Exercise: Authentication

Midnight Engineering are currently adapting their 'Midnight Version Manager' tool for instrument technicians at ACME Water.

Because ACME Water is concerned that instrument technicians will have problems recalling or entering another set of credentials, they are considering the introduction of a biometric authentication mechanism. This will allow MVM credentials (usernames and passwords) for instrument technicians to be stored, together with their fingerprint, and allow technicians to 'login' with their fingerprints.

Questions

1. Discuss the potential cost and benefit of this solution for ACME Water and instrument technicians?

Pros	Cons
Equipment can be added easily (as a peripheral)	Sensors can become dirty
Relatively low cost	Can be overcome through simple attacks.
Easy to position	Staff / training costs
	Storing credentials adds to the MVM architecture's attack surface.
	Adoption issues (association with criminals, fear of digit loss!)

2. Identify different types of attack on MVM based on biometric authentication . What countermeasures would you put in place?

The threats are fairly consistent, but there are different vulnerabilities based on the different stages of authentication that could be attacked.

Risk/Attack	Vulnerability	Threat	Potential Countermeasures
Subvert biometrics process	*Ambiguous enrolment processes*: Ambiguity about how to deal with the enrolment process	*Presentation attack:* Mimic an individual based using a captured or modified biometrics sample.	Verify identity on enrolment. Instrument technician training.
Subvert biometrics technology	*Ambiguous backup process*: Ambiguity about how to deal with enrolment or verification errors.	*Flooding:* Consume mechanism resources with a large number of interactions.	Instrument technician and IT team training.

Risk/Attack	Vulnerability	Threat	Potential Countermeasures
Subvert biometrics enrolment	*Low quality template*: Quality issues with the stored template.	*Presentation attack:* Mimic an individual based using a captured or modified biometrics sample.	Evaluate kit to ensure a minimal FTE rate.
Subvert biometrics verification	*Low quality sample*: Quality issues with the presented sample.	*Presentation attack:* Mimic an individual based using a captured or modified biometrics sample.	Evaluate kit to ensure a minimal FAR rate.
Violate biometrics verification	*Ambiguous verification processes*: Ambiguity about how to deal with enrolment or verification errors.	*Presentation attack:* Mimic an individual based using a captured or modified biometrics sample.	Improve efficiency of related tasks to increase throughput. Instrument technician training.

3. How suitable are fingerprints for use in this particular scenario? Can you suggest a more suitable biometric?

Alternative	Pros	Cons
Face Recognition	* Low FTA/FTE rates * Potentially inexpensive (webcams) * Familiar form of authentication	* High FRR that increases overtime as images age. * Lighting conditions may interfere. * Need to use the same equipment for enrolment AND verification
Dynamic Signature Recognition	* Most instrument technicians can do this.	* Needs space and a trackpad.
Voice Authentication	* Hands-free * Easy to use	* Noise levels in the normal operating environment may be too high. * Cold or stress may lead to false rejection.