

Solutions For The Digital Evidence Lifecycle[®]



TACC1441 Hardware Accelerator

Accelerated Password Recovery

September 27, 2007

- What is a Tableau Hardware Accelerator?
- Reasons for Accelerated Password Recovery
- Tableau – AccessData Collaboration
- Dictionary-Based Password Recovery
- Performance Benchmarks
- Deployment / Use Cases
- How to Buy
- Q&A / Wrap-up



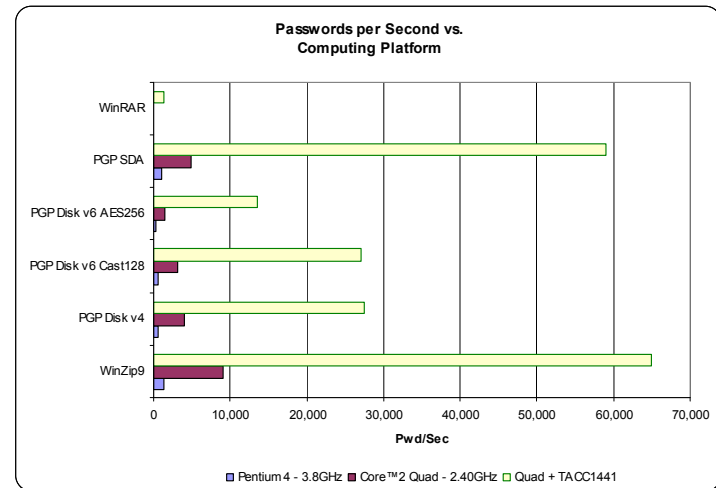
- **Massively Parallel Hardware**
 - Works on many computations at the same time.
- **Plug In & Go!**
 - Works with AccessData PRTK and DNA software
 - Requires special AccessData license.
 - Field-updatable
 - Future algorithms

U.S. & Foreign Patents Pending

1. Reduce password recovery times.
2. Increase chances of successful password recovery.
3. Reduce number of computer systems dedicated to password recovery.
4. Better use existing password recovery computers & clusters.
5. Reduce Total Cost of Ownership (TCO).

Find Passwords in...

One Day or One Month?



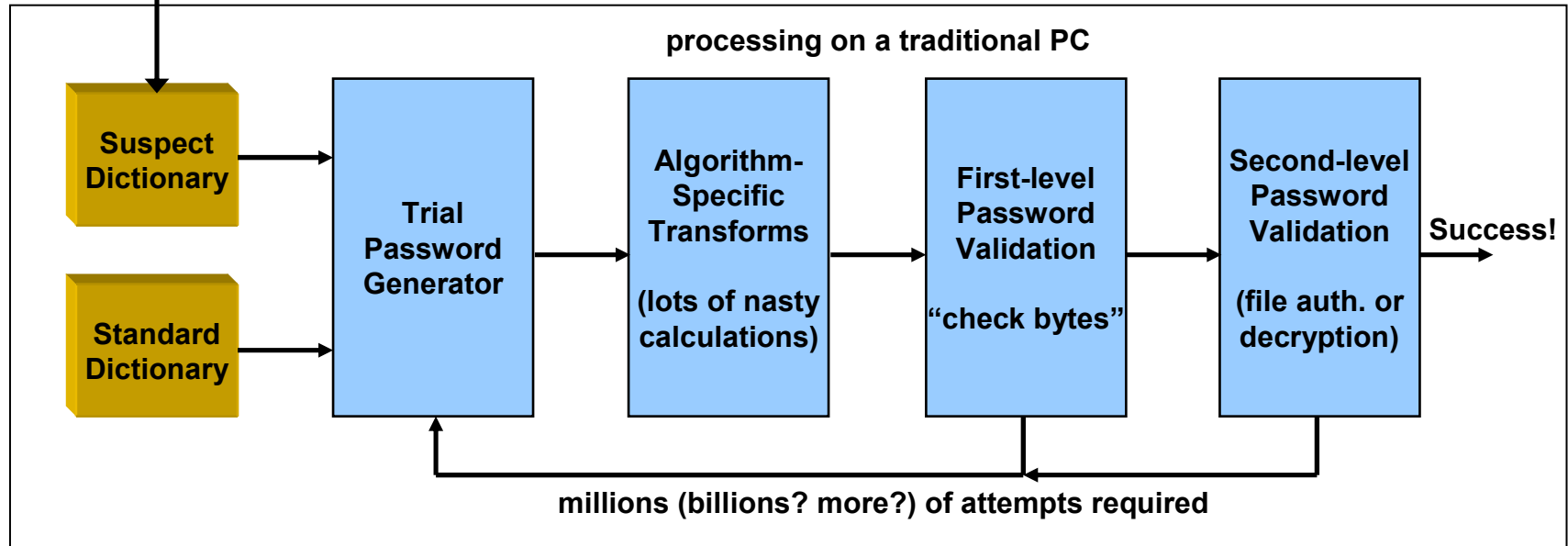


- Collaboration between AccessData & Tableau
 - AccessData: Password recovery expertise
 - Tableau: Forensic hardware device expertise
- Milestones
 - First public demonstration at Techno Security in June, 2007.
 - First production deliveries in September, 2007.

