CPSC 490 Project Proposal
An Exploration of the Universal Name System Authentication System
Michael Sisti
Adviser: Michael Fischer

Introduction:

The Universal Name System (UNS) Project is a technology startup attempting to create an internet authentication architecture for users and services. Readers are encouraged to explore their website at https://www.unsproject.com/. This system promises a distributed architecture that minimizes the sharing of personal identifiable information (PII) by using a combination of private key authentication and public key infrastructure (PKI) to authenticate a user to a service.

This work seeks to evaluate the architecture of UNS and understand how its design differs from other types of authentication systems. Once a firm grasp of the UNS structure is attained, potential vulnerabilities to the confidentiality, integrity, and availability to the system can be analyzed. Using cryptographic concepts, variations of the current UNS design will be evaluated for their ability to mitigate different security vulnerabilities. Of particular interest are ways to mitigate sybil attacks. There is little literature on the subject, and it remains a challenge for services to manage the problem of fake accounts. The author has been in contact with one of the UNS creators, Jonathan Hochman, and will be receiving extensive assistance in materials and expertise from him to understand the system.

About UNS

UNS is an authentication system that promises the ability of users to authenticate themselves to services. What differentiates UNS from traditional authentication schemes is its intermediate architecture of nodes between users and services. This structure is designed to minimize the user information needed by a service to trust and authenticate a connection. UNS claims this authentication process is zero knowledge. This claim will be investigated as part of the system’s evaluation.

In traditional authentication, a user connects to a system and authenticates herself directly with a service. The usual method of authentication involves a user Alice sharing a username and password with a service Bob. The authentication relies on the fact that Alice has a secret, her password, that she previously shared with Bob. Bob assumes that no one else knows Alice’s secret. If he receives Alice’s correct password, he will trust that the user is indeed Alice.

This system of authentication poses multiple problems. First, users have login credentials for dozens of accounts. It is hard to remember so many passwords, causing many users to reuse passwords or store them in unsecure places for easy lookup. Creating new and unique passwords becomes increasingly inconvenient as more accounts are created online. When service or user systems are compromised, their data is often stolen. If similar passwords are used across multiple accounts for a user, this creates a major vulnerability for a malicious attacker to impersonate the user across these multiple accounts. Many people also use weak passwords, making it easy for an
attacker to guess their password and impersonate their identity. Due to the inherent vulnerability of weak passwords and shared passwords across multiple accounts, many attacks leverage stolen or weak passwords.

The UNS architecture consists of four roles:
1. Users
   a. Have trusted devices
2. Guardian nodes
   a. Register trusted devices for each user
3. Comptroller nodes
   a. Register the ownership of user accounts in a table of account numbers and corresponding keys
4. Services
   a. Trust a comptroller node with a list of user account numbers

Similar to two-factor authentication, UNS utilizes trusted devices to verify identity. Authentication in UNS means Alice has access to a trusted device and is able to unlock it. The general steps of UNS authentication of a user to a service is as follows:
1. Alice’s trusted device creates a security certificate.
2. The certificate is sent to the guardian node to verify the user’s identity using symmetric cryptography.
3. This guardian node uses a public key infrastructure (PKI) to securely vouch for the identity of Alice to the comptroller node of the service she is requesting to access.
4. The comptroller trusts a valid key from the guardian node. The comptroller looks up the account number associated with the received key and informs the respective service with symmetric cryptography that this account number has been authenticated.
5. The service now trusts the authenticity of Alice’s connection without receiving any PII about Alice.

Unlike the traditional login requiring a user to share a secret password, the UNS process does not require a service to use any information about the user for authentication. Access to this device and its security certificate are the secret that Alice knows. By not using passwords, UNS avoids those vulnerabilities. This work will see what other vulnerabilities might be found in its design.

Project aims:
This project will consist of analyzing the UNS architecture to understand how it works from a security and useability perspective.
Once the UNS process is understood, it can be compared and contrasted to current authentication methods such as Apple login, Open ID Connect OAUTH, single signon for Google, Facebook, and Twitter, and multi-factor authentication services like Duo Mobile.

Having the perspective of how UNS differs from these other authentication methods will allow for a more rigorous analysis of its strengths and weaknesses.

This project will play with possible design changes and affect how they might improve the system.

Time permitting, coding models of the proposed design changes will seek to understand how these changes affect system behavior.

Deliverables:
- Analysis of how UNS works
- Analysis of how UNS compares to other authentication systems
- Analysis of UNS security strengths and weaknesses
- Create three alternate designs of UNS and analyze their behavior
- Create a program that models an alternate design of UNS

Timeline:
9/16 - 9/27 (2 weeks) Analyze UNS and compare to other authentication systems
9/27 - 10/11 (2 weeks) Determine strengths and limitations of UNS
10/15 - 10/21 Fall break
10/21 - 11/1 (2 weeks) Design three modifications of UNS and determine its effect on security
11/1 - 11/15 (2 weeks) Create a program modelling UNS modified design
11/21 First draft of project report due to adviser
11/22 - 12/2 Thanksgiving break
12/6 Final report due
12/13-12/16 Finals period