PHÂN TÍCH BẰNG SÁNG CHẾ

Phát Hiện Các Cuộc Tấn Công Vishing

Bằng sáng chế US 10,970,394 B2 | Phát triển bởi BioCatch Ltd.

Công Nghệ Phân Tích Hành Vi Người Dùng Để Ngăn Chặn Gian Lận Viễn Thông

Tổng Quan Bằng Sáng Chế

Số hiệu: US 10,970,394 B2

Ngày cấp: 06/04/2021

Chủ sở hữu: BioCatch Ltd.

Lĩnh vực: An ninh mạng & Sinh trắc học hành vi

Ý TƯỞNG CỐT LÕI

Tập Trung Vào "Cách Thức" Giao Dịch

Hệ thống không chỉ xác minh **danh tính** (Ai đang dùng) mà tập trung vào **hành vi** (Đang dùng như thế nào). Ý tưởng trung tâm là xác định xem người dùng có đang bị cưỡng ép hoặc làm theo hướng dẫn của kẻ tấn công hay không.

Phát hiện sự hiện diện của bên thứ ba thông qua dữ liệu cảm biến và tương tác UI.

THÁCH THỨC CỦA TẤN CÔNG VISHING

- **Thất bại của bảo mật truyền thống:** Các phương pháp 2FA hoặc kiểm tra IP thường vô hiệu vì nạn nhân là người dùng thật, sử dụng thiết bị thật và thông tin thật.
- **Sự tự nguyện bị thao túng:** Nạn nhân tin rằng họ đang thực hiện giao dịch hợp pháp (ví dụ: chuyển tiền an toàn) theo hướng dẫn qua điện thoại.
- **Kỹ thuật tâm lý (Social Engineering):** Kẻ tấn công tạo áp lực thời gian và sự sợ hãi để nạn nhân bỏ qua các quy trình kiểm tra thông thường.

3 TRỤ CỘT PHÁT HIỆN CHÍNH

Đối Soát Playbook

So sánh chuỗi thao tác thực tế với các kịch bản tấn công vishing đã biết.

Chỉ Số Hành Vi

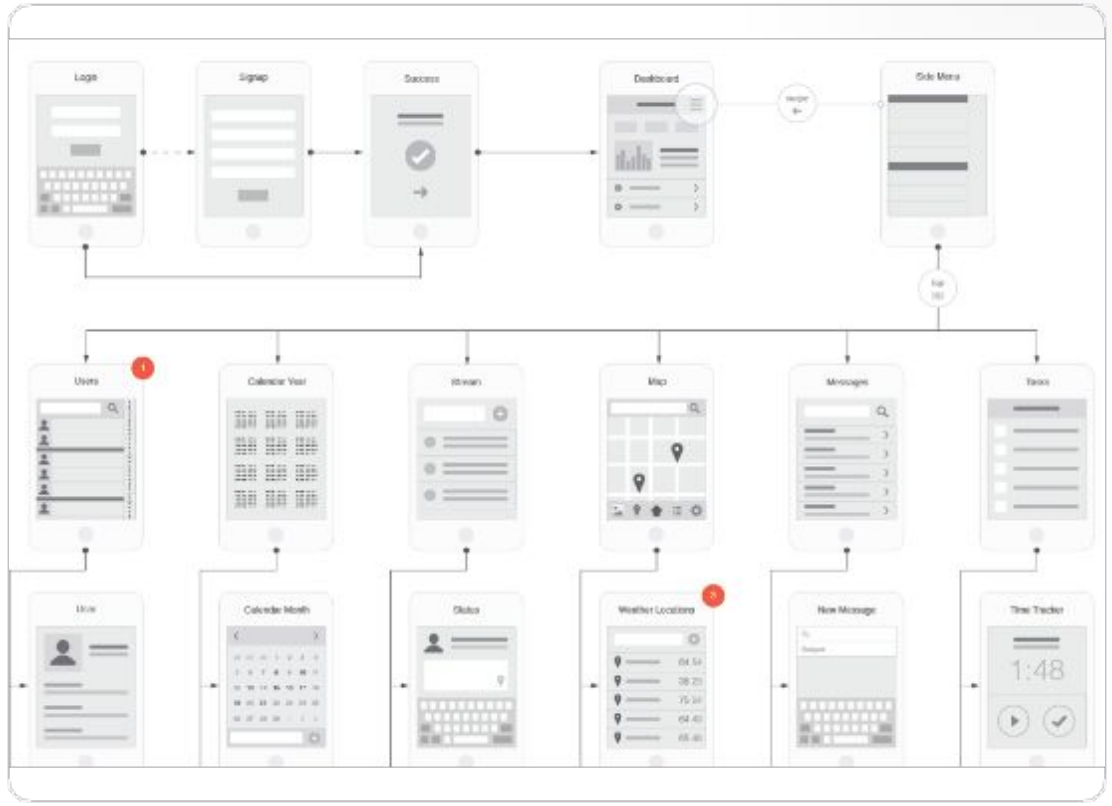
Phân tích nhịp điệu gõ phím, di chuyển chuột và dấu hiệu căng thẳng.

