

## FOREWORD

David Durham  
Principal Engineer  
Security & Cryptography Research  
Intel Labs

*“The Internet now faces threats that are fundamentally unique to the virtual world.”*

*“Like a series of airlocks, partitioning and compartmentalizing software components reduces exposure to a single failure, helping to fundamentally contain a point of compromise.”*

The Internet remains full of promise but also peril. As the world becomes increasingly interconnected, barriers are breaking down: information can travel virtually anywhere in the blink of an eye and be accessible to almost anyone. However, as commerce, content, and personal information move en masse on-line, the motives for malice follow. The Internet now faces threats that are fundamentally unique to the virtual world. While the physical world of brick and mortar deals effectively with malicious individuals who have to abide by the constraints of space and time, in the virtual world, botnets are forming vast overlay networks of zombie machines ready to do the bidding of a single master. Blended threats combine the best-known methods for individual attacks into entirely new composite forms, constantly changing to stay a step ahead of security solutions. Meanwhile, the inherent need for information replication, search, and dissemination creates ample opportunities for eavesdropping and identity theft. The vastness of the Internet requires an equally vast solution, one that makes the old archetypes of the past seem quaint in comparison. This issue of the Intel Technology Journal describes some of the steps Intel is taking to help stem the tide of attack.

The first task before us is redefining the network endpoint itself. No longer just a machine at the other end of the wire, the network endpoint becomes a composition of independently measured and protected software services, establishing a basis of good citizens in the online community. By leaving nowhere for malware to hide, security solutions can detect the stealthy rootkits and viruses that would otherwise infect and then lie dormant, waiting for commands to distribute spam, spread malware, steal information, or launch denial-of-service attacks. New models for attestation can directly validate individual programs thereby enabling remote entities to trust the specific software services with whom they are communicating. Finally, like a series of airlocks, partitioning and compartmentalizing software components reduces exposure to a single failure, helping to fundamentally contain a point of compromise.

Intel is also aggressively improving the power and performance of computing in general and cryptographic operations and algorithms in particular. Securing every network connection is becoming a real possibility. Data can be cost-effectively protected in transit and while at rest. New cryptographic instructions, simultaneous multithreading, and optimized cryptographic algorithms help to make the choice between no security and security obvious.

Another challenge is scaling trust within the vastness of the Internet. Intel is developing new algorithms that provide anonymous attestation, preserving an individual's privacy while still establishing trust at a distance. Revocable group identities can vouch for systems and software anonymously, scaling trust by removing the need for establishing individual identities for everything in the Internet. Also, even as attacks become increasingly distributed, so can the solutions. Intel's research demonstrates that enlisting a broad array of endpoints to detect, report, and analyze anomalies in traffic patterns may be the answer to botnets in the Internet. Finally, community-based security solutions improve awareness and establish reputations in ad hoc infrastructures, absent of central administration.

While the vision of a completely safe Internet will likely remain elusive, much progress is being made. Steps are being taken in hardware to break the cycle and end the arms race between malware and security solutions, finally giving the good guys the upper hand. Endpoints are becoming more robust, enabling better software practices. Information can be kept private, even when distributed broadly, without the performance penalties of the past. Finally, scalable security solutions are being designed to work across the vast scale of the Internet, providing trust of and for the masses. It is my real pleasure to work with Intel Labs with a great team of researchers creating innovative solutions to the Internet's security challenges, now on display in this issue of the Intel Technology Journal.

*“Securing every network connection is becoming a real possibility.”*

*“Steps are being taken in hardware to break the cycle and end the arms race between malware and security solutions, finally giving the good guys the upper hand.”*