NỘI DUNG

eFence
Hàng rào điện tử bảo mật

1. Vấn đề nhức nhối
2. Giải pháp của chúng tôi
3. Công nghệ ưu trội
4. Về chúng tôi - Onyx
5. Khả năng hợp tác

NGUYEN, Tuan
Inventor

D

Giới thiệu eFence

Một sáng chế hàng rào điện tử bảo mật
Không thể bị hack

File version: 1.1

VẤN ĐỀ

1

Các loại rào điện tử hiện nay tồn tại rất nhiều nhược điểm:

- Dễ dàng bị giả mạo chùm tia và xâm nhập
- Phạm vi bảo vệ hạn chế
- Sử dụng nhiều năng lượng

VẤN ĐỀ Hàng rào biên giới

1

Buôn lậu diễn ra trên mọi tuyến

Đường bộ, đường hàng không, đường biển đều ghi dấu sự xung trận của buôn lậu

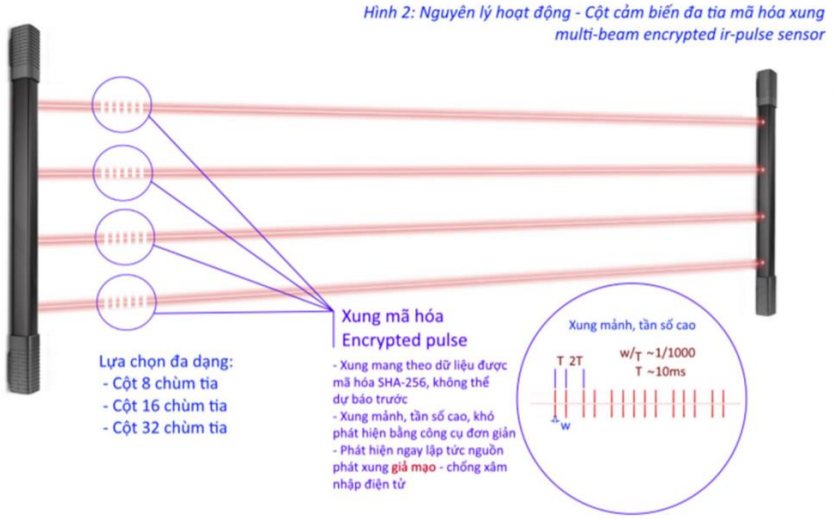
https://vneconomy.vn/buon-lau-dien-ra-tren-moi-tuyen.htm

Hàng rào biên giới rất dài:

- Hàng rào vật lý càng cao càng tốn kém
- Lực lượng tuần tra bảo vệ luôn hạn chế

GIẢI PHÁP

nguyên lý mới, giao thức mới

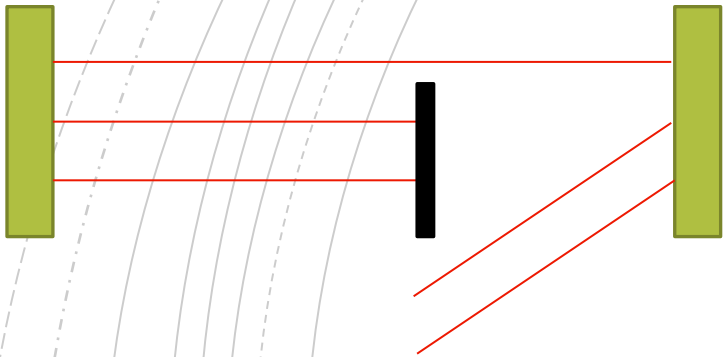


2

WIPO WORLD INTELLECTUAL PROPERTY ORGANIZATION

Nguyên lý cũ:

Gián đoạn chùm tia

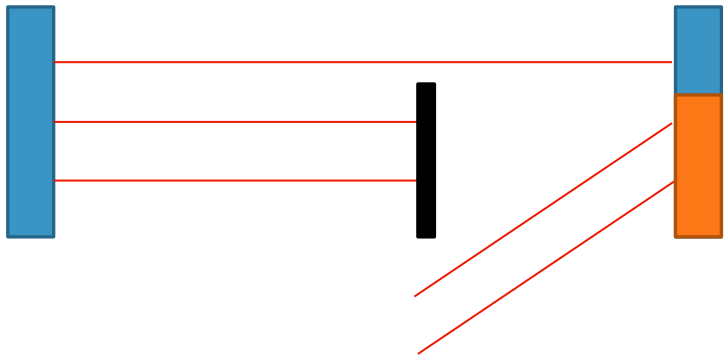


Chùm tia bị che khuất là cảnh báo

***Không thể** phát hiện chùm tia giả mạo*

Nguyên lý mới:

Chùm tia mã hóa



Chùm tia bị che khuất là cảnh báo

Chùm tia bị giả mạo là báo động

Với Token 64 bits, CypherKey 256 bits; ***không thể bị hách / crách với công nghệ điện toán hiện tại***

+ KỸ THUẬT Mã hóa chùm tia

2

Cột A

$Session_k$ *start*

random_token

Gửi: token là 1 số ngẫu nhiên

TruthTable: bảng sự thật
h = SHA(token, CypherKey)
h1 = Swap (h, Seed)
h2 = Swap (h1, Seed)
...
$h_n = Swap (h_{n-1}, Seed)$

Nhận và đối sánh với từng bit trong bảng sự thật - *SmartDectect*

Lặp lại
$Session_{k+1}$ *start*

Cột B

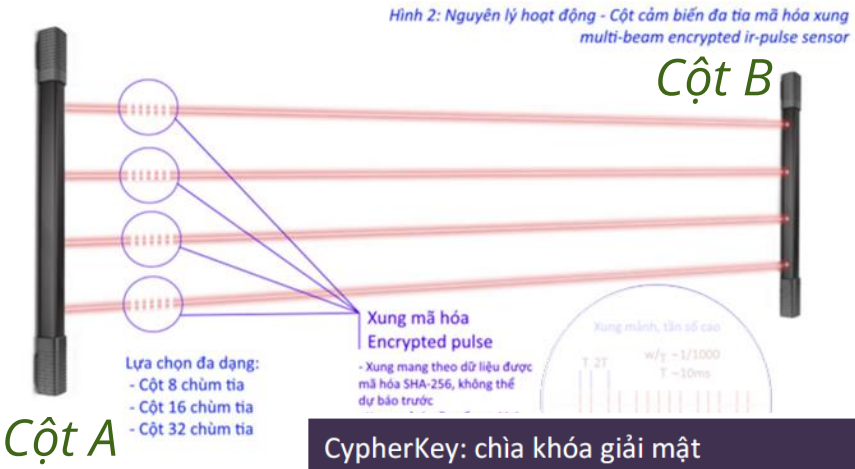
$Session_k$ *sync*

random_token

TruthTable: bảng sự thật
h = SHA(token, CypherKey)
h1 = Swap (h, Seed)
h2 = Swap (h1, Seed)
...
$h_n = Swap (h_{n-1}, Seed)$

