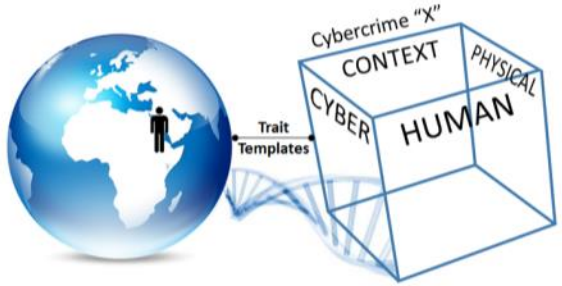


Towards An Adaptable System-based Classification Design for Cyber Identity

PhD Extended Abstract

June 11, 2018

Mary C. (Kay) Michel
School of Computing
Florida Institute of Technology
Melbourne, Florida 32901
michelm1998@my.fit.edu

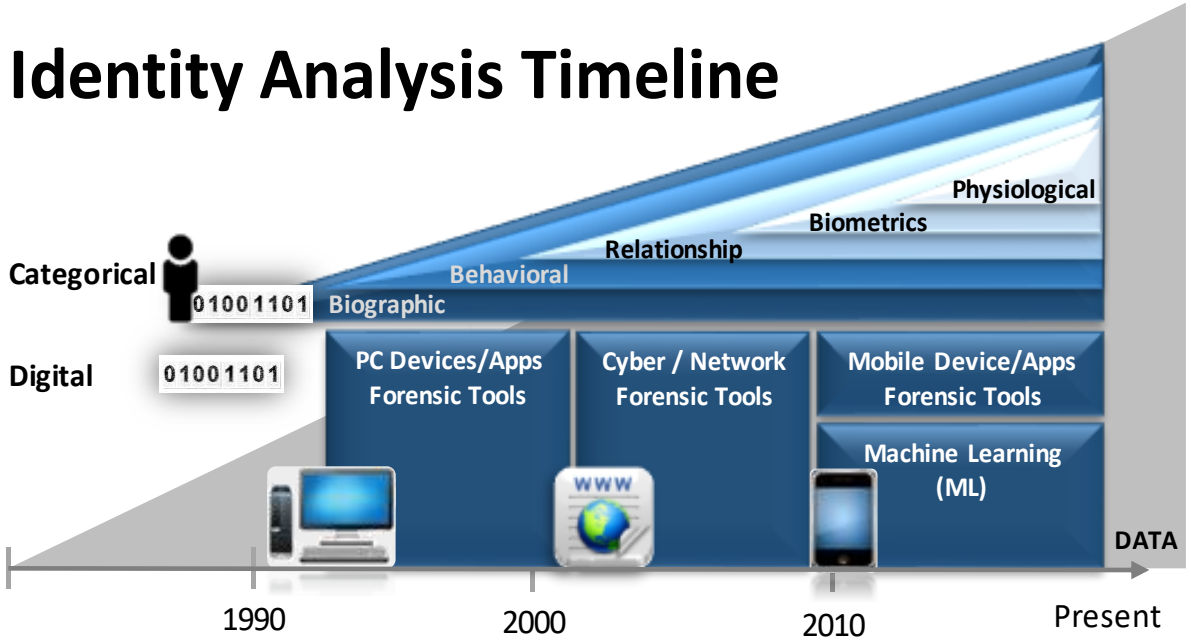
Michael C. King
School of Computing
Florida Institute of Technology
Melbourne, Florida 32901
michaelking@fit.edu

The Internet…

A dynamic, complex infrastructure that connects us all across the globe.

To understand a ***cyber identity*** today, more sophisticated methods are needed.

Identity Analysis Timeline



Cybercrime cases are challenging to solve.
Need to organize data in a meaningful way to resolve an identity.

