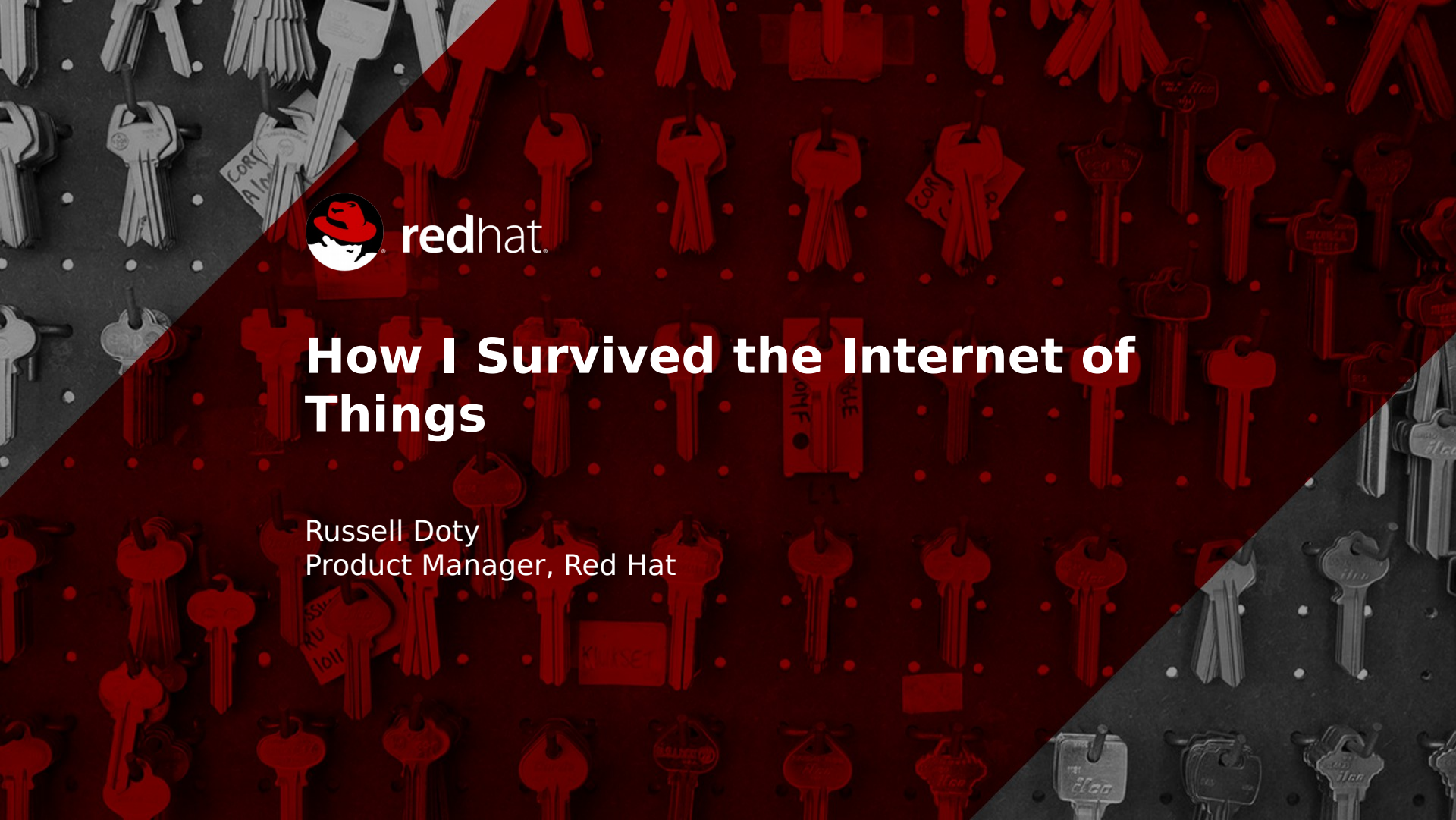
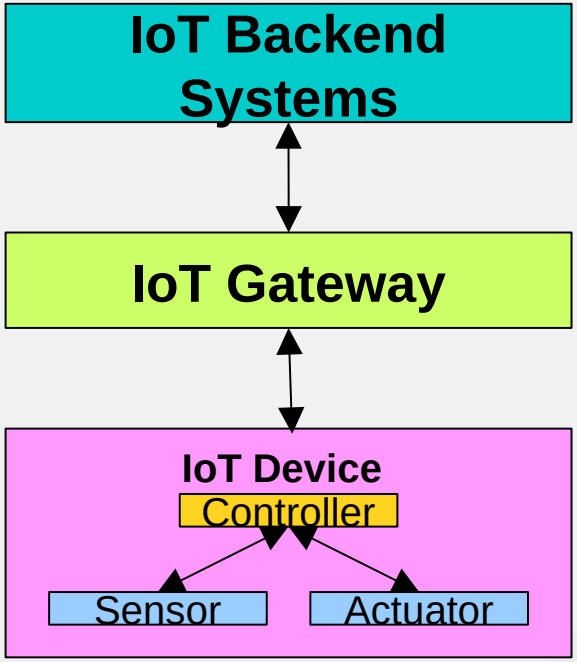


