devastating capability, revolutionary advantage

Extracting Novel Information from Digital Data:

What do behavioral biometrics tell us?

New York Cyber Security Conference (NYCSC) 2016

Robert Dora
dorar@ainfosec.com
Assured Information Security, Inc.
June 8, 2016

Presentation Overview

Presentation Goal:

- Describe the current state-of-the-art in this realm
  - Verifying or identifying users, identifying demographic features, detecting cognitive states, and generating user profiles

Focus:

- Information that can be extracted from a computer without any specialized equipment or hardware
- Using publicly available or open-source sensors
- Paying special attention to keystroke dynamics research over the last few years

Presentation Overview

My Background

- B.S. Software Engineering (2009), minor in Psychology
- M.S. Social Psychology (2013)
- CISSP in 2013
- Joined AIS in 2009
- Expertise in Keystroke Dynamics, Data Analysis, and Human-Computer Interaction

Assured Information Security, Inc. (AIS)

- Cyber Security Research & Development
- Computer Network Operations, Trusted Computing, Computer Forensics, Vulnerability Assessments, Reverse Engineering, Sensor Development

Presentation Overview

Presentation Agenda:

- Technical Background
- User Identification
- Demographics & Physical Information
- Cognitive State Detection
- User Profiling
- Future Research & Development
- Questions

Technical Background

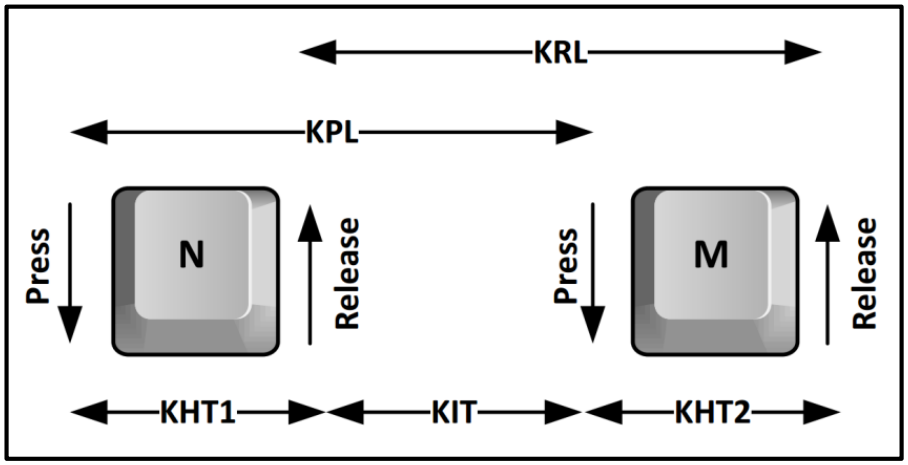
Behavioral Biometrics

- Keystroke Dynamics
  - Used for verification and identification of users (Next Slide)
  - Researchers at Louisiana Tech University, Carnegie Mellon University, Syracuse University, and many other companies and universities have made great strides in this area
- Mouse Dynamics
  - Used for verification of users, typically less accurate than keystrokes
  - Derive movement features: Pusara & Brodley (2004), Schulz (2006), Ahmed & Traore (2007), and Feher et al. (2012)
    - E.g., distance, angle, speed, silence, frequency of actions, trajectory, acceleration, third & fourth moments
- Gait Detection
  - Mobile devices make this more viable
- Voice Identification

Technical Background

Keystroke Features

- Key hold time (KHT) – the time between the press of a key and release of the same key. This is calculated for each key in the pair.
- Key interval time (KIT) – the time between the release of the first key and the press of the second key.
- Key press latency (KPL) – the time between the press of the first key and the press of the second key.
- Key release latency (KRL) – the time between the release of the first key and the release of the second key.



