

Full name : Mehal wiam

Group : g2

Writing a Summary : Security and Cryptography

The security and privacy concerns of the current computer and network infrastructure are hindering the potential applications of the Internet such as e-commerce, medical records, and Internet voting. To address these concerns, a combination of technical, social, and legal approaches is required. The topics under active investigation include mathematical modeling of security properties, implementation and application of cryptographic protocols, secure and privacy-preserving distributed algorithms, trust management, verification of security properties, and proof-carrying code. The FLINT group at Yale is developing a new set of formal techniques and tools to ensure the security of complex security-sensitive systems, guaranteeing users that the systems are trustworthy. This group is developing a new methodology for formally specifying, proving, and propagating information-flow security policies using a single unifying mechanism called the "observation function." This methodology specifies a policy in terms of an expressive generalization of classical non-interference and propagates it across layers of abstraction using a special kind of simulation that preserves security. They are building an actual end-to-end security proof of a non-trivial concurrent operating system to demonstrate the effectiveness of this new methodology. In summary, adequately addressing security and privacy concerns requires a combination of technical, social, and legal approaches, and the FLINT group is actively working to develop new methodologies and techniques to ensure the security of complex security-sensitive systems.

I hope you find my resume to be informative and well-presented. Thank you for taking the time to review it ❤️