HOW TO SELECT YOUR FUTURE HARDWARE SECURITY MODULE (HSM)

Sector, October 3rd 2018
something about me

30+ years in the domain of applied cryptography, key management and cybersecurity
Designed and built the world-leading Luna HSM product line
Government, military and commercial background
Now the CEO/CTO of Crypto4A

CEO/CTO: Bruno Couillard
Co-Founder: JP Fiset
Co-Founder: Jim Goodman
Co-Founder: Brad Ritchie
What’s an HSM?

• Stands for:
  • **Hardware Security Module**

• Basic functions:
  • **Secure Key generation**
    • Internal Random Number Generator (RNG)
  • **Secure cryptographic algorithm processing**
    • Algorithm suite:
      • Symmetric
      • Asymmetric
      • Hashes
      • Key management
  • **Secure storage**
    • Quantity of keys
    • Access controls
HSM Form Factors

- Small portable devices:
  - Smart cards
  - USB tokens
  - PCMCIA

- Server peripherals
  - PCI, PCIe Cards

- Appliances
  - Desk top devices
  - Network-attached
Cybersecurity Complexity

• Government’s Best Practices:
  • CSE’s ITSG publications: ITSG-22/38 …, (Network Security Zoning)
  • CSE’s ITSG publications: ITSG-33 …, (IT Security Risk Management: A Lifecycle Approach)
  • NIST SP 800 (Computer Security 160+ publications)
  • NIST SP 1800 (Cybersecurity Practice Guides)

• Cryptography & Key Management Techniques:
  • Cryptographic Suites, Key Management approaches, Symmetric vs Public Key Infrastructures (PKI), Pay Attention to the looming Quantum Computing threat, etc...

• Assurance Approaches:
  • Software Alone, FIPS 140-2 validation, US’s Commercial Solutions for Classified (CSfC), Canada’s Medium Assurance, Military High Grade (i.e. Type 1)

• Products & Solutions Selection:
  • VPNs, Data Diodes, Data Guards, Network Filters & Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anti-Virus (AV), etc...

• Operational & Physical Security Constraints:
  • Security Policies, Network Operations Center (NOC), Security Operations Center (SOC), Personnel Clearances & Training, Physical and Logical Access Controls, Data Centers Security, Rack Security, etc...

• Life-Cycle Management:
  • Software Patch Management, Key Management Refresh, Personnel Training & Skill Upkeep,

• Security Assessment & Authorization (SA&A)
Cybersecurity Complexity

• Government’s Best Practices:
  • CSE’s ITSG publications: ITSG-22/38 ..., (Network Security Zoning)
  • CSE’s ITSG publications: ITSG-33 ..., (IT Security Risk Management: A Lifecycle Approach)
  • NIST SP 800 (Computer Security 160+ publications)
  • NIST SP 1800 (Cybersecurity Practice Guides)

• Cryptography & Key Management Techniques:
  • Cryptographic Suites, Key Management approaches, Symmetric vs Public Key Infrastructures (PKI), Pay Attention to the looming Quantum Computing threat, etc...

• Assurance Approaches:
  • Software Alone, FIPS 140-2 validation, US’s Commercial Solutions for Classified (CSfC), Canada’s Medium Assurance, Military High Grade (i.e. Type 1)

• Products & Solutions Selection:
  • VPNs, Data Diodes, Data Guards, Network Filters & Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anti-Virus (AV), etc...

• Operational & Physical Security Constraints:
  • Security Policies, Network Operations Center (NOC), Security Operations Center (SOC), Personnel Clearances & Training, Physical and Logical Access Controls, Data Centers Security, Rack Security, etc ...

• Life-Cycle Management:
  • Software Patch Management, Key Management Refresh, Personnel Training & Skill Upkeep, ...

• Security Assessment & Authorization (SA&A)
Zoning Example

Hypothetical Application

Legend:
HRZ Highly Restricted Zone
PAZ Public Access Zone
RZ Restricted Zone

Internet (Public Zone – PZ)
App Server
DB
Public Access Zone (PAZ)
Restricted Zone (RZ)
Highly Restricted Zone (HRZ)
Proxy Server
Network-attached HSM
Zoning Example

Hypothetical Application

Legend:

HRZ  Highly Restricted Zone
PAZ  Public Access Zone
RZ   Restricted Zone

User

App Server

Internet (Public Zone – PZ)

Public Access Zone (PAZ)

Restricted Zone (RZ)

Highly Restricted Zone (HRZ)

Proxy Server

TLS Secure Tunneling

TLS

Internet

App Server

DB
Network HSM - Zoning

Hypothetical Application

Internet (Public Zone – PZ)

Public Access Zone (PAZ)

Restricted Zone (RZ)

Highly Restricted Zone (HRZ)

User

App Server

DB

Proxy Server

Legend:
HRZ Highly Restricted Zone
PAZ Public Access Zone
RZ Restricted Zone

TLS Secure Tunneling

TLS
Cybersecurity Complexity

- Government’s Best Practices:
  - CSE’s ITSG publications: ITSG-22/38 ..., (Network Security Zoning)
  - CSE’s ITSG publications: ITSG-33 ..., (IT Security Risk Management: A Lifecycle Approach)
  - NIST SP 800 (Computer Security 160+ publications)
  - NIST SP 1800 (Cybersecurity Practice Guides)

- Cryptography & Key Management Techniques:
  - Cryptographic Suites, Key Management approaches, Symmetric vs Public Key Infrastructures (PKI), Pay Attention to the looming Quantum Computing threat, etc...