Keystroke Timing Features

Technical Background

Sentiment Analysis

- Methods for identifying user attitudes from a given data source
- Typically employs natural language processing (NLP)
  - Linguistic Inquiry in Word Count (LIWC), Stanford NLP Suite, Apache OpenNLP, Natural Language Toolkit, GATE, MRC Psycholinguistic Database
- Frequently used in advertising, politics, and many other areas
- Analysis performed on textually-rich data, such as email, blogs, or social media (e.g., Twitter)
  - Numerous studies and articles on Sentiment Analysis in Twitter going back to 2009
  - Email Sentiment Analysis goes back much further with several commercial tools (e.g., WarmTouch) produced

Technical Background

Verification, Identification, and Authentication

- Verification is the process of comparing test data against a single signature or predictive model to determine if the test data is consistent with the user's previous patterns
- Identification is the process of comparing test data against a list or database of signatures or predictive models to determine who a user is
  - Typically, identification is going to have higher False Accept Rates, degrading accuracy
  - Fewer behavioral biometric identification techniques are on the market
- Authentication is similar to verification, but typically relegated to login or sign-on
  - Not a continuous monitoring solution
  - Less prevalent in this topic

User Identification

Verification

- **Many solutions:** AdmitOne Security (BioPassword), iMagic, Remote Suspect Identification
- **Numerous Algorithms:** Hidden Markov Model, Naïve Bayes, K-Nearest Neighbor, Random Forest, Neural Networks, Support Vector Machines, k-Means, Distance-based (Euclidean, Manhattan, Mahalanobis)
  - Great Comparison Article Killourhy & Maxion (2009)
- Many achieve accuracy at or above 90%
- Accuracy is a trade-off with speed – time to create a signature and amount of data to use in testing

User Identification

Remote Suspect Identification Program (FA8750-09-C-0191)

- **Motivation:** non-intrusive continuous monitoring solution to protect against insider threats without specialized hardware
- **Goal:** develop a continuous monitoring keystroke dynamics solution for authenticating, verifying, and identifying users
- **Equal Error Rates:**
  - Verification: 0.0498
  - Identification: 0.0692 (See Next Slide)
- Algorithms developed by Phoha and Balagani of Louisiana Tech University (LTU)
- Evaluated based on a dataset collected at LTU with keystroke timings for over 2,200 students
- Pilot Study conducted at United States Air Force Academy (USAFA)
  - No pun intended!

User Identification

Identification

- Scalability is a major concern with identification
- How do you measure success – unique matches, list of matches?

EER for Identification using Keystroke features with RSID

Algorithm	Feature	EER	Unique Match Rate	List Size	Outsider Match Rate
Similarity	KHT1	0.1330	0.1167	5	0.193
	KHT2	0.1842	0.0073	18.98	0.019
	KIT	0.0809	0.1184	12.21	0.237
	KPL	0.1172	0.1511	8.96	0.354
	KRL	0.0829	0.3168	3.56	0.53
	Fusion	0.0692	0.4301	2.35	0.56
Naïve Bayes	KPL	0.173	n/a	10.32	n/a

Enrolled Users	Insider In List	Unique Match Rate	Insider List Size	Outsider Match Rate	Outsider List Size
2	0.956	0.898	1	0.89	0.1
3	0.954	0.852	1.1	0.85	0.2
5	0.957	0.756	1.2	0.76	0.3
10	0.953	0.631	1.5	0.67	0.5
20	0.958	0.451	2.1	0.52	1
30	0.956	0.354	2.7	0.42	1.7
50	0.955	0.26	3.9	0.31	2.8
100	0.957	0.166	6.6	0.24	4.3
200	0.962	0.103	12.8	0.17	10.4
300	0.955	0.081	17.6	0.14	17
500	0.957	0.049	30.7	0.08	31.3
1000	0.961	0.046	53.8	0.07	64.6

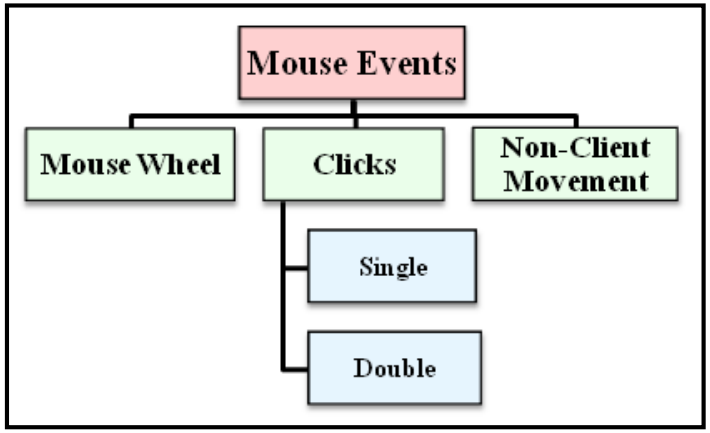
Match results for RSID system as number of signatures in the database increases.
Note: Outsider indicates that the system has found no viable matches in the database