Dictionary-Based Password Recovery



Suspect Computer

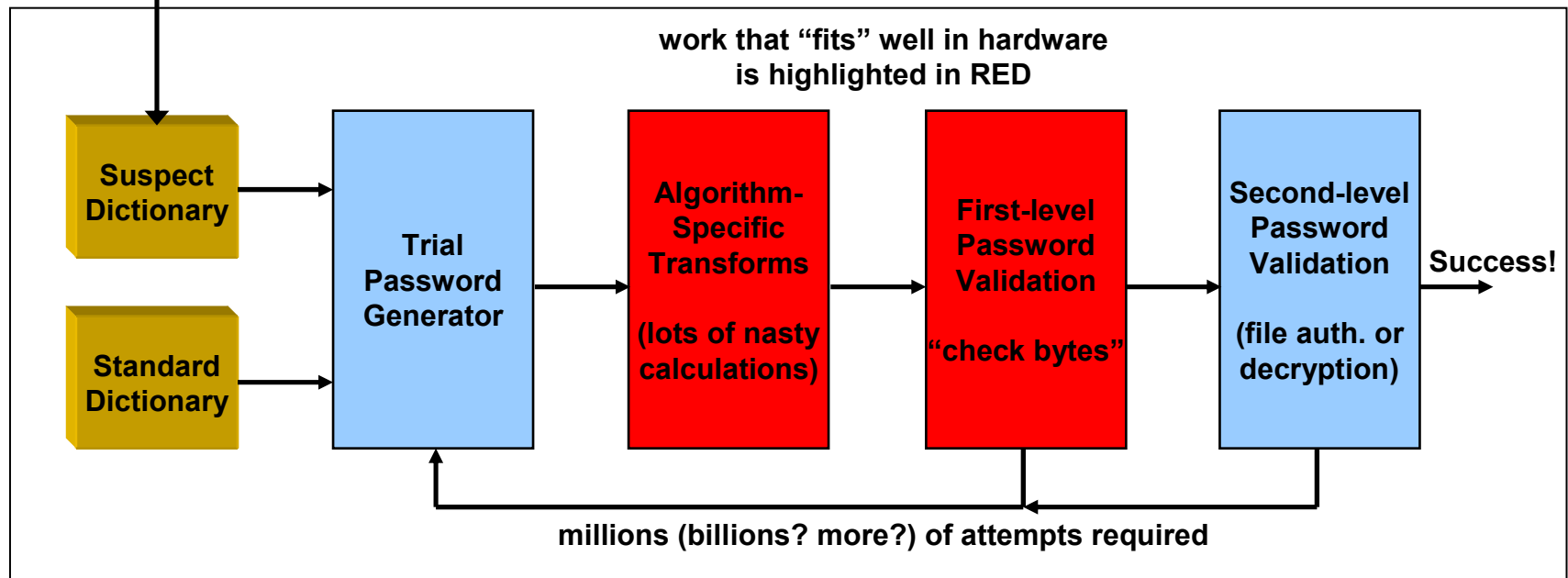


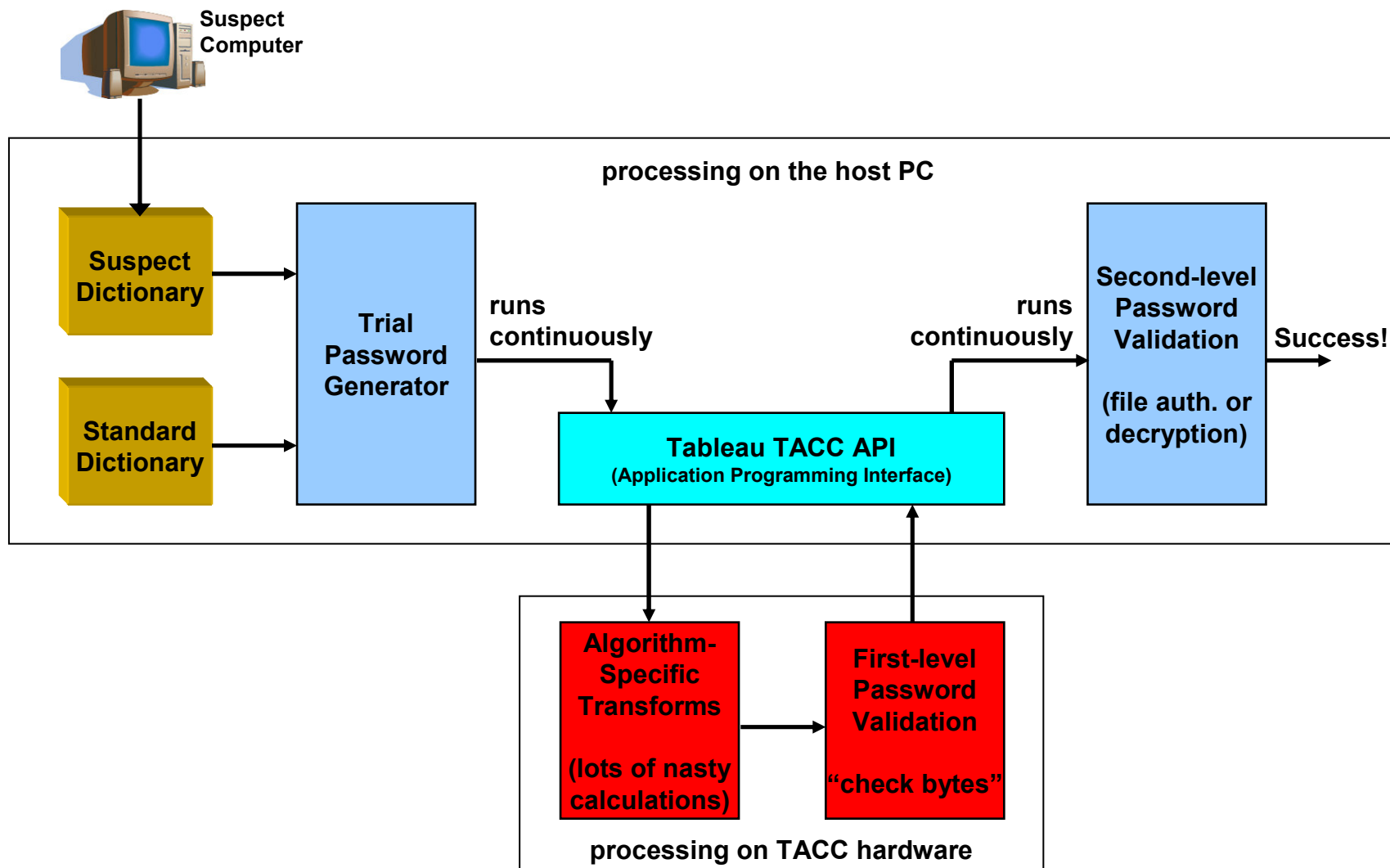
- Password / encryption schemes use password *key transformations*.
 - Designed to be computationally “expensive”.
 - Popular transformations based on SHA-1 hashing.
 - A modern Intel-based computer might be able to do 2 – 20 million SHA-1 transformations / second.

- Transformations fit well in FPGA hardware
 - FPGA = Field Programmable Gate Array
 - Like an ASIC (Application Specific IC), but re-configurable
 - A single “compute engine” inside an FPGA can do 1 million or more SHA-1 hashes per second.
 - Many “compute engines” can be implemented on a single accelerator...running in parallel.
- A single hardware accelerator might have dozens to hundreds of compute engines