Topic Agenda

- Introduction
- Background
- Initial Design Experiments
- Conclusion and Future Work

My background…
- C.S. PhD Candidate in Computer Science at FIT
- 15yrs. as Chief Software Engineer & R&D P.I.
- 10yrs. researching Cyber, Identity, AR, and VW's
- Artist and Market Analyst

Dr. Michael King's background…
- Associate Professor and Research Scientist at FIT
- Director, Applied Research and Innovation
- Program Manager and Research Scientist

Introduction

Novel Classification and Situational Awareness (SA) Approach

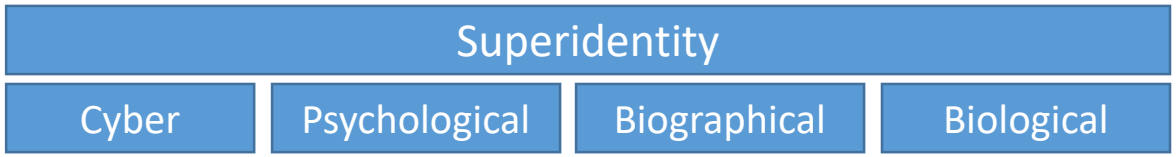
- HYPOTHESIS: If we take a ***holistic approach*** of structurally designed common theoretical attributes of information, cybernetic systems, and adaptable DNA, we can repeatedly assess all observed variables numerically within the four dimensions of context, physical, cyber, and human aspects to resolve an identity in feature set template snapshots and eventual time series.

- QUESTION: Can a person's cybernetic DNA fingerprint be structurally designed with biologically inspired robust feature sets of human, physical, and cyber system-based attributes with high entropy and contextually linkable traits?

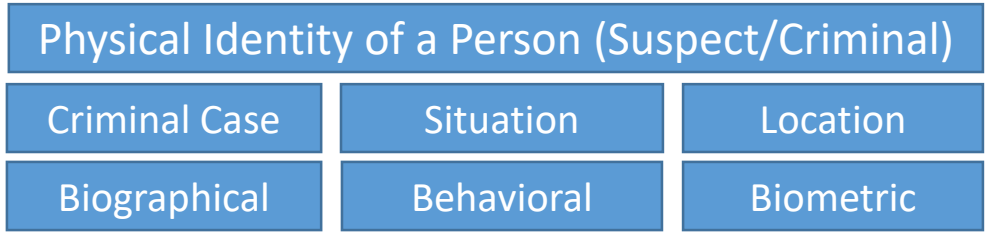
- **TECHNICAL GOAL: Holistic adaptive identity feature classification scheme or information architecture**

Background of Holistic Identity

- **<u>Superidentity Project</u>** [2]**<u>:</u>** our approach is an ***adaptive, system-based design*** with temporal aspects of binding a person's cyber to physical identity core based on ***4 dimensions of context, cyber, physical, and human***



- **<u>Situation, Barwise and Dempster-Shafer Theory Ontologies</u>**[3]: our approach ***adds cyber aspects***



