Advancing USF **Innovation**

Security Technologies

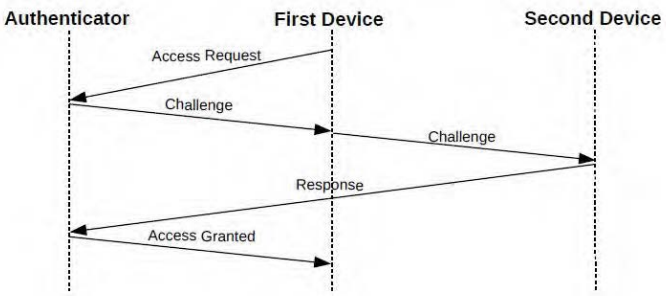
University of South Florida

Cyber Security: Authentication and Biometric Systems

Biometric and Dynamic-Code Protected Token Decryption Method and Device

Compact and portable authentication/decryption device that incorporates a fingerprint biometric, token, and decryption key that attaches to the USB port of any computer. This device is used for various physical security measures.

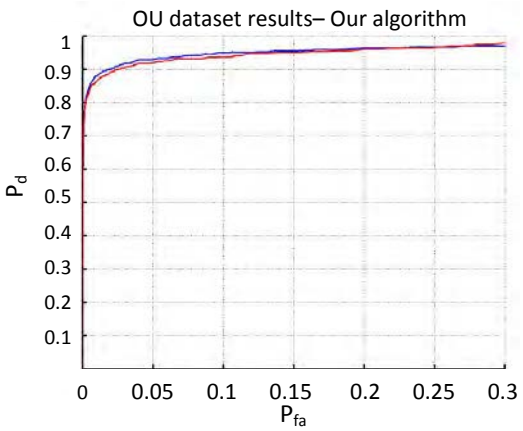
USF Tech ID# 05A052
US Patent # 8,127,142



Systems and Methods for Co-Authentication using Multiple Devices

A co-authentication system where at least two registered devices collaboratively authenticate a user. This allows multi-factor security with single-factor convenience.

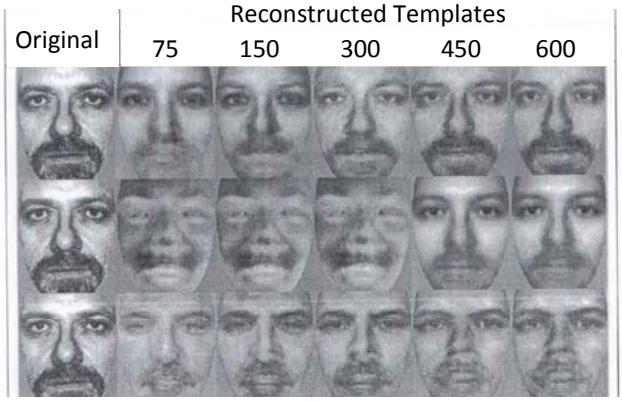
USF Tech ID# 14A079
US Patent # 9,659,160; 9,380,058



Orientation Invariant Gait-Matching

A novel orientation invariant gait-matching algorithm that allows accurate gait recognition irrespective of the sensor orientation without prior training. This can be used to build a robust gait model using wearable devices (smartphones, etc.) which can be utilized as a biometric for various purposes such as authentication.

USF Tech ID# 14B164
US Patent # 9,877,668



Reconstruction of Biometric Image Templates Using Match Sets

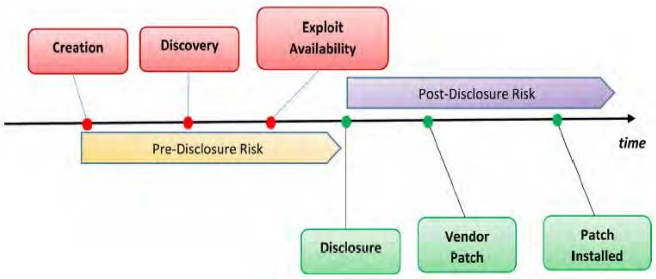
A novel paradigm to reconstruct face templates from match scores while increasing security and privacy by utilizing a linear approach.

