ISA 419: Data Driven Security

16 - Intro to Insider Threat and User Behavior Analysis

Fadel M. Megahed

Endres Associate Professor
Department of Information Systems and Analytics
Farmer School of Business
Miami University
Email: fmegahed@miamioh.edu
Office Hours: Automated Scheduler for Office Hours

Fall 2022

Learning Objectives for Today's Class

Objectives

- **Understand the relationship between useability and user authentication**
- **Describe different types of insider attacks**
- **Describe general approaches to defending insider threats/attacks**
- **Examine a real-world dataset on user profiling**

Outline

Preface

So far in class, we have examined the following datasets that relate to the concept of user authentication. Q: What were these datasets about?

- **Have you been pawned?**
- **Yahoo Password Frequency Corpus**
- **Los Alamos National Lab - User-Computer Authentication Associations in Time**

Authentication: How does that fit in the CIA-triad?

Confidentiality, Integrity, and Availability (CIA)

- **Confidentiality:** Preventing unauthorized reading/disclosure of information.
  - Tools: User authentication, data encryption, ...
- **Integrity:** Preventing unauthorized modification of information.
  - Tools: Cryptographic hashing, digital signature, ...
- **Availability:** Preventing unauthorized withholding of information/ resources.
  - Tools: Intrusion detection, distributed service, ...

Insider Threats: Unauthorized Disclosure of Information [1]

Whether you call him "a traitor or a whistle-blower, he earned one label about which there's no debate: insider threat.'' Lawrence (2015)

Insider Threats: Unauthorized Disclosure of Information [2]

- **Tesla:** A malicious insider sabotaged systems and sent proprietary data to third parties
- **Facebook:** A security engineer abused his access to stalk women.
- **CocaCola:** A malicious insider stole a hard drive full of personnel data.
- **Suntrust Bank:** A malicious insider stole personal data, including account information, for 1.5 million customers to provide to a criminal organization.

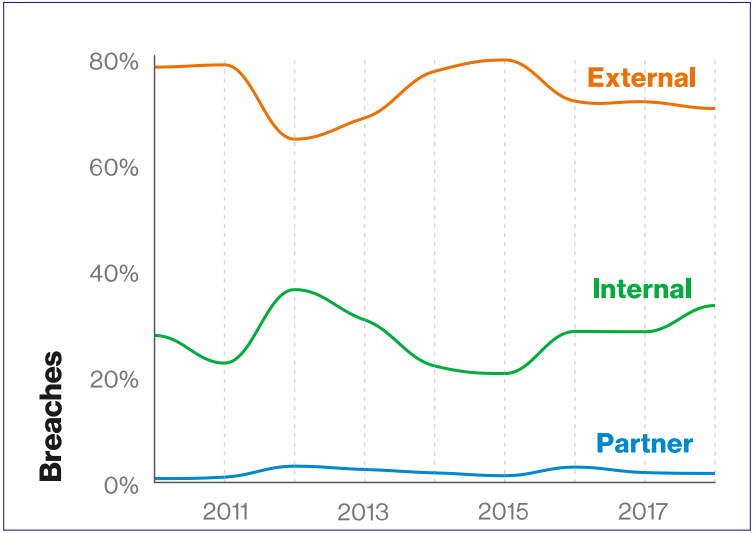
Source: Slide and references are based on Peters (2019). Please read the news/blog articles.

Frequency of Insider Threats [1]

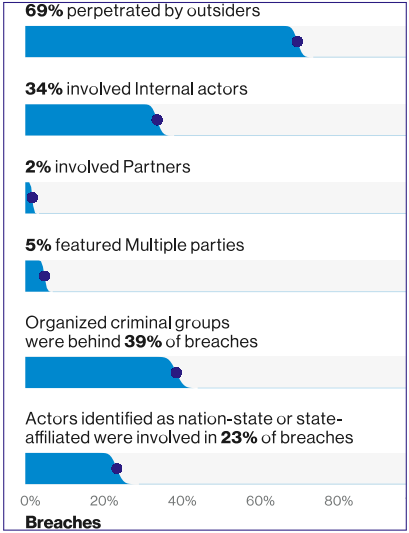
"Despite some variation from year to year, inside jobs occur about as often as outside jobs. The lesson here, though, surely is as simple as this: organizations have to anticipate attacks from all quarters.'' CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 2005

