Open Source Authentication: Security without High Cost

Donald E. Malloy

LSExperts

May 18th , 2016

Why the need for Strong Authentication?

- Fraud continues to skyrocket
- 10 Million Americans were victims of fraud last year
- This amounts to over $3.5B of online fraud last year alone
- Hacking into web sites and stealing passwords continue to be a main focus of fraudsters

Cyber Crime –
A Growing Global Threat

What do these companies have in common?

- https://www.pinterest.com/pin/125889752058560234/

Market size & projections

The worldwide cybersecurity market estimates range from $75B in 2015 -- to $170B by 2020

- Gartner says global IT spending is projected to increase to $170B
- PwC reports that US information security budgets have grown at almost double the rate of IT budgets over the last two years
- $1M+ cybersecurity sales to end-users are on the rise; according to FBR & Co. (Arlington, VA IB and M&A advisory firm) they have increase by 40% over last year
- The only slowdown is due to consolidation and acquisitions

Where did we come from?

- 1961 First computer generated password at MIT

Some Statistics

- In 2015 There were 781 Breaches in all categories: Finance, Government, Healthcare, Education, Business
- 169,068,506 RECORDS BREACHED
- 2005 -2015
  - # of Breaches = 5,810 Breaches
  - # of records = 847,807,830

- Data credit card companies
  - United States represents 27% of world wide credit card volume
  - And anywhere from 46%->50% of the fraud

Hackers are Everywhere

2015:
Bigger Breaches, Bigger Failures

Premera BlueCross (3/18/2015)	11M	Bank accounts Social Security numbers
Anthem, Inc. (02/05/2015)	80M	Social Security numbers Email addresses Physical addresses
OPM (06/09/2015)	21.5M + 1.1M fingerprints	Personal names Date and place of birth Social Security numbers Complete background security application
AshleyMadison.com (07/20/2015)	50M	Personal names Email addresses Credit card numbers Physical addresses

Trends

- EMV (Chip and pin) is being rolled out in the US. Last October 2015, the credit card issuing companies implemented liability shift to merchants. Many merchants still not accepting the Chip Card.
- Fraud will move from POS and onto online transactions as it has in other countries and regions, Europe, UK, Canada.
- Considering that mobile payment and e-commerce are growing exponentially….online transactions are a huge attraction to fraudsters.

Why now?

Pressure is mounting to stop the leakage of secure information

- Rapid growth of attacks (66% CAGR)
- Information that needs protection is growing
- Company reputation is at risk
- Leadership reputation is at risk (it's personal)
- Customers and partners will demand it
- PII regulation is coming (already in Europe)
- Shareholders will demand it to protect profits
- Strong security is a competitive advantage
- Expense of managing exposure is no longer negligible

Authentication Methods

- Simple Passwords
- Challenge Response
- One time Passwords
- Public Key Encryption
- Single Sign On
- Adaptive Authentication
- Biometrics
- Push Technologies
- SMS
- H/W Tokens
- S/W Tokens

Bill Gates declared the Password dead in 2004

Issues Facing IT Managers

The Open Authentication Initiative (OATH) is a group of companies working together to help drive the adoption of open strong authentication technology across all networks.

OATH History

- Created 9 years ago to provide open source strong authentication.
- It is an industry-wide collaboration that..
- Leverages existing standards and creates an open reference architecture for strong authentication which users and service providers can rely upon, and leverage to interoperate.
- Reduces the cost and complexity of adopting strong authentication solutions.

OATH : Background

Networked entities face three major challenges today.

- **Theft** of or unauthorized access to confidential data.
- The **inability to share data** over a network without an increased security risk limits organizations.
- The **lack of a viable single sign-on framework** inhibits the growth of electronic commerce and networked operations.

OATH : Justification

- The Initiative for Open Authentication (OATH) addresses these challenges with standard, open technology that is available to all.
- OATH is taking an all-encompassing approach, delivering solutions that allow for strong authentication of all users on all devices, across all networks.

