

Identity Protection Factor (IPF)

Arshad Noor
StrongAuth, Inc.
arshad.noor@strongauth.com

- What is IPF?
- What is the IPF Table?
- Description of IPF Levels

UserID-Passwords

CardSpace

LDAP

One-time Password Tokens

Smartcards

Biometrics

NIS/NIS+

KERBEROS

OpenID

SAML

Higgins

Liberty

SSL/TLS with Client-Auth

IGF

“Identity Protection Factor (IPF) is a measure of the ability of an I&A technology to resist attack from unauthorized entities.”

- **Resistance to attack**
- What about
 - Cost?
 - Ease-of-use?
 - Convenience?
 - Deployment issues
 - Integration issues
- Answer: "Gallopig Gertie"

IPF	Description
0	No identification or authentication
1	Shared-secret based authentication on a local system, or a network without any network encryption
2	Shared-secret based authentication with network encryption
3	Multiple shared-secret based authentication without an external token, but with network encryption
4	Asymmetric-key based authentication with Private Key in a file
5	Multiple shared-secret based authentication with external token and network encryption
6	Asymmetric-key based authentication with Private Key generated and stored on cryptographic hardware token and using keyboard for authentication to token
7	Asymmetric-key based authentication with Private Key generated and stored on cryptographic hardware token and using an external PIN-pad for authentication to token
8	Asymmetric-key based authentication with Private Key generated and stored on cryptographic hardware token using an external PIN-pad and being physically present at the machine where the resource exists and where authentication is performed
9	Asymmetric-key based authentication with Private Key generated and stored on hardware cryptographic token, using an external PIN-pad, being physically present at the machine where authentication is performed and using M of N control for authentication to token
10	Non-existent/Unknown

- NO identification or authentication *
- Example: Self-service Kiosks

** However, the software is assumed to be executing with the computing environment (and privileges) of a user authenticated with a credential at a higher IPF level.*

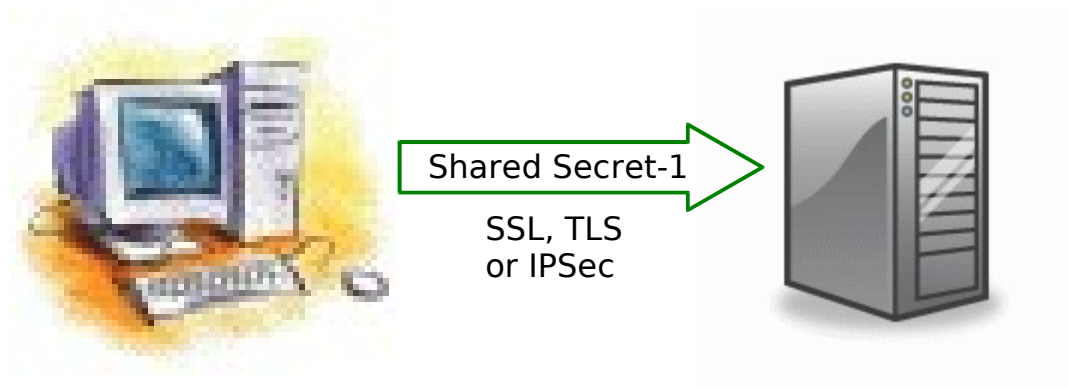


- **Shared-secret** based authentication on a local system, or a network **without** any network encryption



- Adds authentication credential to IPF-0
- Can be compromised by:
 - Dictionary attacks, network snooping, shoulder-surfing, keystroke loggers, phishing, social-engineering, rogue employee
- Compromise-blind
- Example: UserID-Password

- **Shared-secret** based authentication **with** network encryption



- Adds network encryption – such as SSL, TLS or IPSec - to IPF-1
- Can be compromised by:
 - Dictionary attacks, ~~network snooping~~, shoulder-surfing, keystroke loggers, phishing, social-engineering, rogue employee or technology-specific attacks (for biometrics)
- Compromise-blind
- Examples:
 - UserID-Password
 - Biometrics that convert reading to a template

