



Business Innovation & Planning
8(a), DBE, ESB, MOSB



Mind Moto, LLC
an invention company

Teaming Together in Small Business Innovation

Secure Electric Receptacle

an R&D proposal for Hardware Development related to National Security

June 2022

Management Team and Inventors

A Teaming Effort by 2Matoe and Mind Moto



Raul Acosta
CEO/President: 2Matoe



Kas Kasravi, C.Mfg.E., ME, JD
Founder: Mind Moto
Professor: Univ. of Michigan
Retired: HP Fellow and VP
Inventor of 29 patents



Jim Lucari
Senior Manager: HPE
Inventor of multiple patents



Don McKracken
Solution Architect: HPE
Inventor of multiple patents

Need Statement

Any facility with electric power is a security attack surface

- Buildings, warehouses, storage areas, mobile units etc.

An inside cyber threat actor (iCTA) is a person who has bypassed physical access protocols and gained access to a secure facility

iCTAs can set up devices inside a facility and access internal systems:

- Gather sensitive information
- Install malware
- Engage in espionage
- Steal IP
- Expose secrets
- and more...



There is a need to protect an entire infrastructure from iCTAs

Examples

Insider hacking is an underreported, pernicious and difficult-to-detect cyber-security threat.

- [Link](#)
- In 2008, an insider attack occurred when Terry Childs, a network engineer for the San Francisco Department of Telecommunications and Information Services, altered the city's network passwords, locking FiberWAN access for 12 days. Childs was found guilty of felony network tampering. The work required to regain system control cost the city of San Francisco \$900,000, and 60 percent of city services were affected by the insider attack.
 - [Link](#)

Value Proposition

Protects an entire infrastructure and sensitive information systems therein from iCTAs

Denys iCTAs of electric power, rendering their devices useless beyond normal battery life

- Yet provides electric power to all authorized personnel

Highly applicable to areas where iCTAs can operate out of sight

- Storage rooms, conference rooms, unused offices, etc.

Our Innovation's Magic Sauce

Denies electric power to iCTAs

- Render's iCTAs devices useless and unable to access internal systems

A key is assigned administratively to each authorized user or device for access to specific electric outlets(s) during specific times

Physical manipulation of an electric outlet will not help an iCTA

- No backdoor

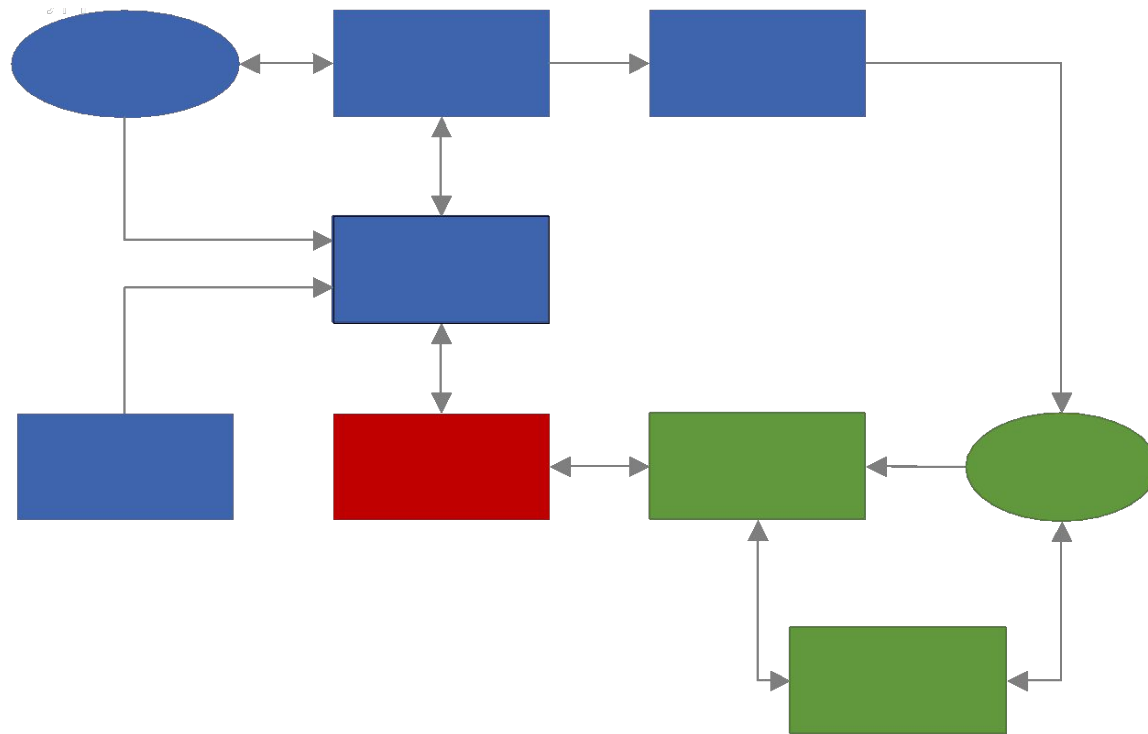
PATENTED

2MAT[®]OE



Illustration

A simple illustration of how our invention works



Competitive Analysis

Existing security systems address different attack surfaces

- Encryption
- Passwords
- Physical access to a building

No existing solution exists for disabling an iCTA by denying electric power

Current Status

Concept developed

Specifications developed

US patent granted (# 11,256,831)

- Additional patent pending (# 17/488,023)

A functional prototype developed and tested



Request

- \$275,000+ requested (estimated)
- 6 – 9 months
- Refine idea, prototype backend software for key generation and analytics, and develop 1-room full-scale operational model
- Investigate multiple use cases
- Evaluate potential for filing additional patent(s)

Want to invest in the Hardware/SITE security of the future? Please contact info@2matoe.com or call (719) 257-3137

