t

Identifying Security Best Practices for Your Supply Chain

Curtis Dukes

EVP & GM Security Best Practices

Center for Internet Security

Overview

- The Challenges
- The Evolving Destructiveness of Attacks
- A Realistic Response
- Call for a Transparency Center

The Challenges

- Fragile Supply Chain
- Increased Connectivity
- Opaque Hardware Life Cycle
- Infinitely Complex Software
- Monocultures
- Legacy Systems

No Easy Fixes

Fragile Supply Chain

- Just in time
- Switch suppliers mid production
- Global sourcing dependent on political stability

Temptation to Overextend

Increased Connectivity

- Putting everyday devices on the network
- Trying to make all devices “smarter”
- Keeping those devices supplied with updates with channel to vendors
- Carrying the ability to do our work on a device that walks out the door

Perimeter?

Opaque Hardware

- Parts sourced from
  - multiple assembly lines
  - multiple countries
- No oversight or insight into manufacturing process

Infinitely Complex Software

- s/w glued together with massive 3rd party, globally sourced libraries
- Interoperability of protocols is achieved with re-use of open source
- Most of the hardware requires software
- Backwards compatibility in OS is achieved with re-use of code

Software development processes?

Monocultures

- Operating systems for desktops and mobile devices
- Browsers
- Firmware in h/w controllers
- Firmware in baseband processors
- Cloud services?

Automation for Attackers

Legacy systems

- It’s the year 2000 problem as “groundhog day”
- No source, no expertise to move s/w forward
- Platforms become unsupported
- No budget for replacement, no will to replace
  - Who believes we will throw out unsupported IoT?

Poor to no life cycle planning

Attacks evolving

- From confidentiality to availability
- Stolen PII to holding systems and data hostage
- Fast attacks with destructive payloads
- Sophisticated attacks stealing economic and military information continuing

Threatening ability to operate

NotPetya

- Supply chain attacks exploit trust to obtain maximum privilege
- Patching paradox: time is of the essence, no time to inspect
- Monocultures allow attacks to spread rapidly
- Updates over the network have exposed the firmware layer to the application layer
- The number of devices with firmware is increasing

Capable of being more destructive

Reality check

- Cannot create products with no vulnerabilities
- Cannot verify all the life cycles of all the products
- Cannot evaluate products and find all vulnerabilities
- Cannot evaluate trust

Complexity Creates Reality

What is realistic?

- Foster accountability
- Quicker disclosure of attack vectors
- Focus on controls that contain spread
- Improved life cycle management (at board level!)
- Introduce inconvenience strategically

More transparency

Accountability

- Vendors need to disclose s/w development methodology adhered to
  - Disclose legacy or TPCs that did not adhere to process
- Signed s/w including updates

Today IT is another form of infrastructure

Disclosure

- Adjust what we are doing based on:
  - What attackers are doing
  - What works
- Pass rules to force quicker disclosure of how system was compromised
- GDPR fines will help but disclosure should be part of penalty
- Every compliance regimen should require disclosure to the community

It’s Public Safety

Fundamental Controls

- Decide which devices, software, and data are the most vital
- Isolate (simplify)
- Disable any unnecessary external protocols
- Patch (keep s/w and h/w inventories of critical components)
- Find your community and share
- Start now on migrating away from legacy solutions

Address prevention and proliferation

Life Cycle Management

- Any new capability should have an update and requirement plan
- All unsupported or soon to be unsupported platforms should be identified
- SLAs need to focus on availability of patches and commitment to platform migration
- In house development must also have plans for patches, updates, and retirement
- Accountability at the board level

No more rationalizing

Accept Helpful Inconvenience

- 2FA
- Latency: time for approval
- Separate chip for security functions (TPM, DSD)
- Separate device for VPN
- Hardware enforcement of tamper resistant back-ups
  - Make certain you can restore data and critical systems

Incur some pain for all the benefits

Recommendation

- Identify mandatory to implement security standards
- Clearinghouse for best practices with mappings between different ones
- Templates for Security SLAs to promote transparency and accountability
- Lab space where government and critical infrastructure can inspect code to verify any claims made by vendor

Transparency (Center)

Conclusion

- More accountability
- More transparency
- More data
- More planning
- Less convenience

Power always has its price