Institution: University College London		
Unit of Assessment: 11 - Computer Science and Informatics		
Title of case study: Automated Reasoning for Amazon Cloud Security		
Period when the underpinning research was undertaken: 2012 – 2020		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s): Byron Cook	**Role(s) (e.g. job title):** Professor of Computer Science	**Period(s) employed by submitting HEI:** 2012 - Present
Period when the claimed impact occurred: 2015 – 2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact (indicative maximum 100 words)

The correctness of code, networks, policies, and protocols are essential for the durability, privacy, and security of public cloud systems such as include Amazon's Amazon Web Services (AWS), Microsoft's Azure, or Google's GCP. Professor Byron Cook's UCL-based automated reasoning research directly changed business practices for Amazon's AWS, the largest public Cloud offering. This research improved customer experience, security and trust for AWS' 1,000,000 business customers in 190 countries, including the UK's Ministry of Justice, the British Broadcast Corporation (BBC), and Vodafone Group Plc. Cook's work has helped an exponentially growing number of AWS customers safely use the Cloud, with a shrinking number of security bulletins reported.

2. Underpinning research (indicative maximum 500 words)

Professor Byron Cook is a world-renowned expert in the area of automated reasoning, in which algorithms are used to find proofs expressed in mathematical logic. Often automated reasoning tools are then applied to prove properties of computer systems themselves—for example, Cook's work on temporal reasoning (**R1, R2**) for computer programs. This research allows Amazon to make precise claims about how computer programs will use resources such as API calls, time, memory, storage.
Amazon approached Cook in 2014 to apply his work to the problem of security assurance for Amazon Web Services (AWS), the world's largest cloud service. As the founder and visionary behind Amazon's **AWS Automated Reasoning Group,** Cook brought his UCL-based research to the development of bespoke AWS customer-facing security controls, including **IAM Access Analyzer**, **S3 Block Public Access**, **VPC Reachability Analyzer**, as well as mathematical proofs about the underlying foundations of the AWS virtualization and encryption systems. This work included UCL PhD students Kareem Khazem and Pavle Subotic.

Reasoning about programs
At UCL, Cook and team created the first known fully automatic method for proving temporal properties expressed in the logic CTL* of computer programs (**R1, R2**). Previously, no automated systems allowed for the verification of such expressive properties (**R1**). For the first time, this enabled automatic verification properties for programmes that mix branching-time and linear-time temporal operators (**R1, R2**).

These ideas were used within Amazon in two key applications: the formal verification of virtualisation infrastructure, and encryption infrastructure. These proofs offer new and previously unseen levels of security assurance for cloud users. For example, when proving properties of the AWS virtualization infrastructure, Cook and UCL-based PhD student Khazem proved key properties of the boot code running in AWS data centres (**R3**). In the

space of encryption, Cook and team proved correctness properties of **s2n**, Amazon's open-source implementation of the Transport Security Layer (TLS) protocol (**R4**).

Reasoning about resources

Building on UCL-based research on resource reasoning (e.g. https://www.resourcereasoning.com/), Byron and UCL PhD student Subotic also developed two automated resource reasoning tools: **Tiros**, which formalises the semantics of AWS virtualised networking; and **Zelkova**, which formalizes the semantics of AWS resource policies (**R5, R6**). These two tools then use automated theorem provers (such as Subotic's Souffle tool) to verify security-related properties. Zelkova is now the basis of Amazon's **IAM Access Analyzer** feature (see https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html) and **S3 Block Public Access** feature (see https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html). Similarly, Tiros is now the basis of Amazon's **VPC Reachablity Analyzer** feature (see https://docs.aws.amazon.com/vpc/latest/reachability/what-is-reachability-analyzer.html) as well as features in **Amazon Inspector**. These AWS features have helped customers avert security breaches.

3. References to the research (indicative maximum of six references)

R1. **Byron Cook**, Heidy Khlaaf, Nir Piterman. 2017. "Verifying increasingly expressive temporal logics for infinite-state systems". *Journal of the ACM*, 15. DOI: https://doi.org/10.1145/3060257

R2. **Cook B.,** Khlaaf H., Piterman N. 2015. "On Automation of CTL* Verification for Infinite-State Systems". In: Kroening D., Păsăreanu C. (eds) *Computer Aided Verification 2015*. Lecture Notes in Computer Science, vol 9206. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-21690-4_2

R3. **Cook B**., Khazem K., Kroening D., et al. 2018. "Model Checking Boot Code from AWS Data Centers". In: Chockler H., Weissenbacher G. (eds) *Computer Aided Verification. International Conference on Computer Aided Verification 2018*. Lecture Notes in Computer Science, vol 10982. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-96142-2_28

R4. Andrey Chudnov, Nathan Collins, **Byron Cook**, et al. 2018. "Continuous formal verification of Amazon s2n". In: Chockler H., Weissenbacher G. (eds). *Computer Aided Verification 2018*. Lecture Notes in Computer Science, vol 10982. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-96142-2_26

