

# *DataPower*

SECURITY HARDENING

SHIU FUN POON (@SPOON)

STSM (NERD) – SECURITY

SHIUFUN@US.IBM.COM

# Agenda

**Security is always excessive until it's not enough - Robbie Sinclair**

- Security
  - Authentication/Authorization
  - Transport vs Message level security
  - In-flight vs at rest protection
  - Misc: Auditing, High availability, Physical protection, CORS...
- DataPower
- Access to DataPower
- Usage of DataPower



# Security

- Authentication
  - Who are you
    - Which group you are in ?
    - What role are you in ?
  - Vouch by a reputable Identity Provider
    - User Registry, e.g. LDAP, Active Directory
    - Social provider (?)
  - Protocol/token
    - Basic Auth ? Username/password
    - OIDC ? JWT
    - Window ? Kerberos
    - WebServices/SSO ? SAML
    - Multi-Factors/StepsUp



# *Security*

- Authorization
  - What is allowed {user, resource, action}
  - Role Based Management
  - ACL
  - XACML
  - OAuth
    - User's permission for an application to access his/her resources

# Security

- Transport vs Message level security
  - Transport – is the pipe secure (point to point)
  - Message Level
    - Can the message be tampered ? If so, can it be detected
    - Who can read the message
- In-flight vs at rest protection
  - In-flight – when the message is left the destination, is it protected ?
  - At rest - when the message is stored, can it be tampered, modified without detection, can it be read by unauthorized user ?
- Misc: Auditing, High availability, Physical protection, CORS...

# Agenda

**Security is always excessive until it's not enough - Robbie Sinclair**

- Security
  - Authentication/Authorization
  - Transport vs Message level security
  - In flight vs at rest protection
  - Misc: Auditing, High availability, Physical protection, CORS...
- DataPower
- Access to DataPower
- Usage of DataPower

# How DataPower Gateways are unique?

## Purpose-Built, Secure Gateway

### ➤ Non-blocking event-driven I/O architecture

- ✓ Architecture similar to Nginx & Node.js
- ✓ Continued enhancements since 2002

### ➤ Parsers & compilers for JSON & XML processing written from ground-up with several patents

### ➤ No third-party arbitrary software can be installed

### ➤ Secure and optimized **JavaScript runtime** called GatewayScript

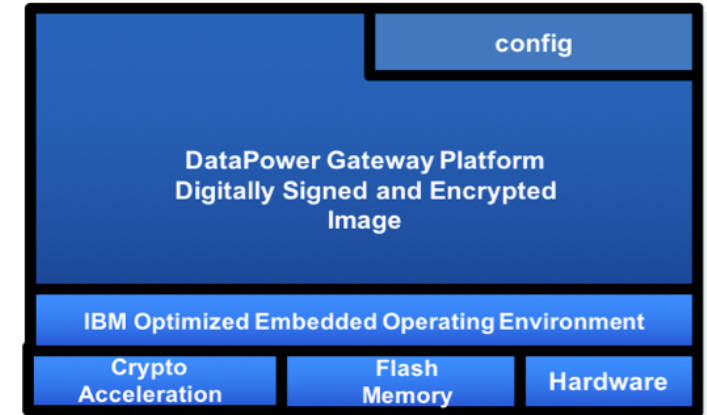
### ➤ Purpose-built, secure gateway image (all form factors)

- ✓ Single self-contained, signed & encrypted secure gateway image without external software dependencies
  - ❑ No arbitrary software
  - ❑ Security exposure minimized due to smaller vulnerability surface (few user-exposed and 3<sup>rd</sup> party components)
- ✓ High assurance, "locked-down" configuration
- ✓ Optimized, embedded operation system

### ➤ Physical security (physical appliance only)

- ✓ Sealed, tamper-evident case
- ✓ No usable USB, VGA, other ports
- ✓ Customized intrusion detection switch
- ✓ Trusted Platform Module
- ✓ Encrypted flash drive
- ✓ Cryptographic acceleration card
- ✓ Optional FIPS 140-2 level 3 certified Hardware Security Module

## API Connect Enterprise Gateway (Secure & Easy to Manage)



Single signed and encrypted image

# Agenda

**Security is always excessive until it's not enough - Robbie Sinclair**

- Security
  - Authentication/Authorization
  - Transport vs Message level security
  - In flight vs at rest protection
  - Misc: Auditing, High availability, Physical protection, CORS...
- DataPower
- Access to DataPower
- Usage of DataPower



