ECE560
Computer and Information Security

Fall 2020

Grab bag: Physical security, organizational security, security auditing, and legal/ethical aspects

Tyler Bletsch

Duke University

Physical security

Based on chapter 16

Physical security

- **Physical security**: “what if I just go over there and take it?”

- Systems:
  - **Physical access is root access**! Attackers holding a system can:
    - Apply BIOS or boot loader settings
      - Want access to a Linux machine? Add “single” to the kernel parameters for single-user mode...
    - Pop out drive and mount it in another system
      - Defeats all restrictions except **encryption**
    - Alter the hardware (e.g., reflash firmware, solder a malicious chip, etc.)

- Facilities:
  - Guarding a thousand computers is harder than guarding a perimeter, so let’s guard a perimeter instead.

Facility access control and high availability

- Physical access control
  - **Restrict building access**
    - Locks or screening at entry points
    - Intruder sensors and alarms
    - Controlled areas patrolled or guarded
    - Issues to consider:
      - Mechanisms of identification (security vs convenience)
      - Fail open or fail secure? Don't forget safety...
      - If fire code says you need more exits than you can guard, alarm some
  - Equip movable resources with a tracking device
  - Surveillance systems with recording and real-time viewing
- Redundancy
  - Allow "fail over" to other facility in the event of a disaster or breach
  - Lots of details here – out of scope for us now.

Adapted from the textbook

Physical security in layers (SP 800-116)

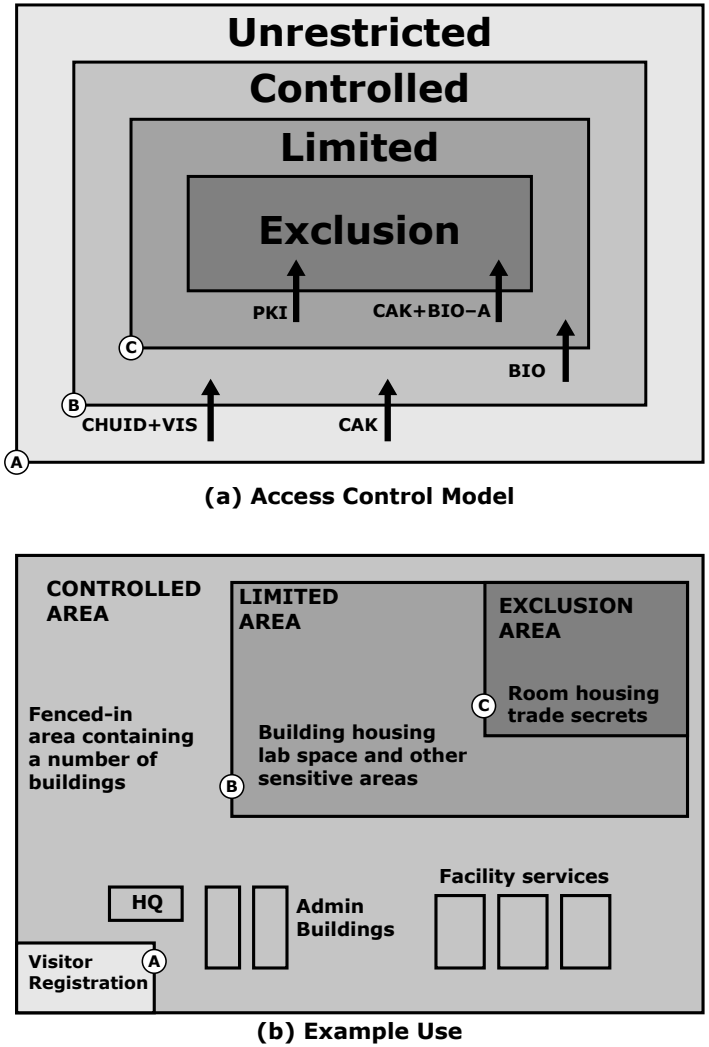


Figure 16.4 Use of Authentication Mechanisms for Physical Access Control

- Four tiers of space priority
- Gates between them with differing credentials
  - CHUID+VIS: **Card Holder Unique Identifier** (badge) plus **Visual** identification (guard looks at you)
  - CAK: **Card Authentication Key** (smart badge)
  - BIO: **Biometric** (e.g., fingerprint)
  - BIO-A: **Biometric with Attendant** (a human watches you do it)
  - PKI: **PIV Authentication Key** (pin-secured public key crypto, counts as multi-factor since you need pin (known) and badge (owned).

