *always* calls into question the decisions on the other fork. What is really needed? Is the product still necessary? How many connections were hidden in the noise of public access?

Without website portals, browsers can be eliminated from secure activity. In 2017 Google's Chrome developer stated it is "Almost impossible to secure a browser's UI". Continuing to conduct secure activity in an environment that the developer admits is corrupt is illogical.

Existence Technology is the beginning of securing data on the world wide web. Existence Technology does not fix everything. It fixes the FIRST highest level mistake.

Figure 3

(A token can take any form-factor and use any connector. Figure 3 is just a representation of *one* option of a token's form-factor.)

An Existence Token must:

- Be device-agnostic
- Install no software
- Use no installed software
- Be serialized, hardened and Read-Only
- Contain RAM to maintain secure data related to secure activity
- Contain software to create a pristine environment each and every time and upon removing the token no footprint can be left behind
- Must be backward compatible so existing browser-based operations transfer with minimal effort

When used, the token is integrated into the operational environment. When the secure interaction is complete, the token is removed, and all session data evaporates. Remove the token during the session, the session implodes, and all session data evaporates.

Step-by-Step Walk-Through

Use of Existence Technology requires the individual to connect their token to a device. Every individual has a uniquely serialized Existence Token that must be present for the entire session. The end user interaction with Existence Technology is a super-simple process:

1. Plug in the token
2. Initiate session (a click)
3. Enter credentials and interact exactly the same as they do through a browser and website portal *(Access Control cannot get any easier for the end user!)*
4. Remove the token when complete and all traces of the session evaporates

Behind the scenes, Existence Technology requires every aspect of the patented system to be present and validated or the model fails, the operational-environment implodes and a new session must be initiated. The entire access methodology and system is secure and in the presence of any alteration, it will not operate. Figure 4 is an overview of the process.

Is Wireless Secure?

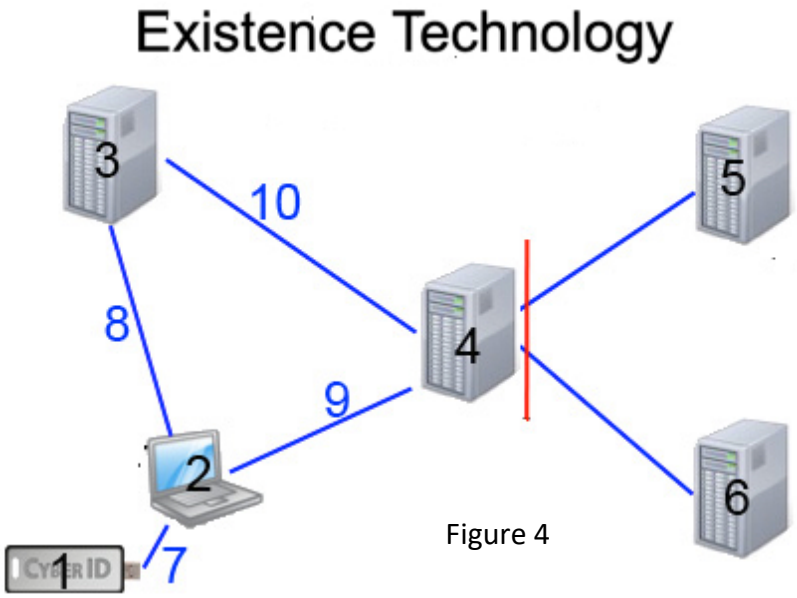

Figure 4

Let's address wireless connectivity now. RFID in security is an inappropriate use of technology at best and I will not waste time on it. Bluetooth is not a "secure option". "What is BlueBorne? Billions of phones, laptops and TVs at risk of silent Bluetooth hack", Jason Murdock – International Business Times.

- The process begins with the token (1) being connected (7) to any device (2) to create an operational-environment, thus initiating the process.
- The token's operational-environment opens and then provisions the token's RAM and connects (8) to an Authentication Server (3) passing a public key.
- The Authentication Server (3) accepts the connection from the originating operational environment and verifies the token hasn't been reported lost or stolen.
    - If stolen, the Authentication Server (3) sends a self-destruct code
    - If not, the Authentication Server (3) initiates a challenge and response protocol
- Authentication Server (3) sends a challenge question back to the originating operational environment (8). The operational-environment (2) uses the token (1) to process the challenge and the response is returned (8).
- The Authentication Server (3) processes the response and if valid, the path to the token's secure environment is passed back (8).