- **Multiple shared-secrets** based authentication **without** an external token, but **with** network encryption

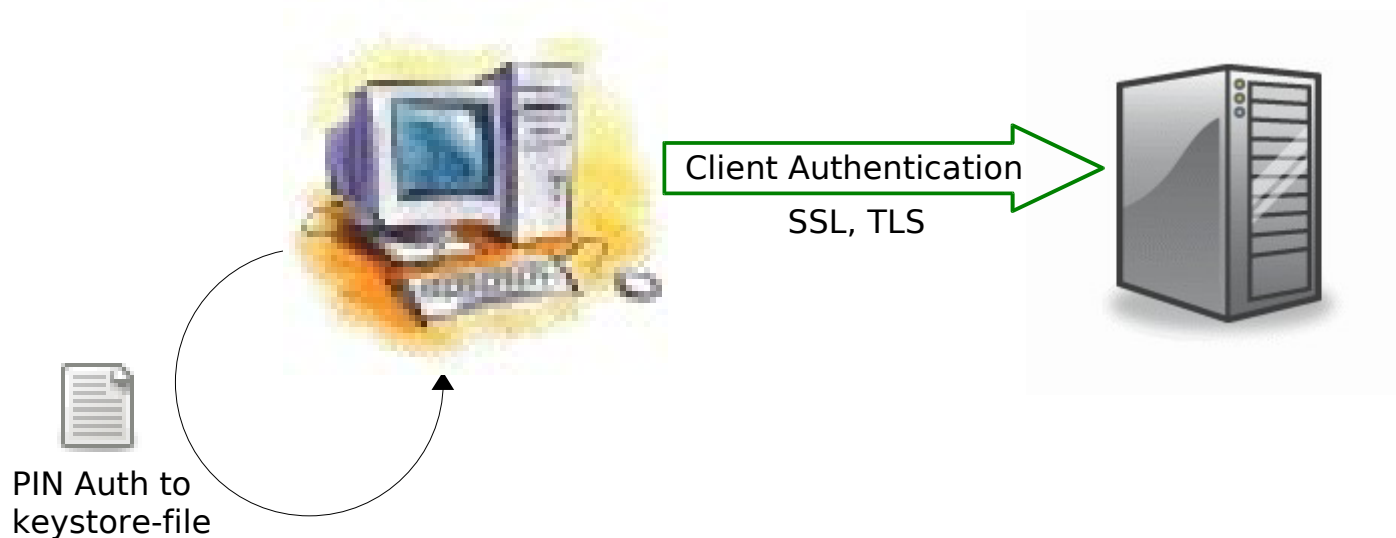


Shared Secrets 1 and 2
SSL, TLS or IPsec



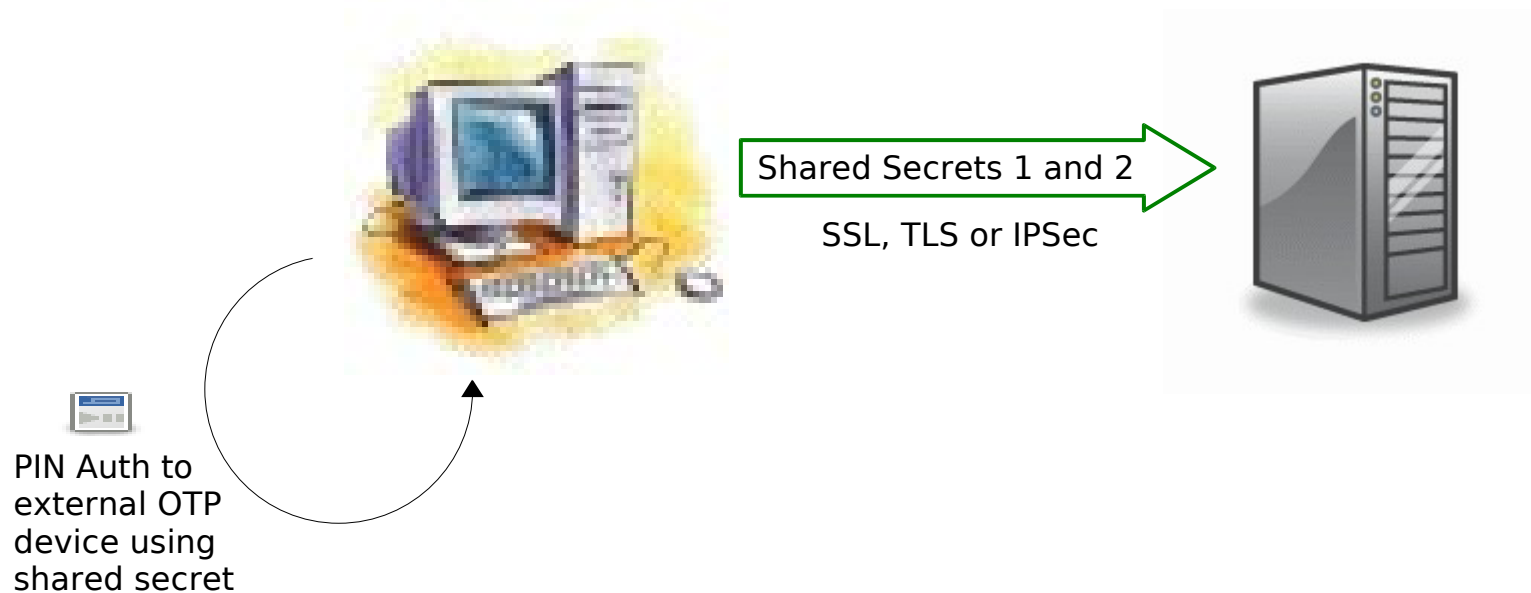
- Adds another shared-secret to IPF-2
- Can be compromised by multiple attacks:
 - Dictionary attacks, ~~network snooping~~, shoulder-surfing, keystroke loggers, phishing, social-engineering, rogue employee and technology-specific attacks (for biometrics)
- Compromise-blind
- Examples:
 - UserID-Password with biometric
 - UserID-Password with image-selection
 - UserID-Password with answer to question

- **Asymmetric-key** based authentication with **Private Key in a file**



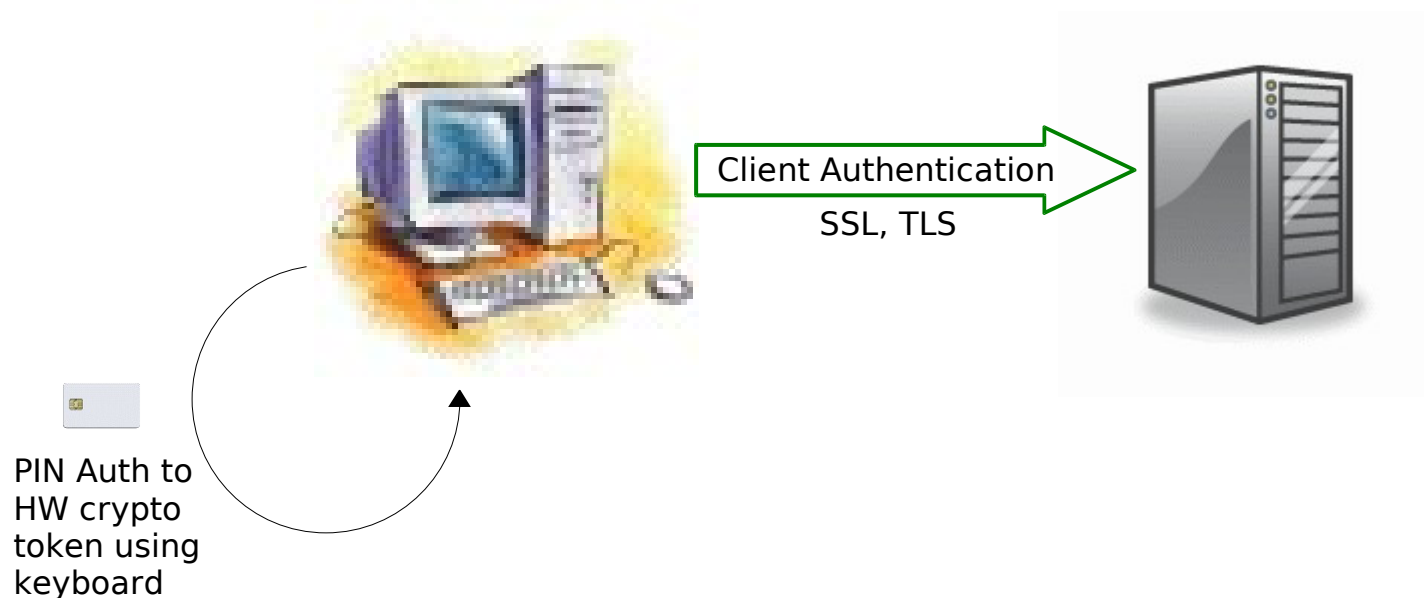
- Uses asymmetric cryptography – does not use a shared secret
- Uses a file-based cryptographic keystore
- Compromised by copying keystore AND:
 - Dictionary attacks, keystroke loggers
- Compromise-blind
- Examples:
 - X509 digital certificate with Private Key in a file
 - Public/Private key-pair with Private Key in a file

