New York City, USA
June 27 – July 2, 2015

SAND2015-5018C

Physically Unclonable Digital ID

Sung Choi, David Zage, Yung Ryn Choe, Brent Wasilow
{schoi, djzage, yrchoe, bwasilo}@sandia.gov

11th IEEE World Congress on Services

Motivation

To avoid technical challenges associated with classical PUF devices

- Granular environmental control
- Pure energy source generation
- Exposure of challenge-response pair (CRP)
- Size, weight, power, and cost to manufacture and deploy
- Security guarantees

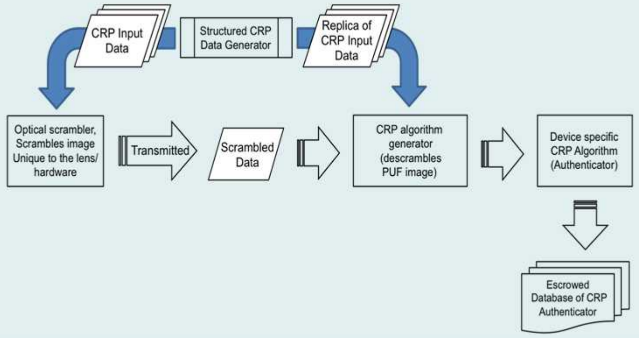
Our Contribution

Physically Unclonable Digital ID (PUDID) and Quasi-PUDID (Q-PUDID):

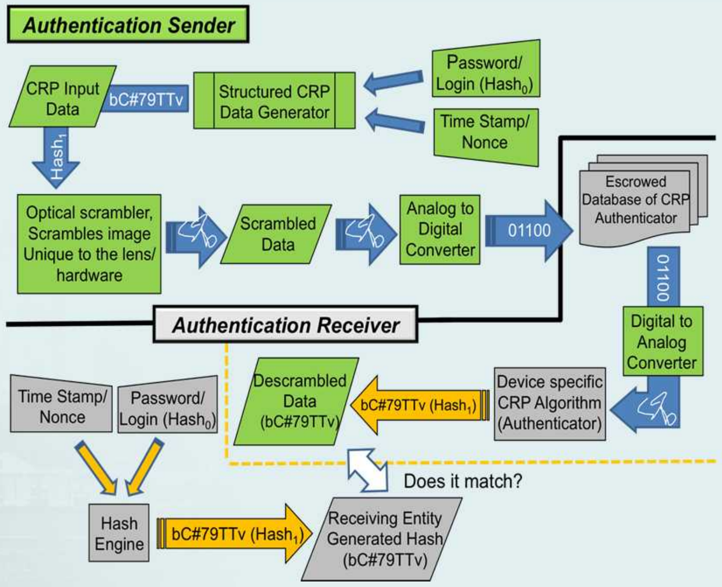
- Uses simple, inexpensive, macroscopic, and pluggable PUF components to produce reliable and difficult to reproduce results
- Q-PUDID leverages PUF-like capabilities by using a tamper resistant device that modifies input data, using a black-box mechanism, in an unpredictable way
- Intertwines a dynamic human component with a unique, physically unclonable device (i.e., true two-factor authentication).
- Q-PUDID Device ID is never exposed to any third parties in its manufacturing process
- Uses a combination of a series of hash functions to produce high mathematical barriers to cryptanalysis
- Randomness can be controlled by modifying the hash size and CRP, offering assurance level calculations
- Separates the CRP; traditional PUF devices produce a response on the same device, exposing it to cryptanalysis
- Makes it possible to physicalize the public/private key model; the PUF hardware acts as the private key and the CRP is the public key; CRP algorithm leakage will not compromise the identity of the device as it is physically impossible and/or cost prohibitive to manufacture that specific device

