Issue 3/2022

The Hacker’s Mindset

What you don’t know can hurt you

> Future and past blurred; what he had already experienced and what he would eventually experience blended so that nothing remained but the moment.
>
> *Philip K. Dick,*
> *Do Androids Dream of Electric Sheep?*

Embracing the metaverse

The metaverse is no longer the stuff of science fiction. A subtle shift to the metaverse is already taking place as we speak, as consumers embrace the metaverse where it makes sense for them – from attending virtual concerts and auctions to using augmented reality furniture apps.

The word “metaverse” is a word created from combining the word “meta,” which means “to go beyond,” and the word “verse” from the word “universe.” It is a combination of augmented reality and virtual reality – an alternate digital reality where people can work, play, and socialize.

The metaverse is essentially the next iteration of the internet. It is an exciting ecosystem for businesses to engage with customers in new ways and take the digital economy to the next level. In fact, there are already plenty of businesses who are building parts of the metaverse and others with a solid vision for what it should look like to function.

Eventually, the metaverse will blend the physical and digital world seamlessly.

Virtual reality (VR):

fully artificial environment; full immersion in virtual environment

Augmented reality (AR):

virtual objects overlaid on real-world environment; the real world is enhanced with digital objects

Mixed reality (MR):

virtual environment combined with the real world; interact with both

Extended reality (XR) / metaverse:

a mix of all the above

However, the sheer complexity and number of moving parts involved in expanding organizations beyond the physical world bring a whole host of new security concerns. The question we need to ask is: How can we prepare for this shift?

What is clear is that your organization’s attack surface will greatly expand as we move into the metaverse. Although we can use existing protection techniques, it may not stop new attacks that have never been seen before.

As we move towards a metaverse, financial transactions will cover not just virtual goods, but also real-world goods and services sold through a broader range of channels that may include AR/VR interactions.

In today's social selling, goods are sold and paid through a social media platform with the seller linking their system to the platform via an API. The metaverse opens near-infinite virtual storefronts – making data privacy and authentication a bigger challenge.

Security in the metaverse era requires security of content created in the virtual world and protection of personal data. The role of an edge platform company like Akamai with the highest edge platform coverage worldwide is very important.

Jonathan Singer of Akamai shared some of the challenges we can expect the metaverse to deliver for CSOs and their teams based on the definition by venture capitalist Matthew Ball.

The metaverse essentially enables a digital version of "you" in a virtual space that can perform various activities and conduct financial transactions. It will gradually establish itself in your daily life like smartphones, which is inevitable for mankind. Someday, it will just become a part of our lives without us even noticing it.

What are your organization's plans as we go into the metaverse?

Definition	Challenges
The metaverse is a massively scaled	authentication, access policies, malware, encryption and secure traffic, DNS security, web app attacks
and interoperable network	uptime, DDoS attacks, flash crowds
of **real-time**	security vs. performance trade-offs, API security, stream protection, anti-piracy
rendered **3D virtual worlds**	fraud, physical/access security, hardware/IoT security, content integrity
which can be experienced synchronously by an effectively **unlimited number of users**, each with an individual sense of presence	flash crowds, MFA, security at scale
and with continuity of data such as identity,	secure registration, credential provisioning, authorization
history,	PII, encryption
entitlements,	encryption, PII, fraud prevention, intellectual property rights, payment security
objects, communications,	encryption, PII, fraud prevention, intellectual property rights
and payments.	PII, encryption, fraud prevention, PCI compliance, tokenization, payment risk

Gaming security – our metaverse security blueprint?

To prepare for the metaverse, and everything that comes between then and now, we recommend that all CISOs, regardless of industry, become familiar with the audience and security challenges of the gaming industry.

Gaming is already providing and influencing a significant portion of the metaverse's foundational technology.

As multitudes of technologies continue to converge into a connected social/technological landscape, it's clear that videogames are one of the key driving industries paving the way forward. The gaming industry has pioneered technologies and interactive models that would be used not only for video games themselves.

Gaming is already providing and influencing a significant portion of the metaverse's foundational technology. Beyond technology, its business models are likewise being adapted and leveraged across industries.

Ten years ago, the primary value of any account was in credit card numbers, and any information that could help a criminal get into a bank account.

Now, gaming accounts themselves have value in the form of a player's time and in-game items. Accounts that have put in time playing and racked up gear can allow purchasers of stolen accounts to play at a high level without putting in the effort. In-game goods can also be sold in third-party markets for real cash.

This form of virtual value is already being reflected in the investment community with people buying up NFTs. As the world, and your business, move toward operating in the metaverse, securing accounts and access will continue to be a top priority.

As every company moves to do business in the metaverse, partnership with your users and employees around account security will become a larger part of the customer experience and the brand relationship, expanding security's role in the enterprise.

At Akamai, we have strong visibility into the problems in the gaming space. Reports published include how and why criminals attack the gaming industry, and two recent "State of the Internet" reports on gaming security: You Can't Solo Security and Gaming in a Pandemic.

Each of these examines several aspects of what it takes to keep systems online and running despite the relentless efforts of attackers.

You Can't Solo Security also features results of a survey of hard-core players, which Akamai undertook in partnership with the international gaming conference organization DreamHack (now ESL Gaming) to better understand how players feel about the security of their games and how much personal responsibility they believe is warranted when it comes to securing their own gaming accounts.

No discussion of the metaverse and gaming during the pandemic would be complete without talking about Roblox. While children and parents were at home with a pandemic raging across the globe, Roblox was there as a social, creative, and educational outlet for children and teens. Estimates point to there being anywhere from 520,000 to 40 million published games on Roblox. If that seems like a bit of a wide range to choose from – it is.

