COLLEGE OF ENGINEERING
SUNY POLYTECHNIC INSTITUTE

project FIBONACCI

Cybersecurity 101

Dr. John Marsh
Assoc. Professor and Chair
Network and Computer Security
SUNY Polytechnic Institute

Outline

- The Importance of Cybersec
- Cybersec Basics
- Opportunities in Cybersec

Cybersecurity 101

- Cybersecurity: Emerging as one of the most important subjects!
  - Why???
- Our computers and networks were NOT designed for security
  - But now that we RELY on computers and the Internet for SO MANY THINGS, we find security lacking
  - Complex: computing + web + mobile
  - More complex → more difficult to secure

Cybersecurity 101

- Cyber threats cause lots of problems these days!
  - Crypto viruses (ransomware), identity theft, data breaches, DoS attacks, attacks on privacy, terrorism, warfare
  - Yesterday: hackers, mostly “for fun”
  - Today: big business “for profit”, cyberwarfare
- **UNSOLVED PROBLEM!**
  - We are counting on **YOU**, the ***cyber generation*** to help solve the **cybersecurity problem**!

project FIBONACCI

Cybersecurity 101

- Cybersecurity basics:
  - Goals: CIA + R
    - Confidentiality, Integrity, Availability, Resilience
  - Tools:
    - Training! Computer users at home and in the workplace
      - SOCIAL ENGINEERING IS THE #1 ATTACK METHOD
    - Cryptography – encrypt data with a secret key
    - Secured protocols (use cryptography)
    - Authentication techniques (use cryptography)
    - Anti-virus and anti-malware tools
    - Firewalls, next-gen firewalls and “security appliances”
    - Intrusion detection: applying Artificial Intelligence (AI)
  - Vulnerability + Threat → Attack
    - Exploit = tool for attacking a vulnerability
    - Zero-day vulnerabilities:
      - Responsibly disclosed by security researchers
      - Sold on black market by malicious hackers

- Crypto basics:
  - Data: all reduced to 0's and 1's
  - One-key crypto: same key encrypts and decrypts
    - Block ciphers – permute groups of bits in a reversible way based on a key
    - Security: "cracking" the encryption requires brute force attack (trying all possible keys)
    - Key length n bits → 2^n keys to try (age of universe for $n \geq 128$)
    - Longer keys → more secure!
  - Two-key crypto: everyone gets two keys
    - Each person gets 2 keys: private key, public key
    - Either encrypts, then the other decrypts
    - Enables both security and authentication
    - Public key certificates used to distribute public keys

- Crypto basics:
  - Public key cryptography
    - With no previous communications, allows for a shared secret key to be established over an insecure data channel (THINK ABOUT THAT FOR A MINUTE!)
    - RSA encryption: security based on difficulty in factoring the product of two primes
  - Quantum computing promises to speed up brute force attacks
    - Computing with Qbits rather than bits
    - Quantum supercomputer: requires MUCH longer keys! (e.g., RSA security ensured only with 8 Tb key!)
    - Lots of research into this area
      → seems like this technology will happen!!!

Cybersecurity 101

- Big picture tradeoffs:
  - Security vs. convenience
  - Security vs. privacy
- Active debate on these issues today!
  - Crypto “back door” for law enforcement?
  - Strong crypto in widely used chat apps?
  - Anonymity while online?
  - Anonymity while in public?
- Other big debates:
  - Net neutrality
  - Regulation of big tech: Alphabet, Amazon, Apple, Facebook
  - How to secure elections

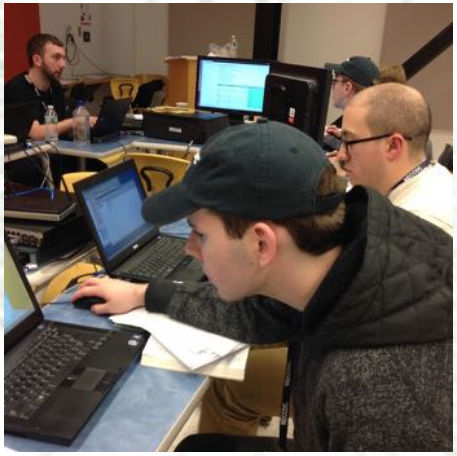
Cybersecurity 101

- Protecting your own cyber existence:
  - Password management
    - Use complex passwords that are easy for YOU to remember – NO DICTIONARY WORDS
    - Different passwords for important accounts like banking, etc.
    - Use a password manager (Apple Keychain, LastPass, OnePass, etc.)
    - Password protect your lock screen
  - Software updates: new vulnerabilities found all the time!
    - Turn on automatic updates on all computing devices
    - Do not use outdated computing devices
    - Download programs only from trusted sources
  - On the web: beware “social engineering attacks”
    - Be wary of links in emails and on social media
    - Do not click on “clickbait” links on web pages
    - Use private browsing windows for everything except accounts you log into – cookies deleted when window closed
  - Wireless security
    - Be wary of public Wi-Fi
    - Wi-Fi routers: change default passwords
    - Wi-Fi Routers: use WPA2 security (WPA3 coming soon!)

