What are Amazon Zelkova and Tiros? AWS looks to reduce S3 configuration errors

Swinhoe, Dan

ABSTRACT (ENGLISH)

According to Skyhigh Networks, 7 percent of all S3 buckets have unrestricted public access, while 35 percent are left unencrypted. First announced in June 2018, Zelkova uses automated reasoning to analyze policies and the future consequences of those policies. A lack of education combined with complexity of deployments and management tools, as well as an ever-growing number of services administrators need to get to grips with, plus the fact cloud environments can easily be spun up outside the view of security teams all mean data leaks continue to be a common issue.

FULL TEXT

To help reduce the chance of AWS S3 configuration errors, Amazon is working on two new tools –Zelkova and Tiros –to provide greater clarity around who has access to your data and resources and what they can do with them. The tools analyze and evaluate access controls and map the openness of your cloud environment.

Amazon Web Services (AWS) continues to have a problem with ensuring its customers are securing their cloud environments. Misconfiguration errors remain common and have left huge amounts of sensitive data exposed. Organizations including Verizon, Booz Allen Hamilton, the WWE Foundation, Alteryx, the U.S. National Credit Federation, the Australian Broadcasting Corporation (ABC), and Accenture have all left information exposed due to configuration errors.

This is despite previous attempts by AWS to help improve the security of its services and reduce the chance of configuration errors. Last year the company launched Macie, a machine learning tool designed to automatically discover and protect sensitive data stored within AWS, as well as a series of new features designed to improve S3 security including default encryption, detailed inventory reports, and permission checks.

In February 2018 –just a few days after news broke that FedEx had exposed over 100,000 documents including passports, driver's licenses, and customer records –AWS made its S3 Bucket Permissions Check service free to all users.

AWS Simple Storage Service (S3) is the company's object storage offering. According to Skyhigh Networks, 7 percent of all S3 buckets have unrestricted public access, while 35 percent are left unencrypted. Recent examples of data left exposed and unprotected includes the login credentials of more than half a million vehicle tracking devices, 200 million U.S. voter records, and sensitive data belonging to U.S. Army Intelligence. As well as stealing information, hackers have locked down data with ransomware and been found using the computing resources to mine cryptocurrency.

What Amazon Zelkova and Tiros do

Zelkova and Tiros were created by AWS's Automated Reasoning Group (ARG), which develops verification tools and techniques for Amazon's products. Automated reasoning is a method of formal verification that takes semantic-based reasoning and applies mathematical formulas to, in short, answer specific questions and verify policies are working as expected. The ARG sits within the AWS security team, and has been developing tools internally for more than two years.

First announced in June 2018, Zelkova uses automated reasoning to analyze policies and the future consequences

of those policies. Compatible with the company's Identity and Access Management (IAM), S3 and other resource policies, it enables organizations to create benchmarks and inform you of the consequences of your current policy settings. For example, when used against S3 policies it can inform you if unauthorized users are able to read or write to your bucket.

Tiros maps the connections among your networks. For example, it can answer questions around whether any of your EC2 instances are reachable from the internet.

Zelkova and Tiros began as internal tools. Zelkova is used internally as part of the S3 dashboard and within AWS Macie. Investment management firm Bridgewater Associates was given early access to test them.

"Bridgewater uses Zelkova to verify and provide assurances that our policies do not allow data exfiltration, misconfigurations, and many other malicious and accidental undesirable behaviors," Dan Peebles, lead cloud security architect at Bridgewater Associates said in the Zelkova announcement. "Zelkova allows our security experts to encode their understanding once and then mechanically apply it to any relevant policies, avoiding error-prone and slow human reviews, while at the same time providing us high confidence in the correctness and security of our IAM policies."

Neither tool is currently available for public release. Bridgewater says they are in a "raw state," not particularly user friendly. Amazon declined to release any information around wider availability or pricing.