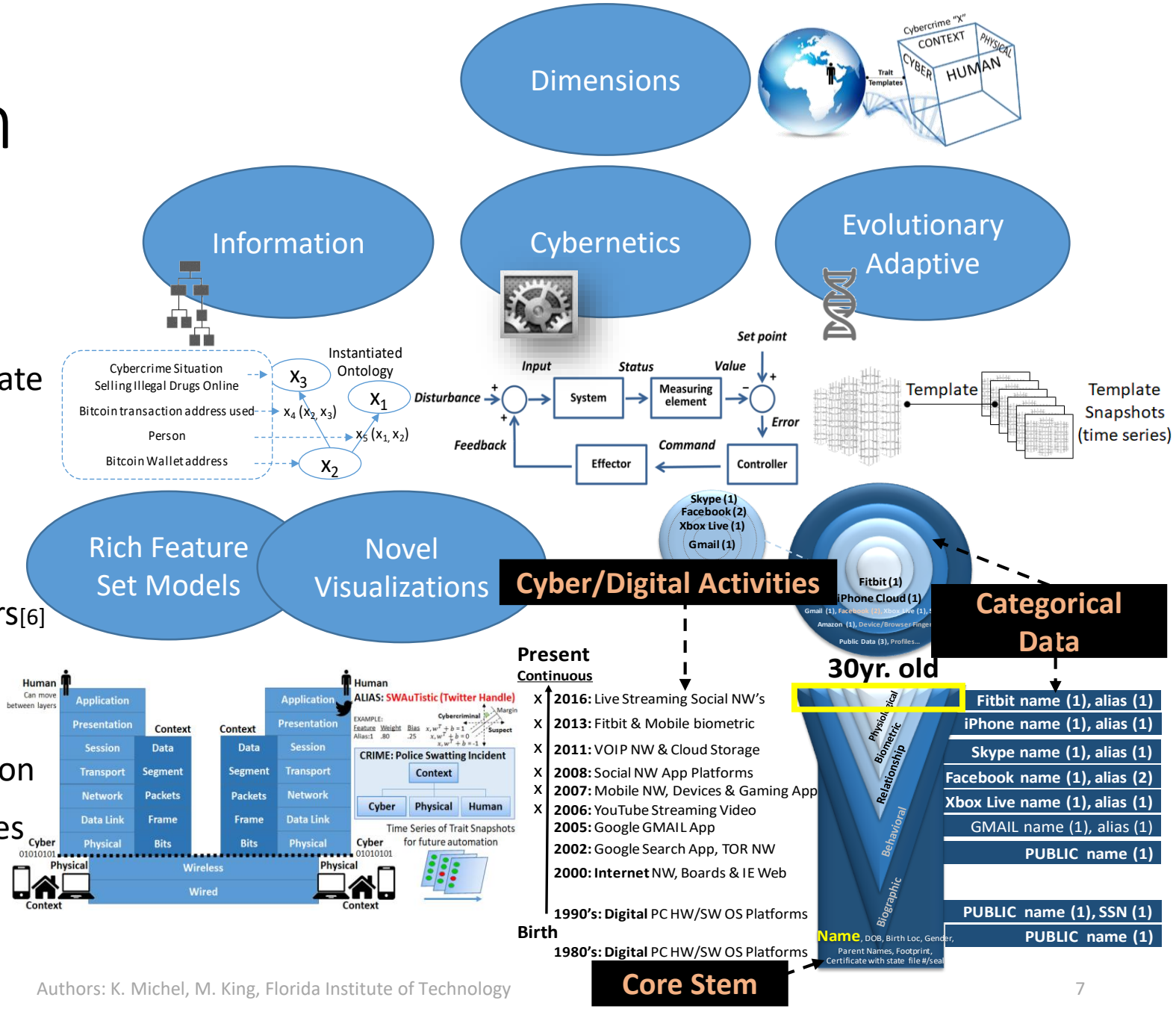
- Other methods:
  - Multi-Biometric
  - Social Network Connections
  - Psychological, relationships, physiological

Design Aspects

- **Structure** to link attributes across temporal dimensions
- **Common, variant and salient categories** of attributes within dimensions[3]
- **Information and set theory** to mathematically measure feature sets[3,6]
- **Cybernetics theory** to determine a type of control system[4]
- **Bio-inspired adaptive sophisticated design structures** to track mutation/change variables over time[5]

Concept Design

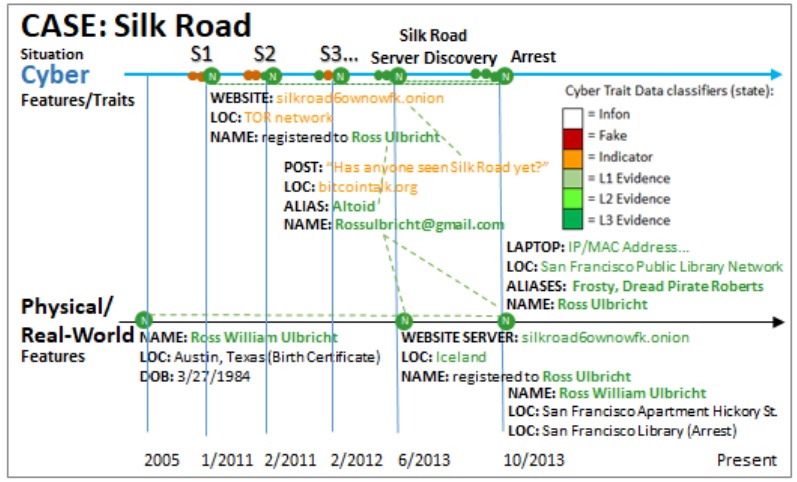
- **Adaptive**, sophisticated linkable structure with types and expression
- **Cybernetic** systems, function, and state
- **4 Dimensions**
- Similarity and variation measures
- Low and high dimensional data
- OSI model paths, links, and identifiers[6]
- Quantitative categorical feature sets
- Consistent models for baselines, cybercriminals, profiles, unique person
- Goal to achieve high match accuracies and rapid identity resolution

