Cybersecurity Research & Updates

Suliman Hawamdeh & Chang Hsiang Ching (Currie)
Department of Information Science
College of Information

UNT®
UNIVERSITY OF NORTH TEXAS®

Historical Perspective

- 1988. the Morris Worm in which Internet slowed down to a crawl
- 1996, Clinton established the President's Commission on Critical Infrastructure Protection
- 1998, the National Infrastructure Protection Center was established in the FBI & the Critical Infrastructure Assurance Office was established in Department of Commerce
- 2001, Office of Cyberspace Security was established
- 2003, National Cyber Security Division (NCSD) was created under Infrastructure Protection Division (IAIP), The United States-Computer Emergency Readiness Team (US-CERT) is the United States government coordination point for bridging public and private sector institutions.
- 2010, National Cyber Incident Response Plan
- 2014, Federal Information Security Modernization Act
- 2015, Cybersecurity Information Sharing Act

UNT®

Cyber Security Threats and Trends for 2019

Phishing Gets More Sophisticated

Using machine learning to craft and distribute convincing fake messages

Ransomware

Kidnap an individual or organization's databases and hold the information for ransom.

Cryptojacking

 Cryptojacking is hijacking third-party home or work computers to "mine" for cryptocurrency

Cyber-Physical Attacks

Targeting electrical grids, transportation systems, water treatment facilities, etc., .

State-Sponsored Attacks

Using cyber skills to infiltrate other governments and perform attacks on critical infrastructure (Cyberwarfare).

IoT Attacks

According to Statista.com, the number of devices connected to the IoT is expected to reach almost 31 billion by 2020.

Connected Cars and Semi-Autonomous Trucks

It is estimated by 2020 90 percent of new cars will be connected to the internet, according to a report titled "7 Connected Car Trends Fueling the Future." (https://medium.com/iotforall/7-connected-car-trends-fueling-the-future-946b05325531)

Shortage of Cyber Security Professionals

Some estimated that there are 1 million unfilled positions worldwide (potentially rising to 3.5 million by 2021 https://cybersecurityventures.com/jobs/

Source: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

Cybersecurity Research Challenges

- **Theoretical foundations: models, logics, crypto**
- **Software & Hardware architecture, Network connectivity**
- **Metrics and Usability**
- **Privacy**
- **AI (AI-based systems like robots and assistants will invite attacks since some initial devices/ software will not be built with security in mind, smart-outsmart-devices)**
- **Cryptography, Traditional cryptography based on RSA is breakable by Shor's quantum algorithm**
- **A distributed denial-of-service (DDoS) will continue to be a challenge**
- **Social, behavioral, ethical and cultural aspects of Cybersecurity** *(Technical approaches alone are not sufficient for cybersecurity, Human behavior affects all stages of the cybersecurity life cycle including design, implementation, evaluation, operation, maintenance, monitoring, revision, replacement, and training.*

Center for Information and Cyber Security (CICS)

UNT Center for Information and Cyber Security is ranked as a National Center of Academic Excellence in Information Assurance Education (CAE-IAE) and National Center for Academic Excellence in Information Assurance Research (CAE-R). UNT is one of approximately 35 universities in the nation to have received both designations (https://cics.unt.edu/)

Areas of research expertise include Internet-based technologies, trust and information assurance, protocol security, digital forensics, watermarking, cryptography, secured electronic commerce, and secured mobile applications and VoIP security

NSF-SFS Scholarship

UNT was awarded $1.2M NSF-SFS Grant in 2012 to fund 6 PhD in interdisciplinary research areas in Cybersecurity. Ram Dantu from computer science is the PI, Dan Kim and Suliman Hawamdeh from Business and IS are the Co PIs.

Funding Provided
- $34,000 stipend, paid over 9 months
- Summer internships/research will provide funding for the remaining 3 months.
- Tuition scholarship of up to $8,100/year
- $4,000/year for travel
- $2,000/year for books
- $3,000/year for health insurance

UNT doctoral students tackle the newest threats in cybersecurity

https://news.unt.edu/news-releases/unt-doctoral-students-tackle-newest-threats-cybersecurity

UNT cybersecurity students and professors (from left) Dr. Suliman Hawamdeh, Quentin Mayo, Yassir Hashem, Logan Widick, Obi Ogbanufe, Josh Talkington, Dr. Ram Dantu and Michael Jaynes. Not shown: Dr. Dan Kim and Dr. Victor R. Prybutok. Photo credit: Michael Clements

NSF-SFS Students Research Example

Dissertation: A Multi-Modal Insider Threat Detection and Prevention Based on Users' Behavior Yassir Hashem, 2018

His work focused on multi-modal framework using psychophysiological measures and computer-based behaviors to distinguish between a user's behavior during regular activities versus malicious activities. He used psychophysiological measures such as electroencephalogram (EEG), electrocardiogram (ECG), and eye movement and pupil behaviors along with the computer-based behaviors such as the mouse movement, mouse clicks, and keystrokes dynamics. Signal based results from (EEG and ECG) show an average detection accuracy of up to 95.93% . Non-signal based results from behavior measures using eye-tracking and an average detection accuracy of up to 94.37% on detecting the malicious Activities.