Roblox was trying to grow into a global entity and needed to deliver secure, consistent experiences for developers and players alike, regardless of where they were in the world. Poor user experiences, such as slow load times or disconnects, could mean lost revenue for the business.

Roblox came to Akamai for help ensuring they were successful in enabling high-performing online multiplayer games and game creation experiences.

Using Akamai, the company was able to deliver secure, consistent experiences for developers and players around the world.

Find out more:

Roblox delivers high-performing, global games

click to read

Chun Chats with... a Developer Advocate

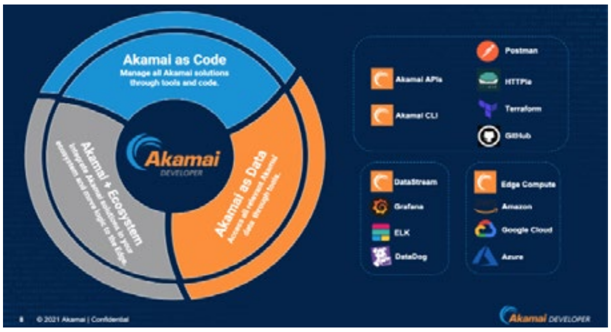
Chun Han

Mike Elissen

Mike Elissen is based in Europe and spends his time helping developers to automate the use of Akamai's solutions. He started in Professional Services and Presales but evolved to his current role two years ago when he saw increased interest in Akamai DevOps and client requests for more developer-friendly APIs and to automate Akamai configuration management.

Chun: In addition to your current role, you are also engaged as an Akamai Developer. What does that mean?

Mike: When I joined as a Developer Advocate, I came up with these three areas to define Akamai Developer.



Akamai as Code
Manage all Akamai solutions through tools and code.

Akamai as Data
Access all relevant Akamai data through tools.

Akamai + Ecosystem
Integrate Akamai solutions to your ecosystem and move logic to the Edge.

Akamai DEVELOPER

Akamai APIs
Akamai CLI
Postman
HTTPie
Terraform
GitHub

DataStream
Grafana
ELK
DataDog

Edge Compute
Amazon
Google Cloud
Azure

8 © 2021 Akamai | Confidential

Akamai DEVELOPER

Firstly, you have **Akamai as Code** – how do you manage all your Akamai configurations as code and reduce the need for the Akamai Control Center. This is where our Create, Read, Update, and Delete APIs come into play.

Next is **Akamai as Data**. Akamai handles a ton of traffic for our customers and offers Reporting/Data APIs that allow customers to integrate the logs we have and events/alerts that we track into any platform.

Finally, we have the concept of **Akamai + Ecosystem** – how Akamai works well with other vendors in any DevOps/DevSecOps ecosystem. This is where tool integrations and connectors come into play, but more importantly is Akamai edge computing – moving logic to the edge to increase performance or security.

Chun: This will make our customers' lives easier. But how does Akamai Developer fit into the customers' DevOps workflow?

Mike: The traditional DevOps workflow can be applied for Akamai solutions, but it is important that you can add Akamai every step of the way during your lifecycle.

When you build, test, and deploy a new application or a new version of your application, how do you ensure that Akamai's delivery, caching, routing, edge functions and security mechanisms are instantly part of this process?

That is where our APIs come into play – they can be integrated in CI/CD tools such as GitHub Actions, GitLab, Jenkins, and so on. Many customers add Akamai in their QA/Test/Staging applications for that extra layer of testing and to reduce risks.

With Akamai as Data, you can completely track everything in the Monitoring phase and have a stronger view of what to work on next in the Planning stage.

Chun: What else are you working on these days?

Mike: My days as a Developer Advocate fly by so quickly. The majority of my time is spent working with our Developer Champions. We started this program two years ago – it is essentially a group of experts within Akamai across different roles and locations working together with Akamai Developer to make it better. We share best practices, templates, and code examples, and work together with our product and engineering teams to make our tools and API better.

We're Customer Zero and test new functionalities first to share in videos and tutorials. It's a great team because everyone is passionate about our customers and Akamai Developer.

Other than that, I create a ton of video tutorials and code examples that we share on our Akamai Developer YouTube channel and Akamai GitHub.

Chun: What coding tools would you recommend?

Mike: A great start is our Akamai Docker, which combines all the Akamai tools that you need. You can install the Docker Desktop or Docker Engine and then run the common docker pull akamai/shell.

This will install a docker image with all the Akamai CLI tools It also installs HTTPie to make direct API calls with Terraform installed as well.

Another tool that I recommend is Postman, a free-to-use API platform to interact directly with Akamai.

I recommend taking a look at https://developer.akamai.com for a full overview.

Chun: What about best practices?

Mike: We've been working on a new documentation platform for Akamai Developer, and you can find all our tutorials there – from how to get started, to how to use the tools, as well as examples, recipes, and best practices. Please take a look at https://techdocs.akamai.com/developer/docs.

And I'm always happy to help. If there are any questions, please reach out to me on Twitter at @securitylevelup or on LinkedIn under Mike Elissen. Or get in touch with your Akamai Account team and they can help you out there.

Chun: Thank you for your time, and I hope to see you in person soon!

▶ View the English language video interview between Chun Han and Mike Elissen.

Chun Han is a Solutions Engineering Manager with Akamai Technologies and is passionate about empowering fast, reliable and secure digital experiences.

If you would like to understand more about Akamai and the solutions we offer, please do

Contact Us