EINPRESSWIRE

Federico Simonetti, CTO, Xiid says "Security was an afterthought. Sadly, it still is."

NEW YORK CITY, NEW YORK, USA, February 14, 2019 /EINPresswire.com/ -- Vint Cerf, by many considered one of the “fathers” of the Internet, has recently stated that—in summary—when the Internet was designed, security was an afterthought.

He also went on to say that security “is retrofittable into the internet”. Good. Then, why isn’t it? Why is security STILL such an afterthought?

I know, I know, many will be crying blasphemy now. How can I say that security is still neglected, when a simple Google search for the term “IT security” produces, at the time this article is being written, about 8.7 Billion results?

Federico Simonetti, CTO, Xiid

Ok, let me explain…

Security will stop being an afterthought, or—even worse—a “given” when every single designer and developer will bear it in mind at all times, and will realize that security is a side-expertise that every creator of every piece of the Internet must have.

> “We are honored to have Federico Simonetti, CTO, Xiid, join us “In The Boardroom” to talk about cybersecurity threats, best practices and Xiid solutions.”
>
> *Martin Eli, Publisher*

This is something that the car industry has understood, maybe not from the start, but in recent times for sure. The windshield designer knows that the glass has to be shatter-resistant to avoid throwing glass shards into the driver’s and passengers’ eyes in case of accident.Tire designers have invented “run-flat” tires and heat-resistant compounds to improve safety. And then we have steering wheels that move away from the driver in case of frontal impact, distraction-free dashboards to help keep the driver’s eyes focused on the street (thus reducing distraction-related accidents), variable tension seat belts to avoid breaking your rib cage, even an emergency handle inside the trunk to pop it open in case you’ve been kidnapped and put in the trunk of your own car. Not to mention the obvious airbags, ABS, ASR, ESP, and the like…

See the pattern? A windshield design team is composed of experts in windshield design, aerodynamics, AND security. A tire design team is composed of experts in rubber compounds, hydrodynamics, static/sliding/rolling friction physics, AND security. And so on. Every statement here ends in “and security”.

Similarly, the Internet will be a truly safer place only when every designer of every piece of it will be also an expert in its security. From the team that designs actual copper cables and fiber optics, all the way up to the web and mobile app developer who’s designing the next regional cooking recipe sharing app.

And—unfortunately—the higher you go in the stack, the less security expertise you find, and the more you realize that, for too many, security is a “given”. Ask the typical app developer “how do you keep communications safe?” and their answer will probably be “oh, my app communicates with the server via HTTPS” or “I use a VPN”. That’s it. That is enough to ease their security concerns. After all, they should be focused on developing their app, right? Security should be a given, should be part of the infrastructure, should come built-in just because you use a TLS-enabled protocol or a VPN, right?

Wrong.

Even when focusing our observations only on a single market, let’s say the IAM market (because that’s where Xiid plays, so we know it well) we see the exact same pattern.

IAM stands for Identity and Access Management. And that’s what most of our competitors do: they focus on MANAGING identities and access. Maybe the market segment should have been called IAMS (Identity and Access Management and Security) to make players more aware that security must be woven into the very fabric of their Identity and Access Management solutions. Instead, the “it is what it is” mentality still pervades almost every IAM solution on the market, and what’s even worse the market accepts their security trade-offs.

Want an example? Here’s a screenshot from the knowledge base of one of Xiid’s primary competitors:
****
****
Active Directory integration: DMZ server ports

If you installed the AD agent on a DMZ server, you must open the following ports:

- 135/TCP RPC
- 137/UDP NetBios
- 138/UDP NetBios
- 139/TCP NetBios
- 389/TCP/UDP LDAP
- 636/TCP LDAP SSL
- 3268/TCP LDAP GC
- 3269/TCP LDAP GC SSL
- 53/TCP/UDP DNS
- 88/TCP/UDP Kerberos
- 445/TCP SMB
- 123/UDP NTP

****
****
In addition, you must open your DCOM RPC ports. In addition to TCP 135, Microsoft RPC (MS-RPC)
****
****
Inbound rules and open ports on the customer’s firewall required by a competing IAM (not Xiid)

See what I mean? If you need to reach a server/service inside your DMZ, you create inbound NAT or port-forwarding rules on your firewall. That’s how it’s been done all along, that’s considered “the way it is”. Secure enough. No one is really acknowledging that each one of those open inbound ports is a potential pathway to reach and attack the server/service to which they lead.