Source: A Multi-Modal Insider Threat Detection and Prevention Based on Users' Behavior Yassir Hashem dissertation, 2018
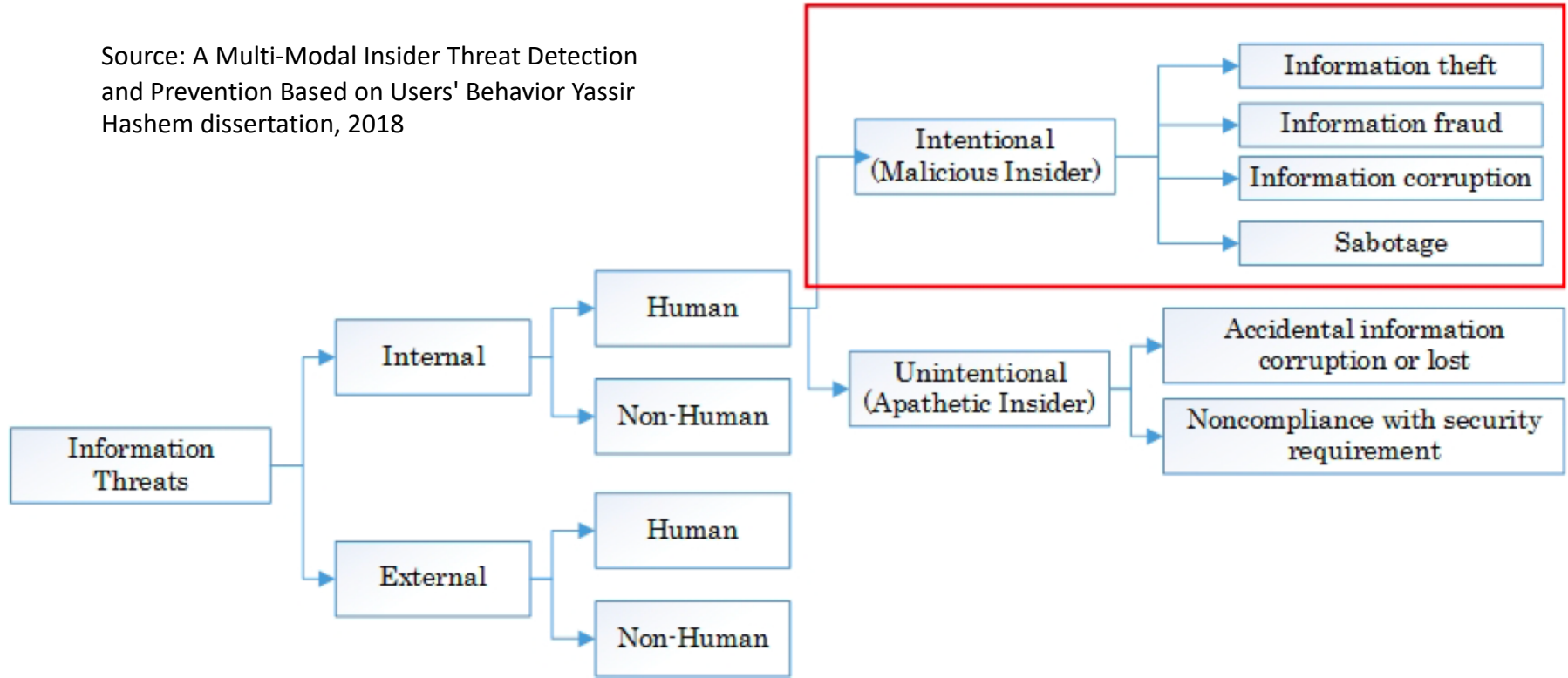
FIGURE 1.1. Information system threat taxonomy adapted from Loch et al.

Cybersecurity Concentration in the IS PhD Program

The Cybersecurity Concentration came about as a results of the collaborative effort with Department of Computer Science and Engineering, and UNT Department of Information Technology and Decision Sciences with the ultimate goal of providing interdisciplinary training, research, and professional services in cybersecurity. The concentration will prepare academics that are capable of conducting research on the critical issues in cybersecurity and related areas, and that are highly focused on information science perspective.

https://informationscience.unt.edu/sites/default/files/cybersecurityconcentration.pdf

Edited Book: Cybersecurity For Information Professionals
Hsia-Ching Chang & Suliman Hawamdeh