Suspect Computer

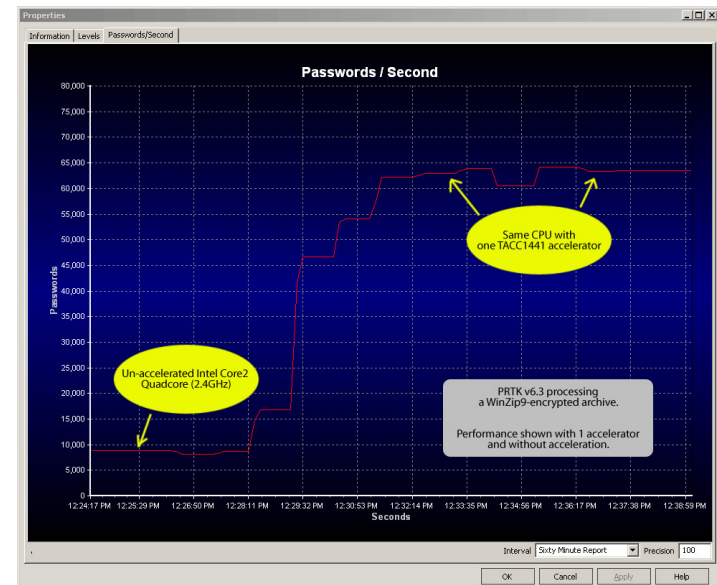


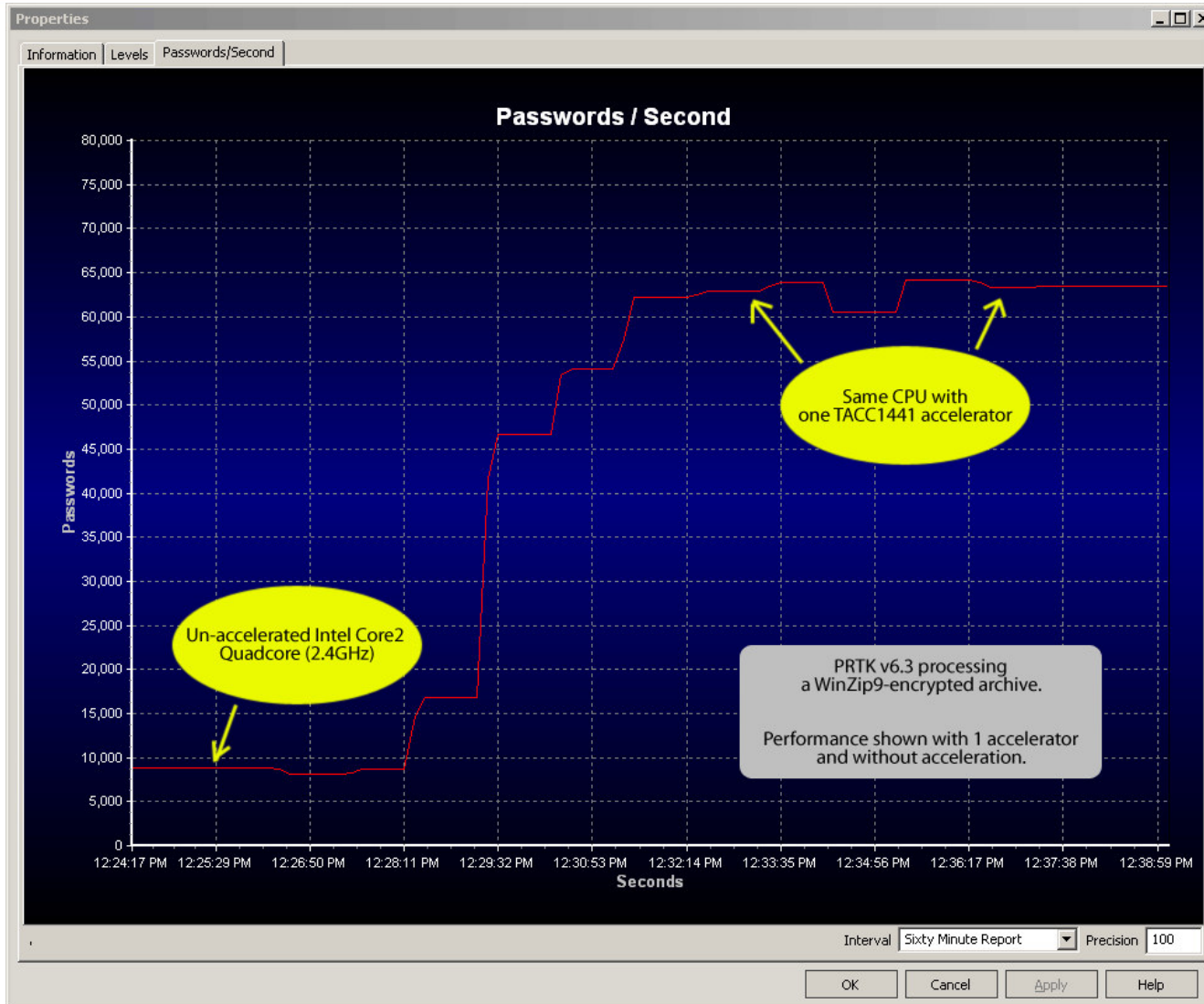


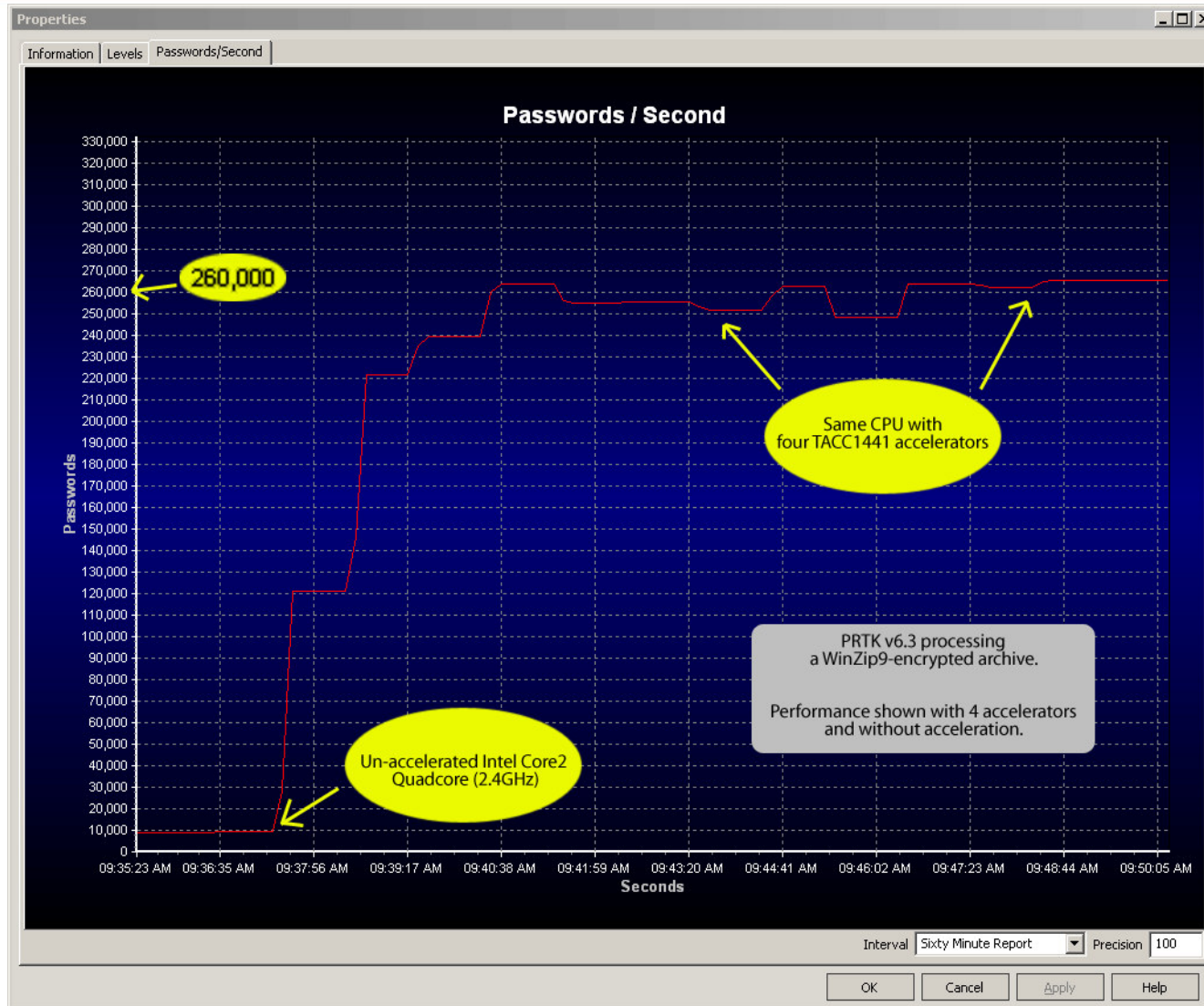
- **Current Intel CPUs**
 - 2-20 million SHA-1 hashes per second
 - 1,000-10,000 WinZip9 passwords per second
