Summary of IFIP WG 10.4 Meeting Session 2 “Ethics, policy, and responsible deployment”

Long Wang
Institute for Network Science and Cyberspace (INSC)
Tsinghua University
June 28, 2026

Session 2

- Morning of June 26, 2026
- Chair: Amy Babay; Rapporteur: Long Wang
- Two talks
  - “Challenges in Biometrics: Security and Permanence”, by Prof. Stephanie Schuckers, UNC Charlotte
  - “Biometrics Are Not the New Password. They Are the New Trust Boundary”, by Stephan Hutchinson

“CHALLENGES IN BIOMETRICS: SECURITY AND PERMANENCE”

Presentation Summary (1)

- 1. Liveness as the foundation of biometric trust
  - Biometric security should rely on liveness, not only secrecy; a stolen biometric should not be useful without a live sample.
  - Effective authentication requires both biometric comparison and liveness verification.
  - Liveness/PAD helps determine whether the sample is from a real person rather than a spoof, replay, or fake artifact.
- 2. Presentation Attack Detection and liveness techniques
  - PAD addresses physical attacks at the biometric sensor, such as fake fingerprints, masks, printed iris images, face spoofs, and replayed samples.
  - ISO/IEC 30107 defines PAD-related categories, including passive liveness detection, involuntary challenge response, and voluntary challenge response.
  - Examples include random light patterns, pupil-response checks, blinking, smiling, speaking random words, and randomized capture designs such as iPhone X Face ID.

Presentation Summary (2)

- 3. Evaluation, benchmarks, and remaining PAD challenges
  - LivDet benchmarks from 2009 to 2025 evaluate fingerprint, face, and iris liveness detection across different systems and datasets.
  - Additional datasets, such as spoofing/obscuration-at-a-distance datasets, test biometric recognition under more realistic and difficult conditions.
  - Despite progress in academic and commercial algorithms, PAD remains unsolved because attacks continue to evolve and robustness varies across modalities.
- 4. FIDO, certification, and biometric product trust
  - FIDO authentication and passkeys use a public/private key mechanism, with user verification required before the private key can be used.
  - A major challenge is the lack of a mature ecosystem of certified biometric products.
  - FIDO biometric certification helps evaluate security, accuracy, bias, liveness, interoperability, and performance based on expert-defined and ISO-aligned requirements.

Presentation Summary (3)

- 5. Deepfakes, injection attacks, and emerging biometric threats
  - Deepfakes can give stolen images apparent liveness by generating realistic motion, expressions, and real-time face swaps.
  - focuses on physical presentation attacks, while Injection Attack Detection addresses digital attacks that bypass the sensor and inject manipulated biometric data.
  - Similar defenses, such as challenge response and deepfake detection, may support both PAD and IAD, but they require different evaluation methods.
- 6. Case Studies: Biometrics for children and responsible deployment
  - Child biometrics have real-world applications, including birth registration, vaccination tracking, and school systems, but raise accuracy, privacy, and ethical concerns.
  - Longitudinal child biometric datasets show that age progression, capture quality, and modality choice strongly affect performance.
  - Iris recognition may remain stable over time, while fingerprint recognition often requires high-resolution sensors, scaling methods, and systems designed specifically for children.

Q&A (1)

- Q1: Were the LivDet data collected from commercial biometric systems?
- A: No. The data were from submitted systems, not commercial systems.
- Q2: What is a finger-attack example?
- A: A finger-attack can use a mold of a finger to spoof a fingerprint recognition system.
- Q3: What improved over the years in liveness detection?
- A: Things became worse rather than clearly better. This likely referred to the continuing difficulty of PAD as attacks evolve and benchmarks become more challenging.

Q&A (2)

- Q4: In FIDO authentication, do systems use the same protocol or different protocols?
- A: They use the same protocol.
- Q5: What happens if society no longer trusts biometrics because of biometric attacks?
- A: The discussion framed this as a trade-off between trust and convenience. Biometrics are attractive because they are convenient, but attacks can reduce public trust in the technology.