USF Tech ID# 07A044
US Patent # 8,165,352; 8,331,632

Contact us: 3802 Spectrum Blvd., Suite 100 Tampa, FL 33612 – 813.974.0994 patents@research.usf.edu | http://www.research.usf.edu/pl

University of South Florida

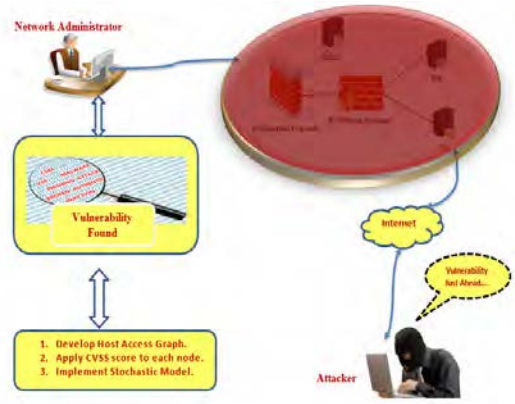
Cyber Security: Diagnostic Tools for Evaluating Network Vulnerability



Stochastic Modeling of Vulnerability Life Cycle and Security Risk Evaluation

Statistical model that can give accurate probability of a vulnerability being exploited as a function of time.

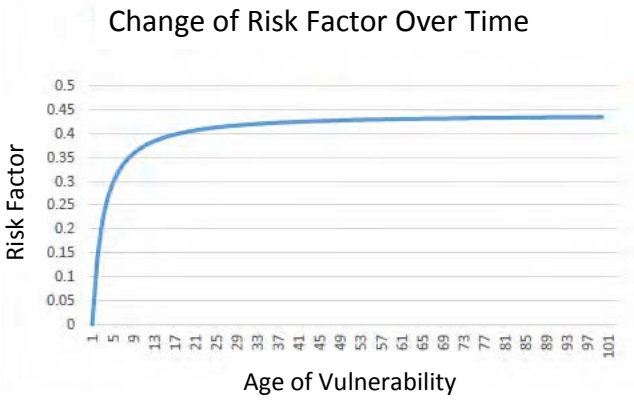
USF Tech ID# 17A015
Patent Pending



Cybersecurity Analytical Methods to Determine Overall Network Security Risk

A stochastic model to quantify the risk associated with a computer network. This methodology provides a ranked list of priorities so network administrators can make software patch decisions.

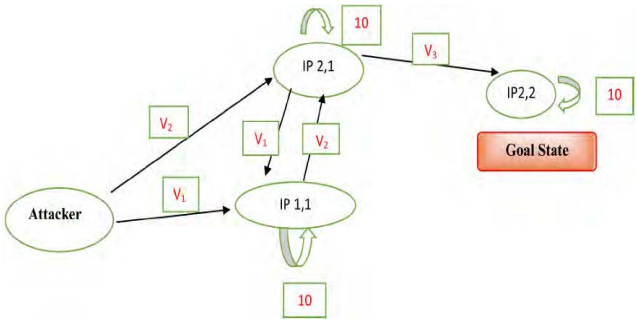
USF Tech ID# 16B141
Patent Pending



Cyber Security: Nonlinear Stochastic Models for Predicting the Exploitability

Statistical models for assessing the risk of a cyber-security risk at time "t" in application and system platforms.

USF Tech ID# 16B171
Patent Pending



Cybersecurity-Statistical Predictive Model for Expected Path Length

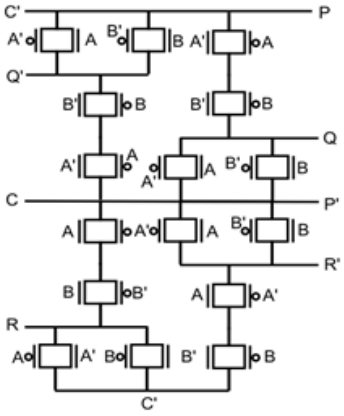
Statistical model that predicts the number of steps an attacker will take to compromise a system (expected path length). Using this information network administrators can take precautions to minimize vulnerabilities.

