Current Authentication Methods

Pro's and con's

Why pins #'s, passwords, smart cards and tokens fail

IDENTIFYING CREDENTIALS

In The Physical World

- Verified by Physical Inspection of the Credential by an Officer
- Photo & Signature "Tightly BIND" the Credential to the Person
- "TRUSTED" issuing authority is clearly displayed

In The Digital World

- How do I "TRUST" your Digital Identity credential?
  - Is it Tightly bound to you.
  - Does it come from a "TRUSTED" source.
- Unattended verification on a server

PROVIDING YOUR 'DIGITAL IDENTITY'

(aka AUTHENTICATION)

Something you Know
PIN's & Passwords

Weak PIN's and Passwords are Not Secure – *not tightly bound*

- 19XX
- Giants08

Strong Passwords are Typically Not Practical

- AX%$ght8
- Ths%#267wbch678z

+

- Different one for every site
- Change every 30 days
- Don't re-use
- Never write it down
- And there are still key-loggers

Match done in a "TRUSTED" Environment = The Server

Something you Have

Tokens or Smart Card

Identifying Credential either

- OTP's
- PKI

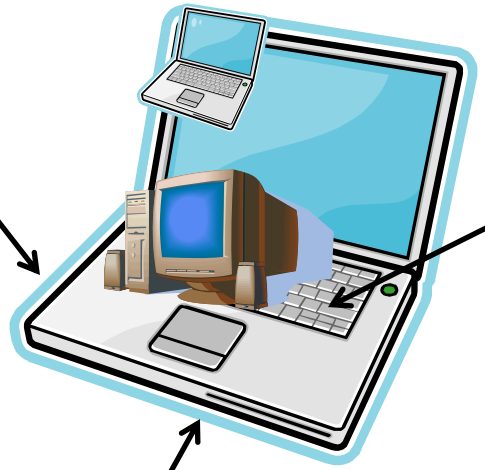
- Must be coupled with something you know, typically a **4 digit PIN** or something you are (Biometrics).
- Inherently Multi-Factor (2 factor)
- "TRUSTED" issuing authority + PIN matched on the "**TRUSTED**" Token

Something you Are
BIOMETRICS

- ***Tightest Binding to the USER***
- *Easiest to Use and Always with You*
- Types
  - Fingerprints
  - Iris
  - Face
  - Hand
  - Veins
- Can be inherently Multi-Factor (2 factor)
- Match should be done in a "TRUSTED" environment.

Multi- Factor for Enhanced Security

CLIENT (USER) COMPUTERS ARE NOT TRUSTED



USB Ports can be “Sniffed”

Key Logger logs Password entries

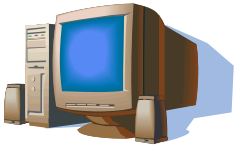
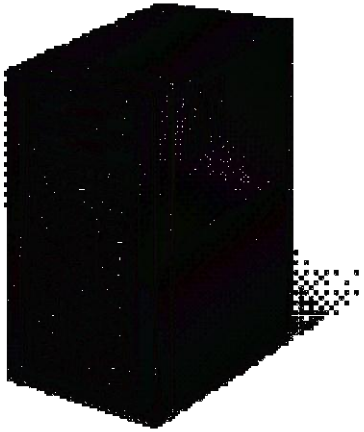
Malware Installed on HDD
- Algorithm Substitution
- Template Substitution
- Modified Output Result

PC’s Hardware Can be Hacked

- Easily downloadable debugging tools that can aid the hacker
- Multiple interfaces that can be attacked
  - USB Ports
  - Ethernet Ports
  - Web connections

WHO DO YOU TRUST?

- Trust is the key element of Security
- You only deal with people or things you Trust

TRUSTED	Typically NOT TRUSTED	Always TRUSTED
 User	  Client (User) Computer	 Enterprise Server
  TRUSTED Peripheral		

WHERE TO MATCH

Inflexis Trusted Peripheral	Client (User) Computer	Server
PRO ↑ Trusted for use in High Value Applications ↑ Centrally Managed and Provisioned ↑ Automatic Two Factor Authentication ↑ Mobile Flash Drive Data Protection Solution ↑ Compatible with multiple Credential Types Authenticating To different Servers ↑ Works even when not connected to the network protecting data & applications not on the network **CON** ↓ Higher initial acquisition cost visa-a-via Match on Client	**PRO** ↑ Lowest Cost **CON** ↓ Not Trusted for High Value Applications … MS only recommends usage for consumer convenience applications, not for Banking ↓ Not Centrally Managed	**PRO** ↑ Trusted for use in High Value Applications ↑ Centrally Managed and Provisioned **CON** ↓ Only works when connected to The network. Can revert to "Match On Client" when disconnected but then not Trusted ↓ Fingerprint is the Credential. Limited flexibility in working with Other credential ↓ Not inherently multi-factor ↓ No Mobile Flash Drive solution ↓ Higher initial acquisition cost visa-a-via Match on Client

SUMMARY

- Identity Management in the Digital World is Accomplished by Delivering a Credential that is:
  - Bound to the User
  - Securely Delivered from a “TRUSTED” Source

- The Inflexis ID Management System
  - Uses Fingerprint Biometrics to “TIGHTLY BIND” the credential to the actual User
  - Makes all decisions and delivers the credential from a “TRUSTED” Device (i.e. a “TRUSTED Peripheral”)
  - Encrypts the Transmission Channel