project FIBONACCI

Cybersecurity 101

- Opportunities for YOU the cyber generation
  - Lots of jobs!
    - Computing field: secure, flexible, safe, satisfying, rewarding
  - IT = Information Technology
    - "All IT jobs are cybersecurity jobs"
    - IT jobs are everywhere!
  - Cybersecurity research
    - Air Force Research Laboratory (AFRL) Information Directorate headquarters in Rome, NY
    - Thousands of computing and cyber research jobs!
  - Cybersecurity at SUNY Poly
    - BS in Network and Computer Security
    - MS in Network and Computer Security



project FIBONACCI

Project Fibonacci

- Thanks for our generous sponsors!

The Shoreline Group

United Way

CHOBANI®
FOUNDATION

- More detailed version of the presentation follows:

The Importance of Cybersecurity

- Cybersecurity is important because…
  - It might be part of your job someday
    - Securely use computing resources at work
    - Actually working in the field of cybersecurity!
  - It already is part of your job whenever you use a computer
    - Manage your online identity
      - Social media, blogs, etc.
    - Manage your privacy
      - Browsing history, etc.
    - Manage your finances
      - Banking, bill payment, retirement account, etc.

The Importance of Cybersecurity

- Computing and Internet are essential to modern (digital) life:
  - Governments
  - Businesses
  - Citizens

  } All increasingly run on computers

- Society depends on computing and networking to support critical infrastructure:
  - Distribution systems for power, water, food, information
  - Transportation systems: auto, rail, air, water
  - Manufacturing and distribution of commodities and consumer goods
  - Financial services and banking
  - Medical – hospitals, first responders, medical records, etc.

project FIBONACCI

The Importance of Cybersecurity

- Cybersecurity is in the news – data breaches, privacy issues, theft, extortion, critical infrastructure vulnerabilities, etc.
- LOTS of "bad actors" out there!
- A big problem – government, corporate, small business, and personal computing all affected
- Computing + Web + Mobile
  → e-commerce, social media, e-health, etc.
  → extremely complex environment

The Importance of Cybersecurity

- Security in the physical world – a mostly solved problem (but still challenging)
  - Securing an area
    - Walls, fences, barriers, etc.
    - Armed guards
  - Securing buildings and rooms
    - Strength of building structure
    - Locks on doors: keys, swipe access, proximity card access
- Security in the cyber world – an unsolved problem
  - We're still learning to build the analog of a house with doors and windows that can be locked!
- **A call to action to the cyber generation! (BTW, that's YOU!)**

project FIBONACCI

Cybersecurity Basics

- Yesterday:
  - Computing and Internet designed without security in mind
  - Incentives to attack were few
- Today:
  - Big business in effort to secure computing and the Internet
    - But security is now applied as an afterthought, making it much more difficult
  - Big business in exploiting vulnerabilities for profit

Cybersecurity Basics

- Cybersecurity goals (CIA triad "enhanced"):
  - Confidentiality
    - Information is kept private – only available to authorized parties
  - Integrity
    - Information is reliable – can only be modified by authorized parties
  - Availability
    - Info systems are available – when and where needed by authorized parties
  - Resilience
    - Acknowledge successful attacks will occur
    - Ability to function after a successful attack

Cybersecurity Basics

- Cyber attack = successful exploitation of a vulnerability by a bad actor
  - Vulnerability: some aspect of systems that enables attack
  - Threat: existence of a bad actor who wishes to attack your systems
  - Exploit: a method of taking advantage of a vulnerability for a successful attack
- Types of cyber attack include:
  - Hijacking resources, misusing credentials
  - Denial of service
  - Financial fraud
  - Theft of industrial secrets
  - Identity theft
  - Warfare, terrorism

Cybersecurity Basics

- One vulnerability can lead to multiple threats
- Vulnerabilities not a problem if no threat exists that targets it
  - However, previously undetected vulnerabilities that become known to bad actors are called "zero-day vulnerabilities" and suddenly pose a great threat since no protections exist
- Vulnerabilities may be due to:
  - Unintentional bugs in software
  - Misconfigured software
  - Malicious code built into software (may be very difficult to detect)

Cybersecurity Basics

- Well-known vulnerabilities are easy targets
  - "Malware" tools exist that can automate attacks on known vulnerabilities
  - Tools also exist to automatically seek out targets with well-known vulnerabilities
  - A "drive by" attack exploits a vulnerability simply by visiting a malicious web site
  - These attacks are usually relatively easy to prevent by keeping all your software up-to-date → enable automatic updates on your computing devices, and don't download software from untrusted sources