Trustworthiness: An Essential Qualification for Cyber Information Professionals
Shuyuan Mary Ho
User Privacy and Security Online: The Role of Information Professionals
Mohammed Nasser Al-Suqri, Salim Said AlKindi and Naifa Eid Saleem
MetaMinecraft: Cybersecurity Education Through Commercial Video Games
Chris Markman
Cybersecurity Challenges and Implications for the Information Profession
Suliman Hawamdeh and Reem Alkhaledi
Bridging the Cybersecurity Talent Gap: Cybersecurity Education in Information Schools
Hsia-Ching Chang, Cary Jim and Suliman Hawamdeh
Information Governance and Cybersecurity: Framework for Securing and Managing Information Effectively and Ethically
Elizabeth Lomas
Healthcare Regulations, Threats, and their Impact on Cybersecurity
Mitchell Parker
Providing Open Access to Heterogeneous Information Resources without Compromising Data Privacy and Confidentiality
Daniel G. Alemneh and Kris Helge*
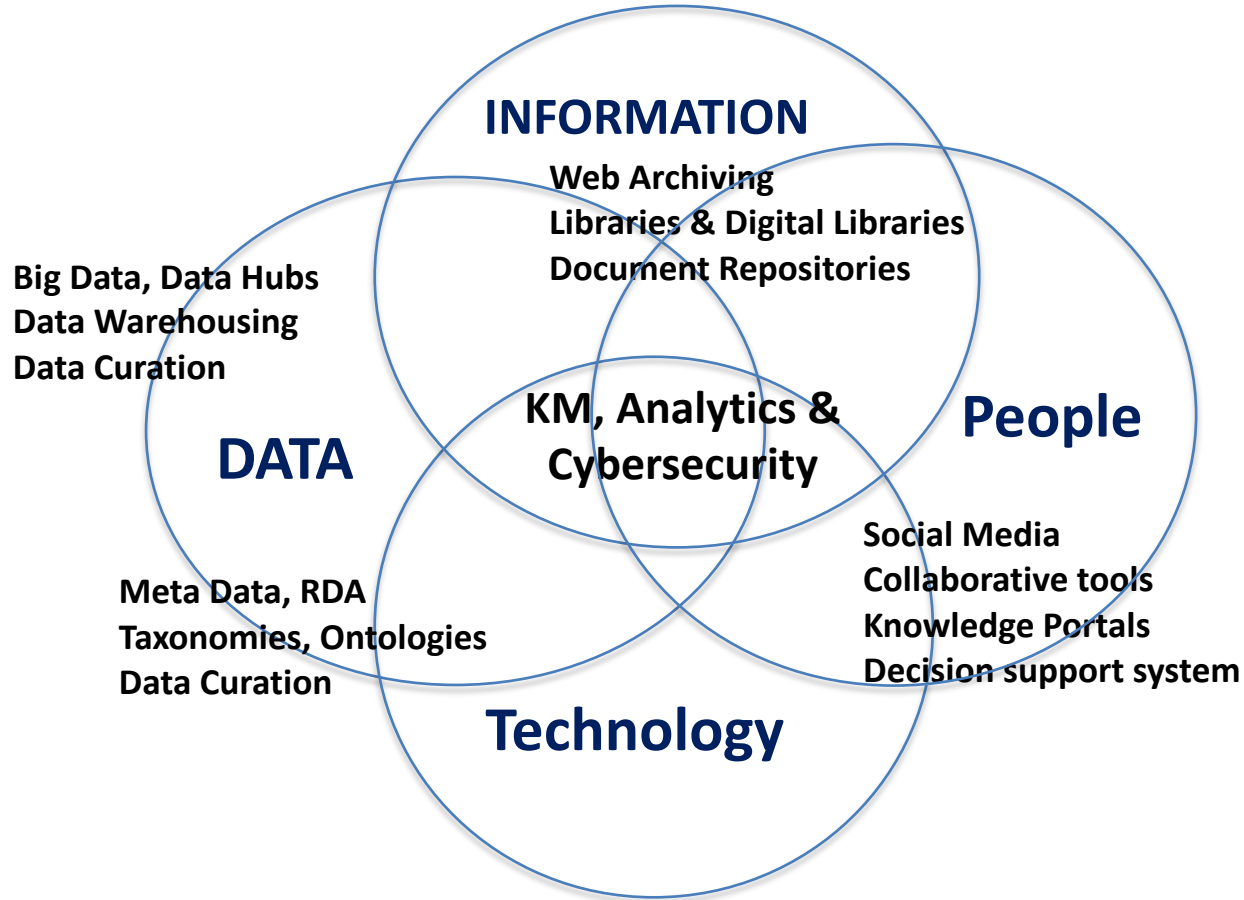**Cybersecurity in the Software Development Life Cycle**
Johnson Kinyua
Mobile Cybersecurity: A Socio-Technical Perspective
Hsia-Ching Chang
Data Security and Privacy
Biodun Awojobi and Junhua Ding

Cybersecurity in the Information Profession

Thank You

Contact: Suliman.Hawamdeh@unt.edu