Source: Slide is from CS259D, Stanford University,
https://web.stanford.edu/class/cs259d/lectures/Session3.pdf

Frequency of Insider Threats: Verizon DBIR 2019 [2]



Frequency of Insider Threats: Verizon DBIR 2019 [3]



Suggested Reading: The New Yorker Article

THE NEW YORKER

News Books & Culture Fiction & Poetry Humor & Cartoons Magazine Crossword Video

NEWS DESK

HOW THE F.B.I. CRACKED A CHINESE SPY RING

By Yudhijit Bhattacharjee
May 12, 2014

In the magazine earlier this month, I wrote about Greg Chung, a Chinese-American engineer at Boeing who worked on NASA's space-shuttle program. In 2009, Chung became the first American to be convicted in a jury trial on charges of economic espionage, for passing unclassified technical documents to China.

Outline

Types of Insider Attacks

- **Unauthorized extraction, duplication, or exfiltration of data**
- **Tampering with data (unauthorized changes of data or records)**
- **Destruction and deletion of critical assets**
- **Downloading from unauthorized sources or use of pirated software which might contain backdoors or malicious code**
- **Eavesdropping and packet sniffing**
- **Spoofing and impersonating other users**
- **Social engineering attacks**
- **Misuse of resources for non-business related or unauthorized activities**
- **Purposefully installing malicious software**

Types of Insider Attackers

Source: Slide is based on Peters (2019).

Indicators of Insider Attackers

Source: Slide is based on Peters (2019).

Insider Threats: Defense

- **Turncloaks:**
  - Decoys/traps (e.g., honeypots)
- **Pawns:**
  - Behavioral profiling & anomaly detection
  - Requires extensive logging of systems & users

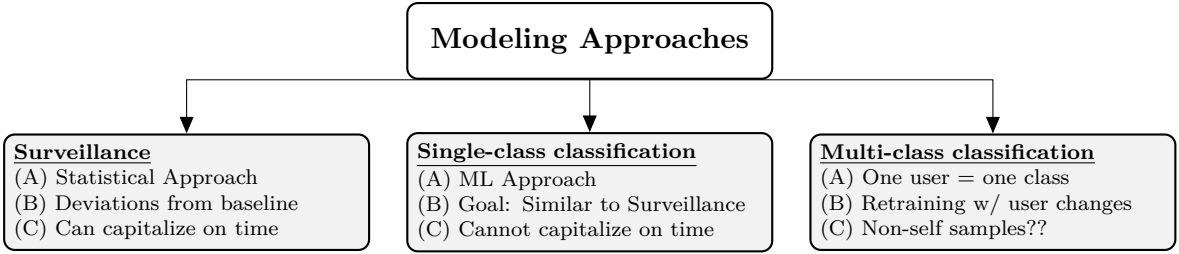
Note that the use of the aforementioned defense mechanisms may be suitable for the other type of attacker as well.

Types of Data Used for Insider Attack Detection

- **CLI command sequences**
- **System calls**
- **Database/file accesses**
- **Keystroke dynamics**
- **Mouse dynamics**

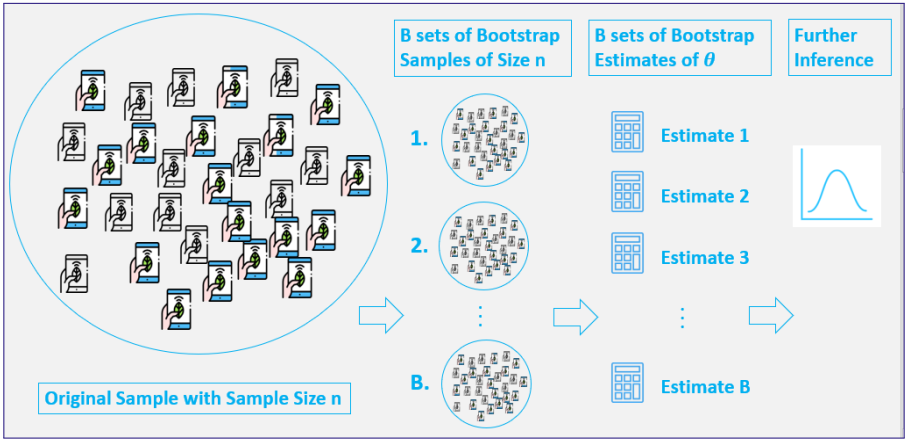
Source: Slide is adapted from CS259D, Stanford University,
https://web.stanford.edu/class/cs259d/lectures/Session3.pdf

A Taxonomy of Modeling Approaches



An overview of three possible modeling paradigms.