153 Brooks Road, Rome, NY | 315.336.3306 | http://ainfosec.com

User Identification

Mouse Solutions

- Promising results for both authentication and verification in controlled environments (> 90%) with fairly quick training and testing times
- Prominent Research in the Area:
  - Shen et al. (2013)
  - Feher et al. (2012)
  - Ahmed & Traore (2007)
  - Schulz (2006)
  - Pusara & Brodley (2004)
- These approaches typically derive different features (e.g., speed, angle) to perform their analysis



Pusara & Brodley (2004) classify mouse data into a hierarchy of mouse events. Non-client movement refers to movement within an applications title and menu bars

Key Limitations

- Utility for intrusion detection
- Outside attackers often only execute keystrokes or have remote connections, limiting the utility of mouse dynamics

User Identification

Mobile Biometry (MOBIO) project (http://www.mobioproject.org/) is a community with the focus on identifying new mobile authentication mechanisms

DARPA Active Authentication program focused on multi-modal mobile solutions.

Gait Detection

- Study of locomotion; specifically using phone accelerometers
- EER 20% (Derawi et al., 2010) increased to $\leq$ 4% (Sprager & Juric, 2015)

Swipe Patterns

- Analysis of touchscreen swipe patterns can reach EER 0.2% with few swipes (Antal & Sabo, 2015)

Keystroke Dynamics

- Using touch screens (BehavioSec, 2013)

Novel Patterns

- Arm Movement (Kumar, Phoha, & Raina, 2016): 85-98% accuracy

Traditional Biometrics

- Fingerprint, Facial Recognition, Iris

Demographic & Physical Information

MYCROFT (FA9550-12-1-0229)

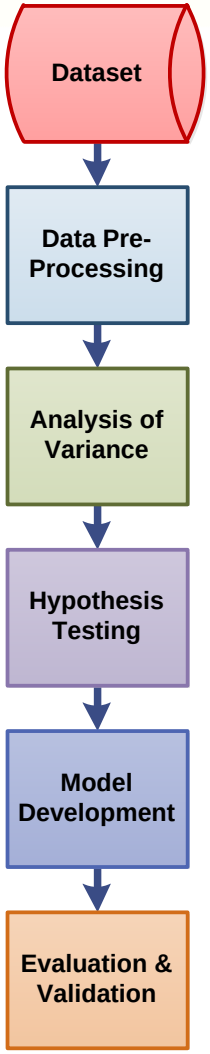
- **Motivation:** Operators have no information regarding unknown users in keystroke dynamics solutions
  - User identification is limited to users with known signatures
  - Operators are provided with no information on outsider attackers
- **Goal:** Determine if there exists a relationship between demographic information and keystroke timings
- Identifying potential physical and demographic features of outsider attackers provide analysts more to go on
- Can help analysts narrow down the region an attacker is from for nation-state attacks
- Build evolving profiles of a user over multiple attacks.

Demographic & Physical Information

Process for Identifying Demographic Information

1. Analysis based on RSID Dataset using data from over 1,500 users coded with demographic information
2. Data pre-processing to derive features (e.g., KHT, KIT) and outlier detection
3. Analysis of variance with Principal Component Analysis
4. Hypothesis Testing using Rank Sum
5. Development of Predictive Models
   - K-Nearest Neighbor, Random Forest, Support Vector Machines
   - SMOTE used in majority / minority cases ($\leq$ 15%, $\geq$ 85%)
6. Evaluation of Predictive Models to identify accuracy and validate the models

More details available in Dora et al., 2013 or the MYCROFT final technical report, available on request.



Demographic & Physical Information

MYCROFT Results

- The MYCROFT program took the data from the RSID program and sought to determine if there was a relationship between demographic features and keystroke timings
- Analyzed numerous demographic features, including:
  - Age, Gender, Height, Ethnicity, Height, First Language, Primary Typing Language, Major, Handedness, Typing Experience (Average Hours/Day), Tying Style (Visual vs Touch), Use of Mobile Devices
- Found a relationship between numerous factors, many of which were predictive with KNN models:
  - Age (19, 20, 22, 23, 24, 25, 26, 27, 28, 30), Ethnicity (African, Asian, Black/African American, Hispanic), Typing Experience (5-7 hours per day, 8-12 hours per day), First Language (Chinese, English, Hindi, Marathi, Nepali, Telugu), Handedness, Primary Typing Language (Chinese, English), and Typing Style (Touch vs. Visual).
- Other researchers have found a relationship between keystroke timings and gender with accuracy of 91% (Giot & Rosenberg, 2012)

