INNOVATRICS

DOT

One-pager

Video Injection Attack Detection

Combating Deepfakes and Preventing Synthetic Identity Fraud

Innovatrics Video Injection Attack Detection feature guards against synthetic identity fraud by inspecting the authenticity of a camera stream during the remote identity verification process.

Synthetic Identity Fraud

Synthetic identity fraud occurs when a new fake identity is created by combining real personal information with synthetically fabricated or fraudulent ones. It may leverage deepfake, stolen, or manipulated photos or videos of a non-existing person in order to gain unauthorized access to information or services of organizations or individuals.

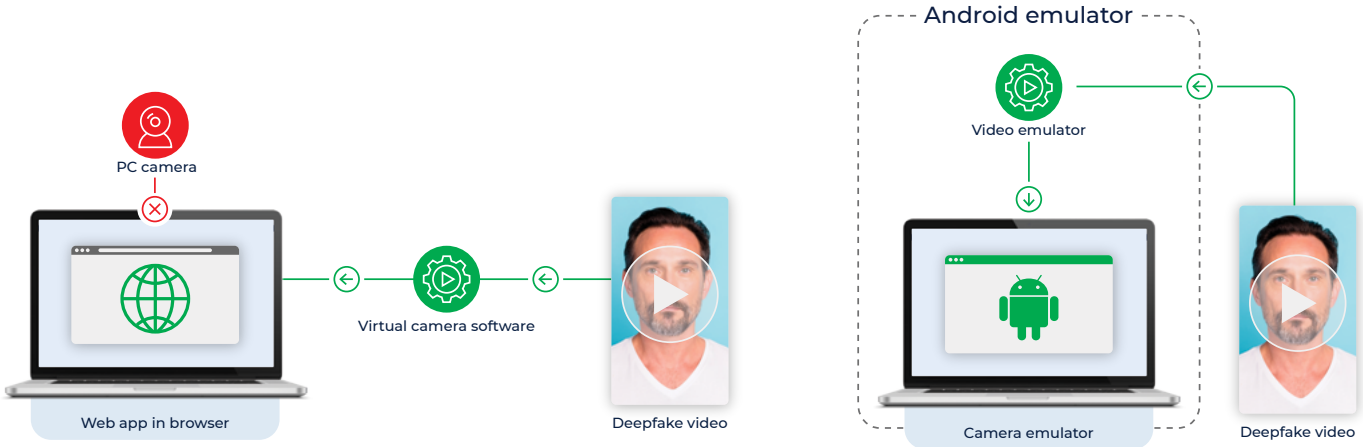
Fraudsters utilize video injection attacks to trick identity verification systems by using synthetic identities.

Recent statistics show that synthetic identity fraud is the fastest-growing form of identity fraud worldwide.

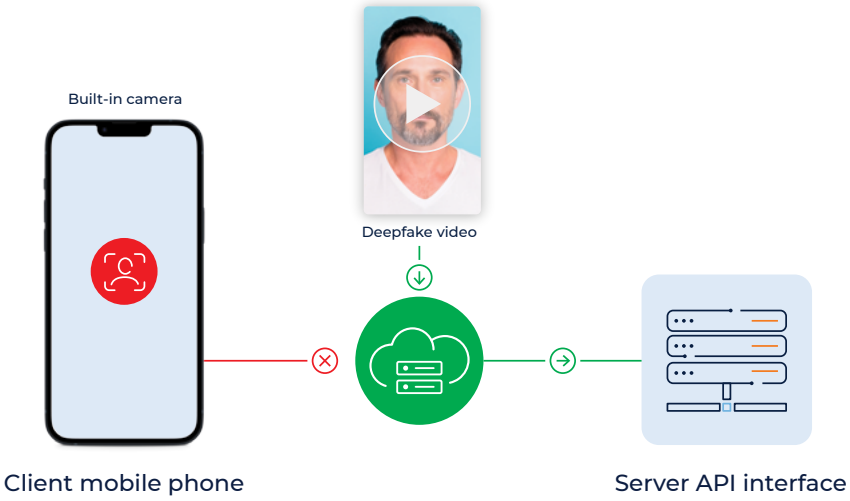
Video Injection Attacks

The process involves injecting fake videos into the remote identity verification process using various methods. These may include video emulation and virtual cameras, physical replacement of phone cameras, hacking apps, and man-in-the-middle attacks as shown below:

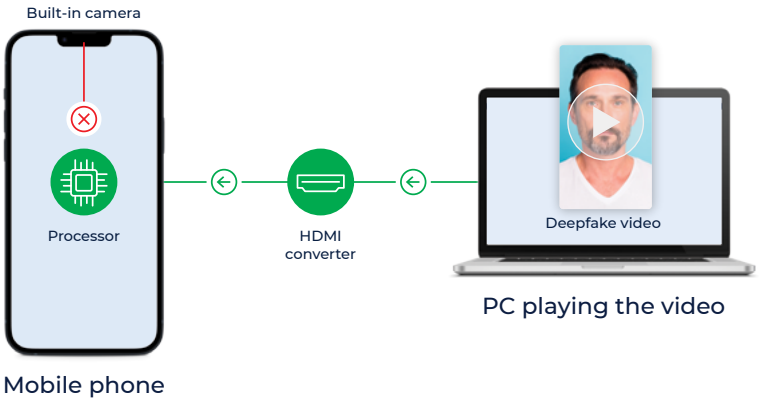
- **Emulation software**
  Emulation software that feeds the video pretending to be a camera input. This is **the cheapest** injection attack that almost **anybody can do**.



- **Man-in-the-middle attack**
  Man-in-the-middle attack is when the communication between a cell phone and the server is intercepted and the data is swapped for the deepfake. This is **more complicated**, as this method requires a **skilled hacker** and ideally **an insider (employee)**.

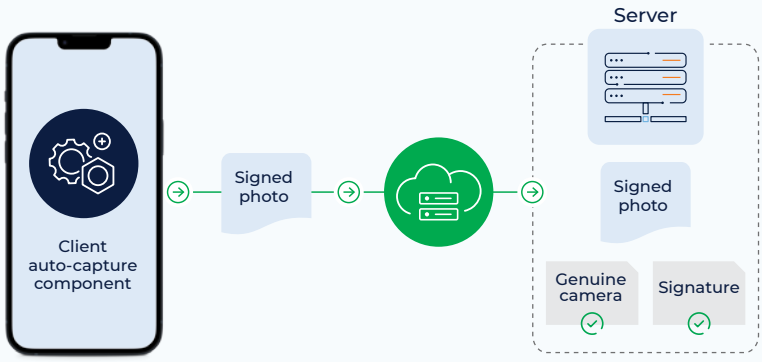


- **Hardware injection**
  Hardware injection occurs when the camera interface inside a mobile phone is replaced by an HDMI converter streaming the video. This is **the most complicated** injection attack where you need **an electronics engineer**.



Solution

Leveraging advanced algorithms, our capture component on the client side collects various information from the camera. The data is then encrypted to prevent altering. Afterward, the data is decrypted by our backend component, Digital Identity Service, which further analyzes the collected information and evaluates whether the video is coming from a genuine camera or not. This way, Innovatrics Video Injection Detection can prevent all types of video injection attacks.



INNOVATRICS

We are an independent EU-based provider of multimodal biometric solutions. Our algorithms consistently rank among the fastest and most accurate in fingerprint and face recognition. Since 2004, we have partnered with all types of organizations to build trusted and flexible biometric identification solutions. Our products are being used in more than 80 countries, benefiting more than a billion people worldwide.

sales@innovatrics.com www.innovatrics.com