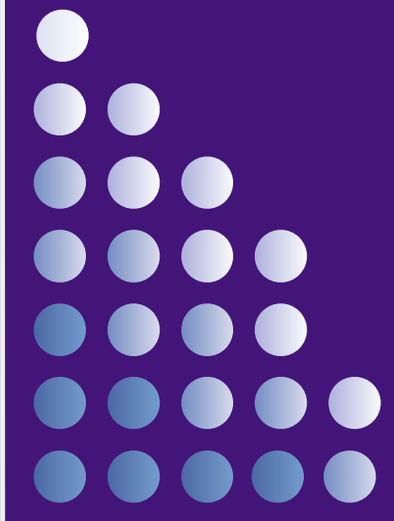
One-time Password Systems



Keith A. Watson

PURDUE UNIVERSITY

CERIAS

GLSP October Meeting

Overview

- Benefits, Costs, Methods
- Brief History of OTP systems
- RFCs and standards
- Attacks
- Software
- Hardware tokens
- Modern OTP systems
  - Online Services
- DIY project

What is a One-time Password?

PURDUE UNIVERSITY

CERIAS

- A single-use password or series of codes used to authenticate a user over an untrusted communications channel
  - Complements a user password
  - Can also replace a user password

- Password Examples:
  - TOTP: 857639
  - S/Key: RUN REND WALK MARY WAG JUNE
  - SecurID: 847596

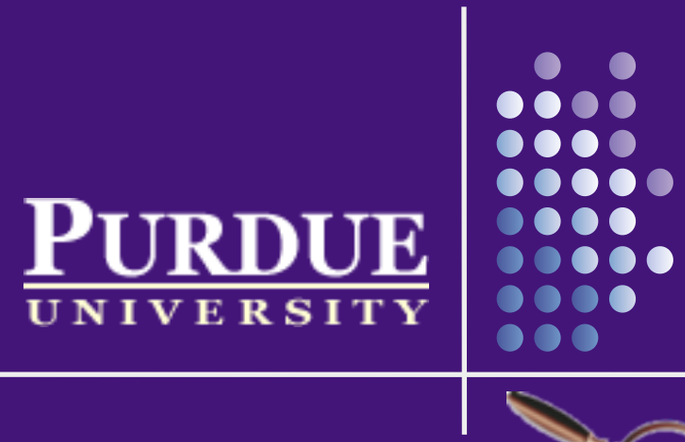
Benefits of OTPs

- Generated out-of-band
- Cannot be reused
- Can be time-limited
- Can be used over untrusted communication paths
  - Telnet, web-based, serial terminals
- Can use with a compromised user password
- Multiple generation/delivery mechanisms

Costs

- A password only used once is hard to remember
- Hardware devices are expensive
- Software tools can be compromised
- Based on a shared secret
- Cost of scaling to large organizations is significant
- Attacks are still possible