Cảm Biến Không Gian

Sử dụng Gyroscope/Accelerometer để nhận diện tư thế cầm máy.

PILLAR 1: ĐỐI SOÁT KỊCH BẢN (PLAYBOOK)

- **Phân tích luồng UI:** Theo dõi trình tự Engagement với giao diện (ví dụ: đăng nhập → kiểm tra số dư → chuyển khoản ngay).
- **Điểm rủi ro:** Nếu trình tự khớp với các bước kẻ tấn công thường yêu cầu, hệ thống tự động tăng mức cảnh báo rủi ro.



PILLAR 2: HÀNH VI DƯỚI ÁP LỰC (DURESS)

Doodling (Vẽ nguệch ngoạc): Chuyển động con trỏ lặp lại vô định trong lúc nghe hướng dẫn.

Typing Rhythm: Thay đổi tốc độ gõ phím và lỗi đánh máy do bị phân tâm bởi cuộc gọi.

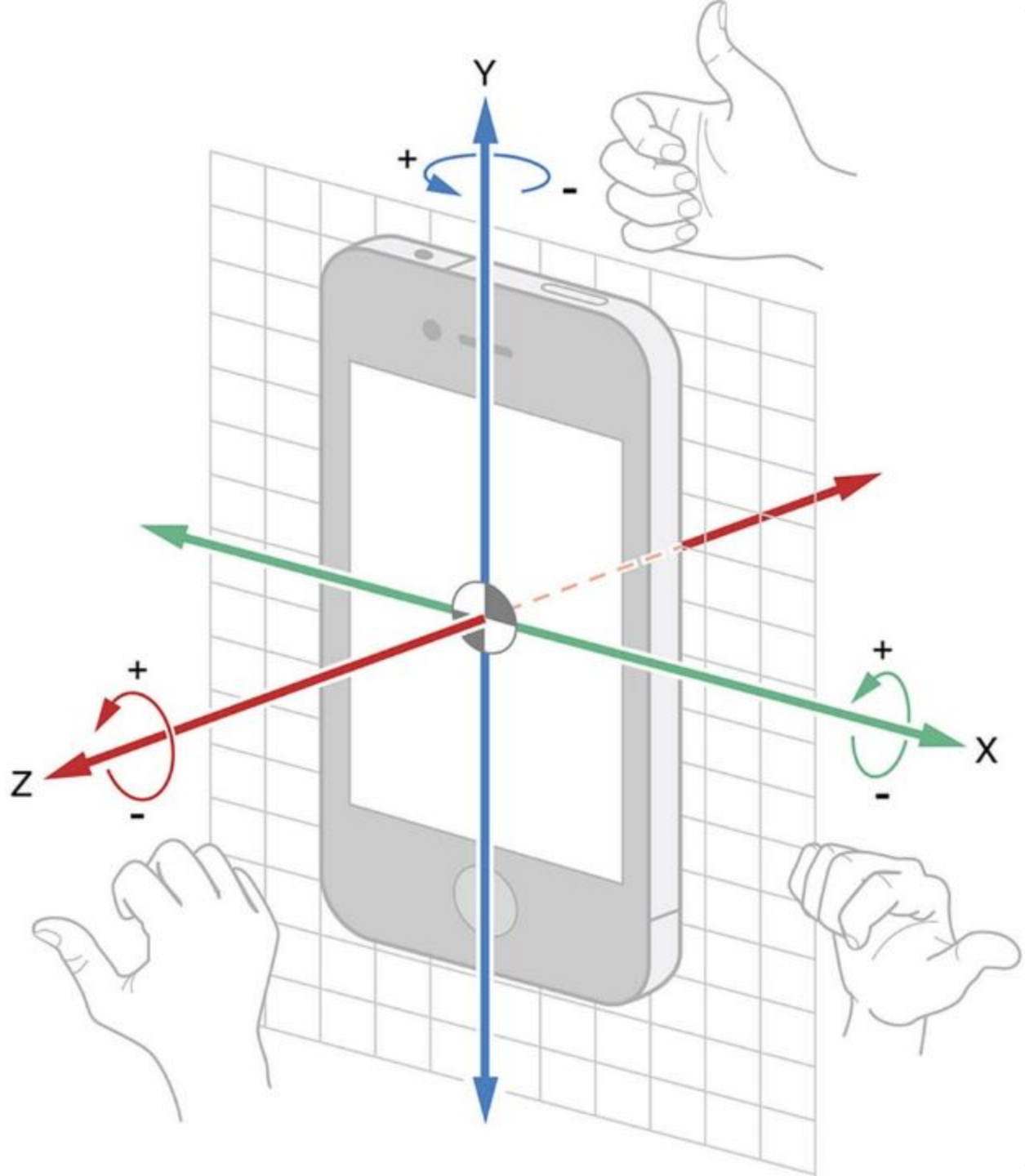
Thao tác một tay: Nhận diện mẫu tương tác đặc thù khi tay kia đang cầm điện thoại.

