Using NIST SP 800-130 to Evaluate Existing Systems

NIST Cryptographic Key Management Workshop 2012

NIST, Gaithersburg, MD, USA


Anthony J. Stieber
mailto:anthony.j.stieber@gmail.com
Introduction
Disclaimer
Three Items
Item 1
Security Domain
Interoperation
Security Domain
Incompatibility
PKCS#11
Security Domain Virtualization?
Maybe.
Item 2
CKMS
Responsibilities
Designers
Implementers
Vendors
Procurers
Installers
Configuration Administrators
Security Domain Administrators
Item 3
Crypto Evaluations
Before

SP 800-130
SP 800-130
Design versus Evaluation.
Requirements become questions.
It’s big.
REALLY
It needs to be big.
It’s wide and deep.
“...perfection is attained
“...perfection is attained not when there is nothing more to add...”

Antoine de Saint Exupéry
Terre des Hommes (1939)
Translated into English as Wind, Sand and Stars (1939)

http://en.wikiquote.org/wiki/Antoine_de_Saint-Exup%C3%A9ry
“...perfection is attained not when there is nothing more to add, but when there is nothing more to remove...”
“...perfection is attained not when there is nothing more to add, but when there is nothing more to remove...”

Antoine de Saint Exupéry

Terre des Hommes (1939)
Translated into English as Wind, Sand and Stars (1939)
http://en.wikiquote.org/wiki/Antoine_de_Saint-Exup%C3%A9ry
85 pages -> 10
Lessons Learned
“...there is always a well-known solution to every human problem

H. L. Mencken

“The Divine Afflatus” in New York Evening Mail (16 November 1917)

“...there is always a well-known solution to every human problem—neat, plausible
“...there is always a well-known solution to every human problem—neat, plausible, and wrong.”
“...there is always a well-known solution to every human problem—neat, plausible, and wrong.”

H. L. Mencken

"The Divine Afflatus“
in New York Evening Mail (16 November 1917)
8 pages too big.
Bits of what?
Bits of security.
Confidentiality
Confidentiality and
Confidentiality and Integrity?
Crypto is hard.
Security is hard.
Information technology is hard.
Quality is Job 1
Quality is Job 1.1
Quality is Job 1.n
New draft.
Profiles.
Thanks.
NIST
My colleagues.
My management.
The evaluated.
Lessig method

Takahashi method

Modified.
My method.
My fault.
Thank You.
Questions?
Using NIST SP 800-130 to Evaluate Existing Systems

NIST Cryptographic Key Management Workshop 2012

NIST, Gaithersburg, MD, USA


Anthony J. Stieber
mailto:anthony.j.stieber@gmail.com
I can neither confirm nor deny your speculations at this time.