CAREER: Tools for building online services that hide metadata

Challenges:

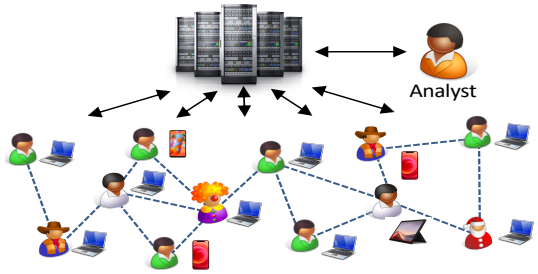
- Enable access and transmission of content without leaking metadata.
- Derive aggregate statistics from federated graph data without revealing the graph.

Solutions:

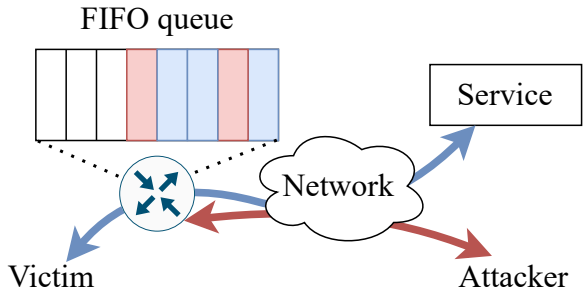
- New PIR protocol with sublinear computation and communication that supports database changes
- New queuing discipline that is resilient to timing side channels.
- New private aggregation protocol for federated graphs.

Sebastian Angel
University of Pennsylvania

Mycelium: Support queries like "if a device is infected with malware, on average, how many of their contacts are infected within a week?" without revealing the social graph.



IFS: Prevent packets queuing at switches from leaking information about other traffic via timing side channels



Scientific Impact:

- New tools to enable interaction with user data without revealing sensitive metadata such as user relationships or access patterns
- New definitions for characterizing the leakage of information and concrete attacks to demonstrate the potential harm

Broader Impact and Broader Participation:

- Collaboration with large financial company to deploy private federated aggregation at scale.
- Current engagement with vendors to incorporate additional privacy features in programmable switches.