OATH Membership (Partial)

OATH Reference Architecture: Establishing 'common ground'

- **Sets the technical vision for OATH**

- **4 guiding principles**
  - Open and royalty-free specifications
  - Device Innovation & embedding
  - Native Platform support
  - Interoperable modules

- **v2.0**
  - Risk based authentication
  - Authentication and Identity Sharing

Standardized Authentication Algorithms

-Open and royalty free specifications

-Proven security: reviewed by industry experts

-Choice: one size does not fit all

HOTP

-Event-based OTP

-Based on HMAC, SHA-1

-IETF RFC 4226

OCRA

-Based on HOTP

-Challenge-response authentication

-Short digital signatures

-IETF RFC 6287

T-HOTP

-Time-based HOTP

-IEF RFC 6238

OATH Roadmap

CHOICE of AUTHENTICATION METHODS

- HOTP
- OCRA
- T-HOTP

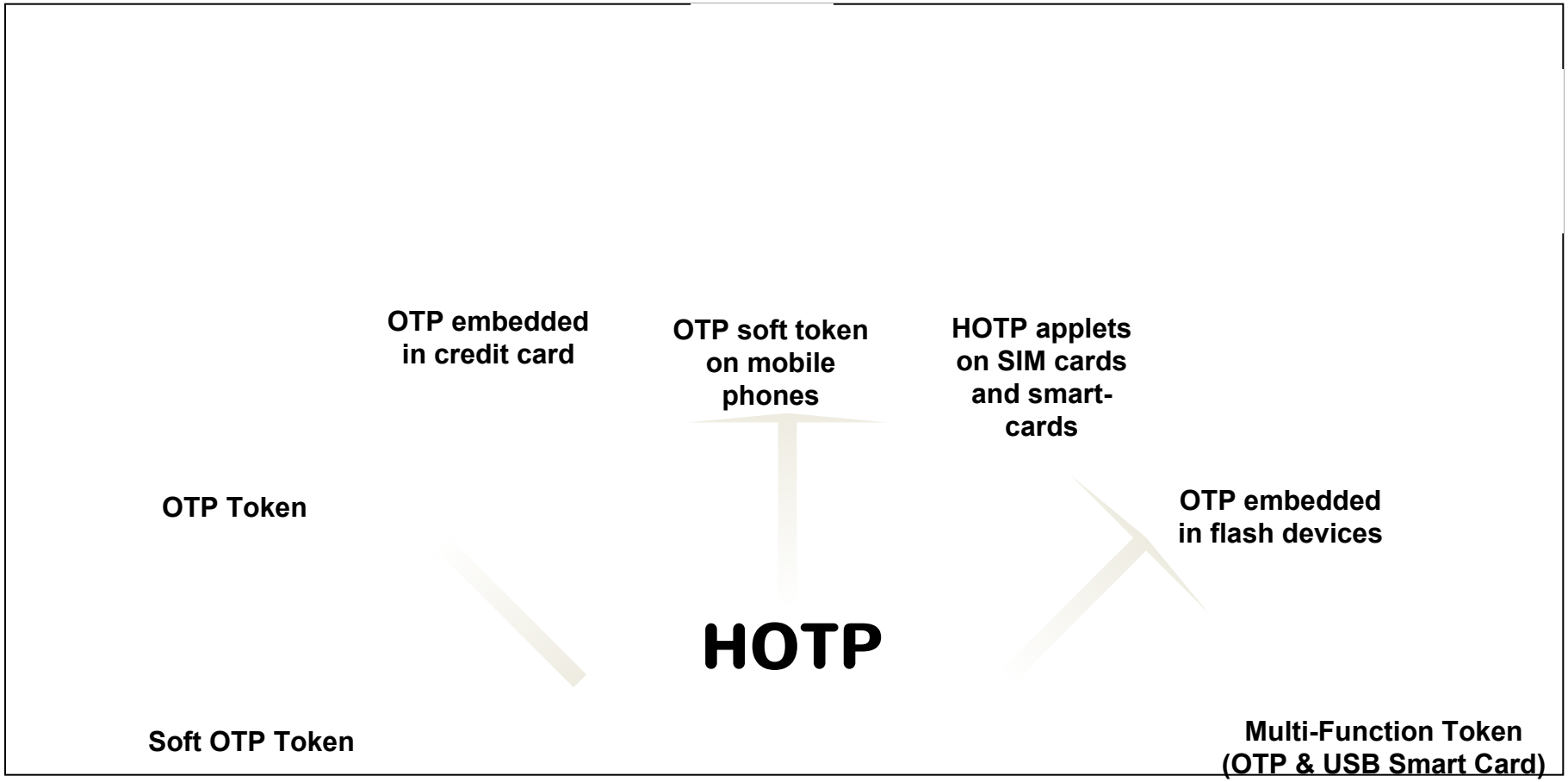
CREDENTIAL PROVISIONING & LIFECYCLE

- PSKC
- DSKPP

APPLICATION INTEGRATION & ADOPTION

- Certification program
- WS Validation
- Auth & Identity Sharing work

Token Innovation and Choice

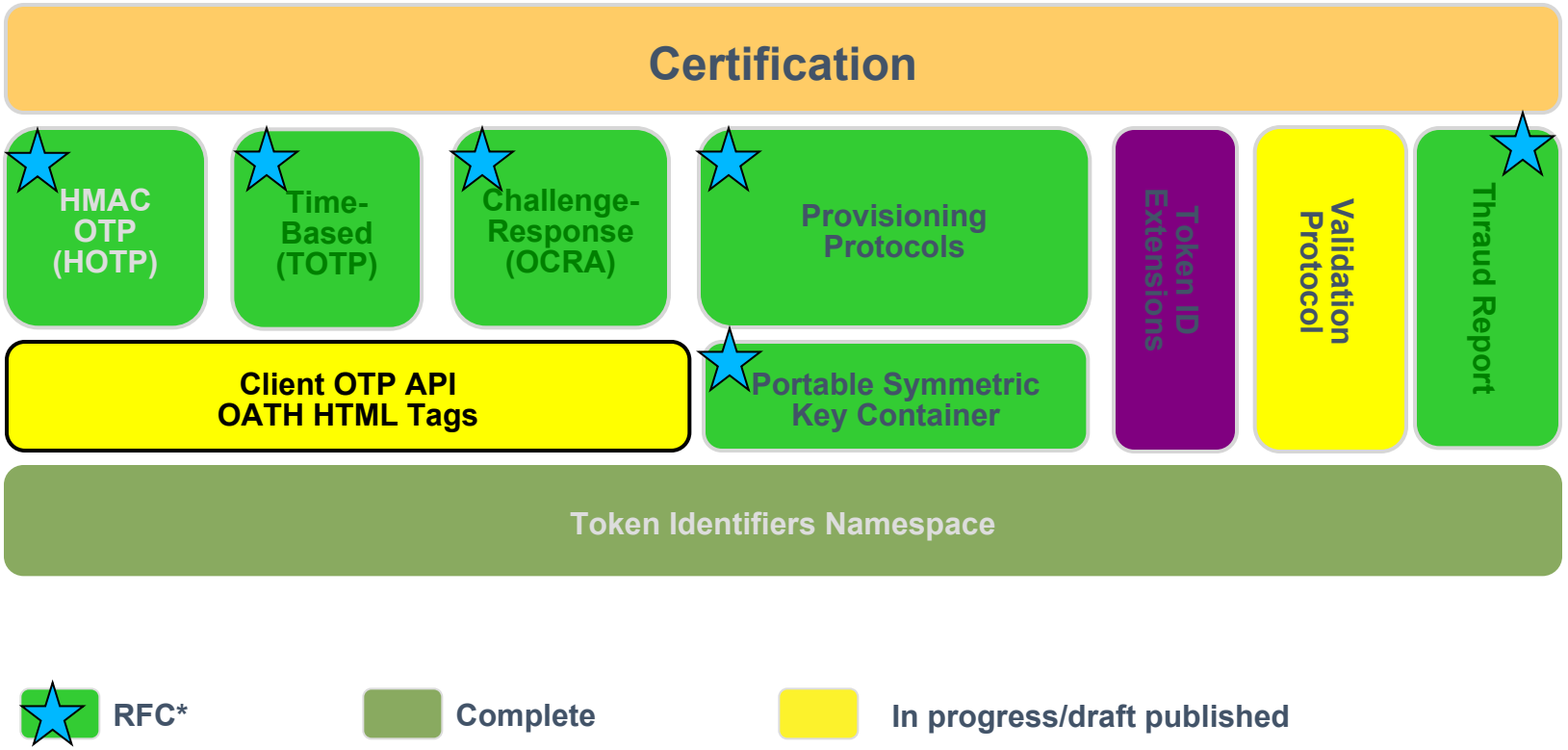


100+ shipping products

Certification Program

- Certification Adoption
  - More products added in 2014-2015
  - Numerous products have been certificated from over 30 companies!
    - HOTP Standalone Client: 14
    - TOTP Standalone Client: 12
    - HOTP Validation Server: 11
    - TOTP Validation Server: 9
  - http://www.openauthentication.org/certification/products