Gửi: dữ liệu là các bit trong bảng sự thật

$Session_{k+1}$ *sync*



CypherKey: chìa khóa giải mật		
MasterKey nhà sản xuất	UserPIN người sử dụng	Random Seed hệ thống

SHA: ➪ không thể dự báo trước,
➪ không thể suy ngược

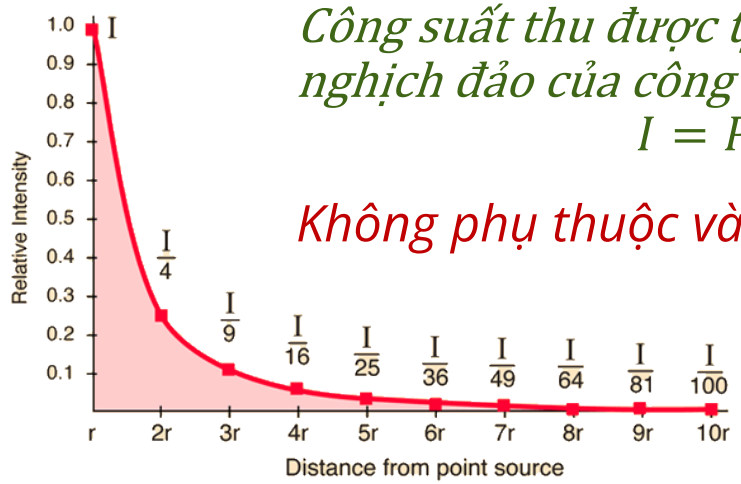
Swap (random **Seed**): khuyếch đại SHA.

➪ Tốn ít tài nguyên tính toán hơn cho 1 session. Cho phép triển khai trên phần cứng có giá thành hợp lý.

Đây là bí quyết công nghệ tạo ra nhiều giá trị của sáng chế.

KỸ THUẬT Xung mảnh

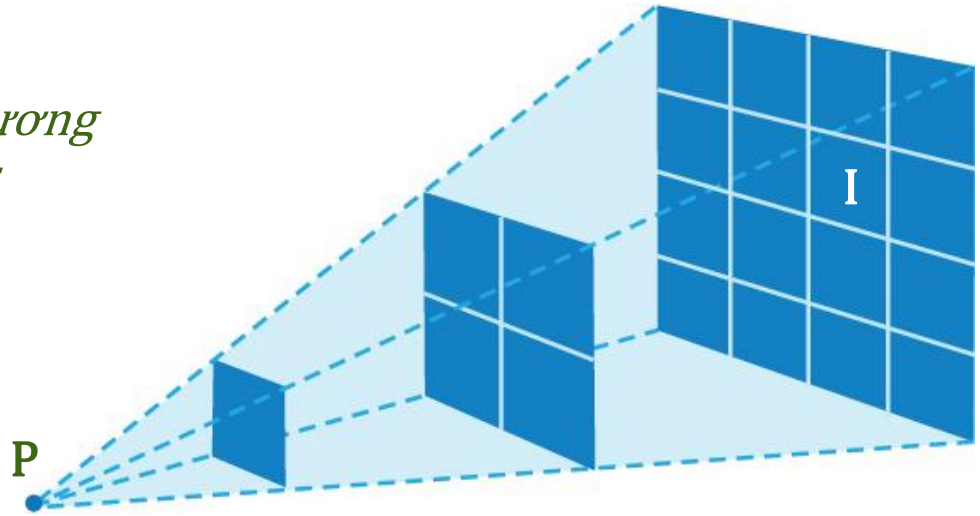
2



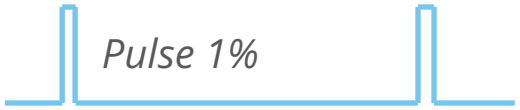
Công suất thu được tỷ lệ với bình phương nghịch đảo của công suất nguồn phát:

$$I = P/(4\pi r^2)$$

Không phụ thuộc vào độ rộng xung



1 tín hiệu xung 50% tốn năng lượng gấp 50 lần tín hiệu 1% ở cùng cường độ nguồn phát



