Better Software on arm

Memory Tagging Extension

What is Memory Tagging Extension?

A security feature built into the Armv9 architecture to detect and prevent *memory safety* vulnerabilities across the mobile ecosystem before and after deployment.

Why is Memory Safety a Challenge for the Future of Computing?

It has been a major source of security vulnerabilities for decades, with Google's Chromium Project team stating that 70 percent of all serious security bugs are memory safety issues.

Why is Memory Tagging Extension Needed?

Smarter devices are coming to market with more advanced compute capabilities, more complex software and systems, and larger attack surfaces, leading to more bugs.

How Does Memory Tagging Extension Work?

It is implemented as a two-phase system, known as the 'lock' and the 'key'. If the key matches, then the lock memory access is permitted, which helps to detect memory safety violations.

What are the Benefits of Memory Tagging Extension?

Alongside providing a more secure and safer user experience, it allows developers to find memory-related bugs quickly, speeding up the application debugging and development process.

What are Arm's Partners Doing?

Google has already adopted Memory Tagging Extension in Android, stating that the technology "*makes it very hard (if not impossible) to exploit memory bugs.*" Also, device manufacturer Honor is enabling the feature on its MagicOS 6.x and MagicOS 7 devices on its developer portal.

5 Key Benefits of Memory Tagging Extension

- Lower Costs
- Reduced Time-to-market
- More Secure, Safer User Experiences
- Flexible Configurations
- Highly Scalable