R5. John Backes, Pauline Bolignano, **Byron Cook**, et al. 2018. "Semantic-based Automated Reasoning for AWS Access Policies using SMT". *Formal Methods in Computer-Aided Design*. Austin, Texas. https://www.cs.utexas.edu/users/hunt/FMCAD/FMCAD18/papers/paper3.pdf

R6. J. Backes, S. Bayless, **B. Cook**, et al. 2019. "Reachability Analysis for AWS-based Networks". *International Conference on Computer Aided Verification 2019*. Lecture Notes in Computer Science, vol 11562. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-25543-5_14

4. Details of the impact (indicative maximum 750 words)

Cloud computing is fast becoming the standard computational and storage platform for businesses and government organisations around the world. Amazon's AWS is the industry's biggest cloud provider. Amazon approached Professor Byron Cook in 2014 to develop correctness-proving tools for AWS security through automated reasoning (**S1**). In response Byron started the AWS Automated Reasoning Group. Cook's research collaboration with Amazon (**R1 – R6**) transformed business practices for AWS (**S2 – S7**), and improved customer experience, security and trust for AWS's over 1,000,000 business customers in 190 countries (**S2, S7**).

New cloud security tools transform Amazon's business practice

Amazon used Cook's automated reasoning research (**R1 – R4**) to fortify critical security applications. Cook's CTL* research (**R1, R2**) led him to develop two proofs for AWS foundations: OS/virtualization (specifically, the memory safety of boot loaders used in data centres **in R3**) and the correctness of Amazon's cryptography (in particular, the implementation of the TLS protocol, **s2n in R4**). Amazon applies Cook's techniques to continuously prove correctness during code development. Thus, in the example of s2n, proof is used to continuously protect the encryption used by S3's 1,100,000 requests per second (**S2**).

Senior stakeholders at Amazon attest to the importance of Cook's techniques in how AWS functions. For instance, AWS Security VP confirmed: "Every time a developer commits code, that proof gets run again." He added that if someone "breaks that proof, we don't find out about it years later… [W]e find out about it during the build" (**S3**). The AWS Chief Technical Officer stated: "AWS has a (not so) secret weapon that helps protect us and our customers—automated reasoning." Furthermore, "[w]e apply provable security to our infrastructure [to] achieve the highest levels of security while our services rapidly grow" (**S3**).

Cook's formal verification infrastructure (**R4**) further ensures that s2n automatically checks properties. This typically eliminates the need for developers to understand or modify the proof following code modifications. An s2n architect and VP attests: "This verification…is built into our public GitHub builds… [and tests] every change…confirming that the tools reject [errors]. [N]o changes to the s2n code were necessary to support the proof" (**S3**).

Cook's new developments transformed Amazon's cloud security offerings, creating a higher security standard for AWS and their 1,000,000 plus daily business customers, including the BBC, the Ministry of Justice, the Met Office, Europol, National Rail and Vodafone Goup Plc. (**S3**). The AWS CTO stated: "With previous tools, auditors could not evaluate all of the code in all configurations [or] evaluate where keys were used. With automated reasoning, millions of customers can use a proof to examine the entire system for a certain value. This creates a higher standard for security beyond today's advanced control measures, such as automated controls, preventive controls, or detective controls" (**S3**). AWS Identity VP stated: "We are excited to have these assets and talent in AWS, and to make it available to all builders and AWS customers" (**S3**).

Enhanced security tools improve AWS customer experience and trust

Customers are responsible for security within their cloud-based applications (**S3**). In some instances, customers have found it hard to get these details right. For example, in 2017, 7% of S3 customers allowed unrestricted public access to buckets; among the consequences were the leaking of over 198,000,000 American voters' names and addresses (**S4**). Professor Cook's work on Tiros and Zelkova (**R5, R6**) formed the basis of new customer-facing features that AWS launched to help customers spot mistakes before they go live, so customers can confidently deploy sensitive workloads (**S4**). Features include **IAM Access Analyzer, S3 Block Public Access, VPC Reachability Analyzer, Amazon Inspector, Amazon Macie,** and **AWS Managed Config Rules.** Customers who have specifically mentioned relying on these tools include global investment firm Goldman Sachs and their 3,000,000 customers, and Bridgewater Associates, the world's largest hedge fund (**S7**). Enterprise-level customers have stated that Cook's enhanced security protection features benefitted them by supporting overall compliance and risk policies, anti-malware, and threat detection:

> "We're closer to the developer, have a faster feedback loop, and they can still be agile in their infrastructure development while maintaining the best security standards." – Goldman Sachs Developer (**S7**)

> "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." – Bridgewater Senior Software Developer (**S7**)

> "Coinbase is one of the most widely used bitcoin wallet and exchange companies. Amazon Inspector is helping companies like ours embrace the immutable future and pull our industry out of the security dark ages." – Coinbase Director (**S7**)
>
> "We [are placing] 80% of our IT resources in the Cloud. Amazon Inspector is a great example of how AWS is accelerating investment in security-focused services… and a highly scalable, API driven security service that we can place throughout our cloud operations." – University of Notre Dame IT Senior Director (**S7**)

Without needing security development skills, millions of AWS customers use automated reasoning thousands of times per minute to defend against security leaks through tools such as S3 Block Public Access. The AWS 'Chief Evangelist' said, "[S3BPA] is designed to be easy to use, and can be accessed from the S3 Console, the CLI, the S3 APIs, and from within CloudFormation templates" (**S3**). The AWS CEO agreed, stating: "S3 is the only object store that allows you to analyse all the access permissions on all your objects and buckets with… IAM Access Analyzer" (**S5**).