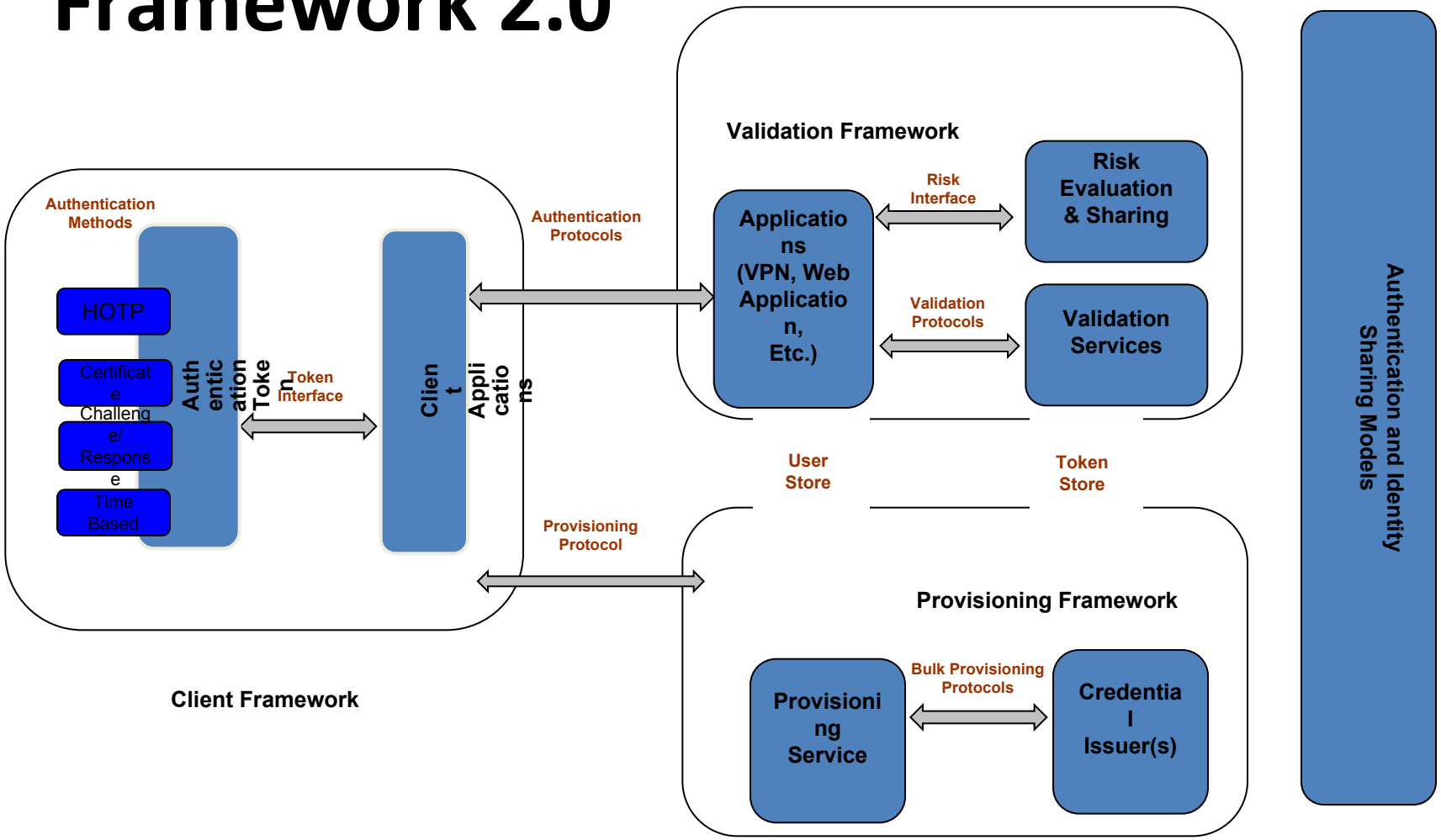
OATH Review


Certification
HMAC OTP (HOTP)
Time-Based (TOTP)
Challenge-Response (OCRA)
Provisioning Protocols
Token ID Extensions
Validation Protocol
Thraud Report
Client OTP API
OATH HTML Tags
Portable Symmetric Key Container
Token Identifiers Namespace
RFC*
Complete
In progress/draft published

