AL2026_01 Deepfakes and Injection Attacks Undermine Identity Verification Systems (March 2nd, 2026)

Description

Researchers have reported a growing trend of cybercriminals bypassing identity verification (IDV) systems using advanced deepfake technology and injection attacks. Threat actors are leveraging AI-generated synthetic identities, manipulated facial biometrics, and direct system-level injection techniques to defeat Know Your Customer (KYC) and remote onboarding safeguards used by financial institutions, fintech platforms, and other online services.

These attacks allow criminals to create fraudulent accounts, bypass biometric authentication checks, and potentially facilitate financial fraud, account takeovers, and money laundering activities.

Attack Details

- **Threat actors:** Organized cybercriminal groups leveraging AI-based deepfake generation tools and automated attack frameworks.
- **Malicious techniques observed:**
  - Use of real-time deepfake video and AI-generated facial overlays to bypass liveness detection mechanisms during remote identity verification sessions.
  - Injection attacks that bypass webcams entirely by directly feeding pre-recorded or synthetic video streams into the verification process at the software or API level.
  - Use of stolen personally identifiable information (PII) combined with AI-generated images to create convincing synthetic identities.
  - Automation frameworks used to scale fraudulent account creation and test weaknesses in onboarding workflows.
- **Systemic risk:**
  - Traditional biometric verification systems relying solely on facial recognition and basic liveness checks are increasingly vulnerable to AI-driven spoofing.
  - Injection attacks represent a more severe threat as they circumvent physical device controls, making conventional anti-spoofing safeguards ineffective.
  - Financial institutions and digital service providers face regulatory, reputational, and financial risks due to large-scale fraudulent onboarding.

Remediation

- **Strengthen liveness detection:** Implement advanced, multi-factor liveness detection methods, including challenge-response prompts, behavioral biometrics, and device fingerprinting.

- **Harden client-side applications:** Protect against media injection attacks by implementing secure video capture pipelines, runtime integrity checks, and anti-tampering controls.
- **Adopt layered verification:** Combine biometric verification with document authentication, device intelligence, geolocation analysis, and transaction risk scoring.
- **Monitor for anomalies:** Deploy fraud detection systems that flag abnormal onboarding patterns, repeated device fingerprints, synthetic identity indicators, or automation artifacts.
- **Update and patch systems:** Ensure identity verification of SDKs, APIs, and third-party integrations are updated to address known vulnerabilities.
- **Employee awareness & testing:** Conduct red-team simulations and penetration testing to evaluate IDV resilience against deepfake and injection techniques.
- **Vendor due diligence:** Assess third-party identity verification providers for their resilience against AI-driven spoofing and require transparency on anti-deepfake controls.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

Reference

- Toulas, B. (2026). How deepfakes and injection attacks are breaking identity verification. BleepingComputer. Retrieved from: https://www.bleepingcomputer.com/news/security/how-deepfakes-and-injection-attacks-are-breaking-identity-verification/