ThinPulse: Kỹ thuật xung mảnh

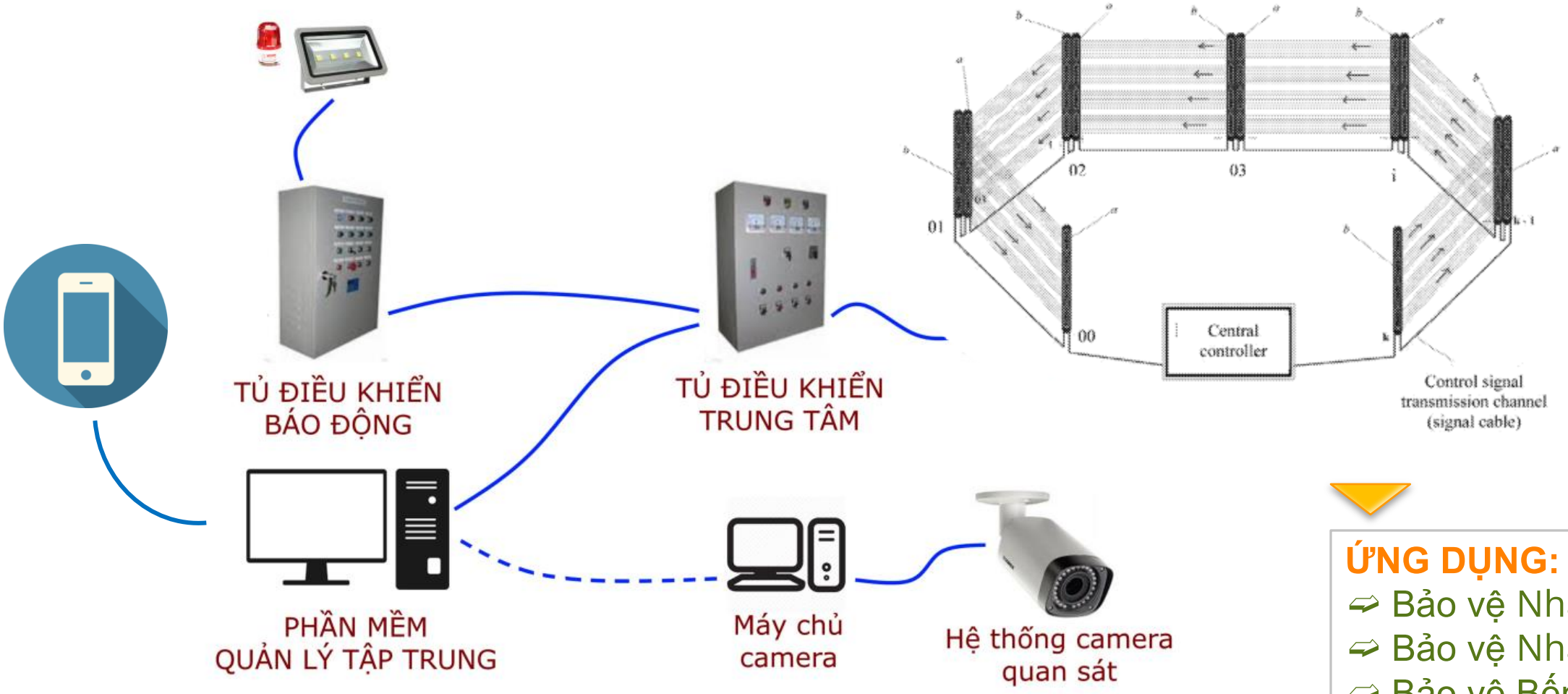
- *Phát xa hơn*
- *Tốn ít năng lượng hơn*
- *Cho phép sử dụng năng lượng mặt trời*

Đây là bí quyết công nghệ tạo ra nhiều giá trị của sáng chế.

+ GIẢI PHÁP

Bảo vệCác khu vực vừa và nhỏ

2



Sơ đồ khối nguyên lý
và kết nối liên động hệ thống hàng rào điện tử với hệ thống camera giám sát

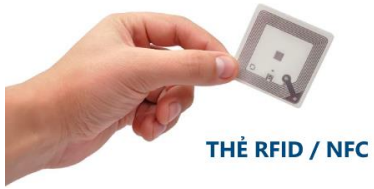
ỨNG DỤNG: Bảo vệ

- Bảo vệ Nhà dân
- Bảo vệ Nhà máy
- Bảo vệ Bến bãi
- Bảo vệ Kho tàng
- Doanh trại, nhà giam

TÍCH HỢP: nhiều tầng bảo mật

5

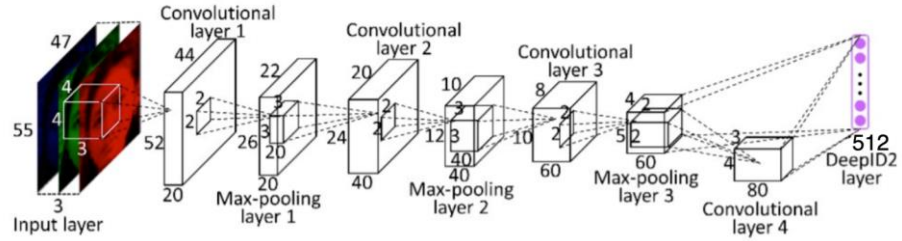
Quản lý vào ra, Thẻ an ninh chống sao chép với iSeal, A.I Nhận diện khuôn mặt, nhận diện vật thể

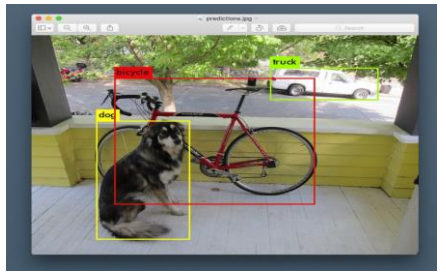


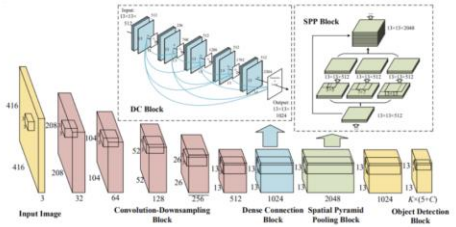
Được bảo vệ bởi iSeal:
Chống sao chép, chống giả mạo
với công nghệ bảo mật 5 cấp độ
Không thể sao chép tùy tiện

Cổng tự động kiểm soát vào ra

A.I Deeplearning





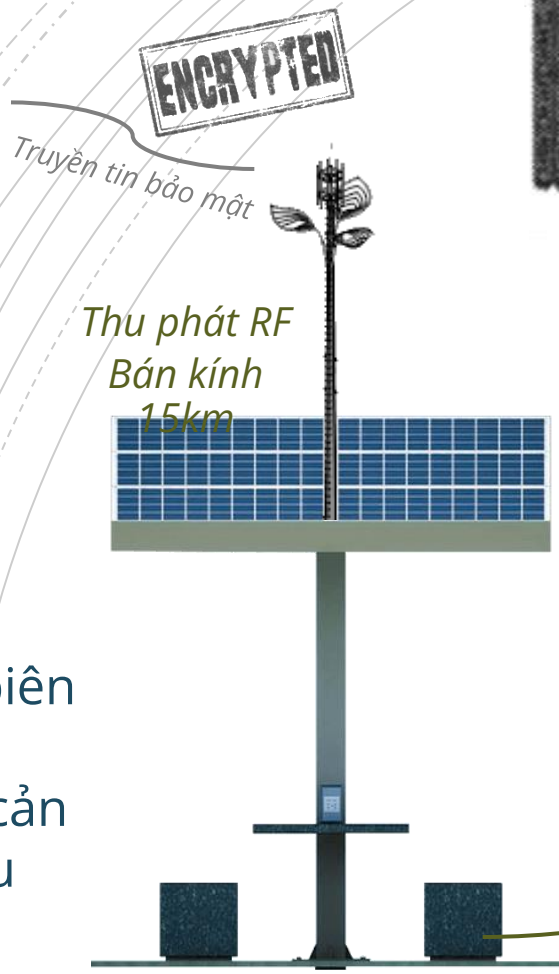


Tích hợp công nghệ khác theo nhu cầu
(ví dụ nhận diện khuôn mặt FaceID, nhận diện vật thể Yolo)