Work Completed in 2015

- Algorithm profile update
  - Proposal and get RFC status
- Expand the certification program
  - Additional profiles
    - Provisioning server (DSKPP)
    - Software token
  - Test enhancements
- VALID specification
  - Adoption support and work completion
- OTP usage with NFC
- SAML 2.0 OTP authentication URI?

OATH Authentication Framework 2.0



OATH and FIDO

- WebOATH Client API
  - Draft done in Feb. 2012
    - Allow vendors to provide various interoperable plug-ins
    - Allow web applications to control security policy
  - Similar initiative now by FIDO (Feb. 2013)
    - FIDO client – biometric or OTP credentials
    - Client and server protocol
- Next step? Possibly work together?

Credential Provisioning

Token manufacturer offline model

- Portable Symmetric Key Container standard format (PSKC Internet-Draft)

Dynamic real-time model

- Dynamic Symmetric Key Provisioning Protocol (DSKPP Internet-Draft)
- OTA provisioning to mobile devices, or online to PC/USB

IETF KeyProv WG

- Current RFC submissions

Objectives

- Understand the full lifecycle support needed for strong authentication integration
- Learn different approaches to supporting strong authentication in your applications
- Take away with the best practices for enabling strong authentication in applications

Certification Program

- The OATH Certification Program
  - Intended to provide assurance to customers that products implementing OATH standards and technologies will function as expected and interoperate with each other.
  - Enable customers to deploy ‘best of breed’ solutions consisting of various OATH ‘certified’ authentication devices such as tokens and servers from different providers.
- Introduced 2 Draft Certification Profiles at RSA
  - Tokens – HOTP Standalone Client
  - Servers – HOTP Validation Server
- 10 Additional Profiles to be introduced throughout the year

Typical Application Scenario

Transaction authentication & Signing

- Log on to Bank's web site
- Give user name and password
- Bank sends a challenge number used to create pin
- User enters number into card and new secure pass code is generated
- User then submits this new number to the bank's web site
- Transaction is then authorized by the bank

Recommended Validation Framework

Why is OTP Still Expensive?

- More the 50 companies offer One Time Password (OTP) solutions in various types and flavors….
  - Soft tokens
  - Hard tokens
  - Credit Card
  - USB tokens
  - SMS
  - Time based, Event Based, Challenge/response

OTP a Commodity?

- Cost per user has consistently been too high, manufacturers continue to have a business model that overcharges the user.
- Competition should drive costs down but it hasn’t happened……until now

Modular Design of LinOTP

- LSE LinOTP is an innovative and flexible OTP platform for strong user authentication.
- Open Source OTP is available for FREE:
- All OATH tokens are supported with SVA – Smart Virtual Appliance
- Only cost is for support and maintenance