# *Overall good practices*

- Protect physical access to DataPower
- Install your own credentials (e.g. replace the shipped profile)
- Separate management traffic from application traffic
  - Why 0.0.0.0 is bad
- Set up ACL on WebGUI, SOMA, ROMA, SSH
- Disable any port that is not used in production (webgui ? SOMA ? ROMA ?) leave cli as devops tool for production
- Setup RBM on DataPower to segregate action for different level of administrators (remember to have a backup administrator)

## *Overall good practices*

- Session time out of the WebGUI/cli interface (0 is bad)
- Reliable NTP configuration
- Offload log event
  - Log from command issued on DataPower thru cli ?
  - Log does rotate, so it is important to offload them periodically
- Track events that may require immediate attention
  - SNMP (like memory exhaustion, CPU high usage)

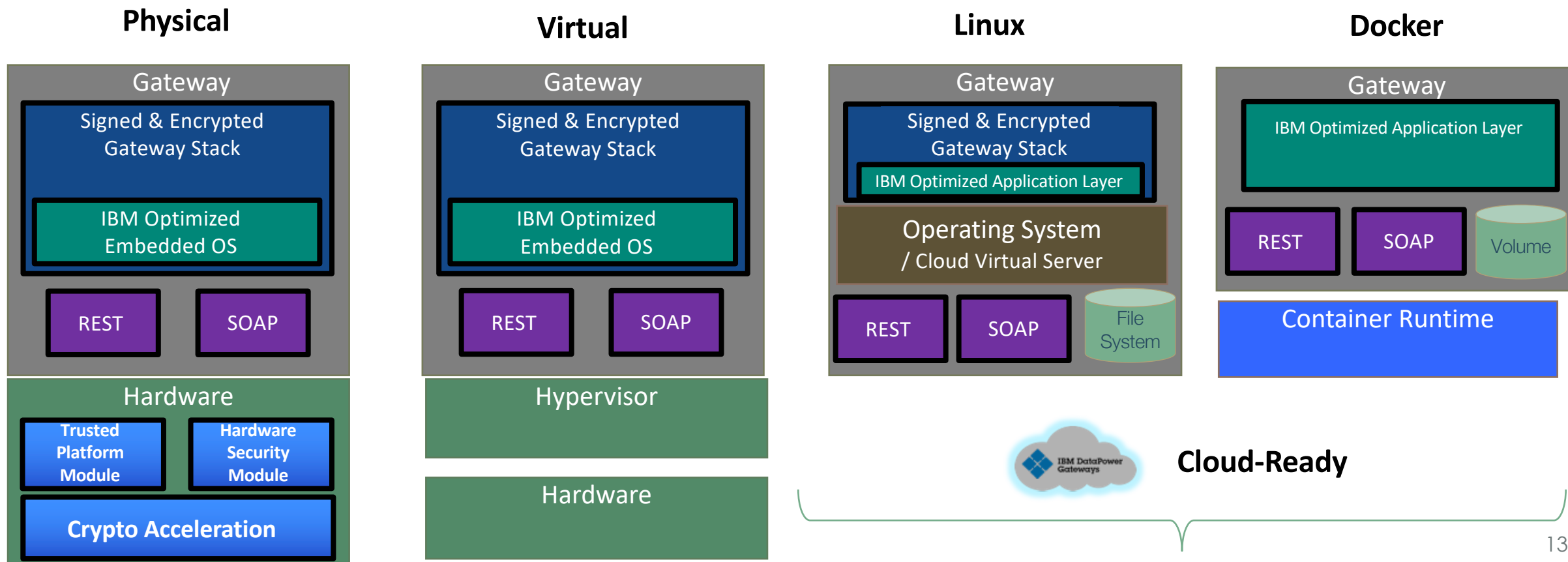
## *Overall good practices*

- Periodically backup your system with secure backup and restore
- HSM vs cert:/// vs sharedcert:/// vs local:///
- Set up certificate monitor for key material
- Validate certificate chain if TLS is used
  - CRL, Trust Store, OCSP
  - `Self & immediate` vs `pkix`

## *Overall good practices*

- Subscribe to IBM PSIRT for IBM DataPower
- Keep your firmware up to date

- **Physical appliances:** All-in-one (HW / SW), DMZ-ready with physical security including crypto acceleration, TPM, and optional hardware security module (HSM)
- **Software:** Docker container, Microsoft Azure, VMWARE ESX Server & Workstation, Citrix Xen, Amazon EC2, IBM ...





