

Active Security

Challenge:

Computer and network security has taken on many characteristics of an “arms race”, and is littered with approaches (packet filtering, signature-based IDS, etc.) that have been overcome by shifts in attacker strategy (e.g., web-based attacks and polymorphic payloads).

Solution:

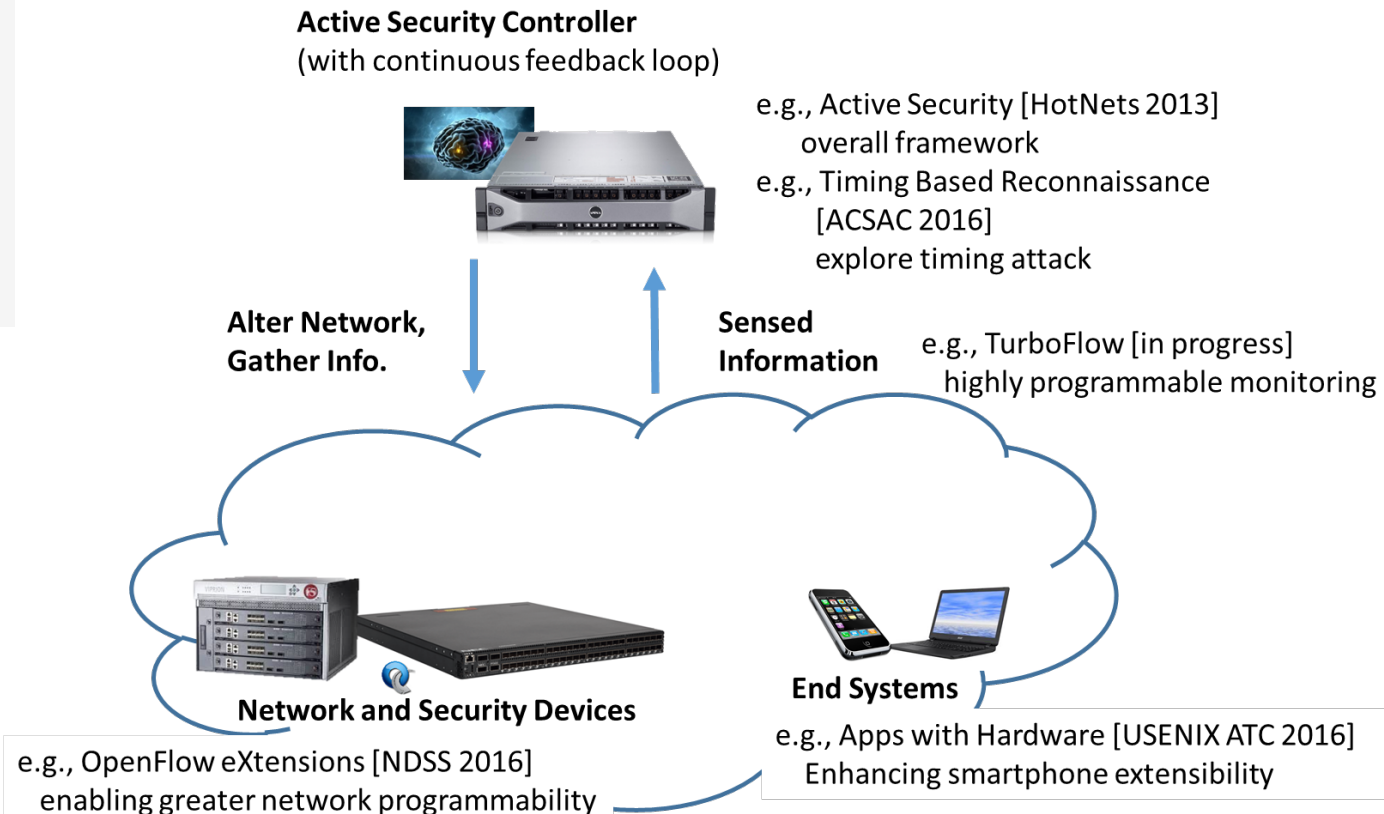
Active security uses a continuous process of sensing and adaptation to discover and defend against threats, including those that have not been seen before.

Broader Impact:

As our dependence on networks grows, intelligent security controls (as in Active Security) becomes essential. Undergraduates are actively involved at all three institutions, including one as a main author of a best paper award.

Scientific Impact:

Active security is an architectural approach that accelerates the defender’s ability to adapt defenses through rapid and automated adaptation. Key research includes leveraging and enhancing programmability of network components.



Pls:

Eric Keller (Colorado),
Jonathan Smith (UPenn),
Adam Aviv (USNA)