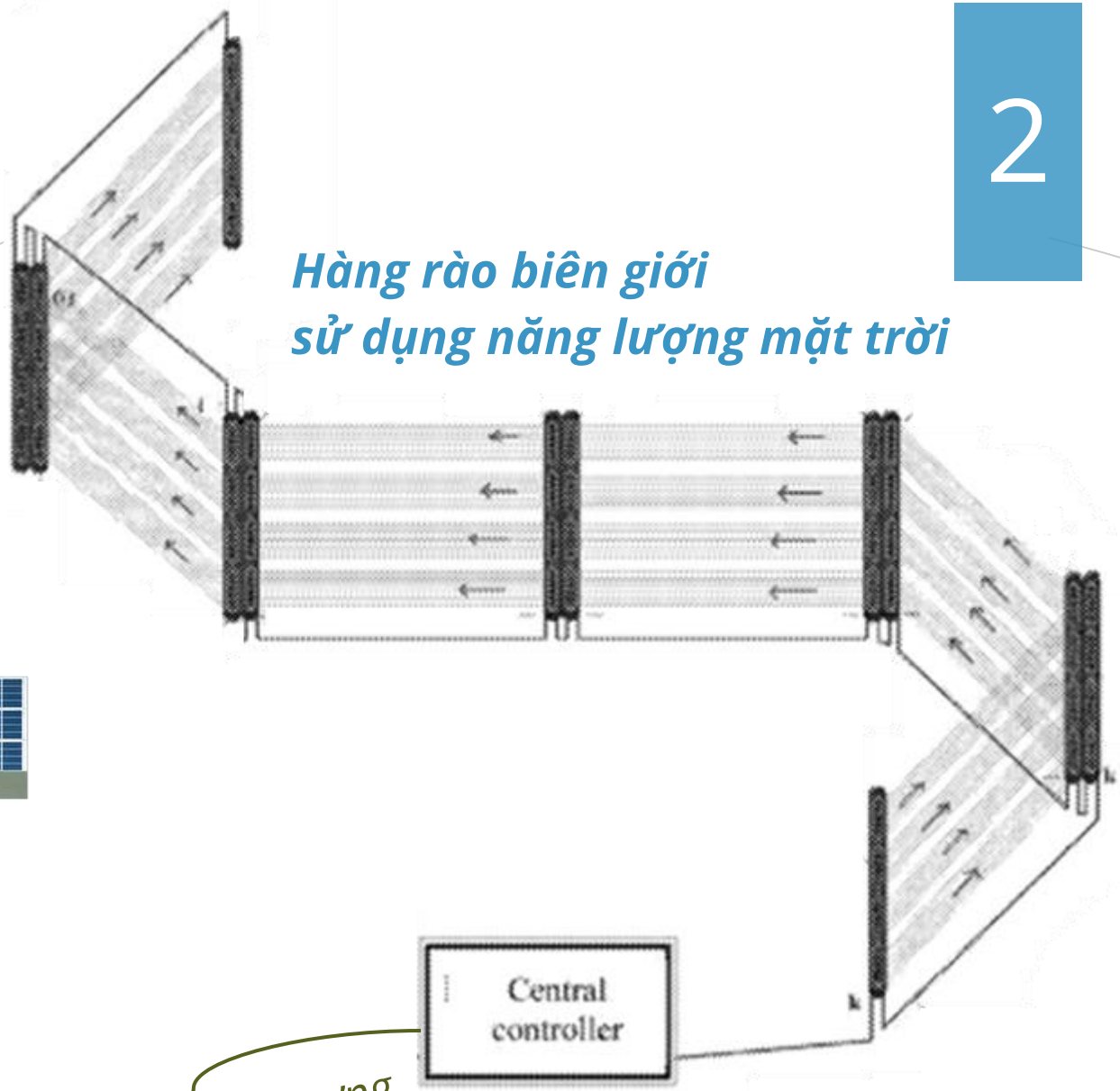
GIẢI PHÁP

2

Trung tâm Chỉ huy



Hàng rào biên giới
sử dụng năng lượng mặt trời

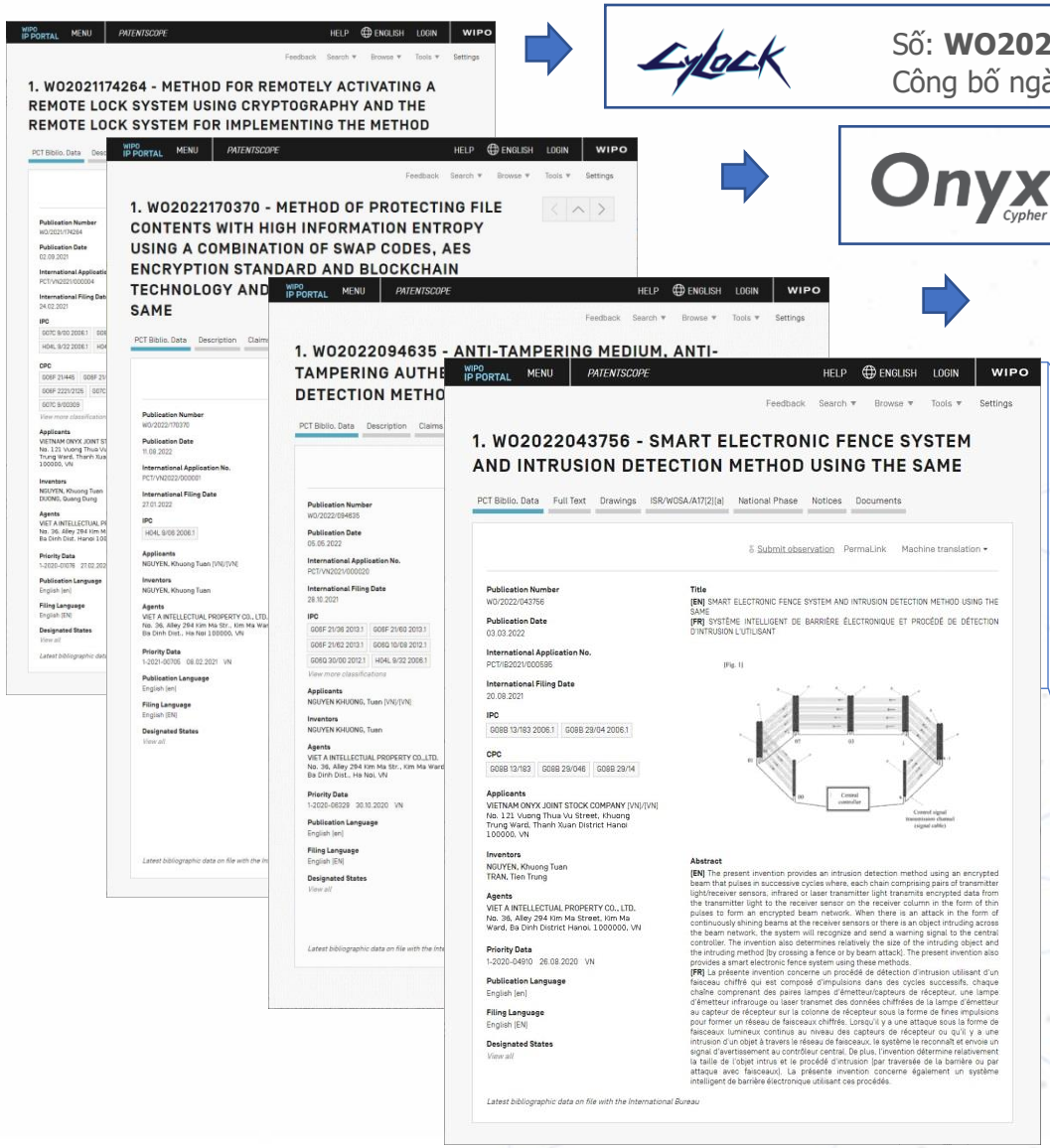


LỢI ÍCH SỬ DỤNG:

- ➪ Cảnh báo xâm nhập biên giới
- ➪ Hỗ trợ lực lượng truy cản
- ➪ Phòng chống buôn lậu

TIÊN PHONG

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION



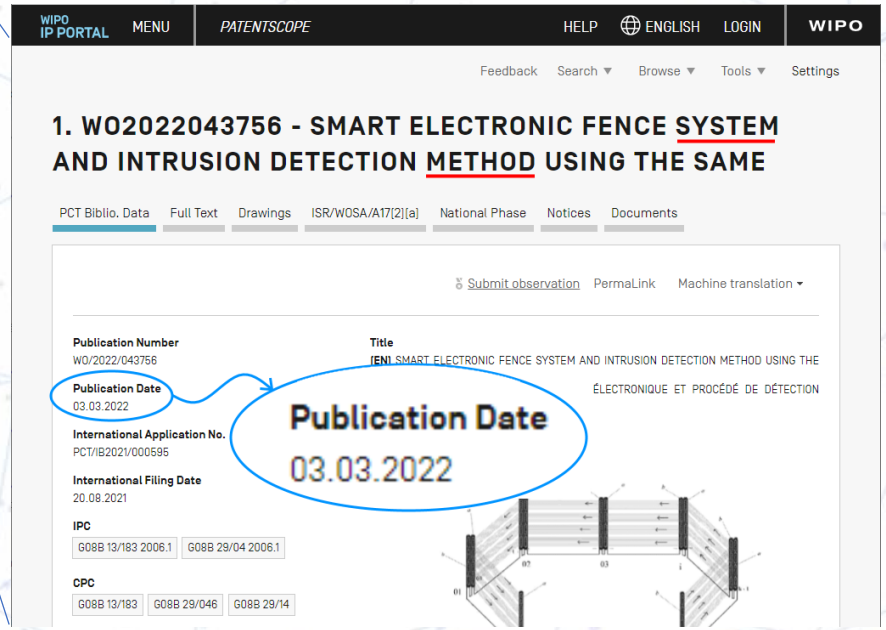
CyLock — Số: **WO2021174264**
Công bố ngày: **2/9/2021**

Onyx Cypher — Số: **WO2022170370**
Công bố ngày: **11/08/2022**

TrueOrigin KEEP BELIEVING — Số: **WO2022094635**
Công bố ngày: **5/5/2022**

eFence electronic security fence — Số: **WO2022043756**