Works Everywhere

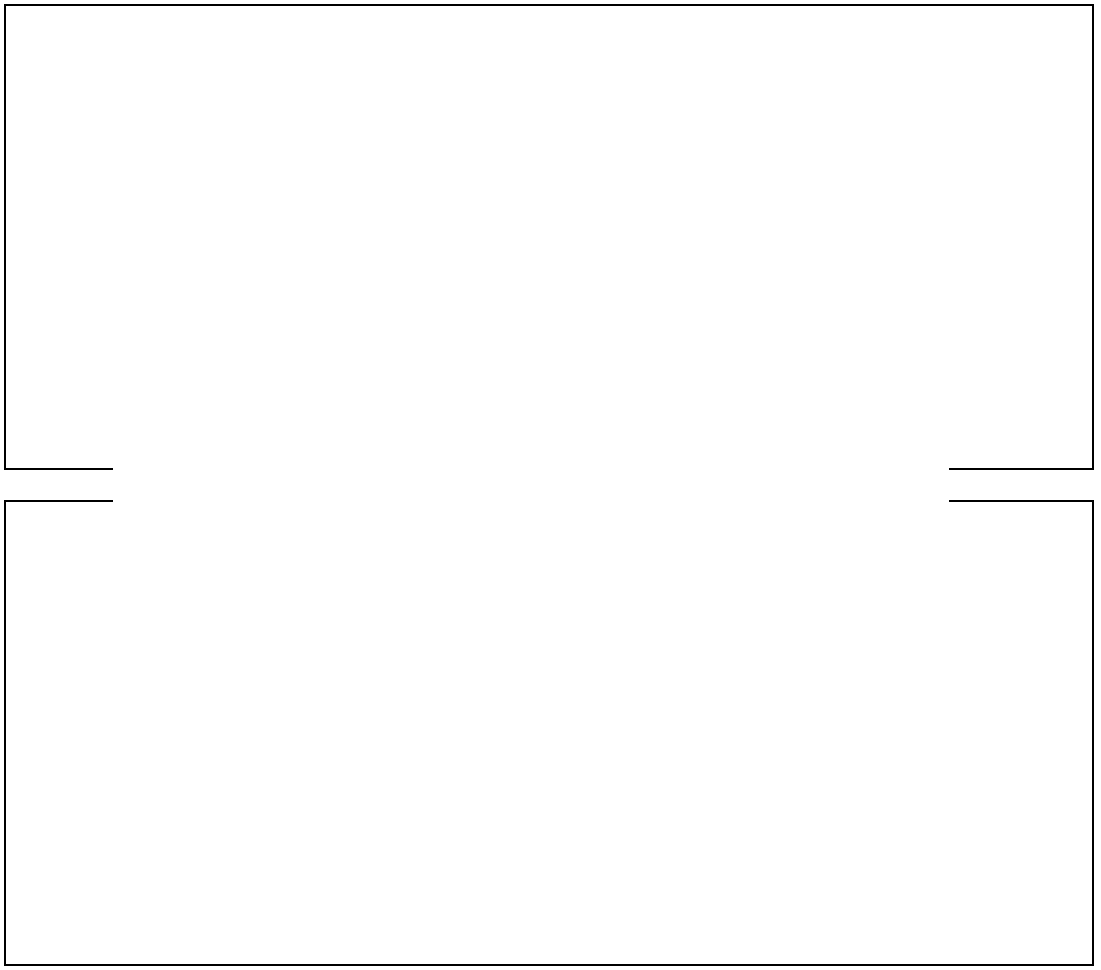
- One Time passwords offer the advantage that they do not require client-side driver.
- Open, generally accepted algorithms in particular are integrated for OTP generation, Listed in RFC4226 algorithm HMAC-OTP.
- LinOTP also supports various other open and proprietary token and procedures. The sending of one-time passwords (as mTAN) via SMS or email is also a function.
- The optional use of hardware tokens, which calculate the one-time password for the user, can help to increase security further.