- **Multiple shared-secrets** based authentication **with** an external token and **with** network encryption



- Adds external hardware token for second shared-secret to IPF-3
- Can be compromised by multiple attacks:
 - Dictionary attacks, ~~network snooping~~, shoulder-surfing, keystroke loggers, phishing, social-engineering, rogue employee or technology-specific attacks (for biometrics)
- Partially compromise-blind; token loss/theft is immediately detectable
- Examples:
 - OTP token with UserID-Password
 - OTP token with biometric

- Asymmetric-key based authentication with **Private Key** generated and stored on **cryptographic hardware token** and using **keyboard** for authentication to token



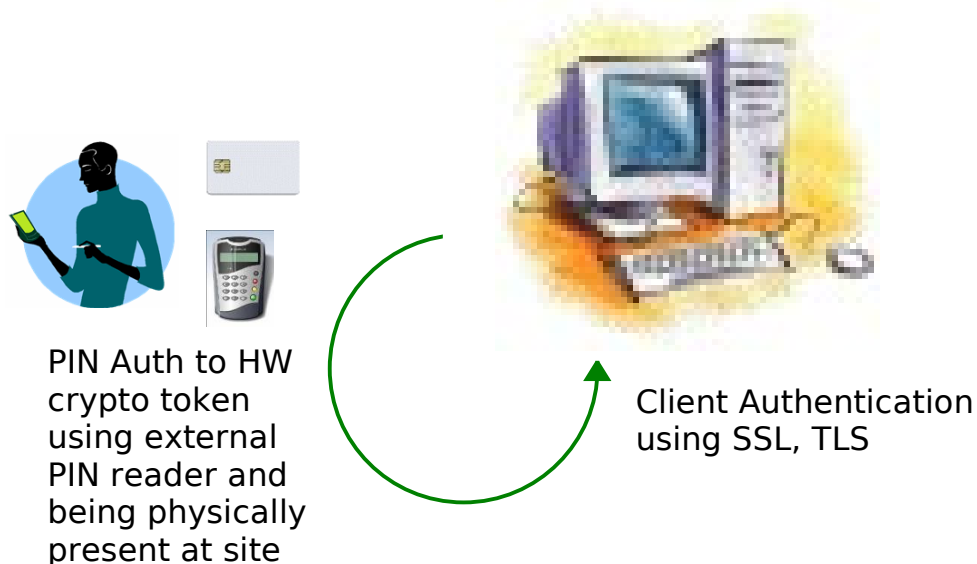
- Asymmetric cryptography – no shared secret
- Adds external hardware cryptographic keystore to IPF-4
- Compromised by:
 - Social-engineering attack
 - Keystroke-logging AND theft of token
- Client is not compromise-blind; but server can be until client certificate is revoked
- Examples:
 - X509 digital certificate with Private Key on token