- Assurance Approaches:
  - Software Alone, FIPS 140-2 validation, US’s Commercial Solutions for Classified (CSfC), Canada’s Medium Assurance, Military High Grade (i.e. Type 1)

- Products & Solutions Selection:
  - VPNs, Data Diodes, Data Guards, Network Filters & Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anti-Virus (AV), etc...

- Operational & Physical Security Constraints:
  - Security Policies, Network Operations Center (NOC), Security Operations Center (SOC), Personnel Clearances & Training, Physical and Logical Access Controls, Data Centers Security, Rack Security, etc ...

- Life-Cycle Management:
  - Software Patch Management, Key Management Refresh, Personnel Training & Skill Upkeep,...

- Security Assessment & Authorization (SA&A)
Connection to NOC/SOC
Cybersecurity Complexity

• Government’s Best Practices:
  • CSE’s ITSG publications: ITSG-22/38 ..., (Network Security Zoning)
  • CSE’s ITSG publications: ITSG-33 ..., (IT Security Risk Management: A Lifecycle Approach )
  • NIST SP 800 (Computer Security 160+ publications)
  • NIST SP 1800 (Cybersecurity Practice Guides)

• Cryptography & Key Management Techniques:
  • Cryptographic Suites, Key Management approaches, Symmetric vs Public Key Infrastructures (PKI), Pay Attention to the looming Quantum Computing threat, etc...

• Assurance Approaches:
  • Software Alone, FIPS 140-2 validation, US’s Commercial Solutions for Classified (CSfC), Canada’s Medium Assurance, Military High Grade (i.e. Type 1)

• Products & Solutions Selection:
  • **VPNs**, Data Diodes, Data Guards, Network Filters & Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anti-Virus (AV), etc...

• Operational & Physical Security Constraints:
  • Security Policies, Network Operations Center (NOC), Security Operations Center (SOC), Personnel Clearances & Training, Physical and Logical Access Controls, Data Centers Security, Rack Security, etc ...

• Life-Cycle Management:
  • Software Patch Management, Key Management Refresh, Personnel Training & Skill Upkeep,...

• Security Assessment & Authorization (SA&A)
Cybersecurity Complexity

• Government’s Best Practices:
  • CSE’s ITSG publications: ITSG-22/38 …, (Network Security Zoning)
  • CSE’s ITSG publications: ITSG-33 …, (IT Security Risk Management: A Lifecycle Approach)
  • NIST SP 800 (Computer Security 160+ publications)
  • NIST SP 1800 (Cybersecurity Practice Guides)

• Cryptography & Key Management Techniques:
  • Cryptographic Suites, Key Management approaches, Symmetric vs Public Key Infrastructures (PKI), the looming Quantum Computing threat, etc…

• Assurance Approaches:
  • Software Alone, FIPS 140-2 validation, US’s Commercial Solutions for Classified (CSfC), Canada’s Medium Assurance, Military High Grade (i.e. Type 1)

• Products & Solutions Selection:
  • VPNs, Data Diodes, Data Guards, Network Filters & Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anti-Virus (AV), etc…

• Operational & Physical Security Constraints:
  • Security Policies, Network Operations Center (NOC), Security Operations Center (SOC), Personnel Clearances & Training, Physical and Logical Access Controls, Data Centers Security, Rack Security, etc …

• Life-Cycle Management:
  • Software Patch Management, Key Management Refresh, Personnel Training & Skill Upkeep,…

• Security Assessment & Authorization (SA&A)
Quantum Computers
Post Quantum Cryptography

- NIST PQC Effort
  - On-going worldwide search
  - Replace RSA, ECDH, ECDSA,... ASAP!

- Hash-Based Signature (HBS)
  - XMSS, HSS, SPHYNCS

![Diagram of HSS and Merkle Tree](image)
Quantum Entropy

Quantis Appliance seeding random numbers to SafeNet Luna HSM
Deployment Challenges

• Cybersecurity Challenges:
  • Insider threat
  • Patch management

• Quantum Computing Challenge
  • Over the Air update
  • Cryptographic agility

• Sensitive Data Processing
  • Unattended/Hostile deployments
  • Complex/Sensitive application deployments
Security Convergence

Selecting your Future HSM
Your Next HSM

- PQC Support
  - Secure Firmware Updates
  - Cryptographic Agility
- Quantum source of entropy
- Multi-zone capable
- Application business flow enforcement
  - Data Diodes, VPNs, Firewalls, Data Guards
- Secure application processing environment
- Advanced authority management
- Ease of deployment
- Remote management