Network traffic inspections, fasten your security belt

Niels de Vos
Senior Software Engineer
Red Hat Gluster Storage

ndevos@redhat.com

redhat.

Internet-of-Things and home-automation

- Great time for engineers to develop new devices that are connected to phone/table and/or the Internet
  - Music installations, lights, curtains, air conditioning, bath tubs, washing machines, cars …
- Main focus for hardware vendors on the functionality
- Often little to no attention to (network) security

redhat

NITTE

Agenda

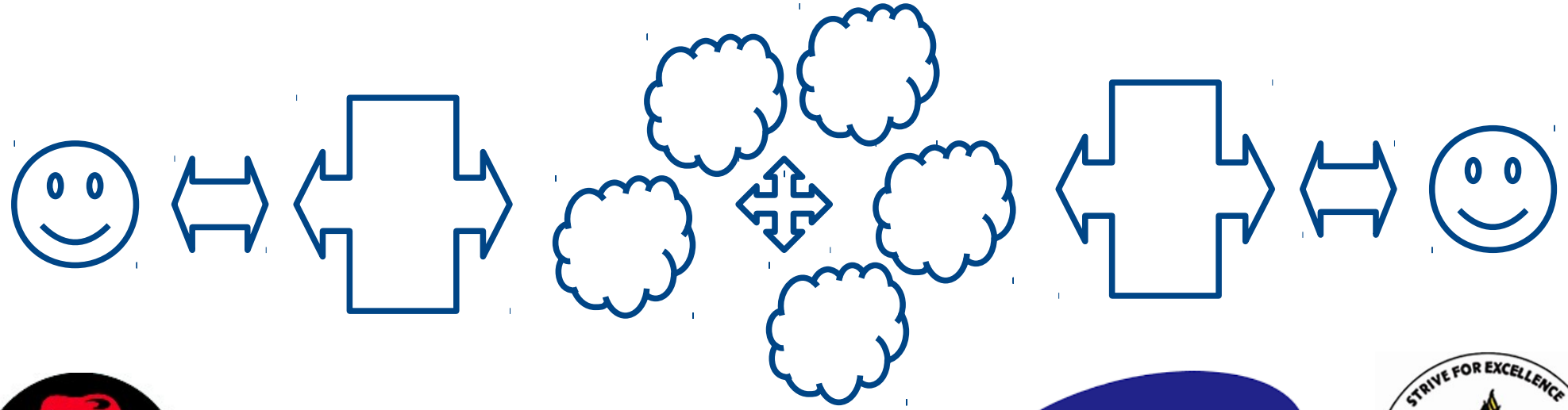
- Networking and internet basics
- Different levels of security
- Network layer security
- Protocol security
- Security in applications

redhat

NITTE

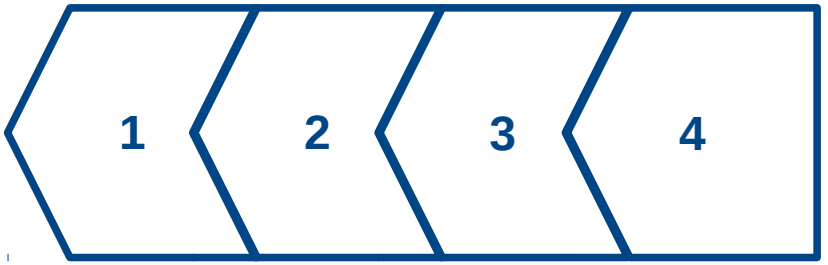
Networking and internet basics

- Many systems are involved in the connection from end user devices to applications running on servers
  - (Wireless) Access Points, proxies, gateways, routers
  - Local network, internet provider, cloud services



Networking and internet basics

- Encapsulation of contents
  - IP on top of Ethernet
  - TCP on top of IP
  - HTTP on top of TCP
  - HTML on top of HTTP



Networking and internet basics

- Capture network traffic on a router

```
# tcpdump -i virbr0 -s 0 -w /var/tmp/trace.pcap
```

- Open the capture file in Wireshark

```
# wireshark /var/tmp/trace.pcap
# tshart -r /var/tmp/trace.pcap
```

redhat

NITTE

Different levels of security

- Authentication
  - Verified identity, you are who you say you are
- Integrity
  - Verify that the data is correct and not modified
- Privacy
  - Outsiders can not understand the conversation (optional with Perfect Forward Secrecy)

redhat

NITTE

Networking layer security

- Virtual Private Network (VPN): IPsec, OpenVPN, ...
  - Network-to-network routing
  - Secure point-to-point connection
  - access through gateways
  - Application agnostic
- Tunnel: OpenSSH, stunnel, ...
  - Single IP-address + port connection security
  - Configuration for selected application

redhat

NITTE

Protocol security

- Implementation as functionality of the application
  - Needs application specific configuration

- Examples:
  - Secure Socket Layer (SSL)
  - Transport Layer Security (TLS)
  - Kerberos (krb5, GSSAPI)

redhat

NITTE

Security in applications

- Trusted login
  - Username/password
  - Certificate or other keys
- Signed/encrypted data
  - Email with GPG/PGP or s/MIME
- Validated source, Web of Trust
  - DNSSEC
  - Certificate chain, (Root) Certificate Authorities

redhat

NITTE

Thank you for your attention!