“BIOMETRICS ARE NOT THE NEW PASSWORD. THEY ARE THE NEW TRUST BOUNDARY”

Presentation Summary (1)

- 1. Biometrics as part of a broader IAM system
  - Biometrics should not be treated as a standalone security solution, but as one design choice within an Identity and Access Management system.
  - They do not simply “replace passwords”; instead, they change where trust, risk, and complexity appear in the system.
  - Centrally stored biometrics can create serious legal, privacy, and liability risks.
- 2. Passkeys shift, but do not eliminate, IAM complexity
  - Passkeys reduce reliance on passwords, but they do not remove the need for IAM architecture and governance.
  - They shift the main security debate from password policies to device trust, recovery, and lifecycle assurance.
  - Passkeys make biometrics more visible to users, but they do not necessarily mean biometrics are centrally stored.

Presentation Summary (2)

- 3. Identity assurance must cover the full lifecycle
  - Biometrics are moving from simple login use cases toward lifecycle assurance, from onboarding to offboarding.
  - Stronger sign-in is not enough if attackers can exploit weaker paths such as recovery, emergency access, or device replacement.
  - Recovery is a critical control plane and should be safer than the primary authentication path, not easier for attackers.
- 4. Biometric risk must be evaluated systemically
  - The key question is not only whether a biometric match succeeds or fails, but what happens when the biometric system fails.
  - Failures can affect recovery, access control, accountability, trust, and the broader IAM workflow.
  - Liveness detection is now an ongoing arms race, requiring continuous evaluation rather than one-time compliance.

Presentation Summary (3)

- 5. Governance should focus on purpose, architecture, and consequence
  - Biometrics are used for different purposes, so they should not be governed as one uniform category.
  - Governance should begin with a clear taxonomy of use cases, system architectures, and possible consequences.
  - “Architecture is the ethics layer”: how biometrics are captured, stored, verified, and recovered determines their real-world impact.
- 6. Responsible enterprise biometrics require explicit commitments
  - Biometric deployments should be classified as appropriate, risky, or inappropriate based on purpose, safeguards, and consequences.
  - Acceptable risk depends on the specific use case, the severity of failure, and the organization’s goals.
  - Enterprise systems need clear commitments around governance, reliability, device trust, recovery, and responsible use.

Q&A (1)

- Q1: How are biometrics handled in your country (Japan)?
- A: The presenter said they could not name a specific country. However, the audience mentioned that there have been relevant cases in the U.S. state of Illinois.
- Q2: What is lifecycle assurance for a session?
- A: Lifecycle assurance covers the full identity lifecycle, from onboarding to offboarding, rather than only the sign-in moment.
- Q3: If consequences are severe but safety controls are costly, how much safety should be provided?
- A: It depends on the options, purposes, and goals of the biometric use case. The appropriate level of safety should be based on the specific deployment context and consequences.
- Q4: Why does end-to-end reliability matter?
- A: End-to-end reliability matters because biometrics are being used at the IAM system level. The reliability of the whole identity workflow is more important than the biometric component alone.

Q&A (2)

- Q5: Why are use cases important for biometrics?
- A: Use cases are important because biometric risk, required safeguards, and acceptable trade-offs depend on what the system is being used for and what consequences follow from failure.
- Q6: If everyone uses passkeys and device security becomes the weak point, how should device protection be handled?
- A: Now device protection becomes a key part of the risk model. Biometrics may also be used for device protection, but the right approach depends on risk. In corporate settings, organizations do examine device protection more carefully.
- Q7: If a device is compromised, can the passkey be stolen?
- A: This depends on the device security model and the level of risk. Passkeys rely heavily on device trust, so protecting the device is critical.
- Q8: How do passkeys compare with OTP tokens?
- A: The presenter said that passkeys are much more reliable than OTP tokens.

Thanks a lot!

Contact: Long Wang
longwang@tsinghua.edu.cn