Công bố ngày: **03/03/2022**

- 24 điểm bảo hộ
- 02 điểm bảo hộ độc lập



Method: phương pháp

System: sản phẩm

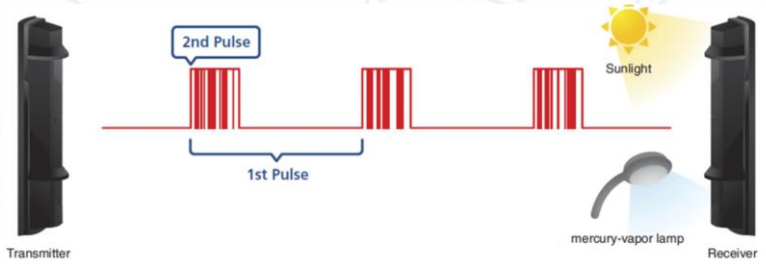
ƯU TRỘI

WIPO WORLD INTELLECTUAL PROPERTY ORGANIZATION

3

Sercured BeamTransfer
Lưới hồng ngoại mã hóa

Hoạt động trong điều kiện trời năng nóng / mưa rào



- Chống nhiễu trắng: không bị ảnh hưởng bởi thời tiết nắng nóng.
- Tối ưu công suất phát tiết kiệm năng lượng.
- Có thể sử dụng nguồn điện từ năng lượng mặt trời
- Không thể nhìn thấy bằng mắt tường để né tránh.
- Vô hiệu các thiết bị xâm nhập: nghe lén lưu lại các đoạn mã, phát xung giả mạo đánh lừa hàng rào.