A Statistical Surveillance Approach: Bootstrap Sampling + Exceedance Probability Limits [1]



A Statistical Surveillance Approach: Bootstrap Sampling + Exceedance Probability Limits [2]

```
B = 500 # number of bootstrap samples
h = 'e2693' # user
p = 90 #% # percentile used for threshold calculation
ep = 95 # exceedance probablity
df = read.csv("../../data/16-insiderThreat.csv", stringsAsFactors = F)

df %>% filter(UserAbbrv == h) -> dfUser
```

A Statistical Surveillance Approach: Bootstrap Sampling + Exceedance Probability Limits [3]

```
x = as.matrix(dfUser$Risk.Score)
n = 100
bootSamples = replicate(B, x[sample.int(n, replace=TRUE),] )

BootstrapQuantiles = apply(bootSamples, MARGIN=2, FUN=quantile, prob= p/100)
threshold = quantile(BootstrapQuantiles, probs = ep/100)
threshold = round(threshold,0)

print(threshold)
```

```
## 95%
## 695
```

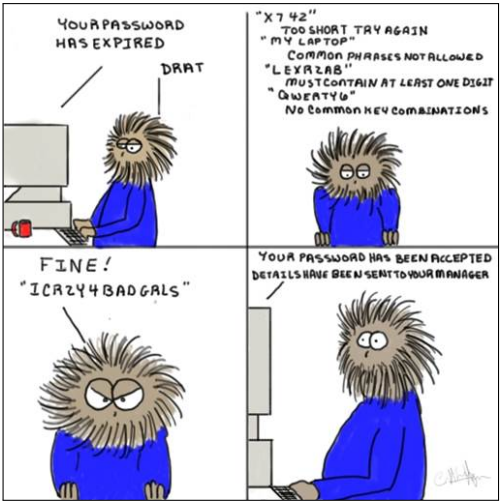
Outline

Human-Human Authentication

- **User authentication**
  - **Differentiate one human user from another**
- **Prominent authentication approaches**
  - **Passwords**
  - **Traditional biometrics**

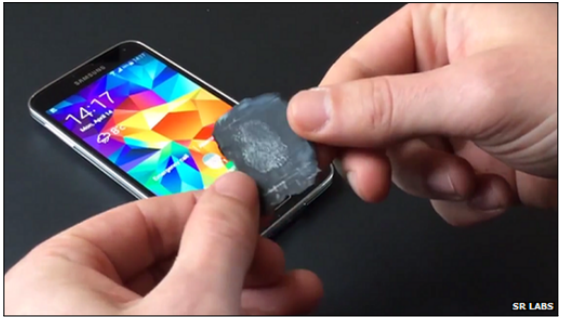
Limitations of Existing User Authentication Solutions [1]

- Passwords
  - Either insecure or unusable
- Traditional biometrics (e.g., fingerprints)
  - Invasive
  - High rejection rates
  - Require additional hardware
  - Susceptible to impersonation or spoofing



Limitations of Existing User Authentication Solutions [2]

- Passwords
  - Either insecure or unusable
- Traditional biometrics (e.g., fingerprints)
  - Invasive
  - High rejection rates
  - Require additional hardware
  - Susceptible to impersonation or spoofing



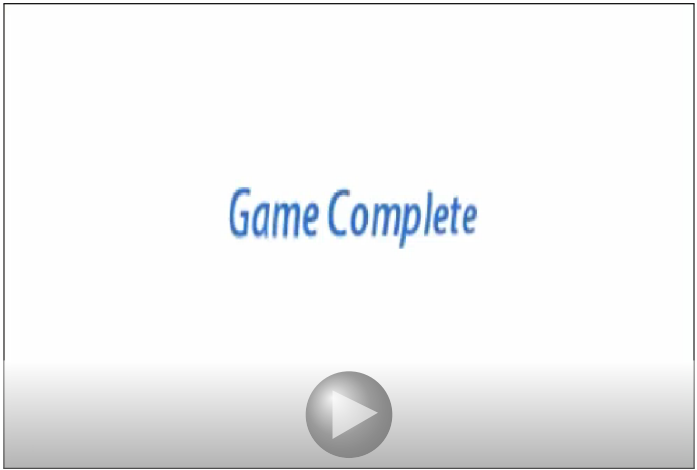
Behavioral Biometrics

- **Keystroke dynamics Monrose and Rubin (1997)**
- **Mouse movement patterns Zheng, Paloski, and Wang (2011)**
- **Touch gesture biometrics**
  - Sliding horizontally and vertically Frank et al. (2012)
  - Sliding up, down, left, and right and tap Li, Zhao, and Xue (2013)
  - Horizontal slide and the pattern unlock De Luca et al. (2012)

