VCRI

THE VALUE CHAIN
RISK INSTITUTE

WOSEC DALLAS

Harvest Now, Forge Later

Post-quantum crypto for people with a day job.

Joshua Marpet

WHO'S TALKING

Joshua Marpet

- Founder and President, The Value Chain Risk Institute (a nonprofit)
- Leads the IANS Post-Quantum Crypto Center; IANS Faculty
- Co-host, Security Weekly; product security engineer
- Ex-cop, ex-firefighter, BSides Delaware organizer

Research and slides with Cairn Viktor, Joshua's AI research partner (built on Anthropic's Claude).

THE SHORT VERSION

A big enough quantum computer breaks the math under RSA and elliptic curve.

That's almost every public-key system you run: TLS, VPN, SSH, SSO, code signing, certificates. Your AES-256 is fine.

WHEN?

Nobody knows.

Estimates keep shrinking. 2025: RSA-2048 with under a million noisy qubits, in under a week. 2026: Google says the elliptic curve behind P-256 falls to under 500,000, in minutes. A good plan doesn't bet on a date.

Gidney, arXiv 2505.15917 (May 2025); Google Quantum AI, 31 Mar 2026

THE GOOD NEWS

The replacements already exist

- NIST published the first post-quantum standards in August 2024: **ML-KEM** (key exchange), **ML-DSA** and **SLH-DSA** (signatures)
- Your browser is probably using one right now: Chrome and Cloudflare turned on hybrid post-quantum key exchange, and about 70% of browser traffic Cloudflare sees is protected. Only about 15% of servers behind it are.
- There's a retirement schedule: RSA-2048 deprecated after 2030, all RSA and elliptic curve disallowed after 2035 (NIST draft, which OMB now tells agencies to follow)
- Federal agencies have deadlines now (EO 14412, OMB M-26-15). If you sell to them, a contract rule has been ordered.

NIST FIPS 203, 204, 205 (13 Aug 2024); NIST IR 8547 ipd (Nov 2024); Cloudflare blog, 29 Sep 2026; EO 14412 (Jun 2026); OMB M-26-15

1

Two attacks

Everyone talks about the first one. The second one is worse.

ATTACK 1: HARVEST NOW, DECRYPT LATER

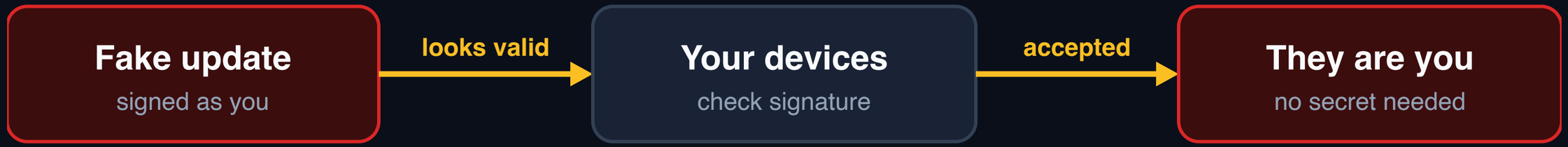
They copy your encrypted traffic today and read it once they can.



This matters if a secret has to stay secret for 10+ years: health records, M&A, government, anything with a Social Security number.

ATTACK 2: FORGE LATER

They don't read your secrets. They become you.



Break the math under a signature and you can mint SSO tokens, certificates, Kerberos tickets and signed software that everything trusts.

WHY FORGING IS THE ONE THAT HURTS

You've already seen the preview

- Golden SAML and certificate-services abuse already forge identity today, wherever PKI is misconfigured
- A quantum computer removes the word "misconfigured."
- Decrypting gets an attacker your data. Forging gets them your keys to everything.

Attacker-perspective framing: public IBM X-Force Red briefings by Dustin Heywood (EvilMog) and Chris Thompson

SO WHY START NOW?

X + Y > Z

How long it must stay safe + how long migration takes > time until a quantum computer?

Then you're already late.

Mosca's inequality (Michele Mosca, University of Waterloo)

THE QUIET PROBLEM

That device you're buying this year has its trust baked into hardware.

Firmware signing keys in ROM, medical devices, OT, cars. It will still be running when Q-Day comes, and you can't patch the root.

2

What to do Monday

One job for everybody in this room.

IF YOU'RE A PRACTITIONER

Find the crypto. You can't migrate what you can't find.

- Inventory where RSA and elliptic curve live: certificates, SSH keys, code signing, identity providers, VPNs, HSMs
- Don't forget what's embedded: devices, OT, vendor appliances
- Ask for a CBOM (cryptography bill of materials, CycloneDX) the way you ask for an SBOM
- Triage: what has to stay secret 10+ years, and what signs things everyone trusts?

IF YOU'RE AN EXECUTIVE

Put it in the contract

- "When do you ship post-quantum, and is it on by default?"
- "Can you swap algorithms without a forklift upgrade?" (That's crypto-agility.)
- "What in your product can't be upgraded?"
- Every renewal that skips these questions locks in the old math for another contract term

IF YOU'RE ON SUPPORT OR THE HELP DESK

Know what breaks

- Post-quantum keys and signatures are bigger: an ML-DSA signature is about 3.3 KB, an elliptic curve one is 64 bytes
- Old clients, middleboxes and appliances can choke on bigger handshakes and certificates
- Old devices that can't update will fail, or quietly stay on the old math
- When a weird TLS failure shows up after an upgrade, think post-quantum first

FIPS 204 (ML-DSA-65 signature: 3,309 bytes)

IF YOU TRACK ONE NUMBER

Crypto-agility coverage

The share of your systems that can change algorithms without code changes or new hardware. It's the best sign you'll survive this migration, and the next one.

VCRI

THE VALUE CHAIN
RISK INSTITUTE

THANK YOU, WOSEC DALLAS

Find it. Ask for it. Make it swappable.

Joshua Marpet · info@valuechainrisk.org · valuechainrisk.org