    - The token is blind to both its owner and its secure environment until this point. Now the token knows only its community (4).
- The operational-environment (2) connects (9) to a secure community Proxy Server (4) passing the tokens public key and session ID.
- The proxy server calls to the community (5)(6) to verify the token is still valid and to retrieve role-based data for session control.
- Proxy Server (4) connects (10) to the Authentication Server (3) requesting the token's session ID.
    - If the session ID does NOT match, the Proxy Server (4) rejects the connection and the operational-environment implodes.
    - If the session ID matches, the Proxy Server triangulates communication (8)(9)(10) and the environment is secure.
- Once the Proxy Server (4) completes securing the environment, access and the communication, the logon screen is passed (9) to the Operational Environment (2) and user interaction begins.

The communication from the community (4) to the individual is direct with no content mining. The only data retained by the process is the IP address of the token and the timestamps for session start and end.

A Physical-Factor (the Existence Token) integrated into an Operation-Factor creates a *UNIQUE* Existence-Factor for every individual/token combination.

A New Landscape Awaits

Once an Existence-Factor is part of cyber security protocols, the entire landscape changes.

Today, credit card data can be compromised in too many places to be trusted digitally. Perhaps the most flagrant example is in card-not-present transactions.

Further, a breach at any retailer provides data that can be used at every retailer. Yet, a bank with an Existence-Factor can mitigate the breach before it happens. Adding an "Existence Check" to authorization protocols requires both the bank and the consumer to act responsibly.

Here's how it works.

The consumer must log into the bank to assert existence when shopping. The Bank captures the IP address of the login and monitors the connection for continued presence.

The consumer goes to a retailer and completes a purchase *exactly* as they do now. The retailer passes the same data they do now.

Existence Technology secures the bank and the consumer from theft. If the Bank requires the IP address of the transaction along with the current credentials, an IP address check can provide additional assurance.

HIPAA Compliance

Medical record access, requiring an Existence-Factor, accomplishes what HIPAA set out to do and so much more. Taking into consideration the convoluted methods by which records have been stored, access is made even more difficult because of product incompatibility. An Existence-Factor still provides a tremendous value beyond access control!

Basic analysis of the landscape: Medical data is decentralized without a unifying method to share the data. The population is mobile so an individual can receive treatment anywhere, anytime. The only uniform location for data, for those who are insured, is the insurance company. Every time an insured is treated, the bill is submitted to their insurance company for payment.

Now let's consider the effect of an Existence-Factor in medical insurance. The insurance company merges Existence Technology into their insurance cards. This part only requires the insurer to act. Of course, the insurer can remove the website portal and browser-based access to insured's data, but this is just the beginning.

When an insured visit's a physician, they present their insurance card. The physician logs into the patient's private portal. The insurance company can provide a treatment overview by adding a simple query to their billing database. They pull every bill, treatment code, diagnosis code, drug code and other required data related to the insured. This data can then be displayed so the physician has a more robust understanding of the patient's health.

Now, if the insurer required a link to the record for payment, the insurer becomes a secure gateway to medical records while exceeding every access standard set by HIPAA.

Proper tracking inside the insurance companies' environment provides a wealth of information that can be utilized. When the physician is reviewing the data with the patient, unauthorized treatments can be identified and reported, placing both the insured and the physician actively into the fraud prevention model.

The fact that the physician and insured's insurance card were present at the same time can be used to identify billing anomalies with a high degree of accuracy. If the card is not present, it triggers a flag. This is just adding a log check to the billing approval process. Again, the consumer is only being asked to act responsibility, the insurer is taking advantage of their responsible action to improve overall security.

Security and Responsibility

No matter what technology is introduced, security will always come down to conscious responsible action. Until we correctly facilitate and demand that action is a required step in the appropriate processes, security will continue to fail.

The first step to responsible action is recognizing that a system design choice that fatally compromised security was made to make adoption easier before most people in cybersecurity were in cybersecurity. This was made clear by Vint Cerf, the Father of the Internet's recent statements on 20 January 2019 (see attached).

The time for cyber security to mature has arrived. Demanding PROOF-of-Identity for secure activity is not only reasonable, it is necessary.

Existence Technology is the first necessary step to a secure cyber environment. The future path of existing technology will be profoundly changed. Let me state:

"I personally stand firmly AGAINST a universal identifier for secure access. The thought of that much power in the hands of a single entity is horrifying!"

Still the cloud's capabilities are just being touched upon. Imagine a cloud offering desktop hosting. Everything currently housed on a local device stored in the cloud and requiring a uniquely-serialized token to create a serialized environment to interact with the desktop. Local devices can go back to dumb terminals with only minimal operability and drivers. This will minimize local exposure to devices being compromised.

All the technology related to Existence Technology already exists, has been proven, deployed and recommended by the US Department of Homeland Security and others. Cyber Security Experts just need to get the technology implemented. The good news is, that Existence Technology is everything they already know, applied in a way they never considered.

U.S Patents Nos. 8,074,261 & 8,484,701

International Patent Apply