TrainLoop PackTransfer
Mạng chuyển mạch gói cấu trúc đoàn tàu

- Cột bất kỳ gặp sự cố mất điện, mất liên lạc: đều được phát hiện để báo cho người sử dụng, phần còn lại của hệ thống vẫn hoạt động bình thường;
- Thường xuyên cập nhật trạng thái hoạt động, cảnh báo xâm nhập, báo động;
- Các gói tin trên đường truyền được mã hóa bảo mật đường truyền; hệ thống sử dụng giải thuật mã hóa AES được chính phủ Mỹ lựa chọn sử dụng làm mã chuẩn để mã hóa các tài liệu mật từ 2004

ƯU TRỘI

3

UltraRange
Phạm vi bảo vệ rộng lớn

- Mỗi cột cảm biến hồng ngoại được trang bị 8 chùm tia (hoặc 16 chùm tia, 32 chùm tia, tùy chọn theo kích thước)
- Mỗi cột có khả năng phát xạ và thu nhận các chùm tia theo 2 hướng (trái, phải), mỗi cột được đánh địa chỉ 16 bits Tạo ra kết cấu hàng rào nối tiếp liên tiếp, lên tới tối đa 2^{16} cột (65536 cột, tương đương 6500km)
- Phát xạ xung hồng ngoại qua thấu kính quang học: khoảng cách phát xạ lên tới 100m (trong tương lai có thể phát xạ xa hơn nữa)

SmartDetect
Nhận diện xâm nhập

- Cùng lúc nhận diện 4 vật thể;
- Nhận diện nhiễu, không báo động, ghi nhận và đo đạc nhiễu. Ví dụ: lá cây rung rinh, bụi, nhiễu nền ánh sáng mặt trời;
- Cảnh báo vật thể nhỏ. Ví dụ: động vật nhỏ, vật thể nhỏ bay qua;
- Báo động xâm nhập. Ví dụ: động vật lớn, người xâm nhập vượt qua hàng rào;
- Báo động xâm nhập điện tử. Ví dụ: Hacker đang tìm cách xâm nhập điện tử;

ƯU TRỘI

WIPO WORLD INTELLECTUAL PROPERTY ORGANIZATION

3

CryptoDefense

Tấn công mật mã hầu như bất khả thi với nền tảng điện toán hiện nay

- CypherKey: Khóa mã nhiều thành phần
- Chống lại 3 cấp độ tấn công mật mã

CypherKey: chìa khóa giải mật		
MasterKey nhà sản xuất	UserPIN người sử dụng	Random Seed hệ thống

Tấn công cấp độ 1:

Điều kiện:

- Không biết CypherKey,
- Không tiếp xúc trực tiếp với hàng rào, không thể nghe lén random_token

➪ không có bảng mã, không có mã rõ

Phương thức tấn công:

- Giả mạo dữ liệu, hoặc thu lại tín hiệu trên đường truyền, hòng tìm ra quy luật lặp lại ➪ **không thể,** vì dữ liệu truyền trên đường truyền là khác nhau mỗi sesion, và trong mỗi session phân bố thông tin trong dữ liệu rất gần với phân bố đều (ngẫu nhiên)

Tấn công cấp độ 2: Tấn công giả mạo dữ liệu truyền qua các chùm tia trong mỗi session

10^{70}/s

NOT AVAILABLE

Điều kiện:

- Không biết CypherKey,
- Tiếp xúc trực tiếp với hàng rào ➪ có thể nghe lén random_token vì random_token được truyền không mã hóa trên đường truyền PackTransfer

Phương thức tấn công: giả mạo dữ liệu,

Để thực hiện được tấn công này, Oscar phải tấn công mã CypherKey dài 256 bits. Cách duy nhất hiệu quả là phương pháp BruteForce 2^{256} trường hợp trong vòng 1 epoch (từ 1 ngày đến 1 tháng); tương đương cỡ 10^{70} phép thử trong 1 giây, sức mạnh tính toán này chưa tồn tại, ngay cả cộng gộp tất cả siêu máy tính và các thiết bị điện tử rời rạc cũng chưa đủ. ➪ Chưa có công cụ đủ sức mạnh để tấn công. Tức là không thể tấn công.

Tấn công cấp độ 3:

10^{30}/s

NOT AVAILABLE

Điều kiện:

- Không biết CypherKey, nhưng bằng cách nào đó biết được UserPIN của User, đồng thời bằng cách nào đó biết được MasterKey của Coder và đã đọc toàn bộ tài liệu này; nhưng không biết Seed. Lưu ý rằng điều kiện này rất khó đạt được, vì user cất rất kỹ UserPIN, nhưng giả định rằng có khả năng xảy ra.
- Tiếp xúc trực tiếp với hàng rào, nghe lén random_token vì random_token được truyền không mã hóa trên đường truyền PackTransfer
- Đây là điều kiện được cho là tốt nhất, khi phe tấn công biết được rất nhiều thông tin về hệ thống đang vận hành (toàn bộ đặc tính kỹ thuật, thuật toán).

Phương thức tấn công: tấn công hòng tìm ra CypherKey

Để thực hiện được tấn công này, Oscar phải tấn công mã khi chưa biết Seed. Trong khi Seed là 1 hoán vị ngẫu nghiên 32 phần tử do hệ thống sinh ra mỗi epoch. Cách duy nhất hiệu quả là phương pháp BruteForce cho 32! (32 giai thừa) trường hợp hoán vị Seed trong vòng 1 epoch cỡ 1 ngày đến 1 tháng; tương đương cỡ 10^{30} phép thử trong 1 giây, sức mạnh tính toán này chưa tồn tại, ngay cả cộng gộp tất cả siêu máy tính và các thiết bị điện tử rời rạc cũng chưa đủ.

➪ Chưa có công cụ đủ sức mạnh để tấn công. Tức là không thể tấn công.

Điều này cũng hàm ý rằng, ngay cả coder hay người vận hành hệ thống cũng không có năng lực tấn công mật mã vào hệ thống này.

Giới thiệu Công ty

Onyx

4

THÀNH LẬP

Được thành lập từ năm 2015, dựa trên đội ngũ nghiên cứu và phát triển sản phẩm của Công ty Cổ phần Công nghệ Thông minh, đơn vị có bề dày truyền thống nghiên cứu và phát triển các ứng dụng điện tử nhúng từ năm 2005.

ĐỘI NGŨ

Onyx Techlab ban đầu là phòng thí nghiệm công nghệ bảo mật phần cứng, một lĩnh vực mới với nhiều bài toán xã hội nóng bỏng.

Vượt qua khó khăn và thách thức, Onyx xây dựng được đội ngũ chuyên gia có trình độ cao, năng động, sáng tạo, khát vọng tạo ra các sản phẩm công nghệ cao cạnh tranh với hàng nhập ngoại.

TRIẾT LÝ

Phát triển bền vững trên cơ sở các giá trị của nhân văn là triết lý kinh doanh của chúng tôi.