Gametrics

- **Interactive game-based behavioral biometrics**
- **Why games?**
  - **Fully supported by web browsers and touch screen devices**
  - **Randomized, interactive and cognitive nature**
  - **Sufficient cues can be extracted in a short period of time**

Game Cognitive Task



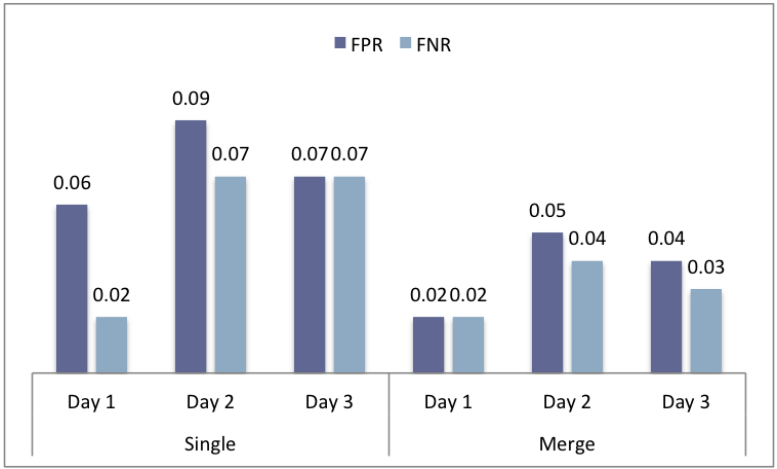
Features & Classification Metrics

- **Features**
  - **Mouse dynamics / touch gesture**
  - **Cognitive ability**
  - **Others (i.e., distance-based features)**
- **Classifier**
  - **Random forest**
- **Classification metrics**
  - **False Positive Rate:** Measures the security
  - **False Negative Rate:** Measures the usability

Inter- & Intra- Session Analysis [1]

- **Web-based study (MTurk)**
- **Data collection methodology:**
  - Day 1: 98 participants – 60 challenges
  - Day 2: 62 participants – 36 challenges
  - Day 3: 29 participants – 36 challenges
- **Number of successfully completed challenges = 9076**
- **Average solving time = 7.5s**

Inter- & Intra-Session Results [2]



Interactive Biometrics Discussion

- **Efficiency**
  - **Short enrollment time**
  - **Short time to identify the user**
  - **Building and updating the classifier and testing a new instance take short time**
- **Application Scenarios**
  - **Point-of-entry**
  - **Integrated with graphical passwords**
  - **Fall-back authentication**

Outline

Experimental Data [1]

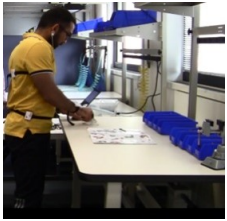


Figure 1: Part assembly

Figure 2: Supply pickup

Figure 3: MMH

Figures are from Maman et al. (2017).

Experimental Data [2]

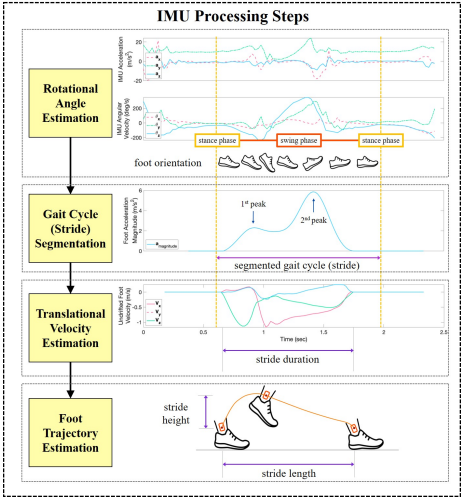
Video is based on research presented in Maman et al. (2017).