Demographic & Physical Information

MYCROFT Results

- Focused on results in which there were at least 14 users
- Two-classifier evaluation (e.g., Asian vs Not Asian) with K-Nearest Neighbor
- Performed preliminary evaluation with Random Forest and SVM
  - Results did not appear promising
- Strongest relationship was for African users and those whose First Language was Nepali
- Multi-factor analysis was not performed

Predictive Features

Feature	Category	No. Users	Accuracy
Asian	Ethnicity	216	81.40%
20	Age	220	80.84%
Nepali	First Language	36	97.02%
Chinese	First Language	32	84.32%
Telugu	First Language	30	82.49%
5-7 Hours/Day	Typing Experience	24	83.07%
Ambidextrous	Handedness	22	83.21%
Hispanic	Ethnicity	20	83.23%
27	Age	17	82.87%
8-12 Hours/Day	Typing Experience	16	82.92%
African	Ethnicity	14	97.81%
26	Age	14	86.06%

153 Brooks Road, Rome, NY | 315.336.3306 | http://ainfosec.com

Demographic & Physical Information

Future Research & Development

- Investigate new predictive models
  - Research deep learning techniques (e.g., neural networks)
- Collect a larger, more representative dataset
  - Dataset biased towards White, American, English-speaking 20-year old college students (bias minimized with SMOTE)
  - Many models are based on a small number of users
- Incorporate new features into models
  - Mouse dynamics, other behavioral biometrics
  - Potential to enhance existing models or find correlations not indicated by keystrokes

Acknowledgements

Funding for this program was provided by the Air Force Office of Scientific Research, Award No. FA8750-12-C-0125.

Cognitive State Detection

Basic Research Initiative (BRI) or Cyber Trust & Suspicion (CTS)

- **Award Number:** FA9550-12-1-0457
- **Motivation:** Humans are a critical attack vector in CNO
- **Goal:** Determine if there exists a relationship between suspicion and behavioral biometrics
- Measuring cognitive state discreetly and remotely has a huge impact on advertising, politics, social media, CNO, and many others
- Better focus or configure offensive techniques (i.e., flying under the radar)
- Determine when cyber operators become less vigilant
- Focus valuable system resources based on anomalous states