- Types of bad actors:
  - Insiders (especially harmful – also trusted actors)
  - Lone malicious hackers
  - Advanced Persistent Threats (APTs)
    - Nation-states or organized crime; armies of experts intent on attacking specific high-value targets
    - Sophisticated attacks carried out “by hand” over long periods of time
    - Include social engineering techniques
    - Include expert knowledge of exploitation techniques
    - Zero-day vulnerabilities often exploited

- Social engineering attacks – especially potent
  - Attacker impersonates a trusted party convinces target to reveal protected information or provide access to protected resources
  - Examples include impersonating…
    - Tech support, say password needed
    - Boss, say some sort of access needed
    - Customer, say password reset is needed
    - Legit malware detection program, say “click here for the fix”
    - Email from trusted colleague or trusted source (bank, government, magazine you subscribe to, etc.), say “click on this link”
      - This is a phishing attack – one of the most successful types
      - Spear phishing is an attack on a specific person of high value using detailed knowledge of their work, interests, or family

Cybersecurity Basics

- Perfect security: does not exist
  - Tradeoffs always exist:
    security vs. [financial resources, time, convenience, liberty, capabilities]
- More complexity → more vulnerabilities
  - Even if you design the system with security in mind!!!
- Security updates fix vulnerabilities, but may introduce new ones
  - All-new "more secure" operating system is probably less secure than one that has been undergoing the "test of time" and has had security patches for many years

project FIBONACCI

- Example: BMW car thefts in London, 2011
  - New, advanced car locks use radio signals and wireless key
  - Radio frequency jammer caused cars not to be locked by key
  - Once in car, computer accessed, code retrieved, and blank key reprogrammed to operate car
  - Dozens of cars were stolen in just a few weeks!
- Example: Many IoT devices
  - Video baby monitors, allow viewing camera on the web
    - Many early-generation devices were very insecure and allowed anyone to view the camera online

What to do???

- Risk analysis
  - Considers both known and suspected vulnerabilities and threats
  - Considers probability of, and the financial impact of, each threat being exploited
    - Impact to reputation is ultimately a financial impact
  - Allows for optimal resource allocation for meeting cybersecurity goals
    - e.g., More hires for security team vs. new equipment?

Cybersecurity Basics

- Cybersec goals apply to
  - Computing resources (processing power, data)
  - Networking resources (connectivity, net devices)
- Technologies supporting cybersec goals include:
  - Access control
  - Cryptography
  - Secure computing platforms and computer defense strategies
  - Secure networking protocols and network defense strategies
  - Operational security – following "best practices" to implement processes and procedures that support security, including employee training

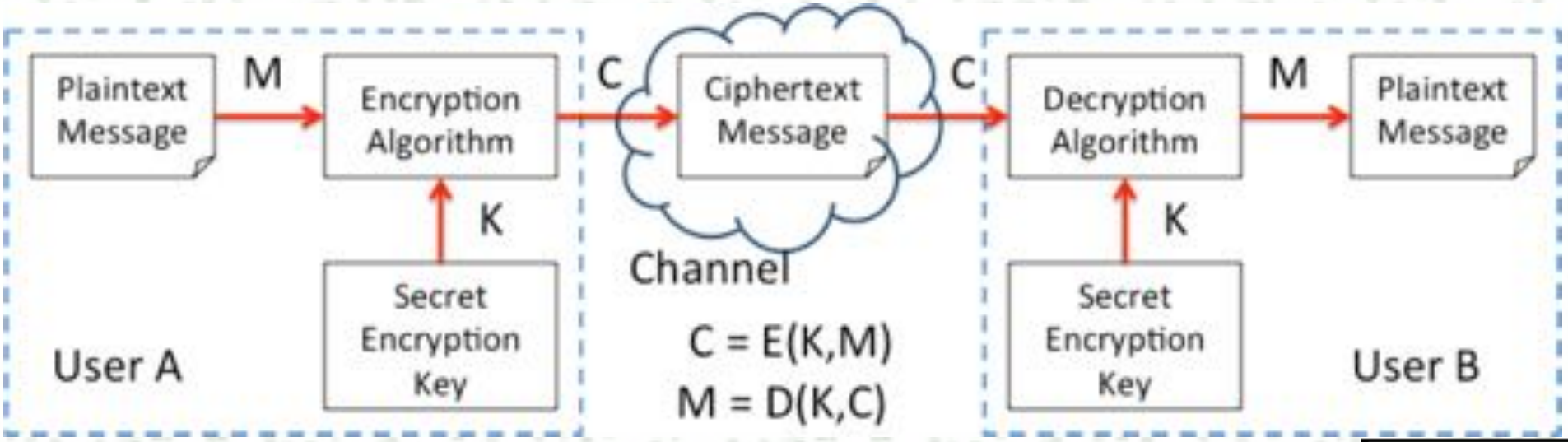
We give a brief introduction to just these two