 - PGP and WinRAR are even slower
- **First generation Tableau hardware accelerator**
 - 120 million+ SHA-1 hashes per second
 - 60,000+ WinZip9 passwords per second
 - PGP and WinRAR scale similarly
- **TACC1441 Hardware acceleration yields 6x – 60x gain in performance over current Intel CPUs**

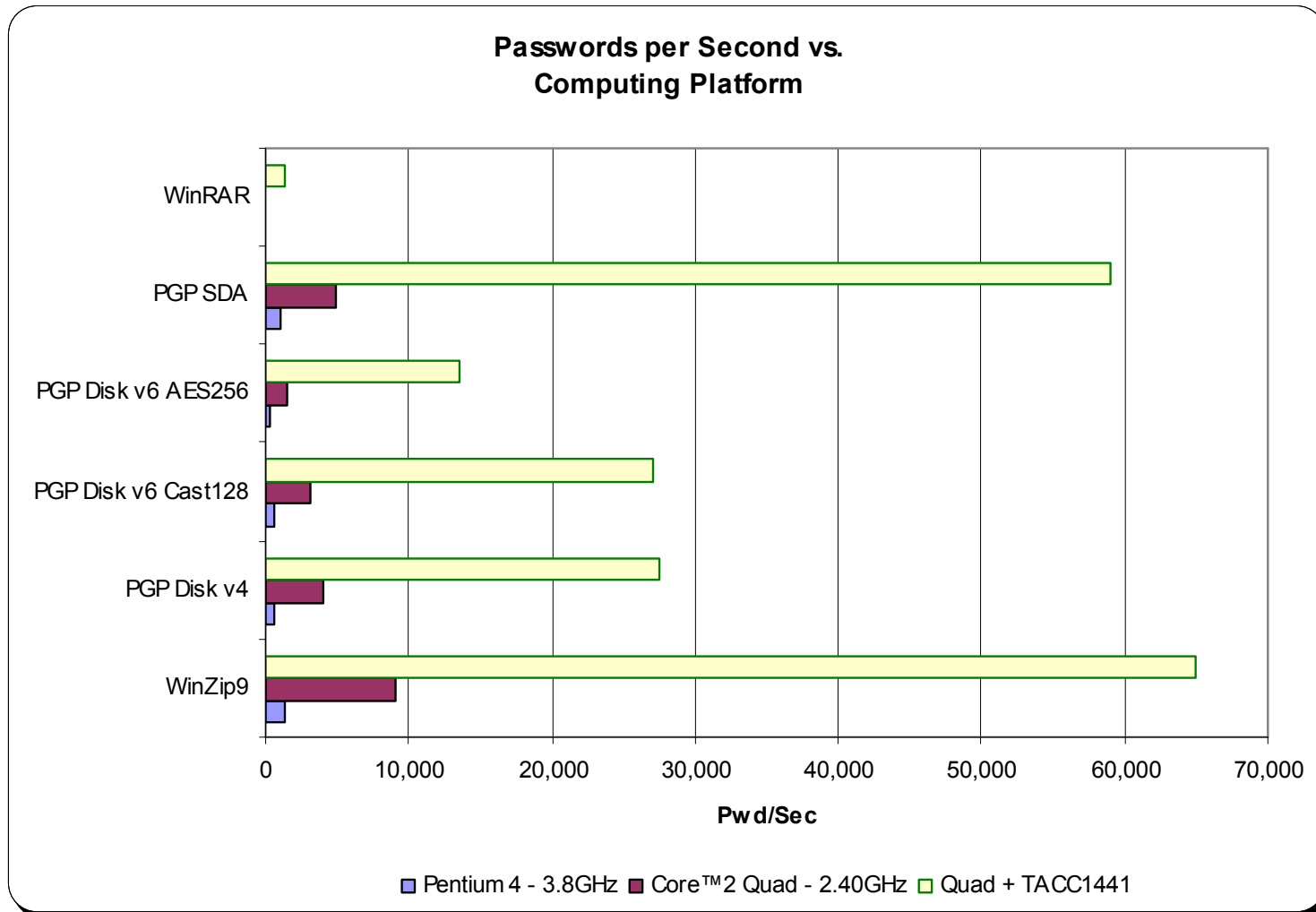
- **Current Algorithm Support:**
 - WinZip9
 - WinRAR
 - PGP SDA
 - PGP Disk v4
 - PGP Disk v6 AES256
 - PGP Disk v6 Cast 128
 - PGP Message SHA-1
- **Future Algorithm Support:**
 - Based on market needs....

