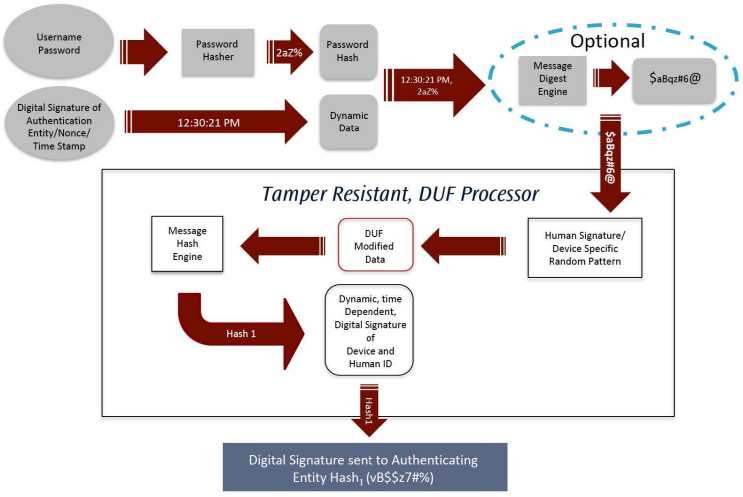
DIGITAL UNCLONABLE FUNCTION

Patent Pending
Technology Readiness Level: 4
Key elements have been demonstrated in laboratory and relevant environments

Almost every day we hear about data breaches, compromise of credit card and social security numbers, identity theft, or exposure of user login credentials. The Internet was created as an open architecture, where security and identities were an afterthought. While the username/password model was the original—and still the most popular—form of user authentication, the cybersecurity industry has been adopting an extra layer of security by utilizing two-factor authentication (e.g., sending an SMS code to a user's phone, using an RSA token or smart card with a pin).



Sandia's Digital Unclonable Function authentication protocol

While many of today's commonly used two-factor authentication schemes are more secure than passwords, the industry has not eliminated human factor vulnerabilities, such as phishing and whaling attacks mainly because they all still depend upon static ID measures (i.e, passwords, pins). Users may become annoyed with multiple authentication requests which may prompt them to bypass security measures by writing down passwords on a notepad or centralizing their passwords with a cloud-based password manager.

The Digitally Unclonable Function (DUF) technology developed at Sandia National Labs takes two-factor user authentication to the next level by making identities of electronic devices (e.g, smartcards, trusted platform modules, IoTs) unclonable and unspoofable. DUF technology makes it nearly impossible for a remote hacker to steal the user's credentials since DUF verification requires processing the identity/transaction data through the unclonable physical device to produce a unique digital signature. It also reduces the "hassle" factors involved in the traditional username/password model. With the DUF protocol, a 4-digit PIN is just as effective as securing an identity with a complex 16 character password. Also, since DUF protocol does not store or transmit any sensitive information (i.e., PIN/passwords), it is impervious to "replay" or crypto-analysis attacks. With the assurance that DUF protocol provides, end-users can use the same PIN/Password without having to worry about changing it every quarter or every year. DUF technology not only improves the security with the unclonable device ID but it also significantly enhances the end-user experience by drastically simplifying the password/PIN complexity requirements. Sandia's DUF technology has broad applicability in financial transactions, credit/debit cards, IoT devices, the automotive industry, and enterprise IT as well as supply chain risk management.

TECHNICAL BENEFITS

- Unclonable/unspoofable identity security protocol
- Reduces end-user inconvenience while significantly increasing security
- Eliminates potential phishing or whaling attacks

INDUSTRIES & APPLICATIONS

- Enterprise IT
- IoT devices
- Financial transactions
- Automotive industry

ip.sandia.gov
ip@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2018-4564 M