Brief and Probably Inaccurate History



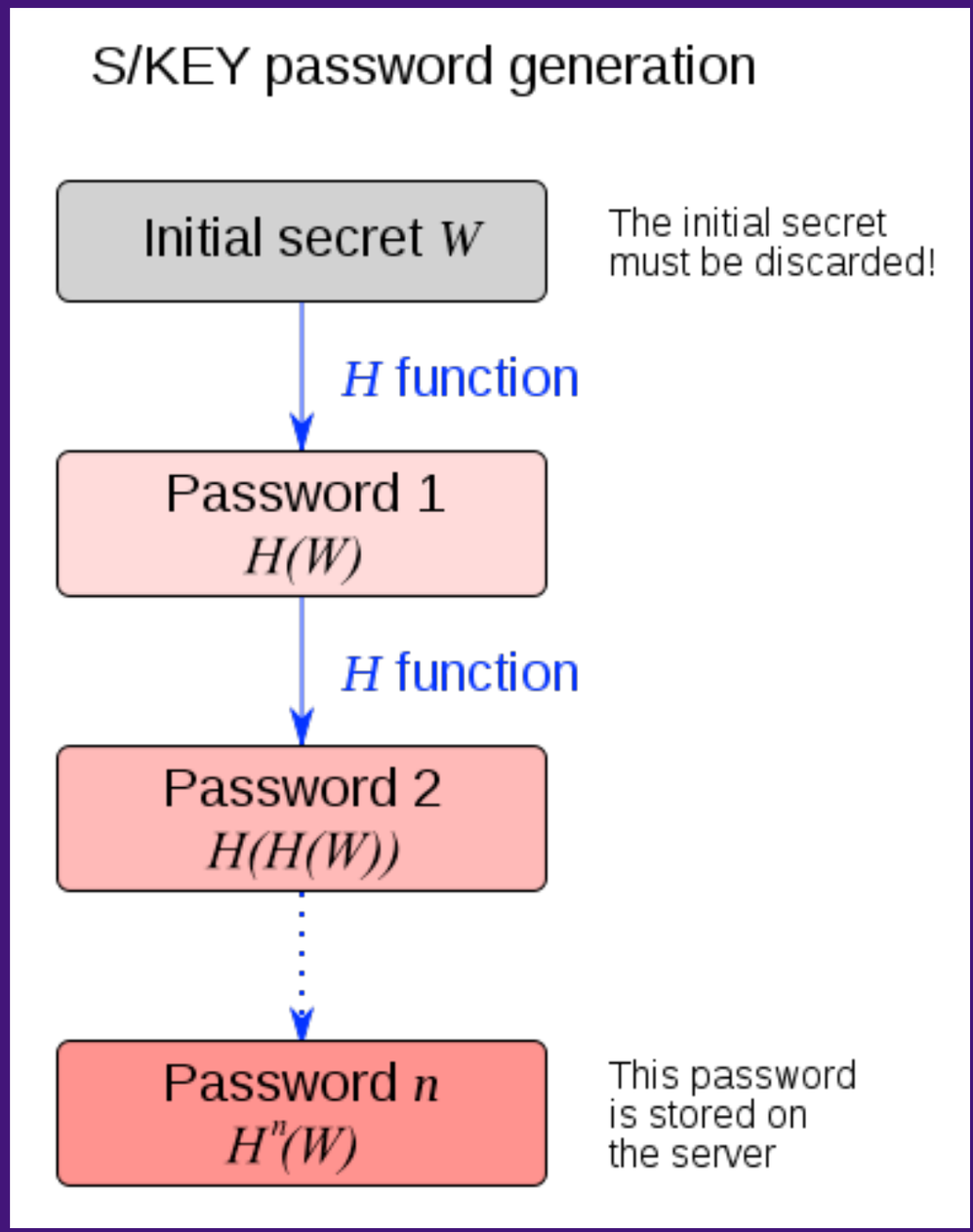
- Leslie Lamport wrote an article on chaining hashes for authentication (CACM 1981)
- Bellcore developed S/Key based on the Lamport scheme (1994)
- Hardware tokens are developed
- OPIE was a more modern implementation and compatible with S/Key
- OTPW developed
- Google Authenticator and Facebook OTP

Categories of OTPs

- Time-synchronized
  - Clocks must be synchronized
- Counter-based
  - Codebook approach; lists of passwords
- Challenge-based
  - User enters a key sent from server plus a password
- Standards-based
  - RFCs defined interoperability and functionality
- Proprietary
  - Blackbox; unless you hacked RSA SecurID

Methods of Generation

- S/Key initialization
  - Uses hash chains
  - Setup involves a secret, seed, iteration number
    - Secret and seed are hashed repeatedly to the iteration number
    - The seed, iteration number - 1, last hash value stored
- S/Key OTPs represented as words (2048 words)



Methods of Generation

PURDUE UNIVERSITY

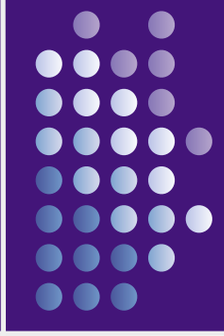
CERIAS

- S/Key Authentication
  - When logging in, a user receives an OTP message with the seed and sequence number
  - User either checks the codebook of passwords using the sequence number or an OTP calculator
  - An OTP calculator takes the secret, seed, and sequence number to generate the OTP
  - User enters the six word OTP
  - The System converts the words into the numerical representation and applies the hash function
  - The compares the user hash to the stored hash