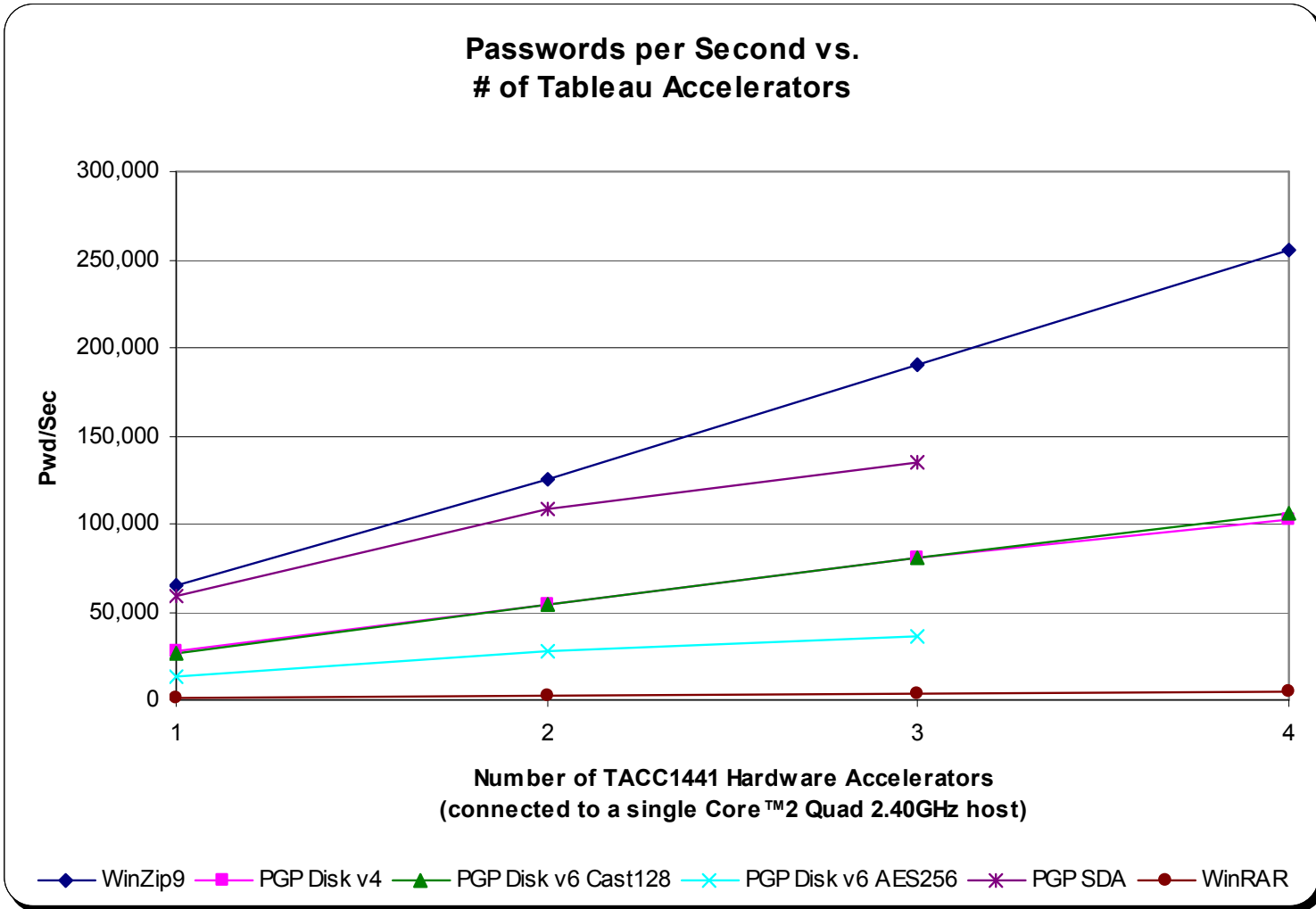
Performance Benchmarks











Deployment & Use Cases

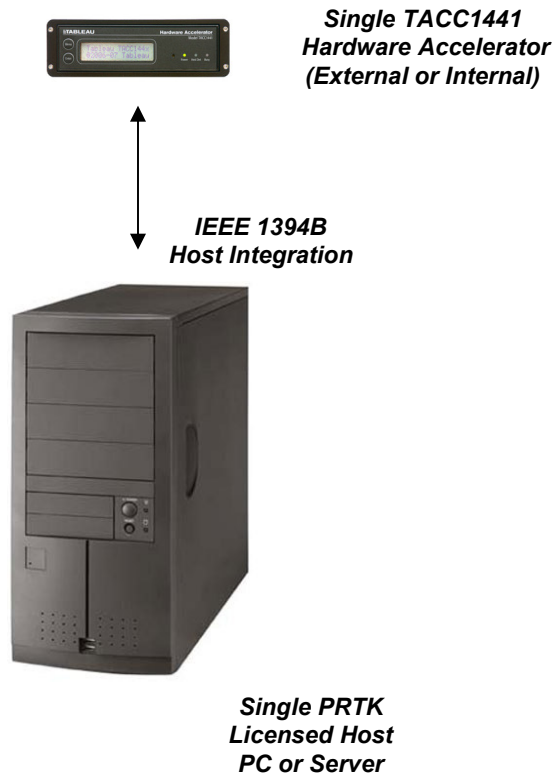


- TACC1441i
 - Internal, bay-mount

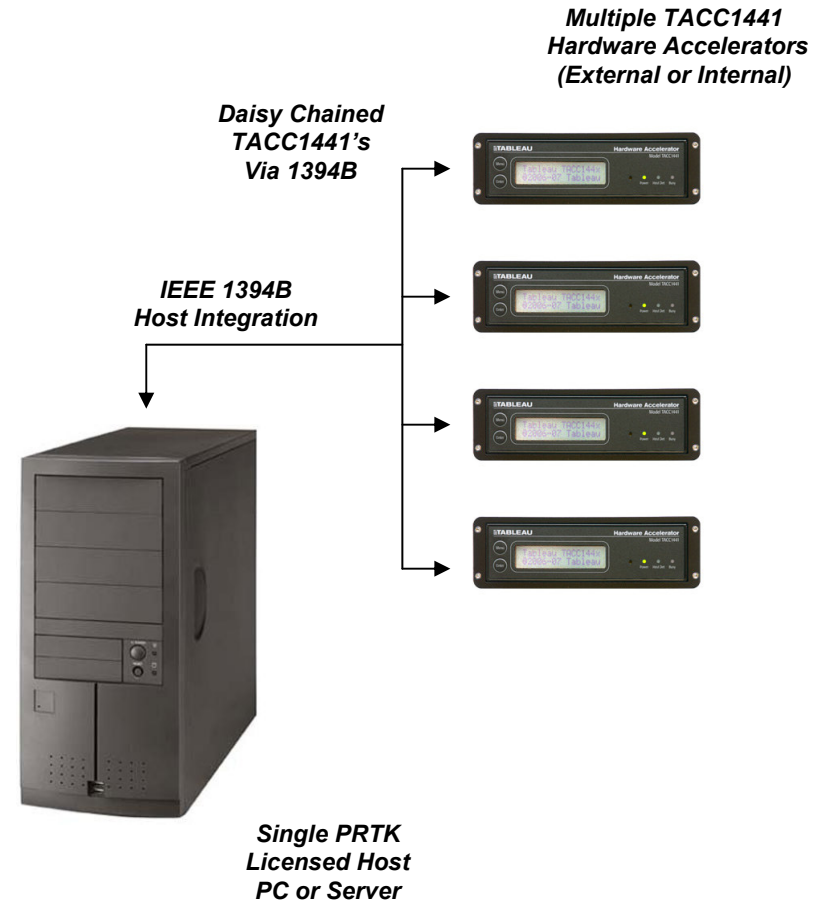
- TACC1441e
 - External, desktop

- Rack-mounted configurations suitable for server room situations
- Password recovery “appliances”
 - Host Computer, Multiple TACCs, Networked, Fully Licensed

