A SOPHISTICATED RFID APPLICATION ON MULTI-FACTOR AUTHENTICATION

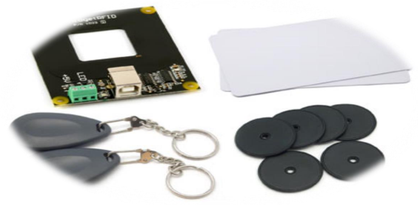
By Dr. Jing-Chiou Liou, Gregory Egan, Jay K. Patel, Sujith Bhashyam

INTRODUCTION

- A myriad of security risks that place a user's data in peril.
- User authentication is first line of defense against attackers.
- Most widely used form of authentication is traditional username / password or pin.
- Concerns:
  - Personal information falling into the wrong hands.
  - Securely transferring data between client and server.
  - Keeping cost of securing data reasonable.
- Possible Solutions:
  - Users provide unique credentials upon request.
  - Use multiple factors of authentication to provide a secure connection.
  - Securely encrypt variables using a reliable algorithm.

BACKGROUND

- The authentication factor encompasses one of three methods:
  - Proof of Knowledge
    Example: Username and Password.
  - Proof of Possession
    Example: Smartcard or Token.
  - Proof of Property
    Example: Fingerprint Scan.
- Two types of authentication:
  - Single-Factor Authentication (S-FA).
  - Multi-Factor Authentication (M-FA).



SINGLE-FACTOR AUTHENTICATION

- Single-Factor Authentication (S-FA)
  - Based on One Factor.
  - Proof of Knowledge Factor.
  - Example: Username and Password.
- S-FA is the traditional security process widely used, but has been proven insecure for users.
- In a recent survey by a data security firm, it had analyzed 32 million passwords that had been stolen from users and posted on an online website called Rockyou.com.
  - The most common passwords of those on the website were "computer," "iloveyou," and even "password."

MULTI-FACTOR AUTHENTICATION

- Problems with Single-Factor Authentication:
  - Hard to remember secure passwords.
    - Users do not take precaution by using "Strong Passwords"
  - Passwords that are attacked by hackers and often cracked.
  - Clients use the same password for a myriad of accounts.
- In Multi-Factor Authentication (M-FA), the client offers more than one factor to authenticate themselves to the server or website. Requiring more factors exponentially increases the difficulty for security breaches.
- One form of Multi-Factor Authentication (M-FA):
  - Two-Factor Authentication (T-FA): Requires two credentials from client at time login into website or server.
  - First Factor: Username and password.
    - Known as Proof of Knowledge factor.
    - Same as Single-Factor Authentication (S-FA).
  - Second Factor: Physical, virtual, or soft token.
    - Known as Proof of Possession factor.
    - Used along with the first factor at time of authentication into the website or server.

NEW METHOD OF AUTHENTICATION

- We propose the use of an application combining multiple technologies
  - Software is installed on client's computer.
  - User is provided with RFID reader and tag.
  - RFID tag's generate a One Time Password(OTP) upon each "scan."
  - Using RFID technology in Two-Factor Authentication, the user can securely connect to desired server.

RFID FACTOR AUTHENTICATION APPLICATION

- An application that will use Radio Frequency Identification (RFID) tags to generate an encrypted One-Time Password (OTP) that the user will use in conjunction with their own username and password.
- The RFID application will be the second factor of authentication.
- RFAA uses an encryption technique called the "Blowfish Algorithm."
- Using the RFAA method, an individual can accomplish a multitude of tasks easily and securely.
  - Users logging into a website to conduct their personal online transactions.
  - Logging into a server to access confidential data and files.
  - Transferring confidential information between user's computer and the server/website.

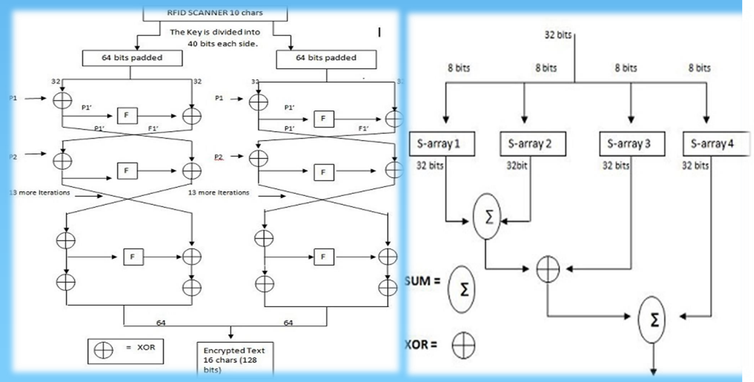
RFAA PROCESS

1. Apply for RFAA service
2. Receive RFID and the activation code.
3. Download the RFAA software.
4. Register username/password and RFID tag with the activation code.
5. Login with username/password and RFID tags.

BLOWFISH

- The Blowfish algorithm was created by Bruce Schneier, is a symmetric cryptographic block cipher.
- This algorithm is proven to be faster than Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA), making it one of the fastest block ciphers.
- The Blowfish algorithm will increase the security of our application.
- Blowfish algorithm requires approximately 5kB of main memory (RAM) to execute.

BLOWFISH ALGORITHM



COMPARISON

Performance	Username/ password	Smart Card	Biometrics	Security Tag	Virtual Tag	Software Tag	SoftTag	RFAA
Hardware requirement	Low	High	High	Medium	Medium	Low	Low	Medium
Deployment complexity	Low	High	High	High	Medium	Low	Low	Low
Portability	High	Medium	High	Medium	Medium	Medium	Medium	Medium
Identity backup	High	Low	High	Low	Medium	High	High	High
Lost recovery	High	Low	High	Low	Medium	High	High	High
Replace cost	Low	High	Low	High	Medium	Low	Low	Medium
MitM prevention	Weak	Medium	Weak	Medium	Strong	Medium	Strong	Strong
Phishing prevention	Weak	Strong	Medium	Strong	Strong	Medium	Strong	Strong
Spoofing prevention	Weak	Strong	Medium	Strong	Strong	Medium	Strong	Strong