(PIV = Personal Identity Verification)

Figure from the textbook. Based on NIST SP 800-116 [A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)

Organizational Security

Based on chapter 17

The human issue

Companies and organizations are made of people;
people are the cause of 100% of all security issues.

(Also 100% of the fixes)

- People problems:
  - Errors and omissions
  - Manipulation by attackers (discussed in the next lecture)
  - Fraud
  - Sabotage
- People solutions:
  - Inform them
  - Get only good people
  - Get explicit agreement
  - Terminate employment securely

Informing the people

- Informing people takes three forms:
  - **Awareness**: Make people know about threats and issues
    - Broad, short messages and reminders (e.g. emails from IT)
  - **Training**: Tell people what to do in specific situations

General users	• Focus is on good computer security practices
Programmers, admins	• Develop a security mindset in the developer
Management-level	• How to make tradeoffs involving security risks, costs, benefits
Executive-level	• Risk management goals, measurement, leadership

  - **Education**: In-depth understanding for security professionals
    - E.g. this course

Security in hiring

- Background checks as part of hiring process –
  do them in proportion to the sensitivity of the role
  - **Screening:** Find fraud in credentials and experience
  - **Criminal record check:** Find records of past crimes or malpractice relevant to the job at hand
  - **Credit check:** Ensure candidate is not in financial duress
    - People with severe money problems can be plied by attackers to betray an organization

Employment Agreements

Employees should agree to and sign the terms and conditions of their employment contract, which should include:

I. Employee and organizational responsibilities for information security

II. A confidentiality and non-disclosure agreement

III. Reference to the organization's security policy

IV. Acknowledgement that the employee has reviewed and agrees to abide by the policy

Termination of Employment

- Termination security objectives:
  - Ensure employees, contractors, and third party users exit organization or change employment in an orderly manner
  - The return of all equipment and the removal of all access rights are completed

Critical actions:

- Remove name from all authorized access lists
- Inform guards that ex-employee general access is not allowed
- Remove personal access codes, change physical locks and lock combinations, reprogram access card systems
- Recover all assets, including employee ID, portable USB storage devices, documents, and equipment
- Notify by memo or e-mail appropriate departments

Security Auditing

Based on chapter 18

Security Auditing

- A **security audit** is a review of system records to:
  - Determine if the configuration is adequately secure,
  - Confirm that existing policies are being followed,
  - Detect any previously undetected breaches, and
  - Recommend changes/improvements.
- Based on an **audit trail**: the chronological record of available **events** and data woven together from multiple sources
- **Events** are found via *instrumentation* or *logging*. They include:
  - Creation/deletion of objects
  - Changes to access rights
  - Authentication events
  - Policy checks performed by the security software
  - Security-related actions taken by an operator/user
  - Import/export of significant data from/to removable media or network

Table 18.3

Monitoring Areas Suggested in ISO 27002

a) user IDs
b) system activities
c) dates, times and details of key events, e.g. log-on and log-off
d) device identity or location if possible and system identifier
e) records of successful and rejected system access attempts
f) records of successful and rejected data and other resource access attempts
g) changes to system configuration

h) use of privileges
i) use of system utilities and applications
j) files accessed and the kind of access
k) network addressees and protocols
l) alarms raised by the access control system
m) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems
n) records of transactions executed by users in applications

```
Jan 27  17:14:04   host1  login: ROOT LOGIN console
Jan 27  17:15:04   host1  shutdown: reboot by root
Jan 27  17:18:38   host1  login: ROOT LOGIN console
Jan 27  17:19:37   host1  reboot: rebooted by root
Jan 28  09:46:53   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
Jan 28  09:47:35   host1  shutdown: reboot by user1
Jan 28  09:53:24   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 12  08:53:22   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 17  08:57:50   host1  date: set by user1
Feb 17  13:22:52   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
```