How I Survived the Internet of Things

Russell Doty
Product Manager, Red Hat

What is IoT?

- **Connection of IT systems to the physical world over a network connection for business value.**
  - IoT *Devices* are able to sense or modify the physical world. Often simple, low cost, low power; may be complex
  - IoT *Gateways* connect Devices to backend systems through the Internet
  - IoT *Backend Systems* perform value added business processing on data and apply control
- IoT is built on *connectivity*, *standards*, and *interoperability*
- IoT systems scale to tens of millions of devices, hundreds of thousands of gateways, and scalable cloud backends
- **Consumer IoT**: home automation & wearable
- **Enterprise IoT**: Transportation, Smart Cities, Smart Buildings, Smart Manufacturing, Retail, etc.
  - Our focus is on *Enterprise IoT*

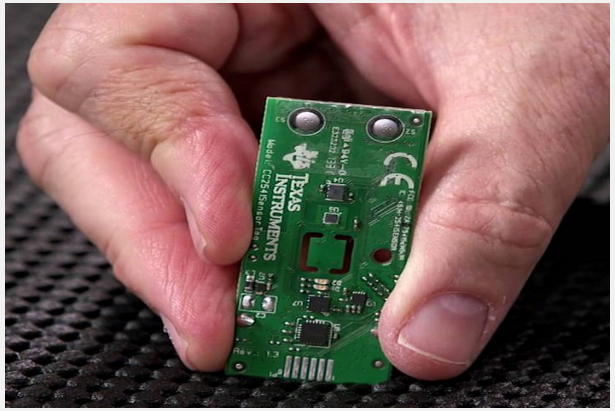


Is IoT New?

- Not really: SCADA, PLC, CNC, Shop Floor Systems, Environmental Monitoring, Intelligent HVAC etc.
- What is new?
  - Network instead of dedicated connections for devices
    - This changes everything!
  - Smart devices
    - This changes everything!
  - Unreliable communications (and systems)
  - New capabilities
  - Lower cost – many devices <$10
  - Greater scale & integration

What is New About IoT?

- ***Devices*** are full fledged computers
- ***Communications*** is over a network
  - Messaging oriented
  - M2M - Machine to Machine
  - New protocols
  - Shared
- 3-Tier Architecture: Device → Gateway → Backend
  - Backend typically cloud based
- Unreliable communications and systems
- Scale: Devices, Data, & Users
- System Life-Cycle



Enough Theory - Time for Real Experience

OCTOBER 2016: MASSIVE DDoS ATTACKS

- Botnet of 500K IoT Devices
  - 10M claimed?
- Largely IP Security Cameras & Routers
- Can take down large parts of the Internet
- Difficult to defend against

IP SECURITY CAMERAS

- Computer with Image Sensor
  - More compute power than the original moon program...
- Full general purpose OS
- Directly connected to the Internet
- Login: admin/admin
- 2 hardcoded maintenance accounts with root access
  - Well known
- Updates difficult to obtain

SOLUTION 1: SECURE THE CAMERAS

- Should do this
- Probably won’t work:
  - Customer ease of use expectations
  - Business model: Low cost, short product lifecycle, minimal updates
  - Installed base of 10M+ units
  - *Lack of Demand for security*
- Should be demanded for Industrial IoT Devices
  - Do **you** demand it?

