Apache Triplesec: Strong (2-factor) Mobile Identity Management

Alex Karasulu
Agenda

1. Drivers
2. Multiple factors & OTP
3. Triplesec Solution
4. Miscellaneous
5. Summary & Conclusion
Agenda: Drivers

- Problems
- Demand
- Market
- Costs
- Logistics
The Identity Problem

An Integration Problem!
The Phishing Problem

Increasing demand for multi-factor authentication.
Multi-Factor Gold Rush

- FEICC-mandated multi-factor for 2007
- Financial companies are desperate
- Many new vendors
- Lack of standards
- Just get into the market mentality
- Lot's of ugly products
- Lot's of suckers to be born!
Commercial Products

- 2-factor products
  - SecureId (RSA)
  - Safeword
  - ActiveIdentity
- Identity Management products
  - Netegrity (CA)
  - Oblix (Oracle)
  - SUN Identity
How much does multi-factor authentication cost?

• One Time Device Cost
  – 15-110$ USD per user
  – logistics costs: delivery & RMA?

• Recurring Cost Per User (server)
  – 10-35$ USD per user per year

• Authentication Server Cost
  – 0-100K USD one time cost
  – Maintenance covered by per user cost

• Integration Services?
How much does identity management cost?

- Recurring Cost Per User (server)
  - 12-30$ USD per user per year
- Server Cost
  - 0-100K USD one time cost (10K users)
  - Maintenance covered by per user cost
- Integration Services?
Identity Management + Multi-factor authentication = too much!

- Combined cost per user can climb rapidly
- Increased entropy: 2 products not 1
- Integration between products required
- More to Manage: each has own interfaces
Agenda: Multiple Factors and OTP

- One Time Passwords (OTP)
- HOTP
- Inhibitors
- Mobile Solution
One Time Passwords (OTP)

- Generated by hardware token
- Changes with each use
- Algorithms
  - Time Based
  - S/Key (MD4/5)
  - HMAC
  - HOTP
HOTP – RFC 4226

• Shared secret
• Counter
• Throttling parameter
• Look-ahead parameter: self service
• Bi-directional authentication
• Low resource utilization
• No network needed
OTP Inhibitors

- A token per account
- Must carry extra device on person
- Replacing broken or stolen device
- Device cost
- Device provisioning
- Invasive changes required to use within existing infrastructure
Proposed Solution

- Use mobile phones to generate OTP
  - everybody has a cell phone
  - no new hardware to buy or carry
- Simple provisioning process
  - WAP push to mobile device
- Standard protocols for authentication
- Standard JSE, JEE & JME interfaces
- Integrated noninvasive IdM
Agenda: Triplesec Solution

- Intro
- Mobile Token
- Authentication & Authorization
- Administrator UI
- Feature Demos
Triplesec “Strong Identity Server”

- FOSS – ASL Licensed
- Identity Management Platform
  - 2-Factor Authentication
  - Authorization (RBAC)
  - Auditing
  - SSO
- JME & JSE OTP client
- Want to see it?
Mobile Token

- JME based OTP generator
  - MIDP 1.0 compatible
  - 33Kb footprint
  - Runs on low end phones
- Connectionless OTP generation
  - No data subscription need
  - No service need
- Uses HOTP from OATH (RFC 4226)
Authentication

- Password & passcode (OTP value)
- Optional realm field
- Kerberos
- LDAP
- JAAS Login Module
Authorization

• Authorization Policy Store
  – applications
  – permissions
  – roles
  – authorization profiles
  – users
  – groups
• Guardian API
Administration Tool

- Manage
  - applications
  - users
  - groups
  - roles
  - permissions
  - profiles
- Let's take a look!
Servlet Demo

• Simple Servlet
• Uses Guardian API
• Application = demo
• Read & report roles and permissions
• Reads profile for each request
• Should respond to policy change events?
Policy Change Listener

- Guardian API has listener interface
- Receives policy change events
  - permission changes
  - role changes
  - profile changes
- Asynchronous notification
- No polling!
Dynamic Policy Demo

• Simple Swing Application
• Uses Policy Change Listener
• Paints menu with permissions of user
• Update dependent:
  – grants
  – denials
  – roles
• UI responds to events to redraw menu
Simple Policy Management

- Simple Schema for Policy Store
- Any LDAP client can be used
- Easy to write access API in any lang
- Easy to administer policy with scripts
- Export Policies for testing
  - Guardian LDIF & LDAP Drivers
Sync Protocol

What happens when the counter gets out of sync?
Better Web Demo

Let's see the sync protocol in action with a better demo.
Agenda: Miscellaneous

- Built on ApacheDS Protocols
- SSO & SAML
- Future Plans
Based on ApacheDS

• Triplesec uses ApacheDS for:
  – LDAP
  – Kerberos
  – ChangePW
• Simple Schema
• Looking inside with LDAP Studio
Single Sign On & SAML

• Use Kerberos for OS authentication
  – Windows (default)
  – Linux (pam_krb5)
  – MacOSX (optional)
• Can be integrated w/ CAS
• Can be integrate w/ Shibboleth
• HOTP transparent to all clients
Future Plans

• Improve various features
• Experiment with Bluetooth for MIDlet
• Make into JACC provider
• Add more polish
• Administrator plug-in for LDAP Studio
Agenda: Summary & Conclusions

- Uncovered Material
- Benefits
- Drawbacks
- Conclusions
- Questions
Things we did not have time to present to you

- MIDLet OTP Generator
  - SMS & Email Provisioning
  - Pin Cracking Protection
- OS SSO & Configuration
- Auditing & Compliance
- JAAS LoginModule
- Configuration UI
- Integration
- Delegation of Administration
- Authentication Delegation to external services
Benefits

• Single device for all OTP generators (accounts)
• Easy to use & simple design
• Dynamic notification of policy changes
• Uses standards: HOTP, Kerberos, LDAP, JAAS, MIDP 1.0
• FOSS – ASL 2.0
Drawbacks

- Waiting on ApacheDS MMR
- Heavy re-factoring needed: prototype
- Schema redesign needed for JACC
- Better management interfaces
Conclusions

• Simple solution for:
  – Simple identity management needs
  – 2-factor mobile authentication

• Low complexity: minimize integration

• No need for extra hardware

• Easy provisioning

• Increased security

• Reduced cost
Questions?