USF Tech ID# 17A014
Patent Pending

Contact us: 3802 Spectrum Blvd., Suite 100 Tampa, FL 33612 - 813.974.0994 patents@research.usf.edu | http://www.research.usf.edu/pl

University of South Florida

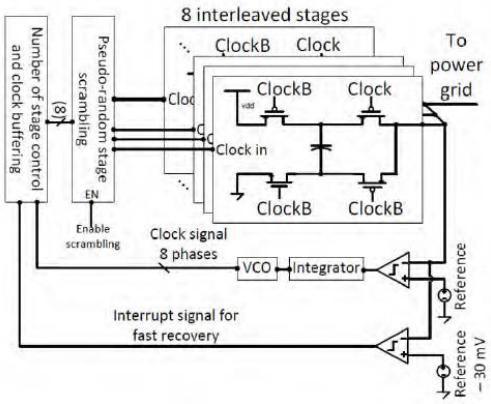
Cyber Security: Hardware-Based Security



Design of Adiabatic Dynamic Differential Logic for DPA-Resistant Secure Integrated Circuits

A low cost method of producing secure integrated chips resistant to differential power analysis (DPA) side channel attacks which are used to break cryptosystems.

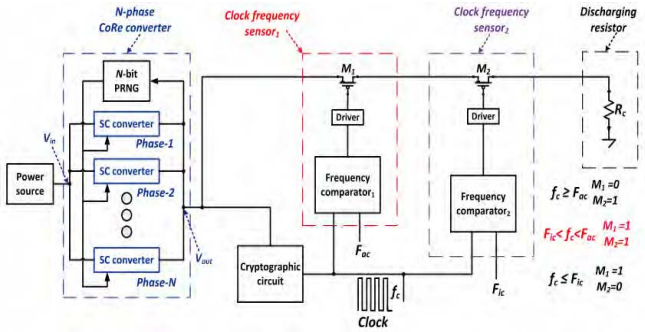
USF Tech ID# 13B129
US Patent # 9,531,384



Converter-Gating for Efficient and Secure Power Delivery

Dynamic power management techniques and voltage converter architectures were created to provide a secure and efficient on-chip power delivery system which is resistant to side channel attacks.

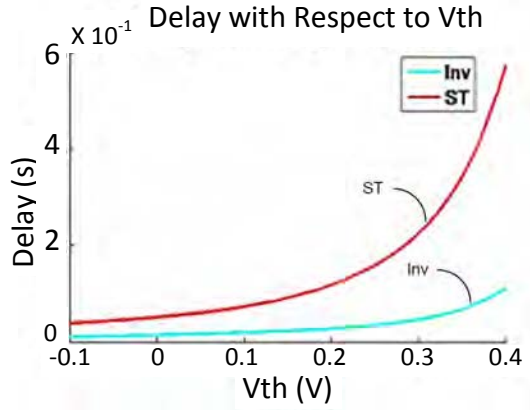
USF Tech ID# 14A066
US Patent # 9,812,954; 9,748,837



Security-Adaptive Voltage Conversion as a Lightweight Countermeasure Against LPA Attacks

A low overhead and lightweight countermeasure to prevent leakage power attacks (LPA) used to crack cryptographic circuits.

USF Tech ID# 17A059
Patent Pending



Aging-Sensitive Recycling Sensors for Chip Authentication

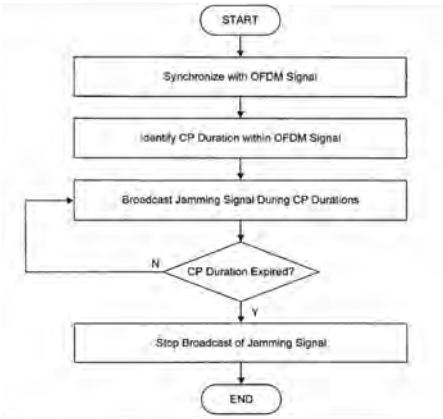
Specifically crafted sensors based on tailored to amplify the aging mechanisms and detect recycling of integrated chips of hours to days.