project FIBONACCI

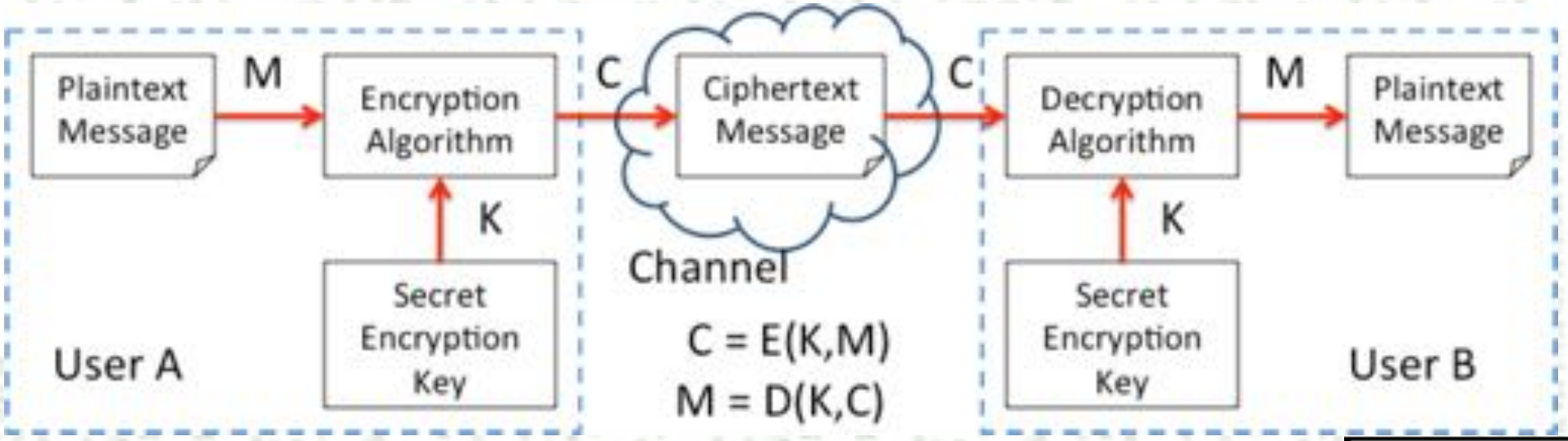
- Access Control
  - Allow authorized access and prevent unauthorized access to systems and data
  - Tough to get right (e.g., cases of B. Manning, E. Snowden)
- AAA architecture for access control
  - Authentication
    - Verifying the identity of a user
    - Users prove identity
  - Authorization
    - Process of implementing polices (user permissions)
  - Accounting
    - Process of keeping records of user activities

- Technologies supporting access control:
  - Authentication methods
    1. what the user knows (e.g., userid, password)
    2. what the user possesses (e.g., security token)
    3. what the user is (biometrics – e.g., fingerprint reader, retina scanner)
  - Authentication database
    - Contains entries for trusted users
      - authentication information to verify identity
      - authorization information to set permissions
  - Authentication protocols
    - Techniques for unauthenticated users to access the authentication database via the network

- Cryptography
  - Plaintext may consist of text, applications, multimedia, etc., all converted to 0's and 1's
  - Plaintext encrypted using the secret key
    - Ciphertext looks like random 0's and 1's
  - Decryption only possible using the secret key



- Cryptography
  - Pictured below is case of symmetric (one-key) cryptography, where encryption and decryption both use the same key



Some Examples

- Asymmetric cryptography (two-key)
  - Two keys – either can be used to encrypt, then the other is used to decrypt
  - Everyone gets their own key pair
    - One key kept secret, the other made public
  - Use #1: Send a secret message to Alice:
    - Encrypt message with Alice's public key, send to Alice
    - Only Alice has her secret key to decrypt the message
  - Use #2: Authenticate sender's identity:
    - Encrypt a message with your secret key, then anyone can decrypt with your public key and be sure it was you who sent it
    - This is how digital signatures work

Some Examples

- Asymmetric (two-key) cryptography
  - Usage requires some way to be sure whose public keys you're using
    - Impersonated public keys give rise to Man-In-The-Middle (MITM) attacks that enable eavesdropping and data manipulation
    - Solution: Public Key Infrastructure (PKI)
  - PKI: Trusted parties called Certificate Authorities (CA) digitally sign file containing a public key and the name of the person it belongs to
    → the resulting Public Key Certificate is something you can use to distribute your public key "with your name on it"

