Towards Stronger Enterprise Security

For Breach-Resilient Security Analytics & Credential Protection

Nikos Triandopoulos, Department of Computer Science

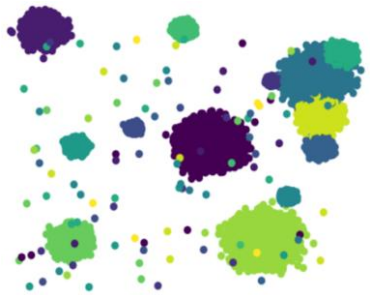
Funded by NSF
SaTC Award #1718782

Private Collaborative Learning

Collaboration w/ NEU, HKUST, Amazon

Forming federated or community-based intelligence tanks (e.g., threat sharing)

Novel cryptographic protocols for **scalable private cluster analysis**



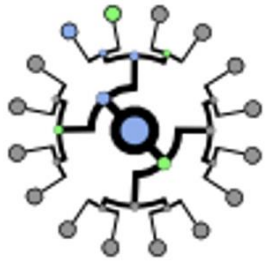
Enterprises can jointly and privately cluster their threat indicators to learn attack patterns

Secure Certificate Validation

Collaboration w/ MIT, UMD, HKUST

Building trust among unknown untrusted entities (e.g., web certs)

Novel distributed protocols for **accurate detection of fake certs**



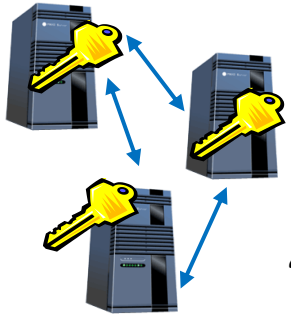
Web-browsers can reliably check that any server's cert is valid via Google's Certificate Transparency service

Secure & Private Key Management

Collab. w/ own security group @ Stevens

Implementing complex security policies for user authorization (e.g., passwords, credentials)

Novel key-rotation protocols for **breach-resilient access control**



Administrators can easily enforce flexible key-management policies that feature a "moving target" quality