Giới thiệu Công ty

Onyx

4

SỨ MỆNH

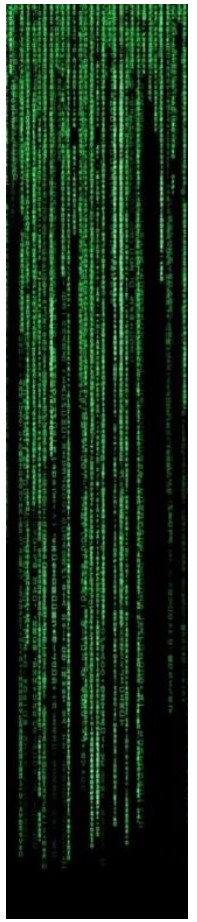
Keep believing!
Sứ mệnh của chúng tôi là bảo vệ con người

TẦM NHÌN: LĨNH VỰC BẢO MẬT PHẦN CỨNG IoT

Ngày nay, khi công nghệ kỹ thuật số đã kết nối vạn vật, lĩnh vực bảo mật không còn là chỉ trọn vẹn trong các ứng dụng phần mềm trên máy tính cá nhân. Thông tin và kèm theo đó là bảo mật thông tin đều lan tỏa đến vô số ứng dụng khác trong cuộc sống.

Chúng tôi hướng tới Ngôi nhà **an toàn hơn**, Xã hội **an toàn hơn**, Thế giới **an toàn hơn**, thay vì thông minh hơn. Trong tương lai không xa, máy móc sẽ ngày càng thông minh nhưng cũng cần tin cậy hơn.

Chúng tôi tiên phong khai phá miền đất mới này. Đây là miền đất mới với nhiều bài toán khó, những thử thách khó nhất, và cũng ẩn chứa những phần thưởng lớn nhất.



Theo Karpersky, trong 6 tháng đầu năm 2021 có 1.51 tỉ vụ tấn công vào các thiết bị IoT trên toàn cầu. Tức là tăng hơn gấp đôi so với cùng kỳ năm trước.

Xem thông tin tại www.iotworldtoday.com

Thành tựu

4

Onyx hiện đã có nhiều sáng chế trong lĩnh vực bảo mật phần cứng. Bao gồm:

- **CyLock**: Công nghệ khóa điều khiển từ xa mới, thay thế công nghệ Rolling-code đã tồn tại 30 năm.
  [Sáng chế thế giới WIPO số WO2021174264 ⇔ do KIPO – sáng chế Korea - thẩm định]
- **eFence**: Công nghệ hàng rào điện tử mới, mở ra ứng dụng Hàng rào biên giới.
  [Sáng chế thế giới WIPO số WO2022043756 ⇔ do EPO – sáng chế Europe – thẩm định]
- **TrueOrigin**: Công nghệ định danh hàng hóa chống giả mạo, Xác thực Xuất xứ.
  [Sáng chế thế giới WIPO số WO2022094635 ⇔ do EPO – sáng chế Europe – thẩm định]
- **OnyxCypher**: Mã hóa ngẫu nhiên Kháng lượng tử.
  [Sáng chế thế giới WIPO số WO2022170370 ⇔ do EPO – sáng chế Europe – thẩm định]
- **TrustFaceID**: Công nghệ xác thực danh tính con người sử dụng trí tuệ nhân tạo, hiệu quả hơn, bảo vệ danh tính.

Onyx Cypher

CyLock SAFETY CYPHER LOCK

eFence electronic security fence

True Origin™ KEEP BELIEVING

TrustFaceID

Startup Academy Vietnam Google NIC

Google Startup Academy

Sao Khuê 2020 2021 2022

Smart City Award 2022

Vietnam Venture Summit 2022

ĐỘI NGŨ CỦA CHÚNG TÔI

Tuan Nguyen Khuong

Inventor, Founder, CTO

Tuấn có hơn 17 năm kinh nghiệm trong lĩnh vực phát triển sản phẩm, công nghệ và kinh doanh với tư cách là người sáng lập một số công ty khởi nghiệp công nghệ. Đam mê đổi mới công nghệ trong ngành bảo mật.

Ngoc Tran Dinh

Co Founder, CEO

Ngọc làm việc tại các công ty đa quốc gia, với hơn 15 năm kinh nghiệm trong thị trường B2B.
Đam mê thiết lập sự hợp tác để mang lại nhiều lợi ích.

Hung Nguyen Van

Co Founder, CMO

Hùng có hơn 15 năm kinh nghiệm trong việc kết nối và cung cấp các giải pháp công nghệ cho khách hàng. Đam mê thiết lập sự hợp tác kết nối để mang lại nhiều lợi ích.

Trung Ha Thanh

PhD in Statistics, Univ. of Florida, USA

Think tank,
Advisor

Tiến sĩ Trung thích giải quyết các vấn đề lớn của cộng đồng. Đam mê thiết lập các hệ thống để giúp đỡ mọi người.
Tiến sĩ Trung là tác giả của mô hình dự báo covid có độ chính xác rất cao:
https://onyx.vn/covid19

Nguyet Nguyen Mai

Advisor

Mrs. Nguyet is the Director of Business Consulting, with 16 years of experience working at Ernst & Young Vietnam,

Bà Nguyệt phụ trách tư vấn các dự án chuyển đổi doanh nghiệp, quản lý và phục hồi rủi ro, cấu trúc doanh nghiệp.

Tan Le Thanh

Market advisor

Với 16 năm kinh nghiệm làm việc cho các Ngân hàng lớn, Ông Tân mang đến góc nhìn chân thực về thị trường.