Some Examples

- PKI used for secure online transactions
  - Two-way authentication: both parties authenticate to each other
    - When you log into your bank account online, MAKE SURE you are at the REAL BANK SITE – otherwise a malicious site could be stealing your bank username and password credentials!
    - The bank authenticates to you FIRST by sending you their public key certificate → your browser verifies it using the public keys of trusted CAs it already has
      - This uses the secure web protocol HTTPS → showing lock icon in your browser
    - Once you see the lock icon, you can safely authenticate to the bank with your username and password

Some Examples

- Asymmetric cryptography also allows shared secret keys to be established over an insecure connection

  (THINK ABOUT THAT FOR A MOMENT)

- Hybrid cryptography
  - Combines symmetric and asymmetric cryptography
  - Symmetric (one-key) crypto: *fast*, but no way to establish shared key over an insecure connection
  - Asymmetric (two-key) crypto: s l o w, not good for big data transfer
  - What we do in practice:
    - Use two-key cryptography with PKI to establish a shared secret key
    - Then use the shared key with one-key cryptography to make data transfer

Some Examples

- Asymmetric cryptography
  - Based on “one way” mathematical problems → easy to calculate one way, hard to reverse
  - Security is ensured by assuming the reverse calculation is practically impossible
  - Two examples of “one way” math problems:
    1. Calculating the factors of the product of two large primes
    2. Calculating the log of a number raised to a large power in modular arithmetic

Some Examples

- Calculating the factors of the product of two large primes
  - Prime number: only factors are 1 and itself
    - E.g., 2, 3, 5, 7, 11, 13, 17, 19, 23, … , 956789, ... , 1247951, ...
  - Prime factorization: any number can be decomposed into a product of primes
    - E.g., $120 = 2 \times 2 \times 2 \times 3 \times 5 = 2^3 \times 3 \times 5$
  - Product of two primes: has only those two primes as factors
    - E.g., $143 = 11 \times 13$
    - E.g., $1{,}194{,}025{,}789{,}339 = 956{,}789 \times 1{,}247{,}951$

project FIBONACCI

Some Examples

- Factoring the product of two primes
  - A mathematically difficult problem
  - Assumed to be practically impossible for large enough numbers
    - Existing techniques (e.g., trying every possible factor) are too slow
    - We use numbers with hundreds of digits to ensure factoring is not possible

a = 956,789 = prime
b = 1,247,951 = prime
a × b = 1,194,025,789,339

easy

1,194,025,789,339 = a × b
a = ?
b = ?

hard

project FIBONACCI

Some Examples

- Calculating the log of a number raised to a large power in modular arithmetic
  - Modular arithmetic "mod p": add, subtract, multiply, and divide but always divide the answer by p and keep only the remainder. Note all remainders are in the range from 0 to p – 1.

$3 \times 4 = 12$

$12 \div 4 = 3$

Normal Arithmetic

$3 \times 4 = 5$

$5 \div 4 = 3$

$12 = 1 \times 7 + 5$ mod 7

$(3 \times 4) \bmod 7 = 5$

$(5 \div 4) \bmod 7 = 3$

Some Examples

- Calculating the log of a number raised to a large power in modular arithmetic
  - Modular arithmetic "mod p": we can also do exponents and logarithms

$4^6 = 4 \times 4 \times 4 \times 4 \times 4 \times 4 = 4096$

$\text{Log}_4(4096) = 6$

Normal Arithmetic

$4^6 = 4 \times 4 \times 4 \times 4 \times 4 \times 4 = 11$

$\text{Log}_4(11) = 6$

$4096 = 19 \times 215 + 11$ mod 19

$4^6 \bmod 19 = 11$

$\text{Log}_4(11) \bmod 19 = 6$

Some Examples

- Asymmetric cryptography
  - Finding the log in modular arithmetic is assumed to be practically impossible for large enough numbers

$7^{3177} = \mathbb{B} =$

easy

$\log_7(\mathbb{B}) = 3177$

easy

$7^{3177} = 953445 \pmod{956789}$

easy

$\log_7(953445) = a = ?$

$a = 3177 \pmod{956789}$

hard

project FIBONACCI

Some Examples

- Another type of “one way” math calculation is called a hash function
  - The hash function takes any size input and produces a fixed-size output
    - Input could range from a single 0 or 1 to an entire hard disk drive of information
    - The output of the hash function is called the “hash” of the input, and acts as a fingerprint
    - Like with humans, it is possible for two to have the same fingerprint, but highly unlikely
    - And two having the same fingerprint certainly does not ensure everything else about them is the same!
  - Hash functions are used to verify that data has not been altered during transmission
    - An encrypted fingerprint of the data is sent along with it!

project FIBONACCI

- Future of cybersecurity
  - The Internet of Things (IoT) is emerging as a new area of great interest

- Future of cybersecurity
  - The cybersec industry will continue to grow along with computing in general
    - Lots of great opportunities for YOU, the cyber generation, to play an important role with rewarding careers
  - We will get better at protecting our critical computing and networking infrastructure
    - But we will also continue to live with successful cyber attacks for the foreseeable future
  - We are hoping to avoid devastating cyber wars, although limited cyber warfare is a reality today