Gait Cycle Analysis [1]

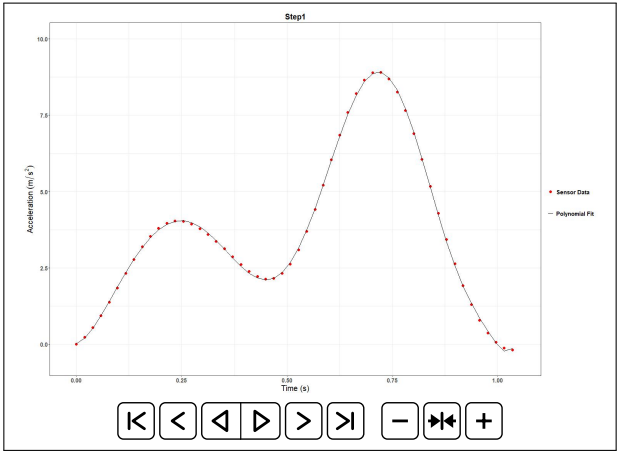
The relative size of the IMU when placed on the right ankle

Figure is from research presented in Baghdadi et al. (2019).

Gait Cycle Analysis [2]

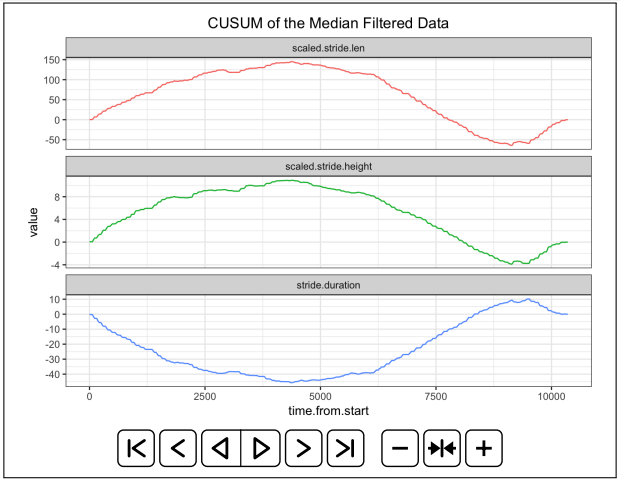


Gait Cycle Analysis [3]



Joint work with researchers at the University at Buffalo.

Gait Cycle Analysis [4]



Based on research presented in Baghdadi et al. (2019).

Outline

Interactive Biometrics Limitations and Future Work

- **Study the effect of user's behavior variation on the accuracy**
- **Test the accuracy when switching devices or hardware**
- **Add more complexity to the game challenges to increase the level of interaction, and improve the overall usability and security**

What you should have learned today

Objectives

- **One class classifiers**
- **Describe different applications for UBA**

References [1]

Baghdadi, Amir, Lora A Cavuoto, Allison Jones-Farmer, Steven E Rigdon, Ehsan T Esfahani, and Fadel M Megahed. 2019. "Monitoring Worker Fatigue Using Wearable Devices: A Case Study to Detect Changes in Gait Parameters." *Journal of Quality Technology*, 1–25.

De Luca, Alexander, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. "Touch Me Once and i Know It's You! Implicit Authentication Based on Touch Screen Patterns." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 987–96.

Frank, Mario, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2012. "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication." *IEEE Transactions on Information Forensics and Security* 8 (1): 136–48.

References [2]

Lawrence, Dune. 2015. “Companies Are Tracking Employees to Nab Traitors.” Bloomberg. https://www.bloomberg.com/news/articles/2015-03-12/companies-are-tracking-employees-to-nab-traitors.

Li, Lingjun, Xinxin Zhao, and Guoliang Xue. 2013. “Unobservable Re-Authentication for Smartphones.” In *NDSS*, 56:57–59.

Maman, Zahra Sedighi, Mohammad Ali Alamdar Yazdi, Lora A Cavuoto, and Fadel M Megahed. 2017. “A Data-Driven Approach to Modeling Physical Fatigue in the Workplace Using Wearable Sensors.” *Applied Ergonomics* 65: 515–29.

Monrose, Fabian, and Aviel Rubin. 1997. “Authentication via Keystroke Dynamics.” In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, 48–56.

Peters, Jeff. 2019. “What Is an Insider Threat? Definition and Examples.” Varonis. https://www.varonis.com/blog/insider-threats/.

References [3]

Zheng, Nan, Aaron Paloski, and Haining Wang. 2011. "An Efficient User Verification System via Mouse Movements." In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, 139–50.