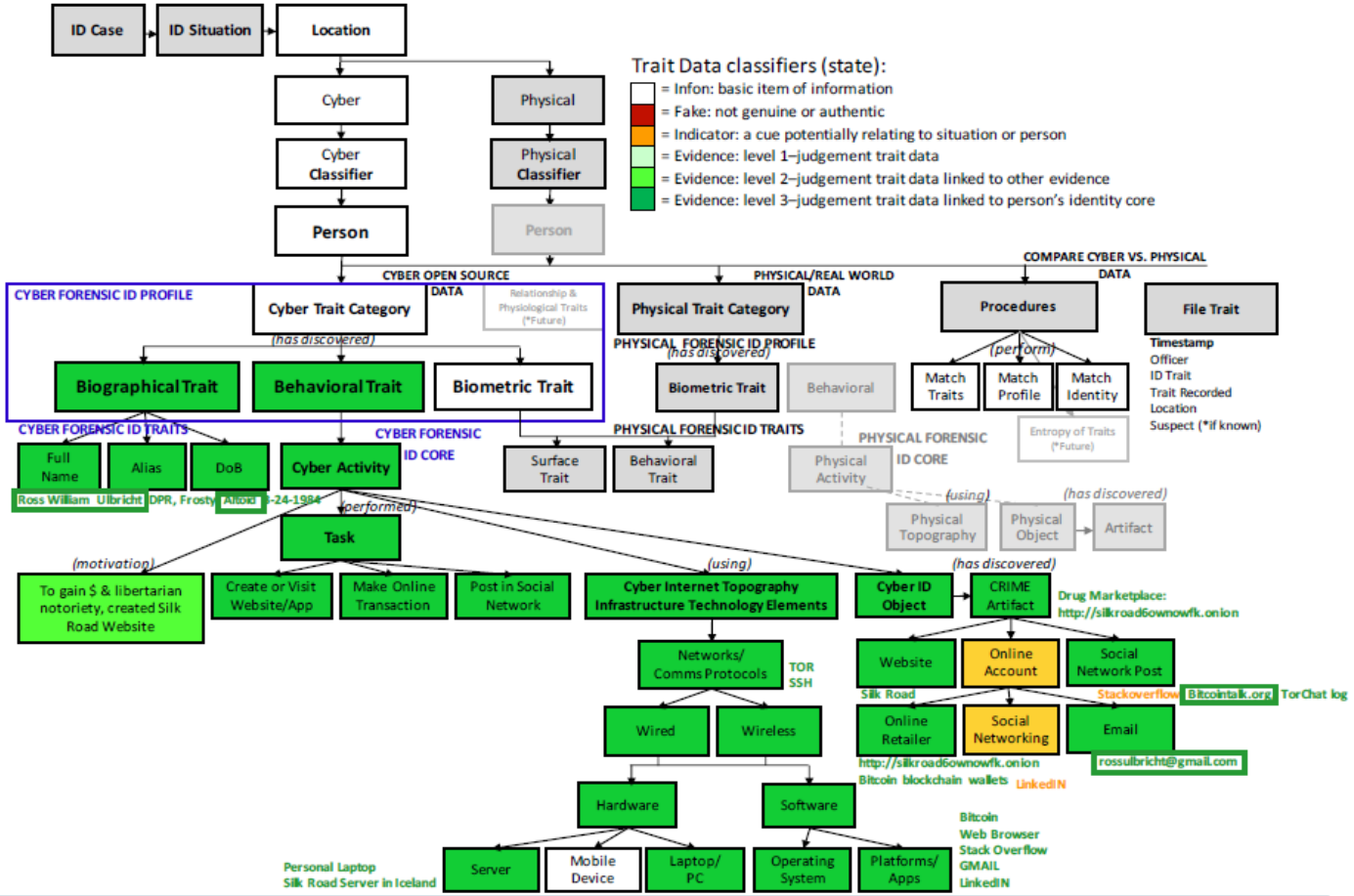


Initial Design Thought Experiments

Initial experiment results are promising yielding technical contributions below:

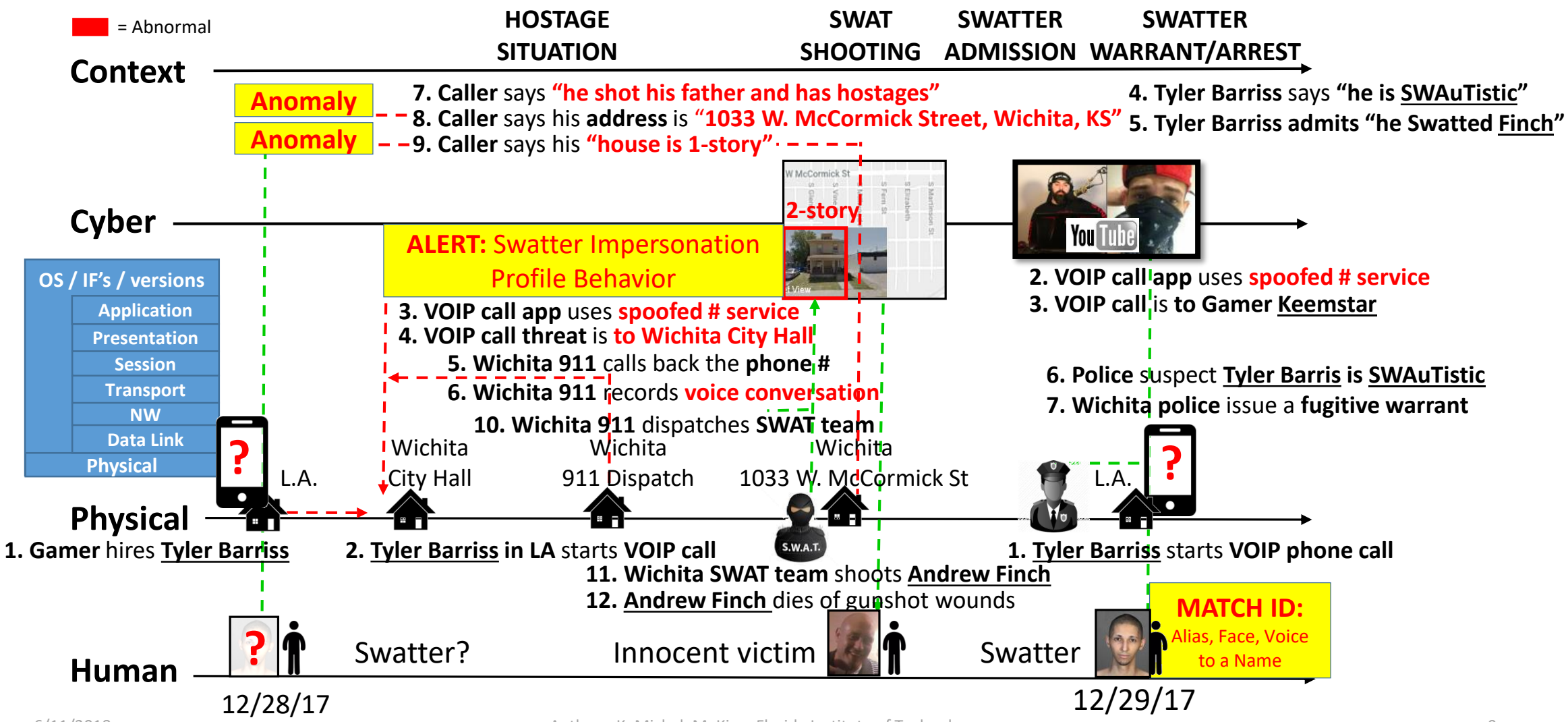
- Identity extended cyber-physical feature set classification-based ontology design
- Identity core with temporal states of mapped features, profile, and unique identity evidence
- Contextual cybercrime salient feature sets with aspects of real-world cybercrime cases





Initial experiments were promising in resolving an identity for several types of cybercrime.