(a) Sample system log file showing authentication messages

```
Apr 9 11:20:22   host1   AA06370:  from=<user2@host2>, size=3355, class=0
Apr 9 11:20:23   host1   AA06370:  to=<user1@host1>, delay=00:00:02,stat=Sent
Apr 9 11:59:51   host1   AA06436:  from=<user4@host3>, size=1424, class=0
Apr 9 11:59:52   host1   AA06436:  to=<user1@host1>, delay=00:00:02, stat=Sent
Apr 9 12:43:52   host1   AA06441:  from=<user2@host2>, size=2077, class=0
Apr 9 12:43:53   host1   AA06441:  to=<user1@host1>, delay=00:00:01, stat=Sent
```

(b) Application-level audit record for a mail delivery system

```
rcp       user1   ttyp0    0.02 secs Fri Apr 8 16:02
ls        user1   ttyp0    0.14 secs Fri Apr 8 16:01
clear     user1   ttyp0    0.05 secs Fri Apr 8 16:01
rpcinfo   user1   ttyp0    0.20 secs Fri Apr 8 16:01
nroff     user2   ttyp2    0.75 secs Fri Apr 8 16:00
sh        user2   ttyp2    0.02 secs Fri Apr 8 16:00
mv        user2   ttyp2    0.02 secs Fri Apr 8 16:00
sh        user2   ttyp2    0.03 secs Fri Apr 8 16:00
col       user2   ttyp2    0.09 secs Fri Apr 8 16:00
man       user2   ttyp2    0.14 secs Fri Apr 8 15:57
```

(c) User log showing a chronological list of commands executed by users

Figure 18.4 Examples of Audit Trails

Protecting the audit trail

How is the audit trail stored?

- Read/write file on host
  - Easy, least resource intensive, instant access
  - Vulnerable to attack by intruder
- Write-once/read-many device (e.g. dedicated log server)
  - More secure but less convenient
  - Need steady supply of recordable media
  - Access may be delayed and not available immediately
- Must protect both integrity and confidentiality
  - Encryption, digital signatures, access controls

Windows Event Log

- Event is an entity that describes some interesting occurrence
  - Contains:
    - A numeric identification code
    - A set of attributes
    - Optional user-supplied data
- Three types of event logs:
  - System: system related apps and drivers
  - Application: user-level apps
  - Security: Windows LSA

Example log entry

```
Event Type:      Success Audit
Event Source:    Security
Event Category:  (1)
Event ID:        517
Date:            3/6/2006
Time:            2:56:40 PM
User:            NT AUTHORITY\SYSTEM
Computer:        KENT
Description:     The audit log was cleared
Primary User Name:   SYSTEM          Primary Domain:   NT AUTHORITY
Primary Logon ID:    (0x0,0x3F7)     Client User Name: userk
Client Domain:       KENT            Client Logon ID:  (0x0,0x28BFD)
```

UNIX Syslog

- UNIX's general-purpose logging mechanism
  - Found on all UNIX / Linux variants

Elements:

syslog()	logger	/etc/syslog.conf	syslogd
API referenced by several standard system utilities and available to application programs	Command used to add single-line entries to the system log	Configuration file used to control the logging and routing of system log events	Daemon to receive/route log events

Syslog service

- Basic syslog service provides:
  - A means of **capturing** relevant events
  - A **storage** facility
  - A protocol for **transmitting** syslog messages from other machines to a central machine that acts as a *syslog server*

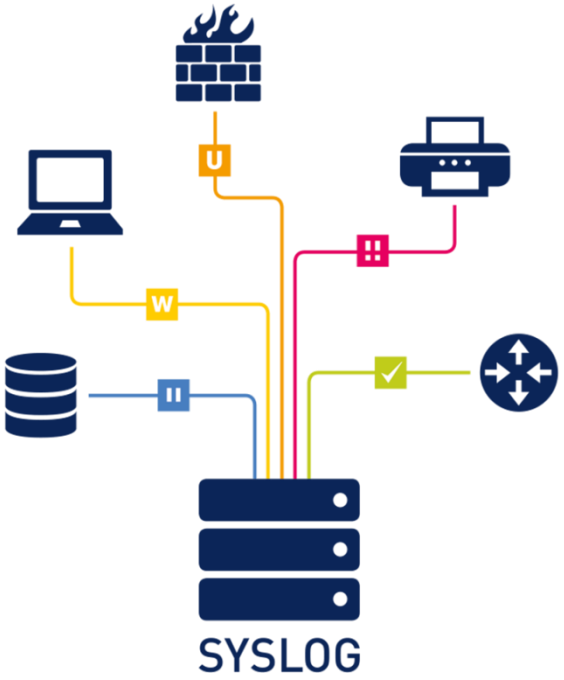


Figure from here.