Open Source Authentication

Authentication Integration Architecture

- Direct authentication integration over standard protocol

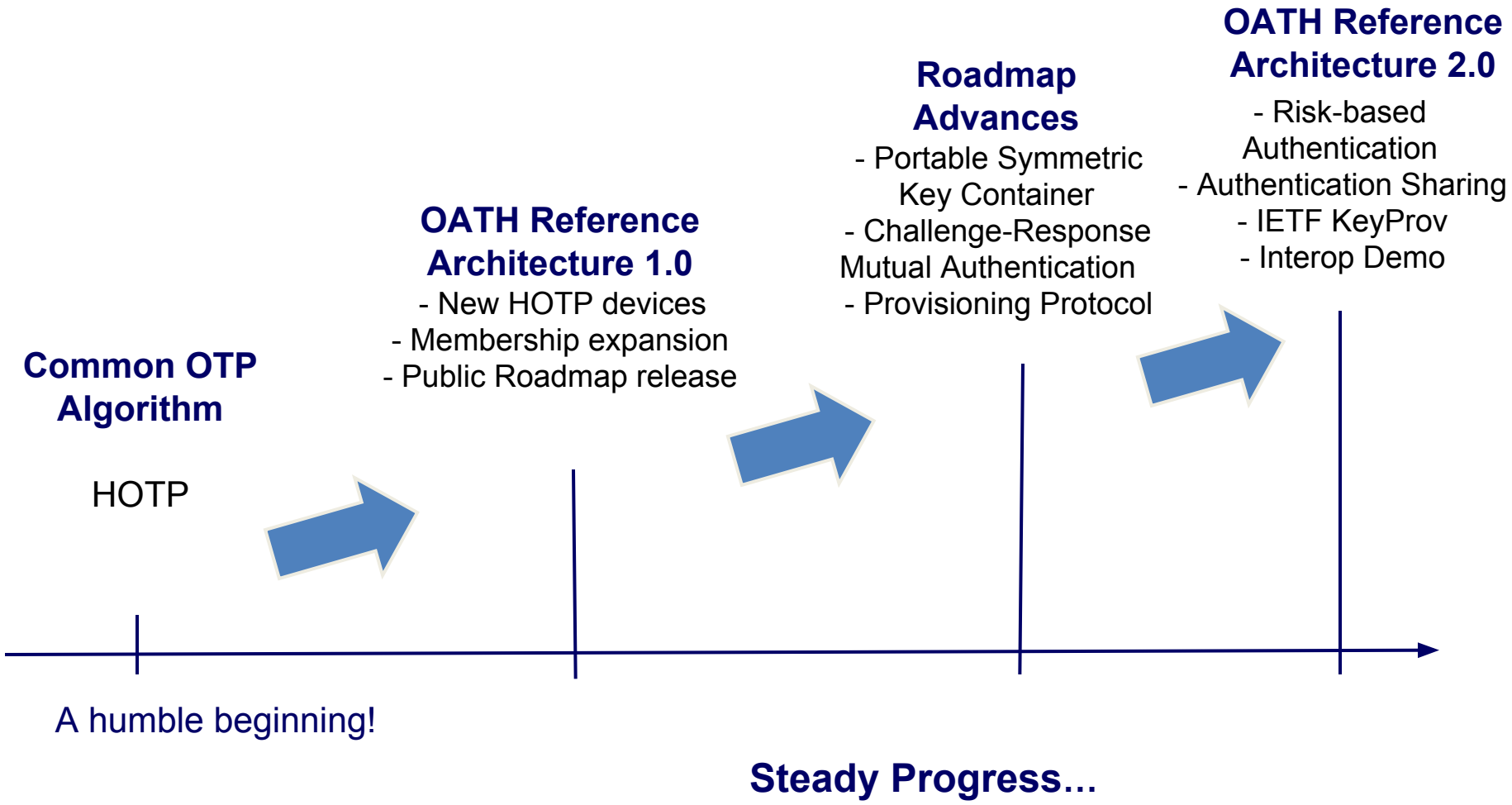
- Plugin based authentication integration



Plugin Based

- Enable two-factor authentication in your existing third party authentication server for user password
  - Your application codes don't need to change
  - Out of box strong authentication support in your existing third party authentication server
    - Integration Connectors available from authentication solution vendors, e.g. RSA, Symantec
      - e.g. CDAS plugin for IBM Access Manager
  - Develop your customized plugin for your existing third party authentication server

OATH Timeline



Risk Based Authentication Architecture

- **Risk-based authentication**
  - Convenient authentication for low risk transactions
  - Stronger authentication for higher risk transactions
- **OATH will define standardized interfaces**
  - Risk Evaluation
  - Sharing fraud information (ThraudReport)

Authentication and Identity Sharing

- Promotes use of single credential across applications
  - Force multiplier!
- Multiple approaches
  - One size does not fit all
- Models that leverage identity sharing technologies
  - Kantara, SAML, OpenID, etc.

- Models to enable sharing of 2nd factor authentication only
  - Simpler liability models

Authentication Sharing – Centralized Token Service model

- Token is validated centrally in the validation service
  - Same token can be activated at multiple sites
- Easy integration for application web site(s).
  - Can leverage OATH Validation Service work!

Authentication Sharing – Distributed Validation Model

- Inspired by ‘DNS’
- Rich set of deployment models
  - Standalone system can join the network by publishing token discovery information
- There needs to be a central Token Lookup Service.
  - OATH considering developing Token Lookup protocol

Authentication Sharing Credential Wallet

- Shared device
  - Multiple credentials
- Credentials are dynamically provisioned onto the device.
  - Leverage OATH Provisioning specifications.