- Asymmetric-key based authentication with Private Key generated and stored on cryptographic hardware token and using an **external PIN-pad** for authentication to token



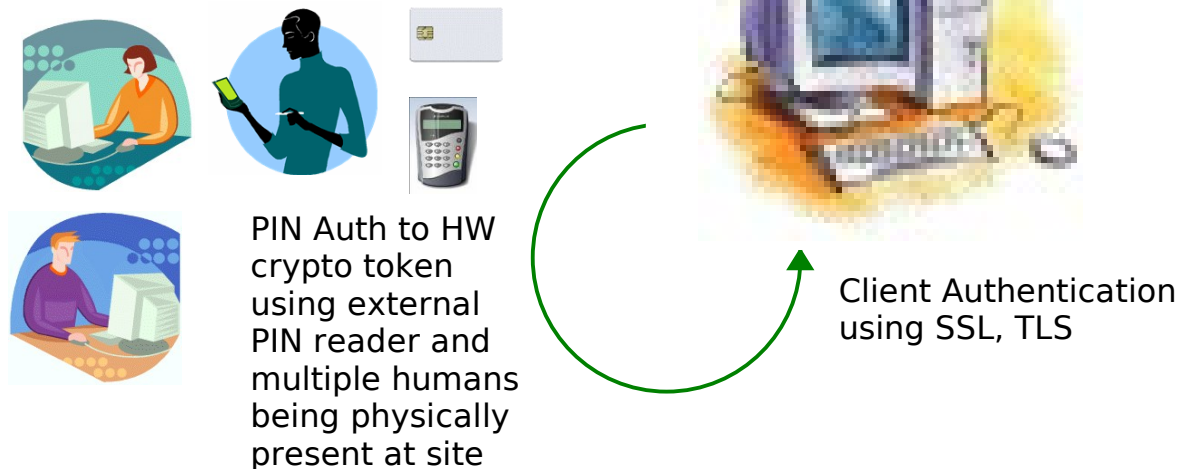
- Adds external PIN reader to IPF-6
- Compromised by: Social-engineering attack?
- Client is NOT compromise-blind; but server can be until client credential is disabled
- Example:
 - X509 digital certificate with Private Key on token with external PIN reader

- Asymmetric-key based authentication with Private Key on cryptographic hardware token using an external PIN-pad and **being physically present at the machine** where the resource exists and authentication is performed



- Adds requirement to be physically present at the authentication site, to IPF-7
- Compromised by:
 - Rogue employee
- NOT compromise-blind
- Example:
 - X509 digital certificate with Private Key on token with external PIN reader and requiring physical presence at authentication site

- Asymmetric-key based authentication with Private Key on hardware token, using an external PIN-pad, being physically present at the machine where authentication is performed and using **M of N control** for authentication to token



- Adds requirement of multiple humans to be physically present at the authentication site, to IPF-8
- Compromised by:
 - Collusion of rogue employees
- NOT compromise-blind
- Example:
 - X509 digital certificate with Private Key on token with external PIN reader and requiring physical presence of multiple humans at authentication site

- Does not exist; there is no perfect authentication mechanism

- No conflict with Liberty (including Identity Governance Framework), CardSpace or Higgins: they all require authentication using some credential at some point which can have an IPF rating
- Some overlap with NIST 800-63
 - Has a broader focus – Level of Assurance - which must look at process controls
 - Mixes technology and process controls – might be useful to define an *Identity Proofing Score* and combine it with IPF to create a compound value

- Validation of model
 - Are these levels sufficient? Or do we need more granularity?
- Probabilities of compromises of I&A technologies with specific IPF ratings based on historical breach data
 - Database of (anonymized) breaches with sufficient technical data to assist researchers
- Repository of IPF ratings for technologies
- Model for risk-assessment model and use of specific IPF technologies to manage risk

- Questions?
- Contact Information
 - www.strongauth.com
 - www.strongkey.org
 - info@strongauth.com
 - (408) 331-2000