Example log entry

```
Mar 1 06:25:43 server1 sshd[23170]: Accepted publickey for server2 from
172.30.128.115 port 21011 ssh2

Mar 1 07:16:42 server1 sshd[9326]: Accepted password for murugiah from
10.20.30.108 port 1070 ssh2

Mar 1 07:16:53 server1 sshd[22938]: reverse mapping checking getaddrinfo for
ip10.165.nist.gov failed - POSSIBLE BREAKIN ATTEMPT!

Mar 1 07:26:28 server1 sshd[22572]: Accepted publickey for server2 from
172.30.128.115 port 30606 ssh2

Mar 1 07:28:33 server1 su: BAD SU kkent to root on /dev/ttyp2

Mar 1 07:28:41 server1 su: kkent to root on /dev/ttyp2
```

Audit analysis

- So you have all this data...now what?
  Apply human brain to it. There's lots of ways to proceed...
  - Some examples...

Basic alerting

- Indicate interesting type of event has occurred

Baselining

- Define normal versus unusual events/patterns
- Compare with new data to detect changes
- Thresholding is the identification of data that exceed a particular baseline value

Windowing

- Detection of events within a given set of parameters

Correlation

- Seeks relationships among events

Audit conclusion

- Most common mistake: doing all of this, then taking no action because of it!
- End of audit should be a set of **concrete recommended actions**
- Should flow directly into project management for taking action

Legal Aspects

Based on chapter 19

Types of Computer Crime

- The U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity:

Computers as targets

Involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability

Computers as storage devices

Using the computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or pirated commercial software

Computers as communications tools

Crimes that are committed online, such as fraud, gambling, child pornography, and the illegal sale of prescription drugs, controlled substances, alcohol, or guns

Article 2 Illegal access
The access to the whole or any part of a computer system without right.

Article 3 Illegal interception
The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Article 4 Data interference
The damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 System interference
The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 Misuse of devices
- **a** The production, sale, procurement for use, import, distribution or otherwise making available of:
  - **i** A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
  - **ii** A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and
- **b** The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Article 7 Computer-related forgery
The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Article 8 Computer-related fraud
The causing of a loss of property to another person by:
- **a** Any input, alteration, deletion or suppression of computer data;
- **b** Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Table 19.1

Cybercrimes Cited in the Convention on Cybercrime

Table 19.1
Cybercrimes Cited in the Convention on Cybercrime (page 2 of 2)

Article 9 Offenses related to child pornography

a Producing child pornography for the purpose of its distribution through a computer system;
b Offering or making available child pornography through a computer system;
c Distributing or transmitting child pornography through a computer system;
d Procuring child pornography through a computer system for oneself or for another person;
e Possessing child pornography in a computer system or on a computer-data storage medium.

Article 10 Infringements of copyright and related rights

Article 11 Attempt and aiding or abetting

Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

Law enforcement challenges

- Law enforcement deterrent is based on probability of being caught/prosecuted. For computer crime, this number is...low.

- Challenges to law enforcement.
  - Law enforcement is usually behind the times (lack of knowledge/tools)
  - Criminals are probably out of jurisdiction (lack of global cooperation)
  - Suspects are diverse and difficult to profile
  - Cycle:
    1. Police have low success rate at solving cyber crime, so...
    2. Victims often don't bother reporting it, so...
    3. Police don't invest more in it, so #1

Key laws/agreements affecting computer security (Focused on United States)

- **Computer Fraud and Abuse Act**: "Prohibits accessing a computer without authorization, or in excess of authorization"[src]. 1984.
- **Digital Millennium Copyright Act**: Implements intellectual property treaties in U.S., allows copyright owners to use technology to protect works and prohibits bypasses of such measures. 1998.
  - Exemptions for: Fair use, reverse engineering, research, testing, and privacy
- **Convention on Cybercrime**: Broad agreement among western nations that cybercrime is bad. 2001.
- **PATRIOT Act**: Broadened surveillance abilities of government (affecting privacy); codified cyber-terrorism ("to cause a person to be injured, a threat to public health or safety, or damage to a governmental computer that is used as a tool to administer justice, national defense or national security"[src]). 2001.

