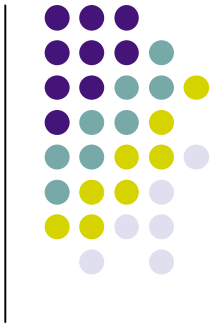
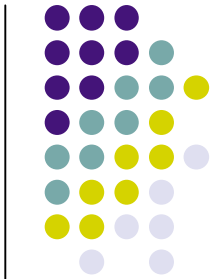


Intro to Info Security

CS 594 Special Topics/Kent Law School:

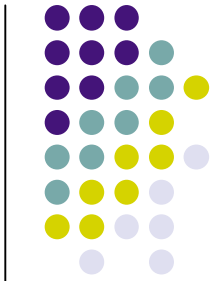
Computer and Network Privacy and Security: Ethical, Legal, and Technical Consideration

Security & Privacy



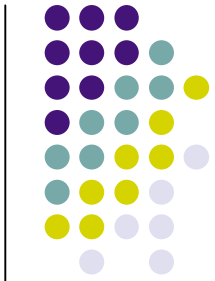
- Name of single most prestigious conference in area
- What we expect at home. Our issues there:
  - Burglars & c. MALICE
  - Natural Disaster MISCHANCE
  - Set house on fire cooking ERROR
  - Police visit GOVERNMENT
  - Unwanted Commercial Intrusion
- Grew up w/crypto; now related but distinct

Responses: Home design



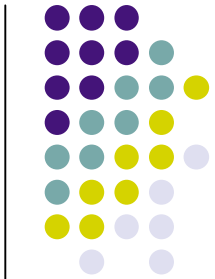
- Opaque walls
- Window coverings
- Locks
- Child-safe stove knobs
- *Many* special issues vis-à-vis government (4th Amendment)
- Some special issues vis-à-vis commercial speech (1st Amendment?)

Economic issues



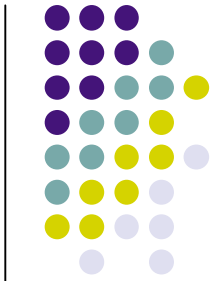
- Many security issues have economic tradeoffs:
- Almost always want medium-plus strength deadbolt lock on your doors
- Whether more expensive superb door lock depends on existence of 1st floor window locks, alarms, etc., *and* neighborhood

Special issues



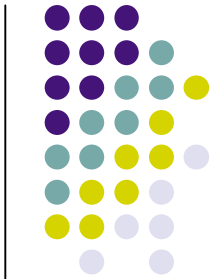
- Many domains have their own special security issues:
  - Banks
  - Military Base
    - Military Base with nukes
  - Hospitals
  - Installations w/classified materials

The two books



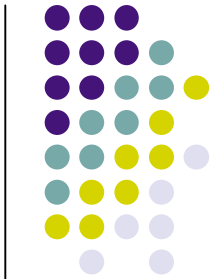
- *Security Illuminated:*
  - 30,000 foot view in Chapters 1–2.1; 3; 7.9
  - Smart bird's eye view: Prof. Venkat's CS 491 (to be renumbered to 487?)
- Anderson's *Security Engineering*
  - Overview in Chapter 1
  - Sundry management issues including risk management in 22.1–22.2, 22.5.

Security Overview



- Key players:
  - Organization: Entity whose security is being protected
  - Attackers: Entities *intentionally* trying to “get past” security
- Colors:
  - White hats: organization’s security guardians
  - Black hats: attackers
  - Red team: Simulated attack to test defenses.

What is security?



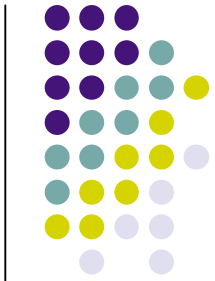
"A computer is secure if you can depend on it and its software to behave as you expect."

—Garfinkle and Spafford

Though a computer scientist probably wants to pull out *correctness* issues:

- Bugs in software
- Misbehavior by *trusted* individuals beyond what was contemplated. (I.e., untrustworthy trusted individuals)

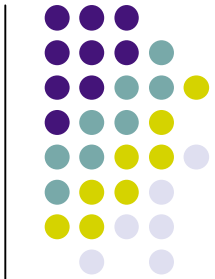
Key security concerns



1. People
2. Trust
3. Limiting Trust

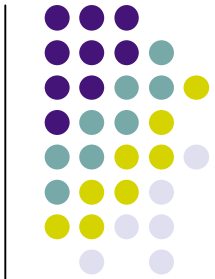
- Traditional names of parties; Alice, Bob, Charlie
- People are very complicated, hard/impossible to model:
  - What will Alice do?
  - How does Bob constrain Alice's behavior?