But it’s always been done that way. Some of the services bound to those ports have already been exploited multiple times (RPC, NetBIOS, DNS, SMB, …) yet… it is what it is… it’s always been done that way, so why change now?

Because that’s not secure! That’s why.

And that’s why we, at Xiid, have done something about it. We have created the first IAM solution that features Active
Directory integration

WITHOUT THE NEED FOR ANY INBOUND OPEN PORT ON THE CUSTOMER'S FIREWALL.

None. Zero.

In our design we always put security first. And we designed our Active Directory integration agent to work without the need for any inbound NAT nor port-forwarding rule on your firewall. There simply is no route to reach Xiid's agent from outside the subnet it's installed in. And

YOU CAN'T ATTACK WHAT YOU CAN'T REACH.

Yet, it works, and it provides comprehensive as well as secure Active Directory integration. It's security innovation by design applied to the world of Identity and Access Management. It's IAM to IAMS.

And this is just one of the many patent-pending security solutions that we have designed here at Xiid, to weave security into the very fabric of each service that so direly needs it. Feel free to contact us privately should you wish to know more about it.

Federico Simonetti is CTO, Xiid (www.Xiid.com)
Former ethical hacker (DDT)
Former professor of operating systems security at the University of Milan
Developed software for the Italian anti-terrorism and anti-pedophile police
Serial entrepreneur with several successful exits in his past
Hardcore software designer, with award-winning software titles on his resume

Learn more about Xiid here: www.Xiid.com
Read all of Federico Simonetti's blogs here:
https://medium.com/hybrid-security-superheroes/security-was-an-afterthought-sadly-it-still-is-55e3ce1e54e6
https://medium.com/@theoriginalddt
https://medium.com/hybrid-security-superheroes

https://www.youtube.com/channel/UCCi2WTHuC8h2nIba2jyA2Jg
https://cyberinvestingsummit.com/
****
****
About SecuritySolutionsWatch.com

www.SecuritySolutionsWatch.com features thought leadership interviews about IT, IoT and security solutions. Our flagship “In The Boardroom” program, now in its 15th year, has delivered outstanding content about solutions from leading global brands such as: 3M, AMAG Technology - A G4S Company, ASSA ABLOY, Cisco Security, Cyberinc, Dell EMC, HP Cybersecurity, Fujitsu, Gemalto, HID Global, IBM, ImageWare, Intel, SAP, Siemens, Stanley Security, SONY, Unisys, and Yahoo, just to name a few.

What's YOUR authentication, cybersecurity, physical security, mobility, or "smart" solution?

What's YOUR Blockchain or FinTech solution?

We invite you to please join us "In The Boardroom" at www.SecuritySolutionsWatch.com.
For a quick tour to see exactly how your brand will be featured, please contact Ali Eng on our publishing team via
email: ALE@SecuritySolutionsWatch.com, or phone: 1+914.690.9351, or, LinkedIn:
https://www.linkedin.com/in/ali-eng-a8a41015b/

For more details, please click here: www.SecuritySolutionsWatch.com/Main/Jan2018.pdf
And for our Media Kit, please click here: www.SecuritySolutionsWatch.com/MediaKit.html

****
****

It's FREE...our monthly newsletter with thought leadership content from leading security experts.
Please click here: www.SecuritySolutionsWatch.com/newsletters/newsletter_2019_01.html
And please visit us on Twitter here: www.twitter.com/SecStockWatch

****
****

All content which appears on SecuritySolutionsWatch.com and in this Press Release is subject to our disclaimer:
www.SecuritySolutionsWatch.com/Main/Terms_of_Use.html

****
****

Martin Eli, Publisher
SecuritySolutionsWatch.com
+1 914-690-9351
email us here