European General Data Protection Regulation (GDPR)

- If you operate in Europe, you gotta do it. Requirements:
  1. **Explicit consent** is needed for any data collection, must explain how it's used
  2. Must collect **minimum data** needed for stated objectives
  3. People can **review** that data and make you **erase** it
  4. You're on the hook for **securing** it
  5. Violate any of the above, **pay a fine**

- Results:
  - Lots of scummy companies with loose practices suddenly having to straighten up or die ☺
  - Lots of "consent mining" (email and web requests asking you to click yes)
    - Most legit
    - Some done in a shady way...

Privacy

- Overlaps with computer security
- Dramatic increase in scale of information collected and stored
  - Motivated by law enforcement, national security, economic incentives
- Individuals have become increasingly aware of access and use of personal information and private details about their lives
- Concerns about extent of privacy compromise have led to a variety of legal and technical approaches to reinforcing privacy rights

Privacy and Data Surveillance

- Business, government, and law enforcement have created new threats to personal privacy
  - Scientific and medical research data collection for analysis
  - Law enforcement data surveillance
  - Private organizations profiling
  - Creates tension between enabling beneficial outcomes while respecting an individual's right to privacy
- Rapid rise in the use of public social media sites
  - They gather large amounts of data on individuals
  - People willingly upload large amounts of personal information
  - The data could be used by employers, insurance companies, private investigators, and others...

Ethical Aspects

Based on chapter 19

Ethics

- **Ethics**: A system of principles relating the benefits and harms of human actions so that their morality and the morality of their motivations can be assessed.
- Computers introduce new challenge:

  Those who understand technology and have access permission (or the ability to bypass such permission), have power to read and change information and affect undue change.

