

COMPUTER SECURITY: Health Care Systems, Democracies and Social Media

Roy Campbell
(rhc@illinois.edu)

Week 1: **Introduction**. The importance of Information Assurance, the Assessment of Risk.

Friday Feb 3 9:30-11:00am.


Osher Lifelong learning Institute
Illinois Classroom



ABOUT THE INSTRUCTOR

- 44 years as Professor of Computer Science
- 3 years as Associate Dean of Engineering for IT
- 20 years as Director of NSA approved Center of Educational Excellence on Information Assurance
- 10 or more Projects in Cyber Security
- His PhD advisor was Brian Randell who discovered the existence of the Colossus machine – a British wartime effort at Bletchley Park to decode automatically German Encrypted war messages
- Now Emeritus Professor with Wife Ann and 6 grandchildren, 3 sons, 1 daughter
- Casey Sutherland (c.sutherland51@comcast.net) is class moderator and will try to keep things running smoothly despite his help. Contact Casey if you cant hear or see me.



Slides marked with  are an opportunity for questions

RULES OF THE ROAD

Slides will be available on web. See:

www.oli.illinois.edu - /downloads/courses/2023 Spring Courses/Computer Security-Campbell/

Please ask questions but at allotted times (middle or end of lecture.)

- Email rhc@Illinois.edu for more lengthy suggestions, questions, and comments.
- Many slides will have an attribution of the information source. If they don't, Google and Wikipedia can probably tell you.
- My knowledge is typical of some Professors – I know a lot about a very small amount of knowledge.
- There are no guarantees or safety assurances implied by anything I might say in class.

WEEK 1: INTRODUCTION

1. Motivation [10-17]:
 1. The Dark Web and Cost/Benefit of Cybercrime
2. A brief introduction to
 1. Cybercrime, Cyberterrorism, Disinformation [19]
 2. Information Assurance Principals [20-32]
 3. The Assessment of Risk [33-37]

WEEK 2: COMPUTER SECURITY: HEALTH CARE SYSTEMS

1. Health care systems and their computer security concerns
2. Major health care systems
3. Health care insurance systems
4. HIPAA, privacy, clinical outcomes, financial resources
5. Recent attacks on health care systems, current controversies, and problems.
6. Practical safeguards

WEEK 3: COMPUTER SECURITY: DEMOCRACY

1. Dissemination and Disinformation
 - a) Conspiracies
 - b) Fake news
 - c) Pictures, Video and Audio
2. Democracy
 - a) News, Freedom of the press, Freedom of speech, Voting process and voting machines, Voting systems, Government
3. Coercion and corruption
 - a) Auditing, verification, certification, authentication, and trust.
4. Surveillance.
 - a) Recent compromises, privacy, and problems.

WEEK 4: SOCIAL MEDIA.

1. Cybersecurity problems with Social Media
2. Tracking & Privacy
 - a) Tracking devices, phones, systems
 - b) Personal/private information
 - c) Blackmail
 - d) People trafficking
 - e) Influencers
 - f) Popular Systems
3. Recent social media problems
 - a) legislation
 - b) proposed controls
 - c) issues.

WEEK 1: INTRODUCTION

1. Motivation [10-17]:

1. The Dark Web and Cost/Benefit of Cybercrime

2. A brief introduction to

1. Cybercrime, Cyberterrorism, Disinformation [19]

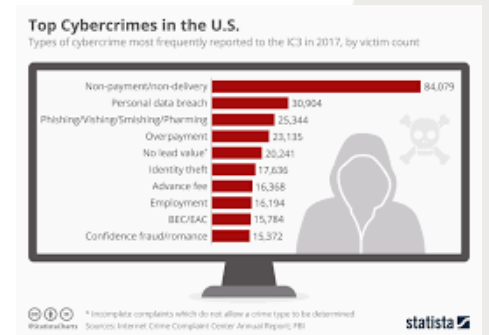
2. Information Assurance Principals [20-32]

3. The Assessment of Risk [33-37]

1. MOTIVATION

- Cyber Security essential for the technology underlying modern society
 - CyberSecurity is really about you
 - What do you want for your life?
 - What do you want for society?
 - What do you want for humanity?
- The Cost/Benefit of Privacy, CyberSecurity, Cyber Attacks, Cyber Crime, Cyber Warfare

HOW MUCH DOES CYBERCRIME COST US?