USF Tech ID# 14B117
Patent Pending

Contact us: 3802 Spectrum Blvd., Suite 100 Tampa, FL 33612 – 813.974.0994 patents@research.usf.edu | http://www.research.usf.edu/pl

University of South Florida

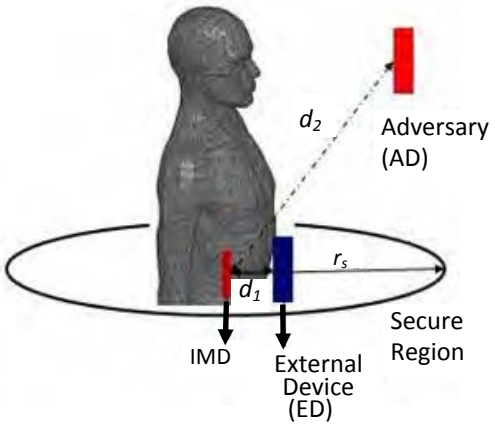
Cyber Security: Secure Wireless Communications



Friendly CP Jamming for Physical Layer Security

Friendly CP jamming is a simple method which broadcasts a jamming signal during the cyclic prefix (CP) to interfere with the signal an eavesdropper receives, which prevents him/her from decoding the information correctly. Since the signal is only sent during the CP the message is properly decoded by the legitimate recipient.

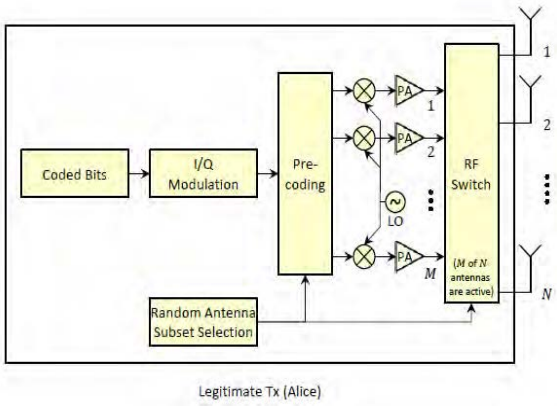
USF Tech ID# 15A034
Patent Pending



Physical Layer Security for Wireless Implantable Medical Devices

Novel authentication mechanism for implanted or wearable medical devices to protect against adversaries malicious attempts to control them.

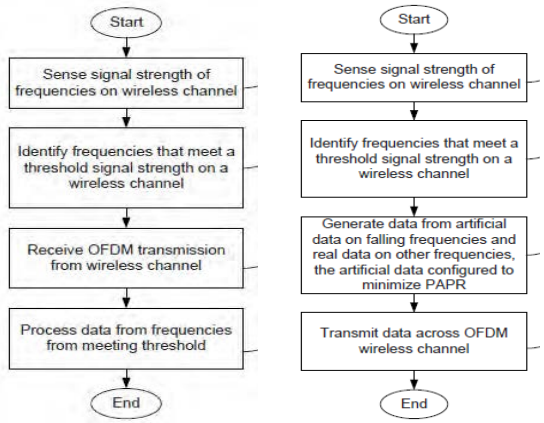
USF Tech ID# 15B112
Patent Pending



Channel-Based Coding for Wireless Communication

An advanced novel transmission scheme based on channel pre-coding and adaptive antenna subset selection in MISO wireless systems for highly secure and resilient communication links between the legitimate transmitter and receiver.

