c on:

Emerging Technologies

Opportunities and Challenges

In association with

WAVESTONE

Emerging technologies continue to redefine the cybersecurity landscape at pace. Join us as we explore the transformative opportunities and challenges posed by advancements in privacy-enhancing technologies and private computation.

As developers increasingly use AI systems to reduce time to deployment, we consider how AI applications and agents can fail in practice, and the strategies that can be used to reduce those risks.

Many organisations providing leading-edge products and services grow through venture capital investment. Understanding how VCs operate strategically - particularly in supporting companies that are responding to, and making use of, emerging technologies - is important for both those companies and their customers.

We'll hear valuable insights from technology leaders on how we can understand and manage the risks presented by these emerging technologies and business practices.

All SASIG events operate under the Chatham House Rule, and there is no charge to attend. Our hosts will kindly provide lunch and refreshments.

Tuesday 13 October 2026

9.30am to 4pm

London

Chair

Professor Andrew Clark Content Advisor, The SASIG

9.30am **Registration, coffee, and networking**

10.00am **Welcome and introductions**
Professor Andrew Clark Content Advisor, The SASIG

10.15am **Keynote presentation: 2030 and Beyond - Navigating Threats, Trust and Transformation**
Florian Pouchet Head of Cybersecurity & Operational Resilience UK, Wavestone
In a world full of uncertainties, we certainly see unavoidable shifts: new threats and attack paths, geopolitical disruption and AI transformation on overdrive; but what are the emerging topics, and what does this mean for organisations and security teams? Florian will open the day by looking forward to 2030 and exploring how these transformations play a key role in reshaping resilience, trust and competitive advantage in the decade ahead.

10.45am **Cryptographic PETs**
Professor Nigel Smart Professor, KU Leuven
Securing data via cryptographic means during transit and storage is now standard. Less well-known, or deployed, is the ability to secure data during processing using cryptographic means. The need for private computation is becoming more important due to both regulatory “push” (such as GDPR and AML regulations) and application “pull” (including AI and users' privacy concerns). Private computation can also enable new applications, which were unviable before. In this talk Nigel will review the properties, pros, and cons of four technologies (TEEs, FHE, MPC and ZKPs) which enable private computation.

11.30am **Tea, coffee, and networking break**

12.00pm **AI, AI everywhere - what are your people really doing with AI tools?**
Tim Ward CEO & Founder, Redflags
AI tools are rocketing in popularity, and as businesses grapple with striking a balance between AI-enablement and information security, there has never been a greater need to understand exactly how your people are using AI tools. Redflags' real time data gives customers insights into how they are using these tools, where risk hotspots are forming and nudging them to make the secure choice; helping businesses to shape their AI governance and human risk strategies.

We will share the trends we are seeing, customer use-cases and explore where the future of "human in the loop" AI governance.

- Deep insight into how humans are using AI tools
- Guidance on where risk hotspots are forming from colleagues' use of AI tools
- Ideas for AI governance policies
- Ideas for Human Risk AI interventions
- Key trend analysis for AI

12.30pm **Breaking AI Agents: Real-World Vulnerabilities**

Nils Amiet Senior Security Researcher, Kudelski Security

AI tools deliver major productivity gains, making them irresistible to developers, who often accept broad permissions as a trade-off. Combined with pressure to ship quickly, this creates a fast-growing attack surface with minimal security. In our assessment of 12+ AI developer tools, we found serious vulnerabilities in most, some with high impact. This talk explains how AI applications and agents fail in practice, highlights key attack patterns, and presents pragmatic strategies to reduce risk while maintaining development speed.

1pm **Networking lunch**

1.45pm **Keeping Pace with AI-accelerated Attacks**

Mark Davis Senior Director, Pentera

AI is accelerating every stage of the attack lifecycle, from phishing and impersonation to reconnaissance, exploitation, and lateral movement. As attackers use AI to move faster and adapt in real time, organisations need new ways to validate whether their defences can keep up. In this session, Mark will explore how organisations can use AI-enhanced adversarial testing to emulate modern attack techniques, identify real exposure across the attack surface, and prioritise remediation to reduce exposure before attackers have a chance to exploit it.

2.15pm **What do cybersecurity investors want?**

Alex Van Someren Strategic Advisory Group Member, Paladin Capital

A venture capital investor explains VC strategy, how investment firms think and work, and what to expect them to do, and not do, for start-ups if organisations take their money. What does that mean for customers who've purchased a VC-sponsored solution?

3pm **Panel discussion: Horizon scanning. Where should organisations be looking to use emerging tech to reduce their risk and increase opportunity?**

Facilitated by Florian Pouchet Head of Cybersecurity & Operational Resilience UK, Wavestone

Alex Van Someren Strategic Advisory Group Member, Paladin Capital

David Porter Senior Advisor, Emerging Threats, Bank of England

Professor Nigel Smart Professor, KU Leuven

Nick Palmer Technical Director, International, Censys

Differentiating between what is important and what is urgent when evaluating new technologies has always been challenging. This panel session will present the members' ideas on which current emerging technologies are both important and urgent, their potential impact and how they may change our working practices.

3.45pm **Closing words**

4pm **End of meeting**

About

The Security Awareness Special Interest Group (SASIG)

SASIG is a subscription-free networking forum, membership now represents thousands of organisations of all sizes from across the world and from all sectors, public and private. Its 11,200+ membership is drawn from CIOs, CISOs and their staff with responsibility for cybersecurity within their organisations. Professionals from other disciplines (risk, HR, legal, supply, etc.) and representatives from government, law enforcement and academia are also being increasingly welcomed at events. The Chatham House Rule is strictly enforced and universally respected at all meetings, and vendors and the Press are routinely excluded. Thus, the level of debate is extraordinarily revealing and rewarding.

SASIG has a members' website at www.thesasig.com. Please register here for membership.

With thanks to our Supporters and Contributors…

01234 707 035
info@thesasig.com
www.thesasig.com