# *Balancing: flexibility vs hardware security*

## *Without Hardware, we lost*

- No embedded HSM/Crypto Card support
- No TPM support

## But we gain...

- Flexibility

## Still have

- Network HSM
- Public/Private key pair stored on z/OS NSS
- Roach motel of the key material, if configured properly
  - Key resides in cert:/// sharedcert:///
  - Private key, ltpa key
  - Only public key is viewable, exportable from the above directory
  - Password is protected with `Password Alias` object

## *To the other extreme (Docker)*



- Orchestrated with Kubernetes, Docker Swarm & Apache Mesos
- Easily to scale up and down based on the load
- By default : run as non-root (drouter:drouter)
- ADD/COPY file (deployment)
  - Modify/change permission to an existing file
    - Certificate/key anyone ?
    - Xslt/gatescript ?

# Best practices

- Do not use lower port (may require additional permission for port < 1024)
- COPY : Mounted file (pay special attention to permission, file ownership)
- Use `USER root` cautiously
- Version control the docker image
- Protect the system that will run the docker
- Protect the access to the orchestrator
  - E.g. kubeconfig if k8s

```
# src contains config and local.
# This form will change permissions of config and local
# to match the permissions in the build tree
#COPY ./src /drouter
# This form will leave the permissions of config and local
# alone, so they remain as IBM produced the image.
COPY ./config/ /drouter/config/
COPY ./local/ /drouter/local/

RUN find /drouter/config /drouter/local | xargs ls -ld

# This will work around a great number of migration problems
USER root
# set-user drouter ensures all directories drouter needs to
# write have appropriate permissions. The find..xargs..chmod
# command ensures every config file could be read. Note
# that █
RUN set-user drouter && \
    find /drouter/config /drouter/local | xargs chmod ag+r
USER drouter

RUN find /drouter/config /drouter/local | xargs ls -ld
```

# What does the gateway configuration look like

## Configure Password Map Alias

[Refresh List](#)

Name	Status	Op-State	Logs	Administrative state	Password	Comments
defreitas	saved	up		enabled	*****	
fred	saved	up		enabled	*****	
Ivan	saved	up		enabled	*****	
jonathan	saved	up		enabled	*****	
ralz	saved	up		enabled	*****	

Add

## Configure Crypto Certificate

This configuration has been added and not yet saved.

### Main

Crypto Certificate: alice [up]

[Apply](#) [Cancel](#) [Delete](#) [Undo](#)

Administrative state ☒ enabled ☐ disabled

File name   [Details...](#)

Password alias  [+](#) [...](#)

Ignore expiration dates ☐ on ☒ off

### Main

Crypto Key: webgui-key [up]

[Apply](#) [Cancel](#) [Delete](#) [Undo](#)


Administrative state ☒ enabled ☐ disabled

File name   [Upload](#) [Fetch...](#) [Edit](#)

Password alias  [+](#) [...](#)

```
FROM ibmcom/datapower:latest
ENV DATAPOWER_ACCEPT_LICENSE=true \
    DATAPOWER_WORKER_THREADS=2 \
    DATAPOWER_INTERACTIVE=true
COPY config/ /drouter/config/
COPY local/ /drouter/local/
RUN cd /root/secure/usrcerts \
    && ln -s /run/secrets/webgui_cert webgui-sscert.pem \
    && ln -s /run/secrets/webgui_key webgui-privkey.pem \
    && mkdir foo \
    && cd foo \
    && ln -s /run/secrets/server_cert server.crt \
    && ln -s /run/secrets/server_key server.key
EXPOSE 80 443 9090
```

So ...

- Key is protected by Password (which in turn is protected by Password Alias)
- Create a crypto file protected by Password
- Securely storing the file
- Lock down the access (auditing ) on who & when on changes to
  - dockerfile
  - docker-compose.yaml
  - Kubernetes
- Still Paranoid ?
  - Network HSM
  - z/OS NSS

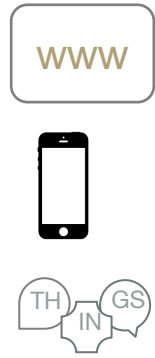


# Agenda

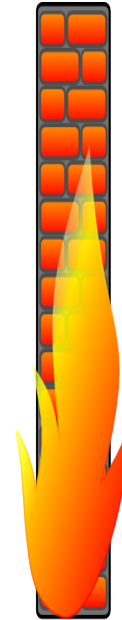
**Security is always excessive until it's not enough - Robbie Sinclair**

- Security
  - Authentication/Authorization
  - Transport vs Message level security
  - In flight vs at rest protection
  - Misc: Auditing, High availability, Physical protection, CORS...
- DataPower
- Access to DataPower
- Usage of DataPower

# Where to put a gateway



business logic and SoR  
functionality exposed  
outside of trusted zone



Trusted Zone exposed  
publicly

Increased traffic and load of  
incoming connections handling  
Rate limiting, validations, threat  
protections, OAuth