Definitions and wording adapted from textbook

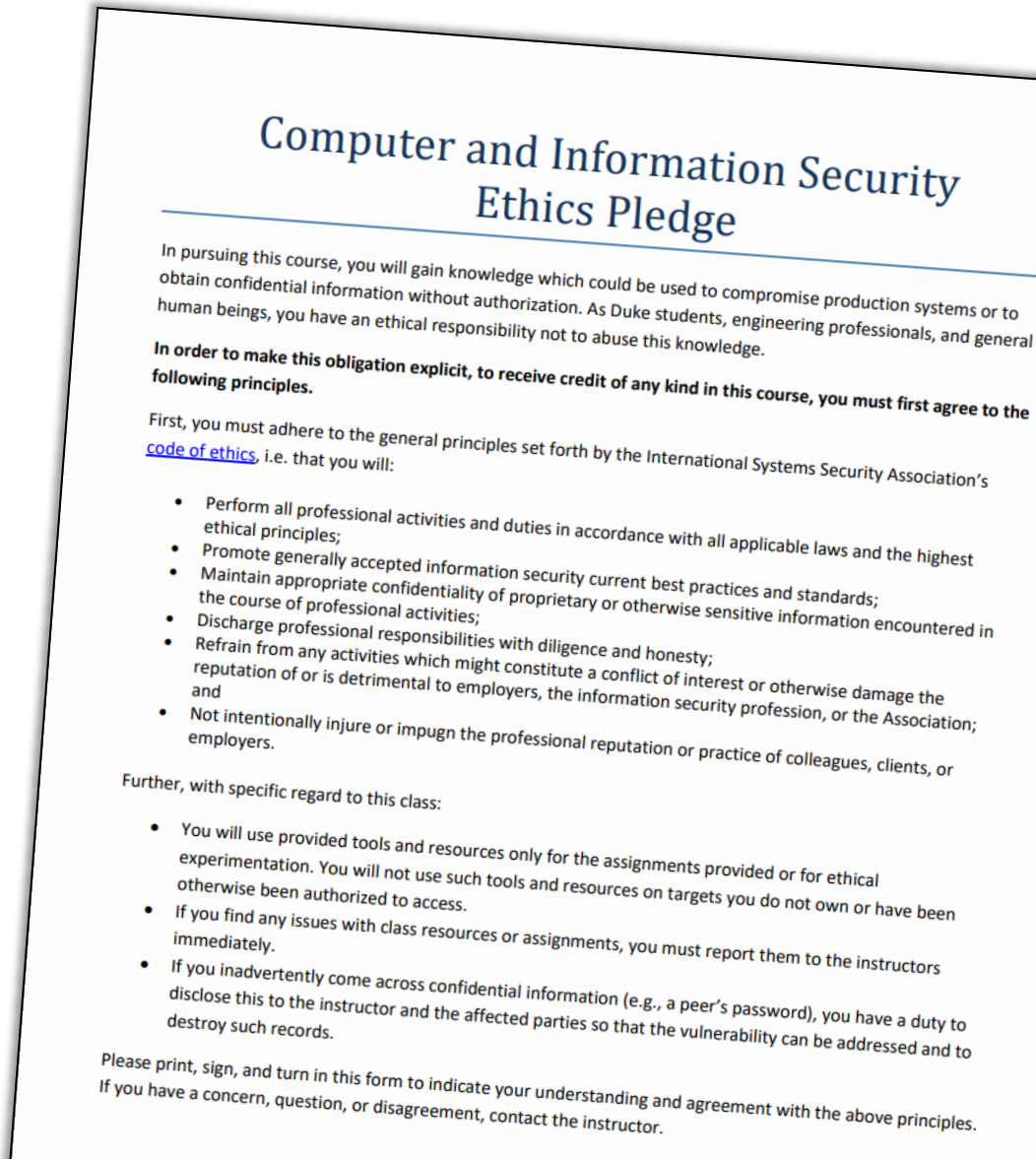
Real ethics are proactive

- Rare: An ethical dilemma where you have a clear choice to make.
  - "Trolley problem"
- Common: An unfolding situation where you can *elect* to take proactive action.
  - May not be in your personal best interest.
  - Examples:
    - Ethical duty conflicts with loyalty to employer, e.g., "blowing the whistle"
    - Expose a situation that can harm the public or a company's customers
    - Potential conflict of interest

- #1 source: **personal ethics**
- #2 source: professional ethics (can be guided by code of conduct)

Codes of conduct

- Can't solve all ethical questions, but can be useful
- Textbook compares three codes of conduct and finds common themes:
  - Dignity of other people
  - Personal integrity and honesty
  - Responsibility for work
  - Confidentiality of information
  - Public safety and health
  - Participation in professional societies to improve standards of the profession
  - Public knowledge and access to technology is equivalent to social power



Computer and Information Security Ethics Pledge

In pursuing this course, you will gain knowledge which could be used to compromise production systems or to obtain confidential information without authorization. As Duke students, engineering professionals, and general human beings, you have an ethical responsibility not to abuse this knowledge.

In order to make this obligation explicit, to receive credit of any kind in this course, you must first agree to the following principles.

First, you must adhere to the general principles set forth by the International Systems Security Association's code of ethics, i.e. that you will:

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Promote generally accepted information security current best practices and standards;
- Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;
- Discharge professional responsibilities with diligence and honesty;
- Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of or is detrimental to employers, the information security profession, or the Association; and
- Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers.

Further, with specific regard to this class:

- You will use provided tools and resources only for the assignments provided or for ethical experimentation. You will not use such tools and resources on targets you do not own or have been otherwise been authorized to access.
- If you find any issues with class resources or assignments, you must report them to the instructors immediately.
- If you inadvertently come across confidential information (e.g., a peer's password), you have a duty to disclose this to the instructor and the affected parties so that the vulnerability can be addressed and to destroy such records.

Please print, sign, and turn in this form to indicate your understanding and agreement with the above principles. If you have a concern, question, or disagreement, contact the instructor.

Conclusion

- One day you will be in a situation where:
  - **Inaction** is feasible, safe, and **wrong**
  - **Action** is difficult, risky, but **right.**

- Ethics is taking action.

Take action.