USF Tech ID# 14A018
US Patent # 9,722,841



Joint Physical Layer Security and PAPR Reduction with Irrelevant Data for OFDM Systems

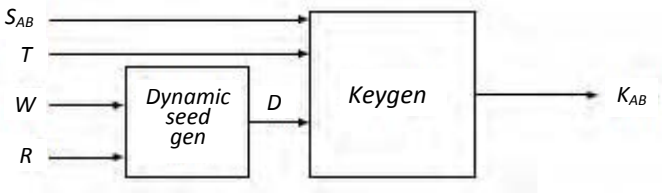
Signal design technique combining physical layer security and peak-to-average power ratio (PAPR) mitigation for Orthogonal Frequency Division Multiplexing (OFDM) based waveforms.

USF Tech ID# 14B149
US Patent # 9,479,375

Contact us: 3802 Spectrum Blvd., Suite 100 Tampa, FL 33612 - 813.974.0994 patents@research.usf.edu | http://www.research.usf.edu/pl

University of South Florida

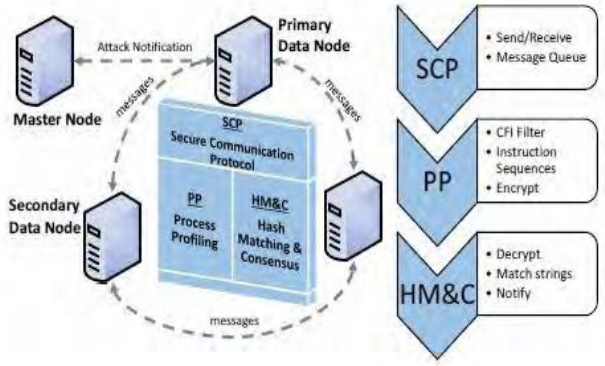
Cyber Security: Cryptography & Intrusion Detection



Systems and Methods for Generating Symmetric Cryptographic Keys from Possibly Different Inputs, Through Cyphertext Communications

This invention enables Internet-of-Things devices within a building to generate strong, time-limited cryptographic keys, unavailable to attackers outside the building.

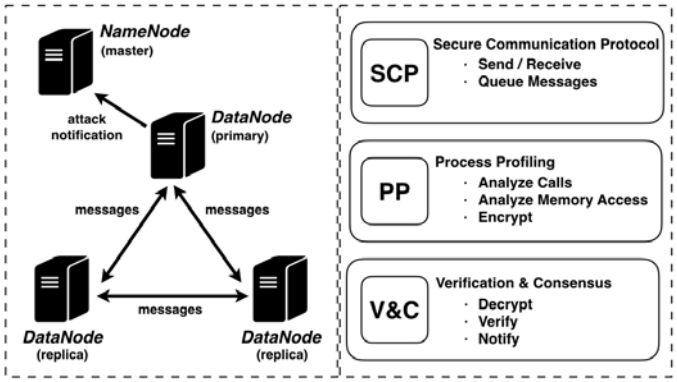
USF Tech ID# 17A042
Patent Pending



A System Architecture for the Detection of Security Threats in Big Data Systems

Two new systems for detecting insider attacks (e.g. authorized IT administrators) and other process level intrusions of big data systems.

USF Tech ID# 16A061
Patent Pending



Runtime Methods for Detecting Attacks in Big Data Systems

Method for real-time detection of insider attacks in big data platforms during runtime .

USF Tech ID# 16B197
Patent Pending

The University of South Florida is a high-impact global research university dedicated to student success. Over the past 10 years, no other public university in the country has risen faster in U.S. News and World Report's national university rankings than USF. Serving more than 50,000 students on campuses in Tampa, St. Petersburg and Sarasota-Manatee, USF is designated as a Preeminent State Research University by the Florida Board of Governors, placing it in the most elite category among the state's 12 public universities.

USF has earned widespread national recognition for its success graduating under-represented minority and limited-income students at rates equal to or higher than white and higher income students. USF is a member of the American Athletic Conference. Learn more at www.usf.edu.

Contact us: 3802 Spectrum Blvd., Suite 100 Tampa, FL 33612 - 813.974.0994 patents@research.usf.edu | http://www.research.usf.edu/pl