Mining/Firmware - secure embedded systems design

James Hilliard - james.hilliard1@gmail.com

Firmware Security

- Exploit mitigation
- Web interface security
- Attack Surface mitigation
- Signature validation of updates
- Vulnerability patching
- Reproducible builds
- Source code auditing
- Supply chain attack prevention

Manufacture Firmware Backdoors

- Often hard to detect
- Potential for wide impact on Bitcoin network
- Can be used to shut off or divert hashpower
- Can cause permanent hardware damage
- Can be difficult to regain control of hardware

Antbleed

- Widely publicized kill switch that Bitmain added to Antminer firmware
- Discovered and patch years after miners were released
- Transmitted serial numbers to Bitmain servers over the internet
- Was designed as an anti-theft feature
- Unencrypted raw TCP socket
- Can be activated by anyone controlling auth.minerlink.com

d-ddos

- Predates antbleed
- Designed as a ddos mitigation tool when Antpool was being attacked
- AES encrypted with static key
- Unauthenticated
- Can reconfigure pools remotely
- Can be activated by anyone controlling d-ddos.antpool.com

Why open source miner firmware is critical to the security of the Bitcoin network

- Bitcoin network's security model depends upon miners being under decentralized control
- Backdoors give control of miners to the manufacturer
- Poorly designed backdoors give control of miners to hackers
- Unpatched security vulnerabilities risk miners being taken over by hackers
- Manufacturers have a poor track record when it comes to handling security vulnerabilities
- Closed source firmware makes it difficult to introduce new more secure mining protocols
- Bugs could cause miners to fail in unexpected ways such as not being able to mine blocks with a stratum difficulty above a certain value