5. Sources to corroborate the impact (indicative maximum of 10 references)

S1. Impact on Amazon's business model, product offerings through AWS:
"Provable Security: Security Assurance, Backed by Mathematical Proof". Byron Cook talks about the impact of the AWS provable security initiative (Amazon endorsed).
https://aws.amazon.com/security/provable-security/
S2. AWS business data: usage, infrastructure, customer size, and market share.
Amazon whitepaper attesting AWS global infrastructure and customer size:
https://docs.aws.amazon.com/whitepapers/latest/aws-overview/global-infrastructure.html.
Amazon article confirming increase in request rates: https://aws.amazon.com/about-aws/whats-new/2018/07/amazon-s3-announces-increased-request-rate-performance/
CNBC article confirming AWS's growth, revenues, and market share:
https://www.cnbc.com/2020/04/30/aws-earnings-q1-2020.html
Amazon article: "Amazon S3 – Two Trillion Objects, 1.1 Million Requests / Second":
https://aws.amazon.com/blogs/aws/amazon-s3-two-trillion-objects-11-million-requests-second/
S3. Colligated testimonials from Amazon senior managers, engineers and architects.
Distinguished Engineer and VP of AWS Security:
https://www.youtube.com/watch?v=x6wsTFnU3eY
S2n architect and VP: https://aws.amazon.com/blogs/security/automated-reasoning-and-amazon-s2n/
AWS Chief Technology Officer: https://www.allthingsdistributed.com/2019/06/proving-security-at-scale-with-automated-reasoning.html and
https://www.allthingsdistributed.com/2019/05/proving-security-at-scale-with-automated-reasoning.html
AWS VP: https://www.youtube.com/watch?v=bqAGpeFUP9g&feature=youtu.be&t=2210
'Chief Evangelist' for AWS: https://aws.amazon.com/blogs/aws/amazon-s3-block-public-access-another-layer-of-protection-for-your-accounts-and-buckets/
S4. Colligated articles about: TIROS and ZEKOVA correcting AWS S3 leaks; prior AWS leaks.
"AWS has new tool for those leaky S3 buckets". The Register, 3 December 2019.
https://www.theregister.co.uk/2019/12/03/aws_s3_buckets/
"Amazon Tests Out Two Tools to Help Keep Its Cloud Secure". Wired. 18 July 2018.
Describes Cook's Automated Reasoning Group and TIROS and ZEKOVA implementation.
https://www.wired.com/story/aws-cloud-security-tools-leaks/
"Amazon is quietly doubling down on cryptographic security". TechCrunch, 30 August 2018.
Describes Cook's Automated Reasoning Group and TIROS and ZEKOVA implementation.
https://techcrunch.com/2018/08/30/amazon-aws-cryptography-security/

"What are Amazon Zelkova and Tiros? S3 looks to reduce S3 configuration errors." CSO, 21 August 2018. https://www.csoonline.com/article/3298166/what-are-amazon-zelkova-and-tiros-aws-looks-to-reduce-s3-configuration-errors.html
Prior S3 leaks: https://www.wired.com/story/aws-cloud-security-tools-leaks/
S5. Articles and video about Cook's AWS IAM Access Analyzer and Amazon Inspector
AWS CEO describes the benefits of Access Analyzer:
https://www.youtube.com/watch?v=7-31KgImGgU&feature=youtu.be&t=3237
Amazon article: "Introducing AWS Identity and Access Management (IAM) Access Analyzer"
https://aws.amazon.com/about-aws/whats-new/2019/12/introducing-aws-identity-and-access-management-access-analyzer/
List of Amazon Inspector partners: https://aws.amazon.com/inspector/partners/
S6. Videos of AWS senior managers endorsing Cook's Resource Reasoning Tools:
VP of compliance at AWS on resource reasoning tools:
https://www.youtube.com/watch?v=BbXK_-b3DTk
VP and Distinguished Engineer of AWS security on resource reasoning tools:
https://www.youtube.com/watch?v=6_1uozMTvIM
S7. Customer testimonials and videos endorsing Cook's Resource Reasoning Tools:
Bridgewater Associates talking about the use of resource reasoning tools:
https://www.youtube.com/watch?v=gJhV35-QBE8
Millennium Capitol talking about the use of resource reasoning tools:
https://www.youtube.com/watch?v=70zvdxE1DPk
Goldman Sachs talking about the use of resource reasoning tools:
https://www.youtube.com/watch?v=Rm4mvVeOYYk
Goldman Sachs Annual Report 2018 (customer numbers):
https://www.goldmansachs.com/investor-relations/financials/current/annual-reports/2018-annual-report/annual-report-2018.pdf