Building a One-Time-Password Token Infrastructure

Jonathan Hanks & Abe Singer
LIGO Laboratory
Distributed
Multi-Institution
International
Kerberos
Shibboleth
Grouper
Open Data

Time Critical

No Do-Overs

Remote Access

Single/Common sign-on
Credential Theft
Separate Credential
Non-Replayable
Not for everything
One Time Passwords
What does (n’t) OTP solve?
Time Based
Sequence Based
Challenge-Response
One Time Pad
Something you Have

What do(n’t) tokens solve?
Delivery
Rolf
Synchronization
Overhead
Integration
Failures
One token to rule them all
Physical device
Trust No-one
Distributed, Fault tolerant
Open
Cheap
Custom Authentication Server

PAM

Yubikey

Kerberos
Why?

Ownership

Trust

Capabilities
Architectures
SP = Service Provider
Replication and Mitigating Replay Attacks

Replication takes Time

Replicate Data w/o global locks
Centralized yet Distributed

No Secrets on Endpoints

There can be only one

Modular, Abstracted
Provisioning Users
Make it simple
Make it safe
Supporting Users

Any auth scheme is a hinderance

Just replace the token
Experiences / Problems

It Works

Tokens get out of sync

When good tokens go bad

Local Account Issues
We like SSO
Cannot afford to support all the client systems
Cannot wait for the OTP extensions to reach end users
Hijack encrypted timestamp

All kinit support this

No custom client SW required
Questions?