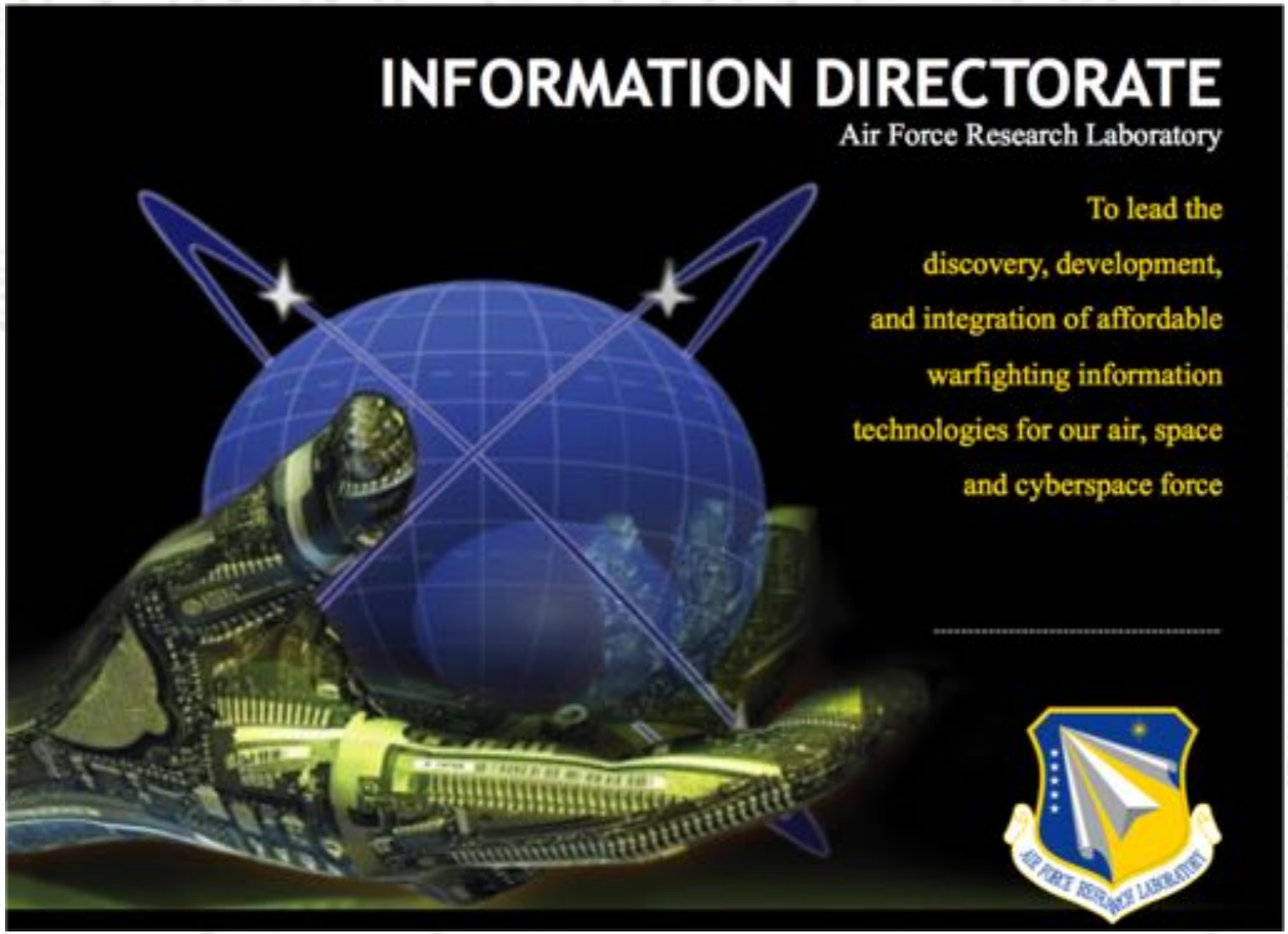
Opportunities in Cybersec **WOW!**

- Cybersecurity professionals are in great demand in industry and government (and academia)
- The largest part of the job market is in the IT (Information Technology) field
  → many cyber defense and incident response teams are evolving as part of IT
- The Utica-Rome area has a special job market due to the Air Force Research Lab's Information Directorate headquarters in Rome, NY

project FIBONACCI

Opportunities in Cybersec

- AFRL Information Directorate



project FIBONACCI

Opportunities in Cybersec

- AFRL Information Directorate

TECHNICAL AREAS OF EXPERTISE

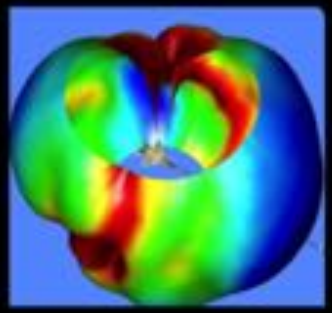
INFORMATION EXPLOITATION & OPERATIONS

- Cyber Assurance
- Cyber Operations
- Sensor Data Exploitation
- Cyber Integration & Transition