Visualization #1: Swatting Identity Theft Sequence Diagram of Evidence[7]



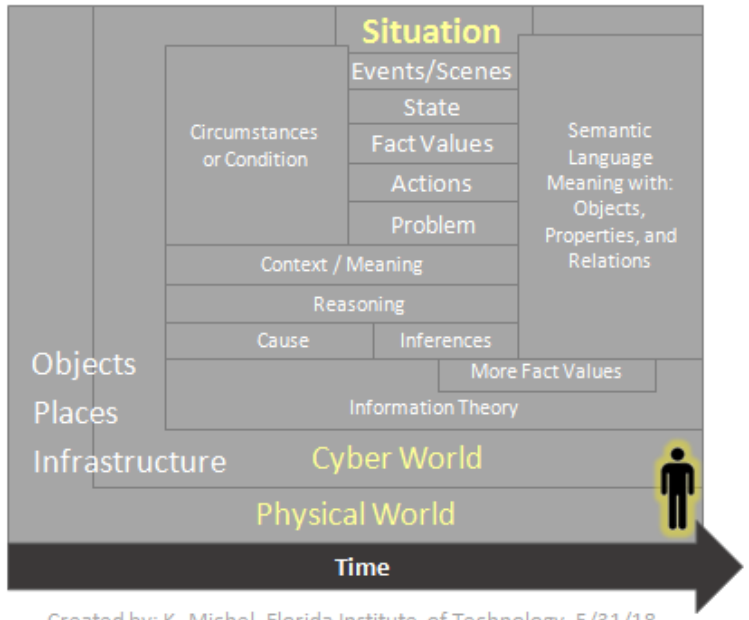
Datasets and Attributes…

Datasets

- Current research involves *simulation* of real-world cybercrime evidence
- Building template models of baseline profiles, cybercriminals, and known persons
- Plan is to use these models with real-world public Social Network (SN) datasets and/or API's (e.g., Twitter)

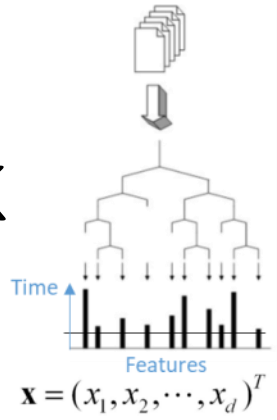
Attributes that create a unique feature sets

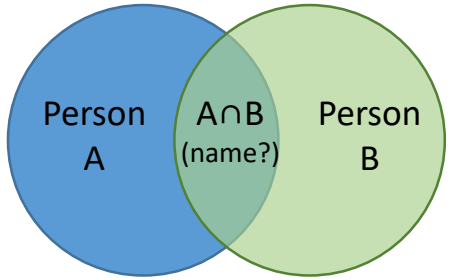
- Salient features in a situation or context
- Categorical (e.g., behavioral)
- Cyber infrastructure, identifiers, aliases
- Physical infrastructure, identifiers, devices
- Person-specific variance
- Linkable features



Created by: K. Michel, Florida Institute of Technology, 5/31/18

Conclusion and Future Work





Identity Theft Scenario Feature Set
A = (**$BiogName_1$**, $BiogAlias_2$, $BiogAlias_3$…)
B = (**$BiogName_1$**, $BiogAlias_2$, $BiogAlias_3$ …)

Classification design is promising.
Ready for implementation and effectiveness evaluation:

1. **Finalize cyber identity design** of feature ontology/RDF models, property graphs, inference engines, and the computational framework
2. **Create representative cybercrime use case scenarios** that include identity theft and fraud feature sets
3. **Create experimental framework prototype and Cybernetic DNA fingerprint feature snapshot templates** (e.g., baseline, cybercrimes, profiles, and unique identities)
4. **Perform match and entropy machine learning algorithm method trade** analysis for feature optimization
5. **Conduct use case scenario prototype trial runs** with varying levels of fidelity in simulated data and online data service methods with publicly available datasets and accessible API's such as Twitter to determine salient identity variables and thresholds for templates → determine signature patterns
6. **Analyze match similarity and variance results** with repeatable experiment trials using feature set evidence

A second set of experiment trials will evaluate the design adaptability and change operators, along with qualitative evaluation of multi-dimensional support for mixed media SA visualizations (e.g., Reality, Augmented Reality, and Virtual Reality) based on the cyber identity classification architecture.