Methods of Generation

- HOTP (HMAC-based)
  - Computes a HMAC-SHA-1 and truncation to compute the HOTP value
  - HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))
- TOTP (Time-based)
  - An extension of HOTP to support time
  - TOTP(K,C) = Truncate(HMAC-SHA-1(K,T))
    - T = (current_time - UNIX epoch) / time_step
    - HMAC-SHA-1 can be replaced with other SHA algos

Methods of Generation



- RSA SecurID (proprietary; details fuzzy)
  - Each token has a external serial number, internal secret, and security algorithm, maybe
  - Server knows the internal secret of each card

Methods of Delivery

- Paper
  - Lists of passwords or codes to use
  - Some systems use paper codes as a backup
- Hardware token
  - Token has a rotating display of the current code
  - May have buttons for challenges
  - USB-based tokens interface with software
- Mobile applications
  - The code is displayed exactly like a HW token
  - OTP calculators can work with counter-based OTP

More Methods of Delivery

- Software applications
  - Command line OTP calculators
- Text messaging
  - Requests are made to send a code via SMS
  - Requests from SMS itself or out-of-band
- Phone call
  - During the authentication process, you receive a phone call and enter a PIN

RFCs and Standards

PURDUE UNIVERSITY

CERIAS

- RFC 1760, The S/KEY One-Time Password System
- RFC 2289, A One-time Password System
- RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm
- RFC 6238, TOTP: Time-based One-time Password Algorithm
- OATH (Open Authentication initiative)

Attacks on OTP

- Man-in-the-Middle
  - Attacker captures and resends authentication data to legitimate server
- Race Attacks
  - Attacker monitors user login while creating a series of concurrent connections to target server
  - Before the user enters the last code word or character, the attacker guesses all possible words/characters over the established connections

Software

- Operating System based
  - S/Key
  - OPIE
  - OTPW
- Mobile Apps
  - Google Authenticator
  - Mobile-OTP clients
  - Software to replace proprietary HW tokens
  - Many other RFC-based mobile apps

Hardware Tokens

- RSA SecurID
- SafeNet eToken
- Yubico
  - Acts as a USB keyboard, enters time-based codes
  - Lots of libraries for integration and development
- Fortezza PCMCIA cards
- Boiler Keys are relabeled SecurID tokens

Other Systems

- Text message based
  - Facebook OTP
  - Google Two-Step Verification (via SMS)
  - PhoneFactor (SMS, voice call)
- Image based
  - Confident Technologies, ImageShield

OTP Development Libraries

- Java: javaotp
- Ruby: ropt, ruby-otp
- Python: POTP
- PHP: OTPHP, multiOTP
- C/C++: OpenOTP
- Many more available

Online Services

- Google Two-step Verification
  - Provides OTP for Google Accounts
  - OTPs generated using the Google Authenticator mobile app for Android, iOS, and Blackberry
  - Enable in your Google Account Settings
- Facebook One-time Passwords
  - Need a Facebook-registered cell phone
  - Send message “otp” to FBOOK (32665)
  - Enter the code you receive in place of your password

The Problems have Changed

- Until '95, telnet/rsh/rlogin were the common methods of remote login for UNIX systems
  - SSH mitigated the clear-text communication problem and added two-factor authentication
  - Plaintext protocols fell out of use
- Modern OTP solutions solve different problems
  - People have too many accounts with the same weak password
  - People use compromised systems and their password has been exposed

The End of Passwords?

PURDUE UNIVERSITY

CERIAS

- Can passwords be replaced with OTPs?
- Have the number of mobile devices reached the point where requiring OTPs makes sense?
- Are attacks against OTP systems significant enough to prevent adoption?

The GLSP DIY OTP Challenge

PURDUE UNIVERSITY

CERIAS

- Over the next three months think about an application where OTP might make sense
  - OTPs for web site admin users?
  - OTP delivery over IM?
  - OTPs for OpenID providers?
- Design and implement a simple solution for demonstration in January