Identity Federation & OATH

- Enables user to use same identity across website(s)
  - Traditional federation (Liberty)
  - User-centric models (OpenID, CardSpace)
- Single Identity becomes more valuable
  - Needs to protected using strong authentication

OATH: promote the user of strong authentication with these technologies!

What about Technology beyond Passwords?

- Adaptive Authentication
- Biometrics
  - Fingerprint
  - Iris Scan
  - Voice
  - Facial Recognition

- Biometrics are great but they are irrevocable

What about Stronger Passwords?

- We have more passwords than ever before – ave. # of passwords used daily is >25.
- Passwords attempt to answer the question: *is this really you?*
- Knowing what to type doesn't authenticate *you*. If that worked, fraudsters wouldn't be successful.
- Behavior analytics confirms who you are.
- Eventually, you won't have to remember a password at all – simply type a phrase, and based on your behavior, will confirm that *it is really you*.

60%

of Internet users have the same password for more than one web account

source: "Adults' Media Use and Attitudes Report 2013" – Ofcom

The Behavioral Advantage

Key Attributes

✓ Good
✓ Okay
✗ Poor

	Can't be Stolen or Shared	Identifies the Person	Gradient Results	Revocable	Nothing to Remember	No PII	No Special Equipment	Easy to Deploy	Low Cost	Usability
Behavioral Biometric	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Passwords	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓
HW Tokens	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
SW Tokens	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓
Fingerprint	✓	✓	✗	✗	✓	✗	✗	✗	✗	✓
Facial recognition	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
Iris Scan	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
Voice Recognition	✗	✓	✗	✗	✓	✗	✓	✓	✓	✓

All the Benefits, None of the Drawbacks

The Time is Now for Behavioral Analytics

Increase in recommendations by advocates of behavioral analytics -- but what is driving this trend?

- Security technologies using white list/black list rules or signature-based strategies are **failing to block** increasingly sophisticated attackers
- Network activity logs are generated and then ignored because human analysts capable to act on them are **not available**
- Attackers are shifting to **targeting individuals** to trick or coerce them into giving up their usernames and passwords
- Fraudsters are become increasingly proficient at assembling full data records from partial information stolen in earlier breaches

Behavioral Login

Using behavior to secure the login, the latest focal point for cyber attacks.

Provides…

- security without PII
- frictionless user experience
- control over subscription sharing

With Nothing…

- to possess, or lose (fobs, smartcards)
- to remember (security questions)
- to fail (devices/readers, cell phones, etc.)

Over

300 million

records breached in 2014, in the United States alone.

source: data-breach.silk.co

Summary

Driving a fundamental shift from proprietary to open solutions!

- An industry-wide problem mandates an industry wide solution
  - Strong Authentication to stop identity theft across all the networks
- A reference architecture based on open standards
  - Foster innovation & lower cost
  - Drive wider deployment across users and networks
- Minimal bureaucracy to get the work done!

How to Get Involved

- Visit the OATH website
  - Download Reference Architecture v2
  - Download and review draft specifications
- Engage - contribute ideas, suggestions
  - Review public draft specifications
  - Get involved in developing specifications
- Become a member!
  - 3 levels - Coordinating, Contributing, Adopting
  - Become an active participant

Open Source Implementation

- RADIUS Client
  - Java
    - http://wiki.freeradius.org/Radiusclient
  - .NET
  - C/C++
- Authentication Server with OTP Support
  - Radius server
    - http://www.freeradius.org/
    - Need to add OTP auth plugin
  - Triplesec
    - http://cwiki.apache.org/DIRxTRIPLESEC/

References and Resources

- **Initiative for Open AuTHentication (OATH)**
  - http://www.openauthentication.org
- **HOTP: An HMAC-Based One-Time Password Algorithm – RFC 4226**
  - http://www.ietf.org/rfc/rfc4226.txt
- **TOTP: Time Based One Time Password Algorithm – RFC 6238**
  - http://tools.ietf.org/html/rfc6238
- **OCRA: OATH Challenge/Response - RFC 6287**
  - http://tools.ietf.org/html/rfc6287
- **OATH Reference Architecture**
  - http://www.openauthentication.org

Questions & Answers

Thank You!