References

[1] “Internet Crime Center Report (IC3) 2016 Annual Report.” https://www.ic3.gov/media/annualreports.aspx, 22 June 2017.

[2] S. Creese, T. Gibson-Robinson, M. Goldsmith, D. Hodges, D. Kim, O. Love, J.R.C. Nurse, B. Pike, and J. Scholtz. Tools for Understanding Identity. In Proceedings of IEEE International Conference on Technologies for Homeland Security (HST), 2013.

[3] M. McDaniel, et al. "Situation-based ontologies for a computational framework for identity focusing on crime scenes." In Proceedings of Cognitive and Computational Aspects of Situation Management (CogSIMA), 2017 IEEE Conference on, 2017.

[4] N. Wiener. Cybernetics or Control and Communication in the Animal and the Machine. The M.I.T. Press, 2013 (created in 1948).

[5] J.D. Watson, A. Berry, K. Davies, DNA: The Story of the Genetic Revolution. Alfred A. Knopf, 2017.

[6] H. Zimmermann, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," in IEEE Transactions on Communications, vol. 28, no. 4, pp. 425-432, April 1980.

[7] “Krebs on Security.” Brian Krebs, 18 Jan. 2018, krebsonsecurity.com/2018/01/serial-swatter-tyler-swautistic-barrisscharged-with-involuntary-manslaughter/.

Thank you!

Questions?

Back-up Reference Slides

IoT Botmaster Use Case:
How did the police *locate* the *suspect*?

Botnet scanning IoT devices | IoT Botnet attack targeting Web Server x | Web Server x down due to IoT Botnet Attack | Mirai code posted to deter authorities | Botmaster Admission

Context

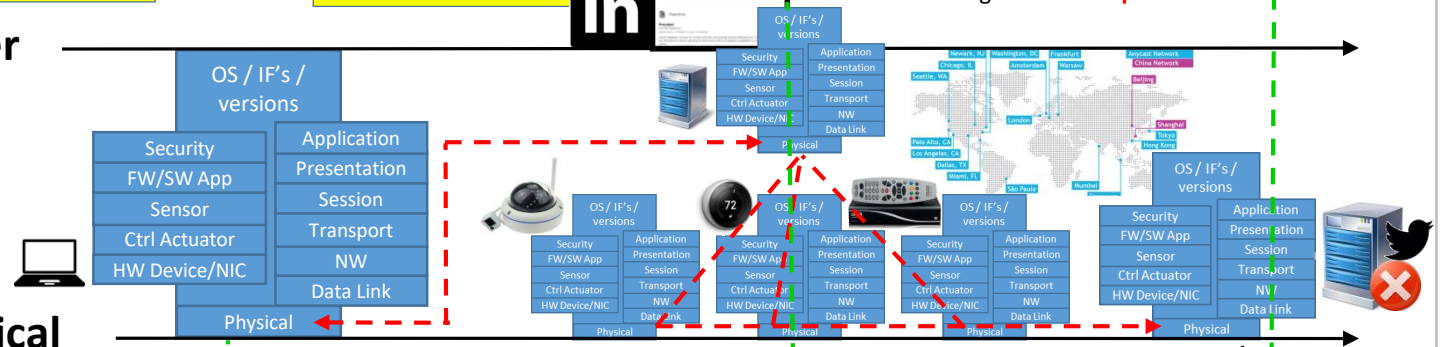
1. **Malware ELF Linux Executable SW Mirai** scans **Internet hosts for open port 23 (telnet)**
2. **Malware ELF Linux Executable SW Mirai loaders** enters **weak password attacks on IoT devices with Busybox OS shell & specific CPU type**
3. **IoT device** **becomes a Botnet listener connected to C2 Botnet server**

ALERT: IoT Bot scanner

ALERT: IoT Botmaster profile behavior

1. **Botmaster Anna-Senpai alias** confesses on hacker sites
2. **Botmaster Anna-Senpai alias** is **Paras Jha, Rutgers Student**
3. **Mirai IoT's** linked to **Jha, Josiah White, and Dalton Norman**
4. **Botmaster** charged with **Computer Fraud**