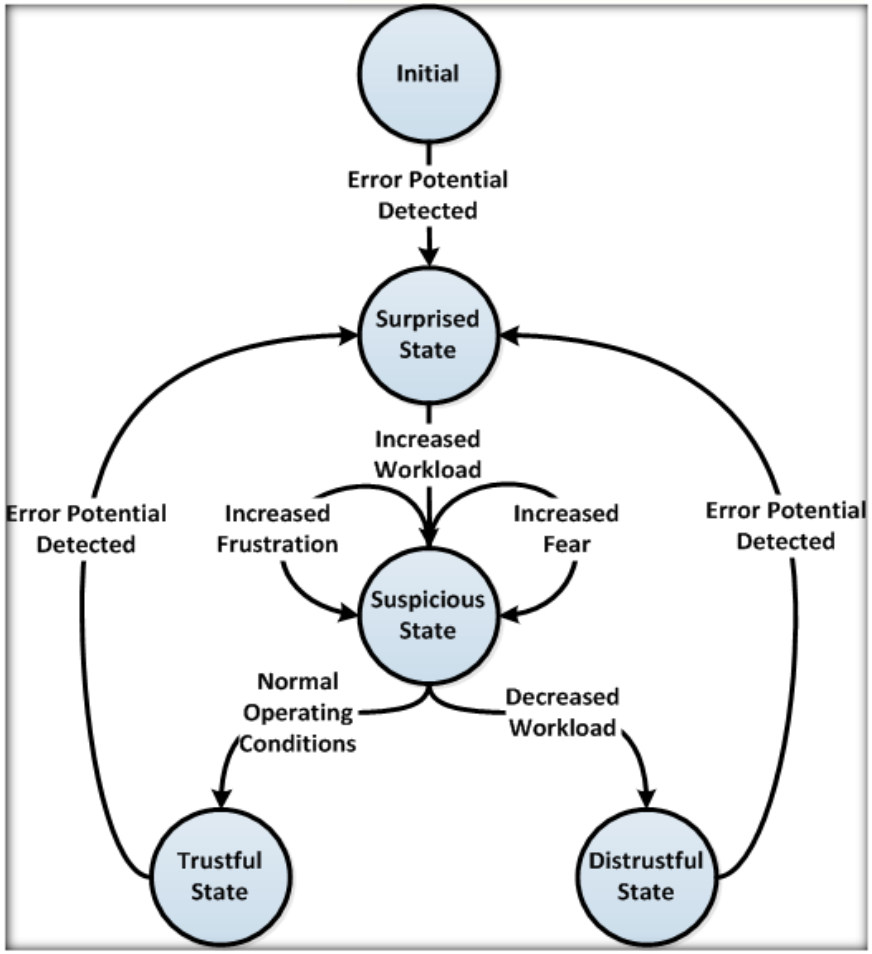
Cognitive State Detection

ais

devastating capability, revolutionary advantage

BRI / CTS

- Consider a red-team and blue-team exercise
  - Red-team is tasked with exfiltration information from a blue-team system
  - Blue-team seeks to protect the system
- How do you configure your exploits?
  - Drop keystroke exploit to distract or degrade performance of blue-team
  - Dropping all keystrokes – noticeable
  - Dropping 1/200 – ineffective
  - How do you maximize effect without being detected?



Trust/Suspicion Transition Model

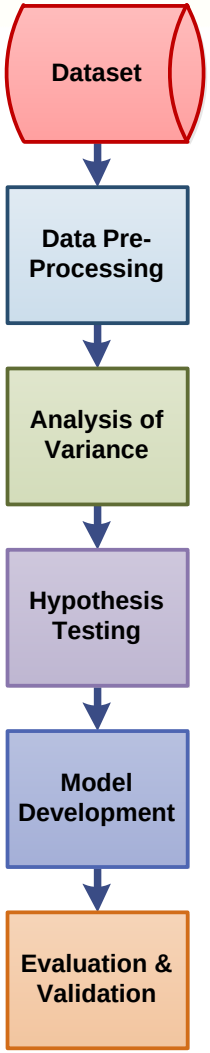
153 Brooks Road, Rome, NY | 315.336.3306 | http://ainfosec.com

Cognitive State Detection

Process to ID Cognitive States

1. Experimental Design & Data Collection
2. Data pre-processing to derive features (e.g., KHT, KIT) and outlier detection
3. Analysis of variance with Principal Component Analysis
4. Hypothesis Testing using Rank Sum
5. Development of Predictive Models
   - K-Nearest Neighbor, Random Forest
6. Evaluation of Predictive Models to identify accuracy and validate the models

More details available on request.



Cognitive State Detection

Experimental Design

- RESCHU Study – Mouse Data
  - Participants used a UAS simulation with specific objectives
  - Targets were periodically removed based on where the user was looking
- Winter Survival Study (WSS) – Keystroke Data
  - Subjects converse over Skype to prioritize a list of supplies in a winter environment
  - After a control trial, some subjects were assigned as saboteurs and other participants were warned of potential sabotage

Data Collection

- 8 users participated in the RESCHU Study with fNIRS data as ground-truth
- 20 users participated in the WSS with the Bobko and Odle-Dousseau's state-suspicion survey (2014) as ground-truth

Cognitive State Detection

Basic Research Initiative Results

- Mouse analysis was inconclusive due to experimental design issues
- Analysis of keystroke data found a negative correlation between KIT and suspicion
  - Mean KIT for Trusting Data: 94.25 ms
  - Mean KIT for Suspicious Data: 76.43 ms
  - More effective for some users
- Predictive models are still in development

Cognitive State Detection

Future Research & Development

- Third phase of the program begins next month
- Experiments designed to collect additional data, attribute the source of suspicion, and manipulate it
- New sensors have been developed to, potentially, enhance the models
  - System Call Monitoring, Application Logging, Gaze Detection, Context Monitoring (e.g., menu clicks)
- New models and techniques will be used to evaluate the data collected

Acknowledgements

Funding for this program was provided by the Air Force Office of Scientific Research, Award No. FA9550-12-1-0457. AIS was a sub-contractor to Dr. Eunice Santos of UTEP and collaborated with Dr. Leanne Hirshfield of Syracuse University.

