HSPD-12: The Killer App for PKI?

Tim Polk

April 10, 2006

Goals

- What is a killer app anyway?
- Is HSPD-12 PKI's Killer App?
  - And if so, who's going to die?
- Is survival the most we can hope for?
  - And if *thriving* is possible what would that look like?

What Is a killer App?

- Softpedia defines a killer app as:
  - an application that convinces you to purchase a certain hardware component, a certain operating system or a gaming console that would allow you to run that application.
- Basically, a killer app is so compelling that you *want* to buy something else just to run it

A brief history of Actual Killer Apps

- VisiCalc sold the Apple II
- PageMaker, Ventura sold the Macintosh and the IBM PC *and* the laser printer
- Photoshop and digital cameras sell computers
- These days, the killer apps may be the latest and greatest gaming software

PKI and the (Fruitless) Search for the Killer App

- Secure email?
  - No.
- Secure workflow?
  - No.
- VPNs?
  - No.

Infrastructures and Killer Apps

- It just doesn’t work that way…
- Think about the interstates
  - They are only useful if they connect where you are with where you want to be!
  - They were built to support a number of applications, not just one
    - Defense, commercial shipping, etc…

A Brief History of the FPKI

- Research underway in 1991
- Started working an a bridge CA in about 1998
- As of April 2006, the FPKI includes 10 agencies, four commercial providers and one state
- HSPD-12 issued
  - FSIP 201 establishes PKI as a core requirement.

So, Is HSPD-12 A Killer App?

- Not in the traditional sense
  - But you are all here!
- HSPD-12/FIPS 201 makes you deploy PKI, it doesn't make you want to
  - There is a difference, and we know it
- However, embracing PKI can help you not only survive, but thrive!

Surviving HSPD-12 and FIPS 201

- Isn’t really that hard!
  - Agencies already have a process in place to ensure that identity credentials are only issued to appropriate personnel
  - Which leaves…
    - Deploy the appropriate supporting infrastructure
    - Issue smart cards with appropriate electronic credentials

Deploying the Infrastructure

- Agencies must:
  - Obtain CA services to issue certificates
    - Establish or obtain supporting RA services as needed
  - Establish LDAP and HTTP repositories for CA certificates and CRLs
  - Establish OCSP services for online status checking

Issuing PIV cards

- Issue smart cards with appropriate electronic credentials
  - FASC-N/CHUID
  - PIV Authentication Key and Certificate
  - Biometric fingerprints

This sounds hard…

- Until you realize that this is what the shard service provider program is all about!

Can We Do Better Than Survival?

- Surviving means issuing the cards. Satisfying the letter, if not the spirit!

- Thriving means using the credentials to enhance security and user experience

Thriving with HSPD-12 and FIPS 201

- Provide an alternative to passwords
- Support optional digital signature and key management certificates to meet user requirements
- Look for opportunities to leverage other agencies' investment

Replace passwords

- Add support for client authenticated TLS in current web applications
- Implement smart card logon for desktops
- Implement PKI-base VPNs to secure access from alternate worksites

Client Authenticated TLS

- How many agency applications currently support tunneled passwords for authentication?
  - All web servers support client authenticated TLS
  - There is no reason that clients should not be permitted to use PKI for authentication instead.

Smart Card Logon

- All major operating systems support smart card logon.
- Use the PIV card for desktop logon and increase security *and* user satisfaction

PKI-Based VPNs

- Travelers and telecommuters suffer through without access to agency applications, or they rely on password-based alternatives
- PKI-enabled VPNs based on SSL/TLS or ipSec are available today

Digital Signatures and Key Management

- Digital signatures and key management keys can enable secure email, document signing and workflow
  - Current users may not all need this functionality, but offer it to those that have a need!

Leverage Other Agencies' Investment

- Automate visitor processing
  - Use the PIV authentication certificates and client authenticated web services to authenticate visitors and "sponsors"
  - Automate process of adding the visitor's FASC-N into the physical security system

Conclusion

- HSPD-12 may not be the Killer App PKI was looking for, but it is the deployment driver
- With the tools that are available, we should all survive HSPD-12 and FIPS 201!
- Better yet, there are real opportunities to thrive in this post HSPD-12 world