MỘT SỐ SẢN PHẨM TIÊU BIỂU TỪ ĐỘI NGŨ ĐÃ THỰC HIỆN

SmartMEDIA

Máy bán hàng tự động

Kiosk

SmartQMAN

Từ 2005

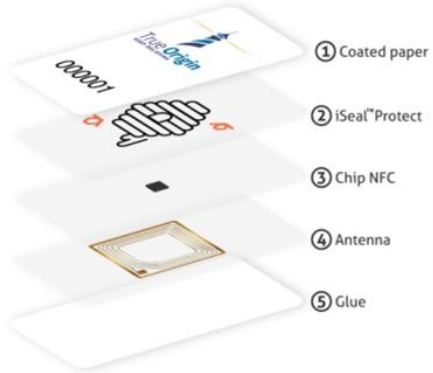
TrustFACEID

CyLock

Unhackable Lock
Khóa từ xa an toàn chống Hacker

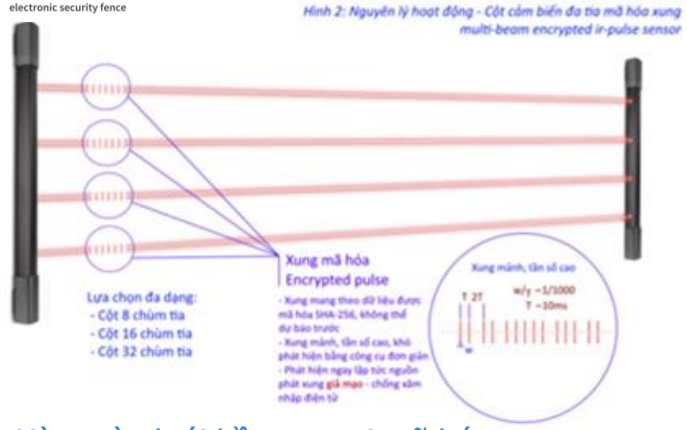
TrueOrigin

KEEP BELIEVING



eFence

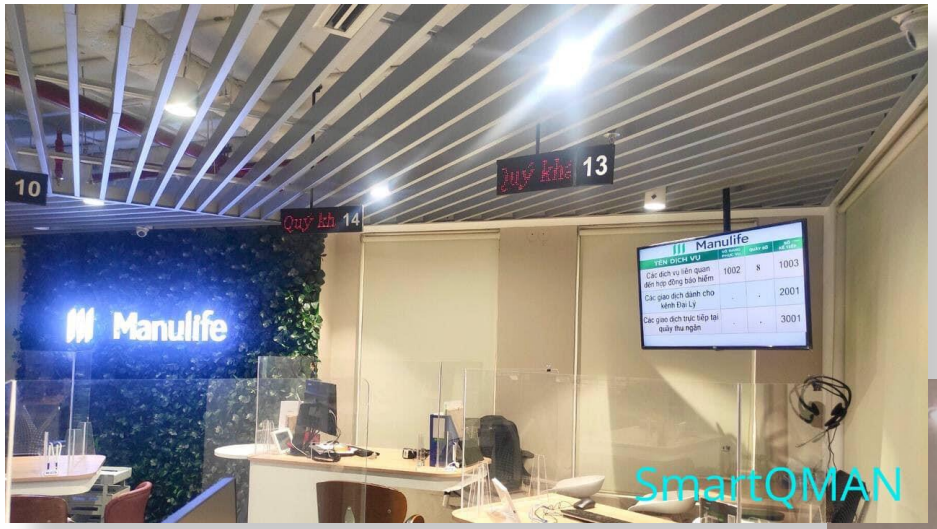
electronic security fence



Hàng rào lưới hồng ngoại mã hóa
Chống hacker

Phần tiếp theo: Giới thiệu công nghệ và trả lời câu hỏi...

MỘT SỐ KHÁCH HÀNG SỬ DỤNG SẢN PHẨM ĐẾN TỪ ĐỘI NGŨ CỦA CHÚNG TÔI



Manulife - the top1 life insurance in Vietnam

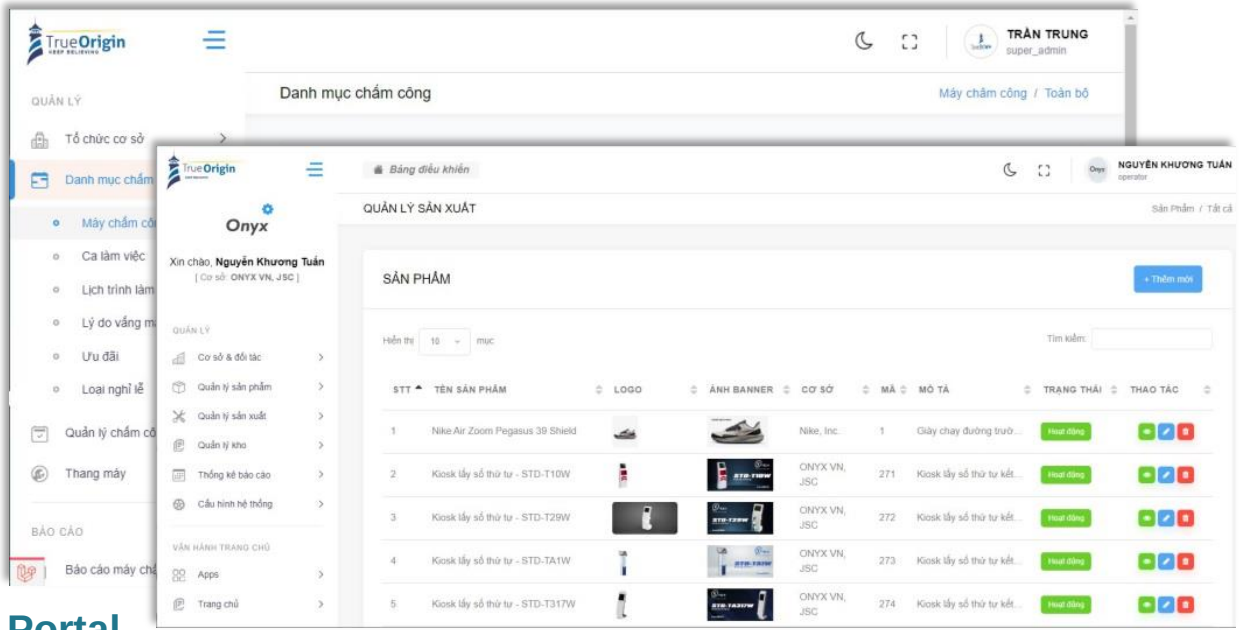
Quality has been verified

Vietnamese solution
Vietnamese technology
Made in Vietnam

Vietcombank - the top1 bank in Vietnam

Samsung - the top1 electronic maker in the world

KHÁCH HÀNG ĐANG SỬ DỤNG



Portal

iStamp

iTap

KHẢ NĂNG HỢP TÁC

5

KHAI THÁC CÔNG NGHỆ

- Đối tác thương mại sản phẩm tại Việt Nam
- Đối tác thương mại sản phẩm phạm vi Quốc tế
- Đối tác thương mại quyền Khai thác sáng chế

CHUYỂN GIAO CÔNG NGHỆ

- Chia sẻ quyền Khai thác sáng chế
- Chia sẻ hệ thống ứng dụng đã hoàn thiện
- Cùng hợp tác khai thác sáng chế và công nghệ lõi

PHÁT TRIỂN ỨNG DỤNG MỚI

- Cùng nghiên cứu khám phá các ứng dụng mới

TrustFaceID

CyLock
SAFETY CYPHER LOCK

Onyx
Cypher

TrueOrigin
KEEP BELIEVING

eFence
Hàng rào điện tử bảo mật

Trân trọng cảm ơn!

think in simple way, do in detailed way,