PUDID Architecture and Applications

Uniquely Identify End-User and Phone Using Optical PUF

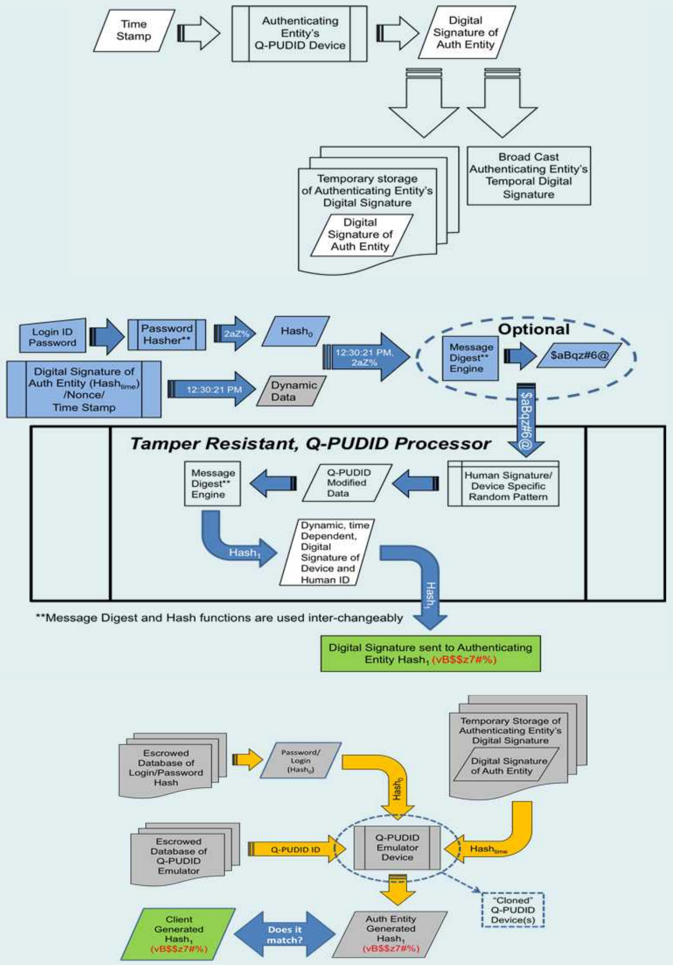

CRP Input Data
Structured CRP Data Generator
Replica of CRP Input Data
Optical scrambler, Scrambles image Unique to the lens/ hardware
Transmitted
Scrambled Data
CRP algorithm generator (descrambles PUF image)
Device specific CRP Algorithm (Authenticator)
Escrowed Database of CRP Authenticator

Uniquely Identify End-User and Phone (PUDID)


Authentication Sender
CRP Input Data
bC#79TTv
Structured CRP Data Generator
Password/ Login (Hash0)
Time Stamp/ Nonce
Hash1
Optical scrambler, Scrambles image Unique to the lens/ hardware
Scrambled Data
Analog to Digital Converter
01100
Escrowed Database of CRP Authenticator
01100
Digital to Analog Converter
Authentication Receiver
Device specific CRP Algorithm (Authenticator)
bC#79TTv (Hash1)
Descrambled Data (bC#79TTv)
Time Stamp/ Nonce
Password/ Login (Hash0)
Hash Engine
bC#79TTv (Hash1)
Receiving Entity Generated Hash (bC#79TTv)
Does it match?

Q-PUDID Architecture and Applications

Uniquely Identify End-User and Phone (Q-PUDID)


Time Stamp
Authenticating Entity's Q-PUDID Device
Digital Signature of Auth Entity
Temporary storage of Authenticating Entity's Digital Signature
Digital Signature of Auth Entity
Broad Cast Authenticating Entity's Temporal Digital Signature
Login ID Password
Password Hasher**
2aZ%
Hash0
Digital Signature of Auth Entity (Hashtime) /Nonce/ Time Stamp
12:30:21 PM
Dynamic Data
12:30:21 PM, 2aZ%
Optional
Message Digest** Engine
$aBqz#6@
$aBqz#6@
Tamper Resistant, Q-PUDID Processor
Message Digest** Engine
Q-PUDID Modified Data
Human Signature/ Device Specific Random Pattern
Hash1
Dynamic, time Dependent, Digital Signature of Device and Human ID
Hash1
Digital Signature sent to Authenticating Entity Hash1 (vB$$z7#%)
Escrowed Database of Login/Password Hash
Password/ Login (Hash0)
Hash0
Temporary Storage of Authenticating Entity's Digital Signature
Digital Signature of Auth Entity
Escrowed Database of Q-PUDID Emulator
Q-PUDID ID
Q-PUDID Emulator Device
Hashtime
"Cloned" Q-PUDID Device(s)
Client Generated Hash1 (vB$$z7#%)
Does it match?
Auth Entity Generated Hash1 (vB$$z7#%)

**Message Digest and Hash functions are used inter-changeably

Sandia National Laboratories

Sung Choi:
Sandia National Laboratories
Albuquerque, NM 87185 USA
schoi@sandia.gov