Three fundamental goals



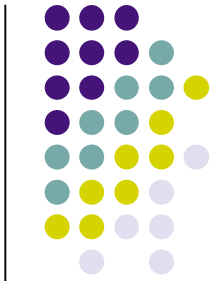
- **Confidentiality**—secrecy, control of information flow. *Preventing the unauthorized release of information*.
- **Integrity**—*Preventing the unauthorized alteration of information.*
- **Availability**—Keep system available for use. *Preventing denial of use to those authorized to use system.*
- Inverse: *Disclosure*, *Alteration* (by hacker or head crash), *Denial*

CIA Triad Examples



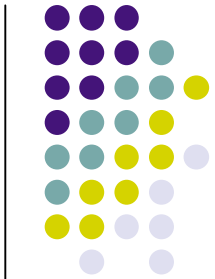
- My credit card: confidentiality—but not my photos
- My files: integrity for all; confidentiality for many
- Ability to append to class blog limited to those in the class
- System available 99.8% of time 6:30 a.m. eastern to 1:00 a.m. Pacific, and at least 70% rest of week, mean response time < 1 sec; 99% of responses < 5 sec.

Computer Security Policies



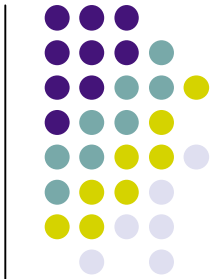
- Security policies are the *goals.*
- Independent of mechanism/implementation
- Intended to ensure sufficient confidentiality, integrity, and availability of organization's information assets.
- Those assets = information (data) + hardware (computers, networks)
- Protection mechanism/implementation and attacks vary by *system*

“System” is ambiguous



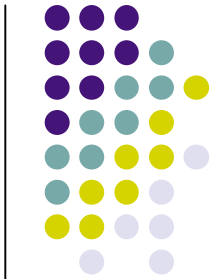
1. Single Component or product
   a) Stand-alone computer
      - Historically important; still a (the?) basic building block requiring high trustworthiness
   b) Any other single component or product
      - E.g., smart card *or* a cryptographic protocol
2. Networked computers
   a) where one still knows all entities & connections
      - Organization’s LAN
   b) **Distributed systems**: ≥2 entities with widely varying levels of trust

System today also. . . .



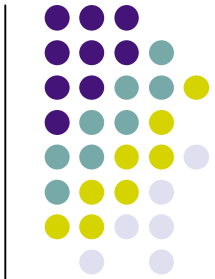
- IT staff, internal users (staff, management), external users (public)
- Then Broad environment:
  - Media, regulators, politicians
  - Competitors
  - Malicious teens from Romania
  - Malicious profit-driven mobsters based in Russia
  - . . .

Overall Goals: Avoid



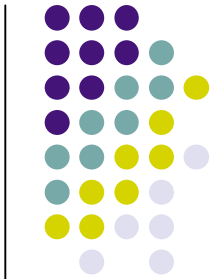
- **Vulnerability:** System property—weakness.
  - E.g., Windows Machine w/no antivirus software.
- **Threat:** External (or malicious insider?) that might allow a vulnerability to be exploited.
  - E.g., any given virus.
- **Vulnerability + Threat = RISK**
- **Risk** = potential; **Security failure** = actual violation of security policy

Risk Analysis



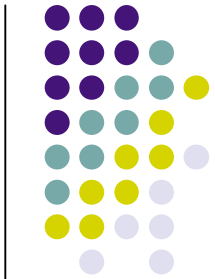
- Large, somewhat specialized area, whose value some question.
- Do need Kindergarten version in back of mind:
  1. Identify & Value Assets
  2. Identify Risks
     - Then assess risks' probability, frequency
  3. Decide what to do—risk management

Risk management & analysis (cont.)