Works for internal facing  
projects



Consumers

DMZ

Trusted Zone

# *Consider the following protocols and standards for security*

- **Data format & language**

- JavaScript
- JSON
- JSON Schema
- REST, SOAP 1.1, 1.2
- WSDL 1.1
- XML 1.0
- XML Schema 1.0
- XPath 1.0, XPath 2.0 (XQuery only)
- XSLT 1.0
- XQuery 1.0, JSONiq

- **Security policy enforcement**

- OAuth 2.0, OpenID Connect, Social Login
- JWE, JWS, JWT, JWK
- SAML 1.0/1.1/2.0, SAML Tkn Profile, SAML queries
- XACML 2.0
- Kerberos (including S4U2Self, S4U2Proxy)
- SPNEGO
- RADIUS, RSA SecurID OTP using RADIUS
- LDAP versions 2 and 3
- Lightweight Third-Party Authentication
- Microsoft Active Directory
- FIPS 140-2 Level 3 (w/ optional HSM)
- FIPS 140-2 Level 1 (w/ certified crypto module)
- SAF & IBM RACF® integration with z/OS
- Internet Content Adaptation Protocol
- W3C XML Encryption
- W3C XML Signature
- S/MIME encryption and digital signature
- WS-Security 1.0, 1.1
- WS-I Basic Security Profile 1.0, 1.1
- WS-SecurityPolicy
- WS-SecureConversation 1.3

- **Transport & connectivity**

- HTTP, HTTP/2, HTTPS, WebSocket Proxy
- FTP, FTPS, SFTP
- WebSphere MQ
- WebSphere MQ File Transfer Edition
- TIBCO EMS
- WebSphere Java Message Service
- IBM IMS Connect, & IMS Callout
- NFS
- AS1, AS2, AS3, ebMS 2.0, CPPA 2.0, POP, SMTP (B2B Module)
- DB2, Microsoft SQL Server, Oracle, Sybase, IMS

- **Transport Layer Security**

- TLS versions 1.0, 1.1, and 1.2
- SSL versions 3
- SNI, PFS, ECC Ciphers

- **Public key infrastructure (PKI)**

- RSA, 3DES, DES, AES, SHA, X.509, CRLs, OCSP
- PKCS#1, PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#12
- XKMS for integration with Tivoli Security Policy Manager (TSPM)

- **Management**

- Simple Network Management Protocol
- SYSLOG
- IPv4, IPv6

- **Web services**

- WS-I Basic Profile 1.0, 1.1
- WS-I Simple SOAP Basic Profile
- WS-Policy Framework
- WS-Policy 1.2, 1.5
- WS-Trust 1.3
- WS-Addressing
- WS-Enumeration
- WS-Eventing
- WS-Notification
- Web Services Distributed Management
- WS-Management
- WS-I Attachments Profile
- SOAP Attachment Feature 1.2
- SOAP with Attachments (SwA)
- Direct Internet Message Encapsulation
- Multipurpose Internet Mail Extensions
- XML-binary Optimized Packaging (XOP)
- Message Transmission Optimization Mechanism (MTOM)
- WS-MediationPolicy (IBM standard)
- Universal Description, Discovery, and Integration (UDDI versions 2 and 3), UDDI version 3 subscription
- WebSphere Service Registry and Repository (WSRR)

# *Usage of DataPower for application/api protection*

- Use the purposely built services
  - Webservice proxy, MPGW, XML firewall, apigw ..
- Enable ACL
- Use the highest secure protocol for TLS (PFS is preferred)
- Disable unnecessary protocol on FSH
- Disable unnecessary method/verb on FSH
- Match rule should be as precise (PCRE)
- MPGW : skip backside !== terminate the call rule

# *Usage of DataPower for application/api protection*

- Schema protection
- Payload size protection (depth)
- SLM (rate limit)
- Time Skew for protected resource (the smaller the range, the better)
- Crypto material
  - HSM vs cert:/// vs sharedcert:/// vs local:///
- Listening interface, why 0.0.0.0 is bad
- Debugging implication (slow, and info leaking)



# *Usage of DataPower for application/api protection*

- TLS communication
  - Trust store mode
    - pkix
    - Self & immediate (byte2byte comparison)
  - CRL/OCSP ?
- Enable streaming if payload allow
  - DP is not designed/ideal for large payload
- Caching
  - DP's sweet spots is stateless
  - However if state is needed, size, HA implication needs to be considered
- Context variable between action
  - Set to null if not needed

# *Usage of DataPower for application/api protection*

- AAA framework
  - Make sure Authentication and Authorization step are set up appropriately
  - [note] as authorization can be set up for anonymous user