- In general, the average cost of a cyber attack in 2020 was **around \$133,000**. That is the total average of all types of cyber attacks.
- Cyber crime costs have grown 15% per year annually over the last 5 years.

HOW MUCH DOES A CYBERCRIME TOOLKIT COST?

- Credit card details, account balance up to 5,000, \$120
- Payment processing PayPal transfer from stolen account, \$1,000 – \$3,000 balances, \$45
- Hacked Facebook account, \$45
- Forged Minnesota driver's license, \$150
- Malware Android OS per 1,000 installs, \$950
- DDOS Attack Premium protected website, 20-50k requests per second, multiple elite proxies, 24 hours. \$200



<https://www.privacyaffairs.com/dark-web-price-index-2022/>

AVERAGE PRICE OF HACKING TOOLS

<https://www.top10vpn.com/research/dark-web-prices/hacking-tools/>

Keylogger	\$2.07
Phishing Page	\$2.28
WiFi Hacking Software	\$3.00
Bluetooth Hacking Software	\$3.48
FBI/NSA Hacking Tools	\$5.64
Cryptocurrency Fraud Malware	\$6.07
Hacking Software	\$8.77
Remote Access Trojan	\$9.74
Anonymity Tools	\$13.19
Forgery Templates	\$13.97
Malware	\$44.99
Password Hacking Software	\$50.64
Cryptocurrency Miner Malware	\$73.74
Fraudulent Account	\$145.05
Cell Tower Simulator Kit	\$28,333.33

RATE YOUR CRIMINAL SERVICE

Feedback received as vendor [1 - 20 of 53]

[First](#)
[1](#)
[2](#)
[3](#)
[Last](#)

Rating	Listing Title	User Comment	Date
5 / 5	(Premium) North Carolina Fake ID/Drivers License w/ Tracking (NC)	None left	2021-02-02
5 / 5	(Quality) New Jersey Fake ID/Drivers License w/ Tracking (NJ)	great id. will be back	2021-02-01
5 / 5	(Quality) Missouri Fake ID/Drivers License w/ Tracking (MO)	ids are amazing	2021-02-01
5 / 5	(Quality) Pennsylvania Fake ID/Drivers License w/ Tracking (PA)	This is my 7th purchase with this vendor and i received the id everytime quickly and the work is actually better then qualityfakeids And the jackass that said this vendor sent a book thats impossle just another LIEING cheapskate trying to get this vendors work for free BUY WITH CONFIDENCE, BEST FAKE REAL IDS ON HERE ! Infact my first ever buy was not on here so this vendor can be trusted off here	2021-01-30
5 / 5	(Quality) Indiana Fake ID/Drivers License w/ Tracking (IN)	a1	2021-01-30
5 / 5	(Premium) Texas Fake ID/Drivers License w/ Tracking (TX)	goated	2021-01-29



PERSONAL INFORMATION AVAILABLE LEGALLY

E.g. Spokeo.com, RocketReach
beenverified.com, peoplesmart.com



Patricia A Crowley

Age [redacted] Champaign, Illinois
Latest report as of 01/25/2022

Results May Include

- ✓ Full Address
- ✓ Family Members
- ✓ Email Address
- ✓ Marital Status
- ✓ Phone Number
- ✓ Location History

Order Summary

DETAILS

Spokeo Report for Patricia A Crowley **\$0.95**

7 Day Spokeo Membership Trial* **FREE**

*Cancel anytime. After your 7 day free trial, you will be billed \$24.95 per month.

YOU SAVED \$1.00 ON THIS ORDER!

Total: \$0.95

SECURE CHECKOUT

CHOOSE YOUR PAYMENT METHOD

Credit or Debit Card

PayPal

EMAIL (THIS WILL BE YOUR LOGIN)

2020 VICTIMS BY AGE GROUP

Victims		
Age Range ⁷	Total Count	Total Loss
Under 20	23,186	\$70,980,763
20 - 29	70,791	\$197,402,240
30 - 39	88,364	\$492,176,845
40 - 49	91,568	\$717,161,726
50 - 59	85,967	\$847,948,101
Over 60	105,301	\$966,062,236

Source: FBI/IC3 - Internet Crime Report

<https://www.computerweekly.com/opinion/The-shape-of-fraud-and-cyber-crime-10-things-we-learned-from-2020>