IF YOU COULD SECURE THE CAMERAS: General Security Model

- Deter
- Detect
- Delay
- Respond
- Remediate
- Recover

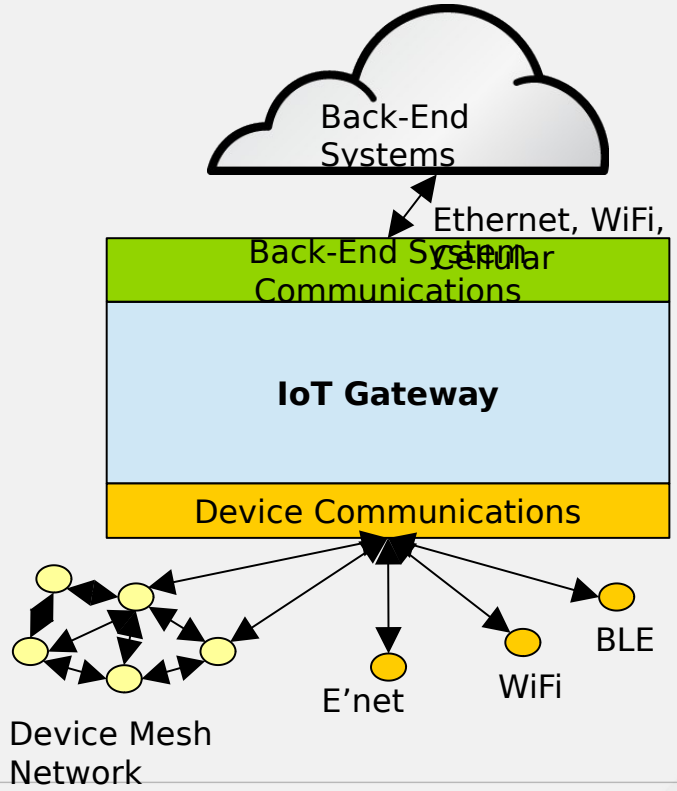
- Security is **combination** of software, configuration, operations, physical security, policies, and people

Implementing the General Security Model

- **Deter**
  - Harden system, patch, access controls
- **Detect**
  - Logging, monitoring, audit
- **Delay**
  - Harden, defense in depth, network security, people
- **Respond**
  - Operations
- **Remediate**
  - Remove malware, restore integrity, reinstall, restore data
- **Recover**
  - Business and operational recovery

SOLUTION 2:
SYSTEM APPROACH TO SECURITY

- Look at overall system
- Design in security
- Use *defense in depth*
  - *Prevention* **and** *Mitigation*
  - Technology
  - Process
  - People
- Spend an appropriate amount on security
  - Spend it wisely



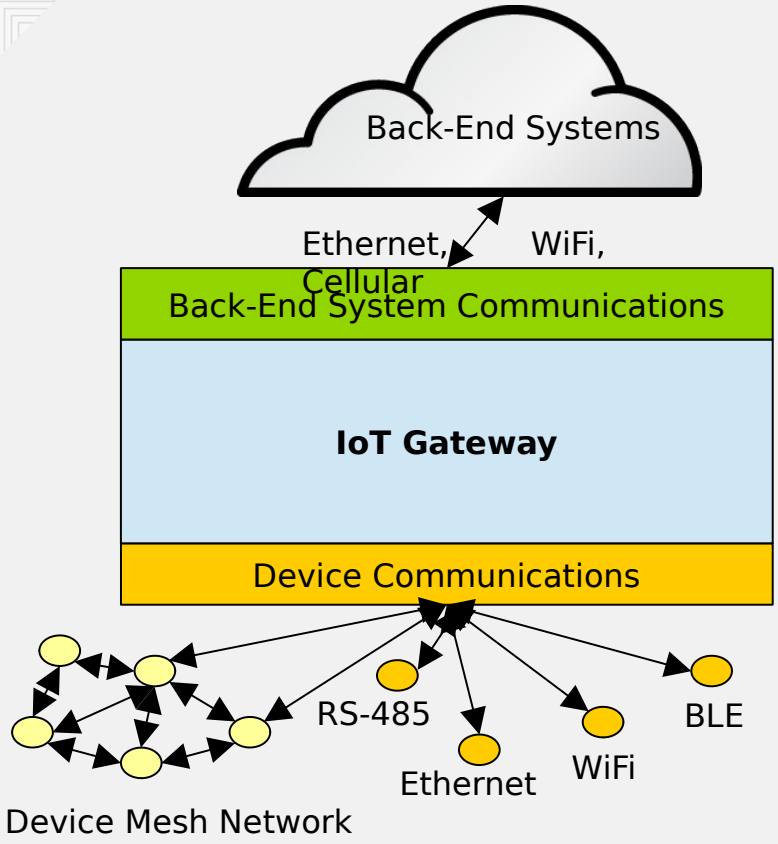
Key Elements of IoT Security

- Minimal Install
  - OS, Services, Applications
- Install, Update and Patch mechanism
  - SW integrity, SW Provenance
  - Robust – can't brick system
- Authentication
  - Multi Factor Authentication where possible
  - Includes authentication of Gateway & Devices
- Encrypted Storage
- Encrypted Communications
- Secure Configuration
- Secure Applications
- Secure Operation