Behavioral Profiling

ais

devastating capability, revolutionary advantage

Profiling Techniques

- Historically, most profiling techniques are manual
- Critical profiling operations are still manual, such as the TSA:
  - Screening of Passengers by Observation Techniques (SPOT) employed by the TSA to identify aberrant passenger behavior
  - Point system used by officers trained to look for specific cues – once a passenger reaches a given threshold, they're further questioned
- Some work has been done towards automation in profiling, but we're still in the early stages

153 Brooks Road, Rome, NY | 315.336.3306 | http://ainfosec.com

Behavioral Profiling

Behavioral Analysis in Social Networks (BASoN)

- **Motivation:** Massive dataset available with information used for past personality profiling in the psychology community
- **Goal:** IR&D program to determine if there exists a relationship between social networking data and personality traits
- Focused on Big Five personality traits (Agreeableness, Neuroticism, Openness, Extraversion, Conscientiousness) and Facebook Data
- Data Sources Analyzed: TV genre, movie genre, music genre, political preferences, celebrity worship, no. friends, no. pictures
- Collected data from 27 participants
  - Subjects each took the International Personality Item Pool, Revised Eysenck Personality Questionnaire, and Myers-Briggs Type Indicator
  - 18 subjects provided access to their Facebook data, while the others filled out a supplemental form containing identical information

Behavioral Profiling

Program Results

- Results were predictive for several of five of the Big Five personality traits compared against normalized random chance
  - Dataset consisted almost exclusively of engineers, leading to some biased results (average values significantly different from standard)
- Extraversion only required number of friends to be predictive
- Predictions were significantly greater for users who provided their social networking data
- Agreeableness was not predictive in any context and actually decreased for Facebook users

Behavioral Profiling

Impact of Behavioral Profiling Research

- Much like extracting demographic information, personality profiling can reveal hidden traits about a user, especially outside attackers
- Can be combined with other features to improve models
- Personality assessment is frequently used in the workplace to help with the creation of teams and/or hiring decisions
- Personality assessment is also used in clinical psychology to identify and help with underlying disorders
- Most importantly, however, is **behavioral prediction**!
  - In order to predict user behavior, you must first be able to quantitatively represent an individual
  - Require finer-grained personality measurements
  - End-goal is to predict user responses to specific stimuli

Behavioral Profiling

myPersonality Project

- Researchers at the University of Cambridge run the myPersonality Project to perform research into relationship between social networking data and personality traits
- Based on PhD thesis from 2007
- Massive dataset of over 7.5 million users social networking data coded with personality traits
- Dozens of publications have come out of the program
- Most of the work to date has primarily focused on linguistic analysis / natural language processing
- Represents a huge step forward for this research area

myPersonality Project

Future Research & Development

Develop New Predictive Models

- New machine learning algorithms or implementations thereof may be more predictive
- Recently, deep learning techniques have become more popular and better developed to address the needs of *Big Data*
  - Neural Networks, Belief Networks, etc.

Data Collection, Testing, Refinement, and Validation

- Data collection is key!!
  - Predictive models can likely be improved by incorporating other behavioral data (e.g., mouse dynamics, mobile biometrics, system logs) into current models
- More data can help better test and refine our models, allowing us to select the best model
- Large shared datasets allow researchers to validate each others work and test new algorithms against the same baseline
- Avoid sample bias as much as possible
- Collect samples for different cultures (harder than it seems!)
- Allows us to identify cultural differences and better understand them

Future Research & Development

Automate Model Creation and Evaluation

- Automatically detect anomalies (e.g., aberrant cognitive states)
- Assess risk based on behavior to predict malicious behavior before it occurs
- Automated Intrusion Detection Systems that can use unconscious cues from operators to better protect systems
- **Insider Threat Detection**
  - Prominent area for implementation of automated solution
  - Identify masquerading user based on behavioral cues
  - Identify an insider threat before he carries out his threat
  - Identify vulnerabilities in operators

Mobile / BYOD

- New biometrics modalities are constantly being identified
- Devices are especially vulnerable to physical access attacks
- Access to more data
- Internet of Things

Questions?

Robert Dora
dorar@ainfosec.com
Assured Information Security, Inc.
315.336.3306 x595