1.264 Lecture 25

Security basics

Next class: Anderson chapter 3. Exercise due after class

Case study: Public transport fare collection

- Cash/token transit fare collection
  - What is core security feature of transit system fare collection system?
  - What are internal risks?
  - What are passenger risks?
  - What are risks in getting funds to bank?
- Smartcard transit fare collection
  - What is core security feature of transit system fare collection system?
  - What are internal risks?
  - What are passenger risks?
  - What are risks in getting funds to bank?

Security engineering

- So far, we’ve covered requirements, UML, business rules, data models, databases, Web
  - Focus on correctness, completeness, consistency
  - These are important for security too: a buggy system is an insecure system
    - If it doesn’t do what it’s supposed to do correctly, it won’t handle other things correctly either
- Security engineering focuses on guarding against malice, and against errors that can be exploited
  - Malice is the key additional factor for security
- These lectures are just an introduction to security
  - We cover basic principles and core issues/examples

Definitions of system

- System:
  1. Product or component: protocol, smartcard, computer
  2. Collection of products, plus operating system and its communications
  3. Collection of above, plus application software
  4. Any of above, plus IT staff
  5. Any of above, plus users and management
  6. Any of above, plus customers and external users
  7. Any of above, plus environment: competitors, regulators

– Security vendors, security evaluators focus on 1, 2

– Businesses focus on 5, 6, as does Anderson, and so do we

Definitions of actors

- Person: physical person, company or government
  - Security definitions relate to legal definitions
- Role: function assumed by different persons in succession
  - E.g., your database administrator
- Principal: entity that participates in security system
  - Can be person, role, communications channel or other component, including an attacker
- Identity: names of two principals that are the same person or component
  - E.g., a user and his or her username/password, or his or her iris scan or fingerprint

Exercise

- In accessing your apartment or home, define:
  - Person
  - Role
  - Principal
  - Identity

Solution

- In accessing your apartment or home, define:
  - Person:
    - George, Katie (occupants)
    - Cambridge Savings Bank (mortgage holder)
    - Various plumbers, electricians, cat sitters, etc.
  - Role:
    - Occupant, owner, building management
  - Principal
    - Occupant, landlord/owner, building management
    - Lock, keys, alarm
    - Burglar, George, Katie, …
  - Identity
    - Katie, George, Katie's key, George's key, alarm code
      - Burglar can adopt our identity if we lose our key
    - Jessica (cat sitter), our house key

Definitions of trust and secrecy

- Trusted system: one whose failure will break security policy
  - E.g., your building access system
- Trustworthy system: one that will not fail
  - E.g., a well administered, technically correct access system
- Secrecy: mechanisms to limit principals who can access information
  - Confidentiality: obligation to protect other person’s secrets
    - Secrecy for the benefit of the organization (strategic plans)
  - Privacy: ability/right to protect your personal secrets
    - Secrecy for the benefit of the individual(bank account number)
- Anonymity:
  - Message content confidentiality
  - Message source or destination confidentiality
- Authenticity:
  - Participation of genuine principal, not a copy or a fake

Trust and identity example: certificates

- Consumer user identity in certificates is email address (e.g., your MIT certificate)
  - Actual identity for users is most often established using credit card number or account number
- Company identity based on domain name/URL
  - Trading partner trust is not based on encryption, certificates, etc. but on knowledge of each other from face-to-face business dealings
- Computer security is only one element, though crucial, part of trust and identity
  - Global computer-based trust and identity seems impossible: no centrally trusted organization

Premises for Internet security

- Client-network-server are the 3 key components
- Client (browser or application) premises
  - Remote server is operated by organization stated (identity)
  - Documents returned by server are free from viruses (trustworthy)
  - Remote server will not distribute user's private info, such as identity, financial, Web use… (secrecy/privacy)
- Network premises (for both client and server)
  - Network is free from third party eavesdroppers (secrecy)
  - Network delivers information intact, not tampered with by third parties (secrecy, trustworthy)
- Server premises
  - User will not attempt to break into or alter contents of Web site or database (secrecy/confidentiality)
  - User will not try to gain access to documents or data that he/she is not allowed (secrecy/confidentiality)
  - User will not try to crash the server or deny service to others
  - If user has identified him/herself, user is who he/she claims to be (identity)

Client risks

- Infection and hijacking (botnet, spam server)
  - Malware, viruses, trojans, worms, etc.
  - Zero day vulnerabilities
  - Social engineering to visit Web pages, respond to email
  - Short term solutions are virus checkers, education
  - Long term solution is cloud w/few apps on client?
- Privacy loss
  - Cookies. Abused to track user habits
  - Email. Spam. (What % of email is spam?)
  - Short term solution is email verification (IP addresses)
- Identity loss (phishing, other attacks)
  - Confidential information sent to unauthorized party
  - Solution: education, IP improvements, certificates…

Server risks

- Web site break-in
  - Database theft is usual objective
  - Operating system, basic apps fairly secure
  - Solutions are primarily database protection
- Systems compromise
  - Insiders (what % of attacks are inside jobs?)
- We seem to be losing the battle
  - Millions of credit cards disclosed annually
  - Tailored worms/trojans steal from business and consumer accounts
  - 75% of corporations report significant breaches
  - Virus checker/intrusion detection don’t prevent sophisticated attacks
  - Look at www.threatexpert.com for some statistics

Network risks

- Denial of service
  - Attacks that cause system to expend large resources in response
  - Distributed denial of service attacks
  - Solutions are distributed filters, identification of attacking servers, changes in Internet protocols to limit spoofing in open Internet
    - And use of private networks under Internet protocols
- Packet sniffers
  - Look for unsecured servers, ports to attack. Mostly small/medium businesses
  - Cracking encryption is rare; there are easier holes to exploit, usually