PILLAR 3: CẢM BIẾN KHÔNG GIAN

Nhận Diện Tư Thế Thiết Bị

Sử dụng dữ liệu từ con quay hồi chuyển (gyroscope) và gia tốc kế (accelerometer) để xác định vị trí thực tế của smartphone.

- **Mẫu sử dụng luân phiên:** Thiết bị thay đổi liên tục giữa vị trí áp tai (nghe) và nằm ngang (tương tác UI).
- **Góc cầm máy:** Phát hiện độ nghiêng bất thường chỉ có khi người dùng vừa nghe điện thoại vừa nhìn màn hình.



CẤU TRÚC HỆ THỐNG & MODULE

Module Chính	Chức Năng Chi Tiết
Vishing Attack Detector (177)	Đơn vị phân tích trung tâm, tổng hợp dữ liệu từ UI, cảm biến và hành vi để đưa ra quyết định.
Fraud Mitigation Module (156)	Thực thi các biện pháp ngăn chặn tự động: Tạm dừng, gắn cờ rủi ro hoặc khóa tài khoản.
Phân Tích NLP (Tùy chọn)	Quét mẫu âm thanh từ microphone để tìm các từ khóa chỉ dẫn thường gặp trong kịch bản lừa đảo.

PHẢN ỨNG & GIẢM THIỂU RỦI RO

Ngăn Chặn Tức Thời

Hệ thống có thể tạm dừng giao dịch ngay khi phát hiện dấu hiệu vishing, yêu cầu xác thực bổ sung qua kênh an toàn hơn.

Bảo Vệ Tài Khoản

Khóa tạm thời các quyền truy cập nhạy cảm nếu điểm rủi ro vượt ngưỡng, bảo vệ tài sản ngay cả khi nạn nhân bị lừa cung cấp OTP.

Giá Trị Thực Tiễn & Chiến Lược

Bằng sáng chế này cung cấp một **lớp bảo vệ tự trị (autonomous)**, giúp các tổ chức tài chính bảo vệ khách hàng ngay cả khi họ đang "tự nguyện" thực hiện giao dịch dưới sự thao túng của tội phạm.

> Giải pháp vượt xa các hệ thống xác thực tĩnh hiện tại.

Hỏi & Đáp

Cảm ơn bạn đã theo dõi bài thuyết trình về bằng sáng chế US 10,970,394 B2.

liên hệ: info@biocatch.com

www.biocatch.com

IMAGE SOURCES

https://media.istockphoto.com/id/1444868168/vector/footprint-digital-technology-on-blue-drak-background-biometric-identity-protection.jpg?s=612×612&w=0&k=20&c=DHbRrKq6a4Zo9P0Ovusre_oa4VkPEDijRHz9hZ7_e70=

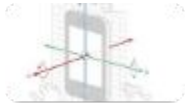
Source: www.istockphoto.com

http://uxkits.com/cdn/shop/products/mobile-flows-1.png?v=1575404446&width=2048

Source: uxkits.com

https://res.cloudinary.com/peloton-cycle/image/fetch/f_auto,c_limit,w_3840,q_90/https://images.ctfassets.net/6ilvqec50fal/1kftmlLZc2gNKm8QW9NRqs/fb5dc751901d69e1695af69717305a0d/mentally-exhausted-01.jpg

Source: www.onepeloton.com



https://miro.medium.com/v2/resize:fit:1400/0*bS8im7IxVmW4DK9o.jpg

Source: medium.com

https://static.vecteezy.com/system/resources/previews/006/970/875/non_2x/shield-icon-of-cyber-security-digital-data-digital-data-network-protection-global-network-5g-high-speed-internet-connection-and-big-data-analysis-background-photo.jpg

Source: www.vecteezy.com