kloke™
ai-driven security

IoT, 5G, Cars and Kloke

Where Are We, Where Are We going?

by Doug Peckover | November 2019

IoT devices can be traced back to World War II for the identification of friend or foe aircraft. Radio signals were beamed and collected by RFID devices that in turn sent back an identify response. This technology is still in use today in Dallas TollTags and EZ-Passes in the northeast.

In large numbers, a tag costs just 1¢ but adding onboard encryption increased this to 10¢, so there has always been a conflict between cost and security. And this onboard security is really weak – the encryption on new British passport tags was cracked the same day is was introduced. This is important because if Kloke can protect simple RFID tags, it can protect all IoT devices.

What have the experts been doing?

Kloke's technology was presented to the RFID Experts Group (REG) to see if Kloke's token security could be adapted to protect 1¢ tags, and the answer was 'yes' because tokens do not require any hardware or on-board processing. As a result, Kloke's design is data agnostic and device agnostic because it protects all data, from enterprise databases all he way down to dumb 1¢ devices. This means that all of Kloke's benefits – being breach safe, GDPR safe, quantum safe, and ransomware safe – are available for all IoT devices.

Network bandwidth for IoT

The 40 billion IoT devices expected within 5 years will generate unimaginable amounts of real-time data, something the current networks were never designed to mange. This is one reason why the fifth generation (5G) cell network was designed. 5G is so fast that one reporter downloaded *Spider-Man: Into the Spider-verse* not in 5 minutes, but in *5 seconds*. This speed improvement will support the billions of needed IoT devices, but what about their security?

Has IoT security also improved?

No. Some failures are funny but most are not. IoT's 'staggering' growth and lack of security has cities worried about threats like ransomware attacks. But there is an even most urgent need for secure IoT devices in smart and self-driving cars because they must continuously make life-or-death decisions. One *USA Today* article warns that:

- A hacker could launch a massive attack against our automotive infrastructure, potentially causing thousands of fatalities and disrupting our most critical form of transportation.
- Two-thirds of new cars on American roads will have online connections to the cars' safety-critical system, putting them at risk of deadly hacks.
- Tesla, Daimler, Ford, General Motors and BMW have disclosed these cyber risks to their investors.

IOT Security Use Cases

- Mary uses her phone's biometrics to open the car and start the engine.
- A message shows that hackers tried to gain access to her car, were denied, and the details were forwarded to her security provider.

Why did Kloke reinvent security?

We believed that traditional data security has failed:

- Perimeter defenses have failed to keep hackers out. Citrix is a company that protects the data of 400,000 clients but had no clue that hackers had gained access to its own systems.
- IT managers are being asked to follow the advice of leading crypto experts like Bruce Schneier who says 'Trying to get ahead of it is the wrong way of thinking… it's better to react as quickly as possible. You can't defend. You can't prevent. The only thing you can do is detect and respond.' Translation: work on a problem after car crashes.
- Quantum computers are being developed that will break encryption, and this will put all data and IoT devices at risk. NIST is working on a quantum-safe solution, but its earliest ETA is 2022, and it will take years more to implement. IBM has announced its own solution but admits it only addresses a single known risk.

IoT, 5G, Cars and Kloke

[continued]

- Ransomware is a global problem that could lock any system, device, or car. These attacks are often started by human error and therefore cannot be prevented. Even worse, recovery may be impossible as hackers are learning how to also infect backup data.
- Encryption requires keys, and these are a major attack surface.
- A stolen encrypted file has no way of notifying a firm that it is under attack. The hacker has unlimited time can try millions or billions of keys without being detected.
- Authentication systems are either too weak or getting too complex for many users, and credentials can be stolen.
- Enterprise-grade security does not scale down to protect IoT devices, nor does it focus on privacy which is crucial for car applications that make emergency calls when sensors detect an accident.

How does Kloke work?

We believe that the only way to really protect data is to hide it so that it cannot be stolen or compromised. This 'token' security is not new because it has successfully protected credit cards for more than a decade. Kloke knows a lot about token security – the US Patent Office says that our co-founder was the first to invent token security. Kloke's designs address all of the risks:

Risk	Kloke AI-Driven Security
Perimeter defenses	Assumes systems have already been compromised and hackers have full access to the data at risk
Can't detect or prevent	Detects and prevents hacker attempts before they occur, and notifies about failed attempts in real time
Quantum computers	Is safe from quantum attacks because if you can't find the data, you can't break its security
Ransomware	Enables fast recovery without the loss of data
Encryption keys	Does not require encryption keys
No detection	Warns when under attack without being at risk, thus enabling new AI-learning and SaaS revenue models
Authentication systems	Continuous biometric authentication cannot be stolen, and passively learns about each user
Does not scale down	Enterprise-grade security protects even the smallest IoT devices without the need for additional hardware
Does not protect privacy	Complies with GDPR, the most stringent privacy regulations

From the very beginning, the industry has known that IoT devices would be a risk:

> ***'It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible is designed with no security constraints whatsoever.'***
>
> *– NY Times in 2006*

Kloke's patented AI-driven security is the right product at the right time:

- **The IoT security market will reach $35 billion by 2023** *(more)*
- **5G is expected to add $17 trillion to the global GDP by 2035** *(more)*
- **The IOT car market will exceed $132 billion by 2024** *(more)*

Doug Peckover is Co-Founder and Chief Scientist at Kloke — a developer of AI-driven data security solutions. He holds numerous data security and technology patents.