WEEK 1: INTRODUCTION

1. Motivation [10-17]:
 1. The Dark Web and Cost/Benefit of Cybercrime
- 2. A brief introduction to**
 - 1. Cybercrime, Cyberterrorism, Disinformation [19]**
 - 2. Information Assurance Principals [20-32]**
 - 3. The Assessment of Risk [33-37]**

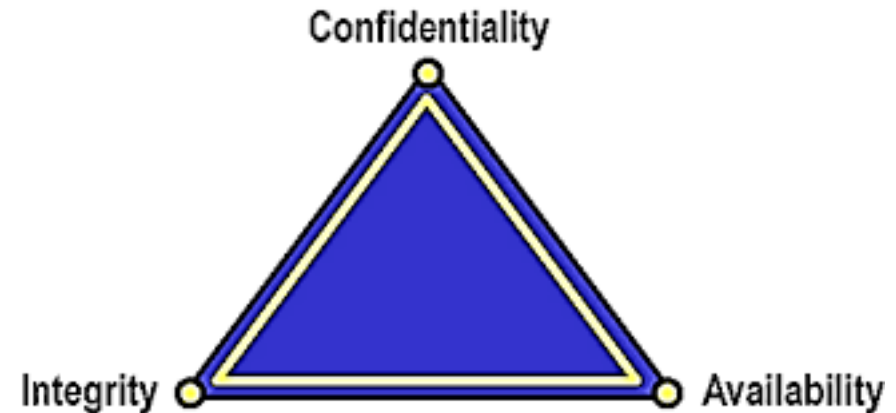
Cybercrime, Cyberterrorism, Disinformation

- **Cybercrime** - Criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data (First use: 1991)
- **Cyberterrorism** - Terrorist activities intended to damage or disrupt vital computer systems (First use: 1994)
- **Disinformation** - False information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth (First use: 1939)



2.1 INFORMATION ASSURANCE AND ITS PRINCIPLES

- Measures that protect and defend information and information systems or CIA
- **Confidentiality,**
- **Integrity, and**
- **Availability** along with
- Authentication and
- Non-repudiation
- Computer Security
- Access Control



CONFIDENTIALITY



Information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO 27000, Common Criteria ISO/IEC 2014)

Note: Privacy \neq Confidentiality.

Confidentiality is a component of privacy that implements to protect our data from unauthorized viewers.

INTEGRITY



Maintaining and assuring the accuracy and completeness of data over its entire lifecycle. (ISO 27000, ISO/IEC 2014)

Note: involves human/social, process, and commercial integrity, as well as data integrity. Touches on aspects such as credibility, consistency, truthfulness, completeness, accuracy, timeliness, and assurance



AVAILABILITY

Information should be consistently and readily accessible for authorized parties.

Make security audits routine. Auto-update or stay abreast of system, network, and application updates.

AUTHENTICATION

Multi factor authentication



- Authentication is the act of verifying a claim of identity.
- Something you know: PIN, password, or your mother's maiden name
- Something you have: driver's license, magnetic swipe card, usb security key (offers 2FA).
- Something you are: biometrics, including fingerprints, face, iris, voice prints

AUTHORIZATION

After identification and authentication, then it must be determined what informational resources a person, program, or computer can be permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change).

Authorization is often implemented using access control

NON-REPUDIATION



- Non-repudiation implies one's intention to fulfill their obligations to a contract.

It also implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction.

COMPUTER SECURITY

In computer security, general access control includes authentication, authorization, and audit.

Authentication and access control are often combined into a single operation, so that access is approved based on successful authentication, or based on an anonymous access token.

Authentication methods and tokens include passwords, biometric analysis, physical keys, electronic keys and devices, hidden paths, social barriers, and monitoring by humans and automated systems.

ACCESS CONTROL MATRIX

In any access-control model, the entities that can perform actions on the system are called subjects, and the entities representing resources to which access may need to be controlled are called objects (see also Access Control Matrix).

Subjects and objects should both be considered as software entities, rather than as human users: any human users can only have an effect on the system via the software entities that they control.