Amazon's cloud configuration challenges

While cloud vendors such as Amazon and Microsoft's Azure offer some level of security around their services and provide recommended best practices, they operate under a shared security model in which much of the onus is still on the customer, which is where problems often occur. "The security challenges being reported around AWS S3 buckets have little to do with the platform itself," says Steve Smith, senior site reliability engineer at UK-based MSP Claranet, "but everything to do with the people using it, who are the biggest weakness here.

"AWS sets a lot of sensible defaults designed to support configuration; S3 buckets are now private by default, but unfortunately, it's very easy to get things wrong if you don't know how to use the platform," Smith adds.

A lack of education combined with complexity of deployments and management tools, as well as an ever-growing number of services administrators need to get to grips with, plus the fact cloud environments can easily be spun up outside the view of security teams all mean data leaks continue to be a common issue.

"As a consumer you have to do your part by understanding the shared responsibility model and applying best practices to protect your data," says George Gerchow, CSO at log management and analytics provider (and AWS customer) Sumo Logic. "AWS does not do much to provide this education, so it is easy for consumers to believe that everything is done for them."

With these new tools, AWS is looking to reduce the chances of human error and reduce the likelihood of data leakage. But will they help? "Our security objective here is to stop data exfiltration from AWS," Bridgewater Associates security architect Greg Frascadore said in a presentation around Zelkova and Toris during the AWS New York Summit 2018. "What we're trying to get is a formal analysis and a methodical way that we have gone about verifying that the security controls we put into place are working the way we think they're working."

Frascadore said use cases for these tools include verifying individual security controls, creating benchmarks around security controls, locating relevant controls across a fleet of accounts, automating verification, and verifying during the design phase. "A very important thing about these tools is that you can verify things during the design stage. One of the things that we would really like to be able to do is security verification before we make a change to the actual AWS infrastructure, so before we put a vulnerability into the account," he said.

Others warn that these new tools have both benefits and potential downsides. Sumo Logic's Gerchow says that while they are a good start, they are expensive and need to be properly configured, which could add more complexity, and won't help in multi-cloud or hybrid deployments.

"There's a ton of potential upside for Zelkova and Tiros, but those teams must be able to operationalize the data, otherwise they're just running a tool," says Matt Wilson, chief information security advisor at BTB Security. "They still require someone at the organization to execute them, analyze their output, and act upon the information provided.

Advanced algorithms and a slick interface are great, but they’re not enough alone.”
Credit: Dan Swinhoe

DETAILS

Subject:	Design; Automation; Data integrity
Business indexing term:	Subject: Automation; Corporation: Amazon.com Inc
Location:	United States--US; New York; United Kingdom--UK
Company / organization:	Name: Australian Broadcasting Corp; NAICS: 516120; Name: Verizon Communications Inc; NAICS: 513210, 517111, 517112; Name: Department of the Army; NAICS: 928110; Name: FedEx Corp; NAICS: 484110, 492110, 551114; Name: Claranet; NAICS: 517112; Name: Microsoft Corp; NAICS: 334610, 513210; Name: Amazon Web Services Inc; NAICS: 518210, 541513; Name: Amazon.com Inc; NAICS: 334310, 454110, 518210
Publication title:	CSO (Online); Framingham
Publication year:	2018
Publication date:	Aug 21, 2018
Publisher:	Foundry
Place of publication:	Framingham
Country of publication:	United States, Framingham
Publication subject:	COMPUTERS--COMPUTER SECURITY, Criminology And Law Enforcement--Security
Source type:	Trade Journal
Language of publication:	English
Document type:	News
ProQuest document ID:	2090921499
Document URL:	https://login.leo.lib.unomaha.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Ftrade-journals%2Fwhat-are-amazon-zelkova-tiros-aws-looks-reduce-s3%2Fdocview%2F2090921499%2Fse-2%3Faccountid%3D14692
Copyright:	Copyright CXO Media, Inc. Aug 21, 2018
Last updated:	2024-02-05

Database: ABI/INFORM Collection,SciTech Premium Collection

LINKS

Linking Service