Cyber



Physical

4. **Botnet server x** receives **Botnet attack cmd**
5. **Botnet server x** sends **Botnet attack cmd**
6. **Botnet server x** uses **MAC Addr x**
7. **Botnet server x** uses **IP Addr x in Country x**

8. **Botnet device x** receives **Botnet attack cmd/logon**
9. **Botnet device x** sends **Botnet attack reqs (SYN, HTTP, ACK)**
10. **Botnet device x** uses **MAC Addr x**
11. **Botnet device x** uses **IP Addr x**

1. **Botmaster x** sends **Botnet attack cmd via C2 API (in TOR)**
2. **Botmaster x** uses **MAC Addr x**
3. **Botmaster x** uses **IP Addr x**

ALERT: IoT Botmaster profile behavior - attack Code has Minecraft game server links

12. **Target Web Server x** receives **Botnet attack cmd**
13. **Target Web Server x** hangs due to **DDOS**
14. **Target Web Server x** uses **MAC Addr x**
15. **Target Web Server x** uses **IP Addr x in San Jose, CA**

Human

8/2016 | 9/19/16 OVH attack | 9/20/16 Krebs attack | 9/30/16 Malware code posted | 10/20/16 Dyn, Twitter, etc. attack | 12/13/17

MATCH ID: Alias, Face, NW IP logs to Email, cell #, Name

Sources:
[1] https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
[2] https://www.rsaconference.com/writable/presentations/file_upload/hta-w10-mirai-and-iot-botnet-analysis.pdf
[3] https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/
[4] https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/


```
root@odroidrouter:~/lexar/domecam# telnet 192.168.1.10
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^]'.
LocalHost login: root
Password:
Welcome to Monitor Tech.
# cat /proc/cpuinfo
Processor       : ARM926EJ-S rev 5 (v5l)
BogoMIPS        : 218.72
Features        : swp half thumb fastmult edsp java
CPU implementer : 0x41
CPU architecture: 5TEJ
CPU variant     : 0x0
CPU part        : 0x926
CPU revision    : 5

Hardware        : hi3518
Revision        : 0000
Serial          : 0000000000000000
```

```
# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 0.0.0.0:34561          0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:8899           0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:34567          0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:554            0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:80             0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:9527           0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:23             0.0.0.0:*              LISTEN
tcp        0      0 192.168.1.10:23        192.168.1.1:59127      ESTABLISHED
```

GOAL: To weaponize 100+K hardware devices to DDOS target servers

Q: How do authorities link IoT Botnet attacks to Botmaster?

Alaska FBI identified infected IoT devices IP address, then subpoenaed GCI state telecom to link a name and physical location. Then, they confirmed these owners did not permit the malware on their devices. They tracked connections back to Mirai C2 server, then court ordered server account owner emails and cell phone # that link to names. Some connections were cloaked in France TOR exit nodes.

Challenges:

Tracking game servers, TOR, attacks, financial records, and alias via packet capture (PCAP) analysis

IoT Botmaster Motive:

Initially DDOS to slow Mindcraft competitor servers so players go to theirs for $, then to make $ for fixing the website server attacks

Results:

- Attack Signatures based on rate (e.g., Tbps)
  - ~600mbps -1Tbps UDP Flood Port 53 (Krebs)
  - ~1 terabit (OVH)
  - ~1.2 terabit (DYN)
  - 130M SYN per second
  - 450M HTTP per second from 175K IP Addr
  - 4M ACK
  - Target entire IP Range
  - Scanner behavior
  - Malware in flash volatile memory

```
// root    xc3511
// root    vizxv
// root    admin
// admin   admin
// root    888888
// root    xmhdipc
// root    default
// root    juantech
// root    123456
// root    54321
// support support
// root    (none)
// admin   password
// root    root
// root    12345
// user    user
// admin   (none)
// root    pass
// admin   admin1234
// root    1111
// admin   smcadmin
// admin   1111
// root    666666
// root    password
// root    1234
// root    klv123
HC\x51\x4F", 1); // Administra
// service service
\x51\x4D\x50", 1); // super
// guest   guest
```