INFORMATION INTELLIGENCE SYSTEMS & ANALYSIS

- Activity Based Analysis
- Information Handling
- Analytical Systems
- Special Security

INFORMATION SYSTEMS



- Information Management Technologies
- Resilient Synchronized Systems
- Advanced Planning & Autonomous C2 Systems
- Warfighter Integration

COMPUTING & COMMUNICATIONS

- Trusted Systems
- High Performance Systems
- Training and Evaluation
- Integration & Transition
- Information Transmission
- Networking Technology

project FIBONACCI

Where are SUNY Poly NCS (Network and Computer Security) graduates now employed?

- Assured Information Security
- RSA division of EMC
- MA Polce Consulting
- New York Central Mutual
- North Point Defense
- Dell Secureworks
- Target Mobile Care
- Secure Network Technologies
- Intercloud Systems
- Quanterion Solutions
- Target
- R.I.T.
- Integritechs
- Harris Communications
- Booz Allen Hamilton
- NBT Bancorp
- TIME WARNER CABLE
- Air Force Research Lab
- Nfrastructure
- Excellus BCBS

project FIBONACCI

Thanks for Visiting SUNYIT!

QUESTIONS?

- Here is a short introduction to SUNY Poly's cybersecurity BS and MS programs

Welcome to
SUNY Poly!

Cybersecurity at SUNY Poly

- Cybersecurity is one of the hottest sub-fields of computing today…
  ... and we are capitalizing on this trend with our Network and Computer Security (NCS) programs
- Cybersecurity Programs:
  - BS-NCS
  - MS-NCS

Bachelor of Science Network and Computer Security

A. Core Courses 6 courses

- CS 108 Computing Fundamentals
- NCS 181 Introduction to Cybersecurity
- NCS 205 Introduction to Linux
- NCS 210 Network Transmission Technology
- CS 220 Computer Organization
- CS 240 Data Structures and Algorithms

B. Intermediate Coursework 5 courses

- NCS 315 Networking and Information Systems
- NCS 320 Information Assurance Fundamentals
- IS 320 Systems Analysis and Design
- NCS 330 Information Assurance Ethics, Policies and Disaster Recovery
- NCS 350 Wireless Systems and Security

C. Advanced Electives 3 courses

D. Capstone 2 credits

- NCS 495 Network and Computer Security Capstone

C. Advanced Electives 3 courses

- NCS 316 Data Network Design
- NCS 384 Network Intrusion Detection
- NCS 416 Digital and Internet Telephony
- NCS 425 Internetworking
- NCS 430 Penetration Testing
- NCS 435 Computer and Network Forensics
- NCS 440 Virtualization
- NCS 450 Network Security
- NCS 460 Advanced Wireless Security
- NCS 490 Special Topics in Network and Computer Security
- NCS 494 Network and Computer Security Internship

project FIBONACCI

Network and Computer Security (MS)

Program Requirements

The M.S. in Network and Computer Security consists of **33 credit hours**

Core Courses: 18 credit hours

Technical Electives: 9 – 12 credit hours

Thesis/Project: 3 – 6 credit hours

Core Courses (18 credit hours)

- NCS 511 Information Assurance Fundamentals
- NCS 521 Data Communications
- NCS 531 Computer Security
- NCS 541 Network Security
- NCS 543 Secure Protocols
- NCS 598 Research Methods

Technical Electives (9-12 credit hours)

- NCS 522 Network Administration
- NCS 532 Network Intrusion Prevention and Detection
- NCS 542 Advanced Network Protocols and Standards
- NCS 552 VoIP and Multimedia Security
- NCS 562 Wireless and Mobile Networks
- NCS 563 Wireless Security
- NCS 590 Special Topics in Network and Computer Security

Thesis/Project (3 – 6 credit hours)

- NCS 597 Research Project (3 credits)
  OR
- NCS 599 Thesis Research (6 credits)