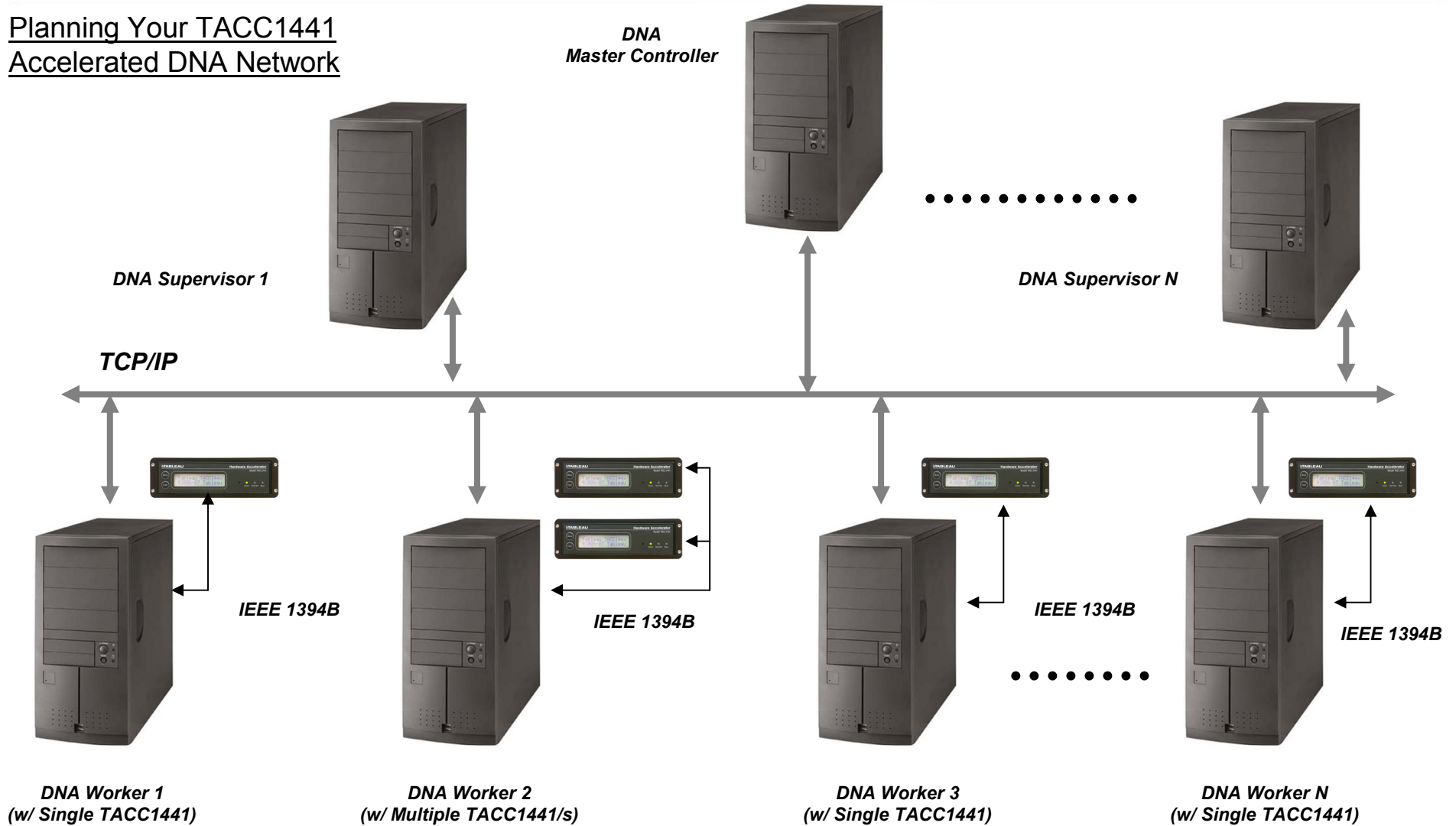
Scenario #1 One Host : One TACC1441



Scenario #2 One Host : Multiple TACC1441's



Planning Your TACC1441 Accelerated DNA Network

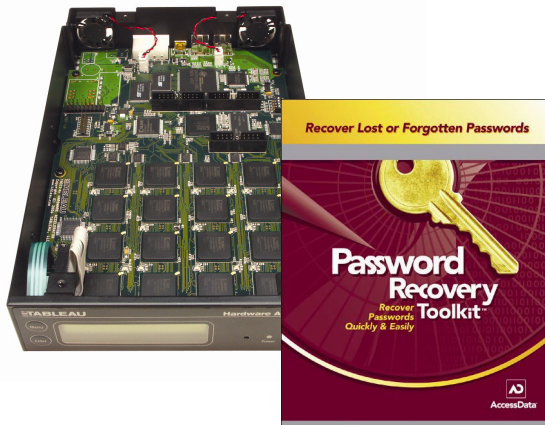


- TACC1441 supported integrated with AccessData PRTK or DNA installer.
- No changes to familiar PRTK / DNA user interface.
 - But...There is a separate PRTK / DNA dongle license requirement for TACC.

How to Buy

- Three solution offerings:
 - TACC1441 for existing DNA or PRTK installations
 - TACC1441 + new DNA-50 license
 - TACC1441 + new PRTK license

- Each offering includes one TACC1441 unit, Tableau software, and all required Access Data software



- Available through:
 - AccessData Sales
 - AccessData Authorized Resellers
 - Tableau Authorized Resellers
- Introductory Pricing:
 - \$ 4995 (USD) + cost of PRTK or DNA (if needed)
- Warranty: One year from date of purchase



- Questions?
- Thank you for being here!