ACCESS CONTROL

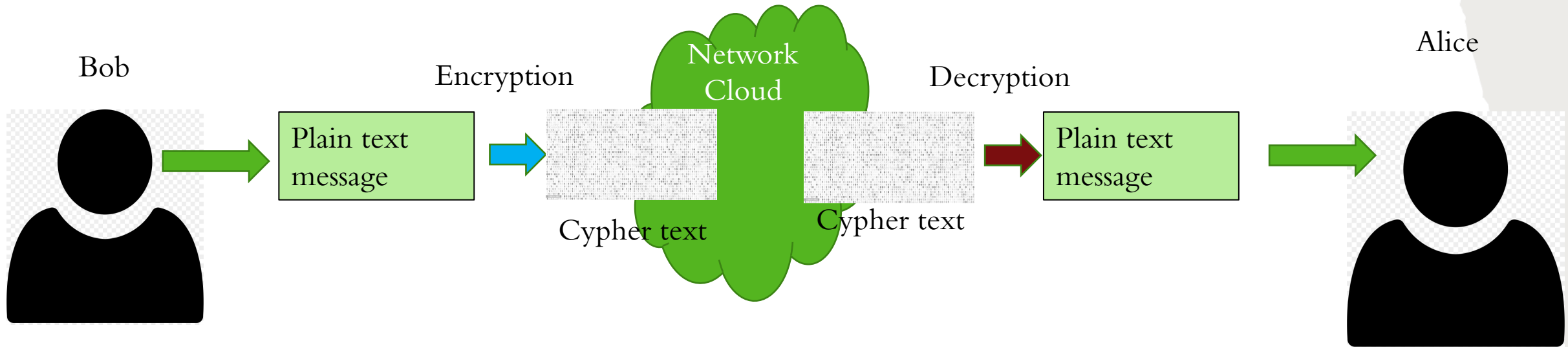


- Non-discretionary. Consolidates all access control under a centralized administration
- Need-to-know. A principle that gives access rights to a person, program, or computer to perform their job functions
- Mandatory access control. Access is granted or denied basing upon the security classification assigned to the information resource.
 - Role-based access control
 - File permissions
 - Group policy objects
 - Kerberos
 - Simple access lists

ZERO TRUST SECURITY MODEL

- **Assume the network is always hostile:** Basic practice before zero trust had been to assume that if you were accessing a known network, you could be relatively certain it was secure. With zero trust, you assume it is not secure.
- **Accept that external and internal threats are always on the network:** Traditional security methods assumed networks were secure until a threat was detected. Zero trust turns this model on its head.
- **Know that the location of a corporate network or cloud provider locality is not enough to decide to trust in a network:** Traditional security rules based on IP address are no longer reliable.
- **Authenticate and authorize every device, user and network flow:** A zero trust model authorizes and authenticates user access by least-privilege access on a per-session basis.
- **Implement policies that are dynamic and calculated from as many data sources as possible:** End-to-end data analytics should be established, providing monitoring and threat detection across the entire architecture, including cloud environments, which support both IT and security operations requirements.

ENCRYPTION BASICS



$\text{Decryption}_{\text{key1}} (\text{Encryption}_{\text{key2}} (\text{plain text})) = \text{plain text}$

Sometimes $\text{key1} = \text{key2}$ symmetric encryption

Sometimes $\text{key1} \neq \text{key2}$ asymmetric encryption

https://en.wikipedia.org/wiki/Category:Cryptographic_protocols

USES OF CRYPTOGRAPHY IN SECURITY

- Keeping password private
- Keep data private – either in motion or on storage
- Authenticate the identity of a sender or receiver of messages
- Ensure the integrity of data
- Show sender really sent message (non-repudiation)
- Prevent repeating a message (once only message)
- Prevent confusion over which message was sent first
- Delegate authority from someone to someone else
- Provide credentials for access control
- Show program code was written by particular author

https://en.wikipedia.org/wiki/Category:Cryptographic_protocols



INFORMATION RESOURCES

- <https://cybersecurityventures.com/movies-about-cybersecurity-and-hacking>
- 2020 Internet Crime Report
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- 10 Biggest Cyber Attacks in History <https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/>
- Dark Web Price Index. <https://www.privacyaffairs.com/dark-web-price-index-2021/>
- 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics, <https://cybersecurityventures.com/cybersecurity-almanac-2022/>
- FBI/IC3 - Internet Crime Report
<https://www.computerweekly.com/opinion/The-shape-of-fraud-and-cyber-crime-10-things-we-learned-from-2020>





Thank
you!!