Security Technology

- **Key Features:**
  - Access Control: SELinux
  - Policy Kit & Capabilities
  - Firewall
  - Systemd
  - Containers
  - Crypto & DNSsec
  - Secure build – RELRO, PIE, ASLR, Non-executable memory
  - Logging, Linux Audit Subsystem, Integrity Measurement Architecture, AIDE, OpenSCAP
  - Identity Management, authentication, SSO, HBAC, certificates

IoT SYSTEM ARCHITECTURE



Back-End Systems

Enterprise application/Enterprise security

Gateways

Outside the Data Center

Harden

Manage

Use to protect devices

Devices

Difficult to secure

Isolate

Harden where possible

Identity

Don’t trust!

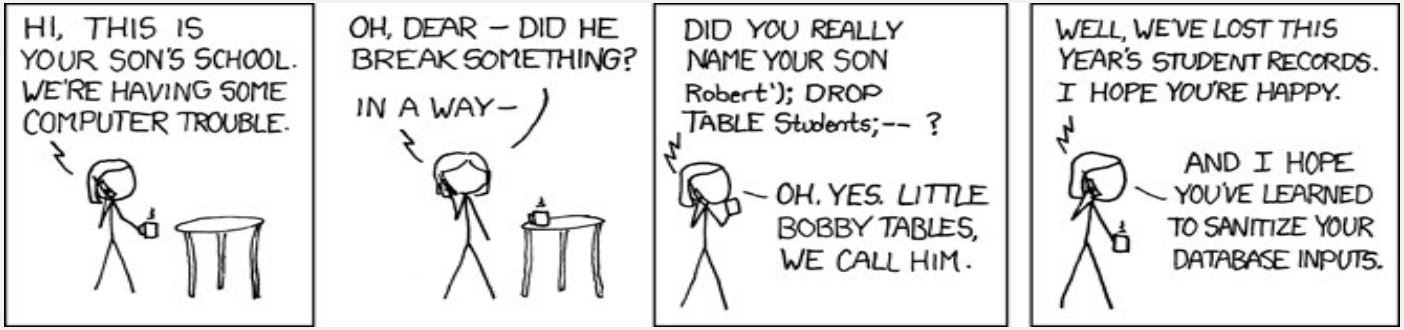
HARDENING IoT GATEWAY

- *Appliance* model – dedicated to specific function
- Isolate
  - Put on separate physical network
  - Put on separate VLAN
  - Use Firewall
  - Use VPN or TLS
  - Remove services
  - Control access
- Encrypt Storage
- Provide system identity
  - Recommend using certificates and SSSD
  - Unique certificate per system!

REAL SECURITY: IT'S IN THE APPLICATIONS

- Must develop secure IoT applications
  - Security experts ≠ system experts ≠ domain experts
- Key considerations:
  - Build on solid foundation – don't reinvent wheel
  - Taking advantage of compilers and libraries
  - Using static analysis tools
  - Packaging and deploying applications
  - Using crypto
  - Authentication and access controls (IdM, pam, SSSD)
  - Using system security features (SELinux, firewalls, handling privilege, Integrity Measurement Architecture, polkit, account management, systemd)

SANITIZE YOUR INPUT!



It's not just for databases:

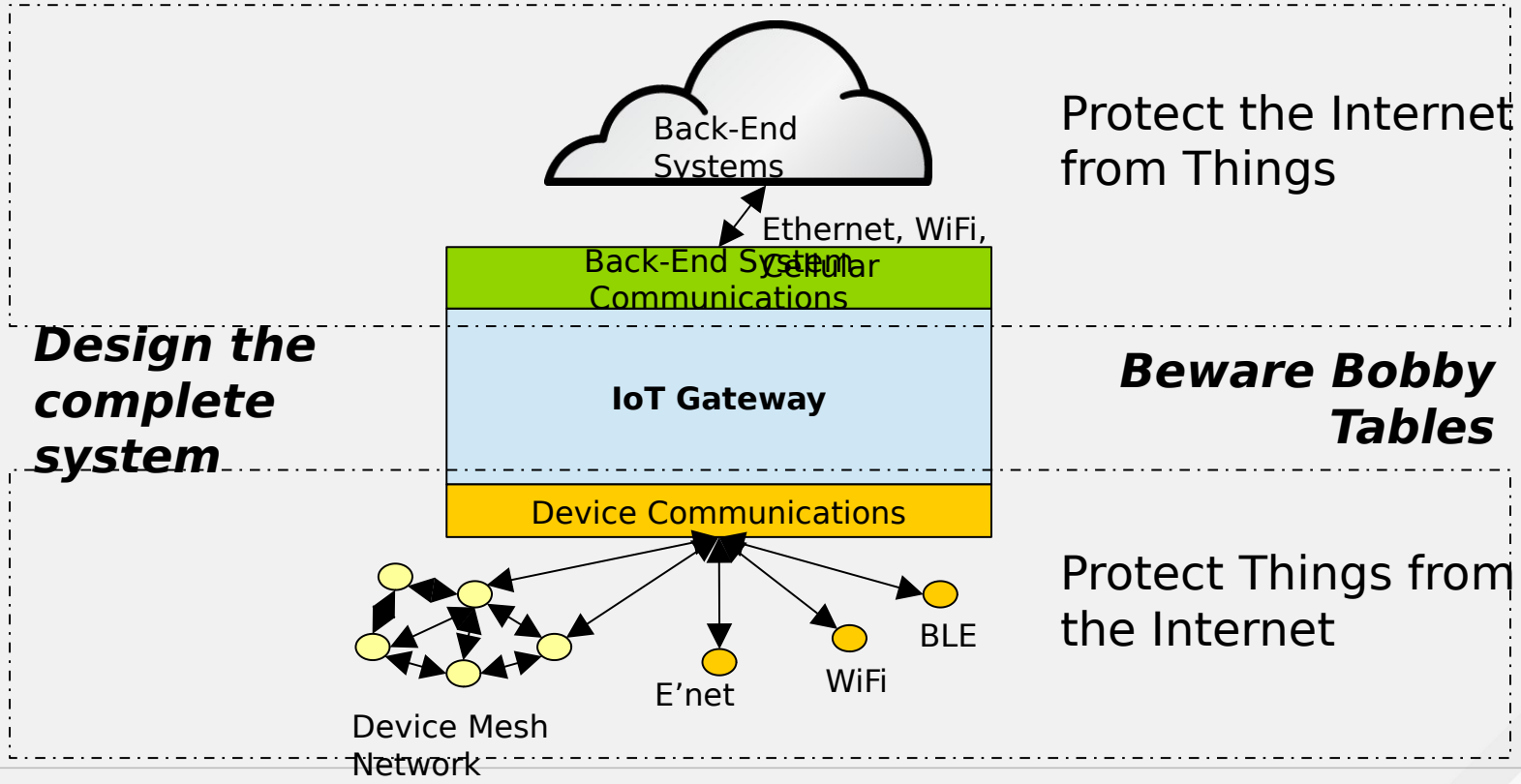
Temperature = "Four score and seven years ago our fathers brought forth on this continent" - *classic buffer overflow attack*

Read 4096 bytes of data from Temperature - *this is the HeartBleed exploit against OpenSSL*

Summary

- IoT - it’s computers all the way down!
- Traditional IT Security difficult to apply at scale
  - Business, economic and technology factors
- IoT Security Matters
  - Expect more bad things to happen
- IoT **In**security is the reality we have to deal with
- We can help improve IoT security
  - If we damage the economics or usability of IoT we will be ignored
- We have to look at total system design, not individual features
- Need **Resilience in Depth** - maintain the ability of systems to continue to operate correctly in the presence of multiple attacks and failures.

CONCLUSION


Back-End Systems
Ethernet, WiFi, Cellular
Back-End System Communications
IoT Gateway
Device Communications
Device Mesh Network
E'net
WiFi
BLE
Protect the Internet from Things
Design the complete system
Beware Bobby Tables
Protect Things from the Internet

WHAT I ACTUALLY DID...

- Purchased cheap grey market IP cameras from Amazon
  - 3MP, <$100, excellent video, solid mechanical build, no updates available
    Supported versions of these cameras ~$400
  - Yes, this is bad. I'm cheap. This is the reality we deal with.
  - At least I changed the default IP address and admin password.
- Connected to cameras over Ethernet using PoE. No WiFi.
- Placed cameras on a dedicated VLAN with no TCP/IP gateway
  - Cameras have no access to Internet
  - Cameras designed to connect directly to Internet - this is blocked
- Used a local video monitoring application instead of a Cloud based system
  - Dedicated system
  - Gateway with two NICs
  - Keep the Gateway and video monitoring application updated

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/
RedHatVideos