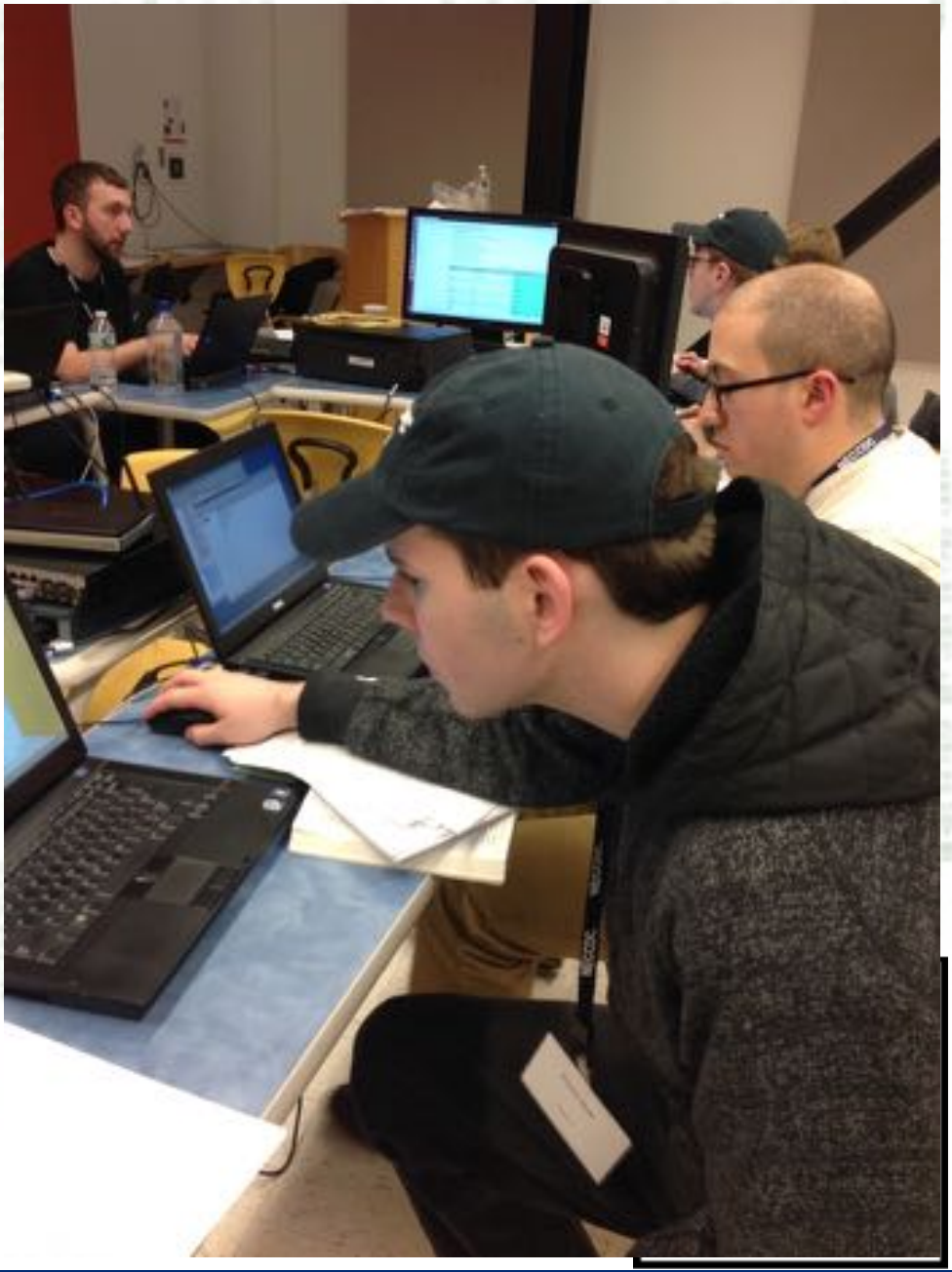
project FIBONACCI

Cybersecurity at SUNY Poly

- NCS Program – One of SUNY Poly's newest academic programs
- Our first full class graduated May 2015
- Academic year 2015-16 headcount: 125 undergraduate students

NCS Club and Activities

- NCS/CS Interns
  - Our NCS system administrator leads a team of student interns maintaining our NCS network and computer labs
- NCS Club
  - Active on campus – student club of the year 2 years running



NCS Club and Activities

- NCS Club
  - Weekly meetings, dedicated “hackerspace” for club members

NCS Club and Activities

- NCS Club
  - SUNY Poly participates and has led the way in creating the CNY Hackathon
    - Event rotates between SUNY Poly, Utica College, and MVCC campuses
    - Participating schools include SUNY Poly, MVCC, HCCC, Syracuse University, and Utica College

Extras

- Bibliography
  - A great introduction to cybersecurity
    - Cybersecurity and Cyberwar, P.W. Singer and A. Friedman, Oxford Univ. Press 2014
  - AFRL Information Directorate Overview
    - http://www.wpafb.af.mil/Portals/60/documents/afrl/ri/afrl-ri-overview.pdf?ver=2016-07-13-142035-373
  - Intro video:
    - https://e-discoveryteam.com/2014/04/27/the-cia-cyber-security-triad-and-9ec4c12949a4f31474f299058ce2b22a/

project FIBONACCI