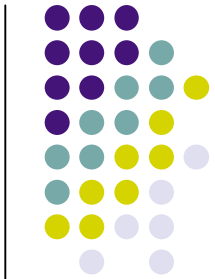
- Risk analysis is general purpose; occurs elsewhere in software engineering (Therac-25), Transportation (Hindenburg), etc.
- Risk management should be done for organization as a whole
- Typically calculate **Annualized Loss Expectancy**
  - Using WAG for amount & frequency of loss, especially for very rare very big loss

Most common threats in Information Security



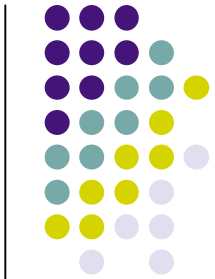
1. Hackers/crackers/malicious outsiders
2. Malware/malicious *code* objects
3. **Malicious insiders**

Reminder: Security = Tradeoffs



- Security is never absolute, and security costs money
- Goal is enough security that
  - Cost-benefit ratio makes sense
  - Always achieved once info sec is no longer the weakest link

Players in Security



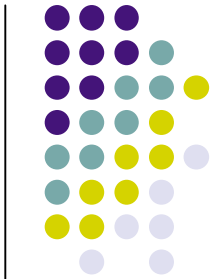
Much of literature speaks blithely of "subjects," the active entities.

But 2 sets of thorny issues re exactly what subject is.

First, is Alice the human I trust, or a logon session of Alice, or a process of Alice?

Rich source of subtle bugs

Anderson list of players



Subject = Physical person

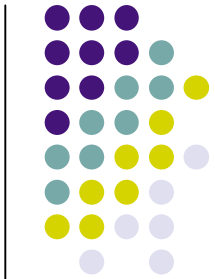
Person = Physical or legal (i.e., company/corp)

Principal = Any one entity

Group = Set of principals

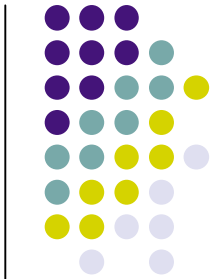
Role = Function assumed by 1 or more persons

General-purpose security: the 3 pieces



1. Physical security—Limiting (or preventing) physical access to computer hardware
2. Administrative or Personnel Security—Vetting at hiring, role change. Also training, user monitoring. Key issue: How do you decide whom to trust, and how much? Sufficiently serious position: oaths, investigations, lie detectors, references, credit reports. . . .

3rd Component: Technical

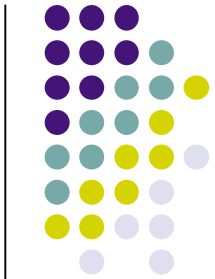


3. Logical or Technical or Procedural controls. Typically implemented via software/OS, and main thing that most computer scientists think about as security.

E.g., User ID and authentication, crypto.

Based on organization's rules and/or laws, professional standards.

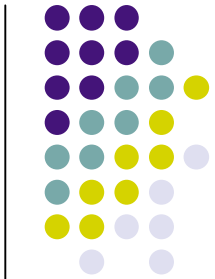
A Very Delicate Balance



If technical security is too onerous, it will be bypassed.

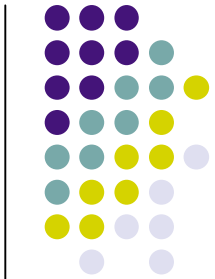
If technical security is too lax, it will be ineffective.

Goals of technical security



- Prevent certain types of attacks
- Detect security breaches
- Stop further occurrences
- Identify the bad guy(s)
- Punish the bad guy(s)

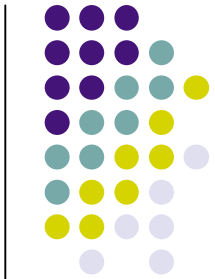
Some general Principles



Defense in depth: The physical security of a high-value destination, e.g., military installation with nukes will have, e.g.:

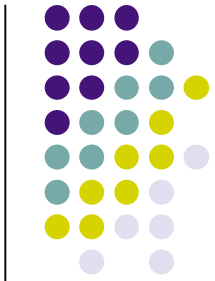
- Fences
- Alarms
- Locks
- Armed Guards

Other key principles



- Separation of duties/privileges
- Least privilege

Examples of attacks



- Stand-alone: Buffer overflow, authentication attacks
- Networked: Injecting bogus packets, reading packets not intended for the node
- Distributed System: Distributed Denial of Service (DDoS)