Network Security

Module 13

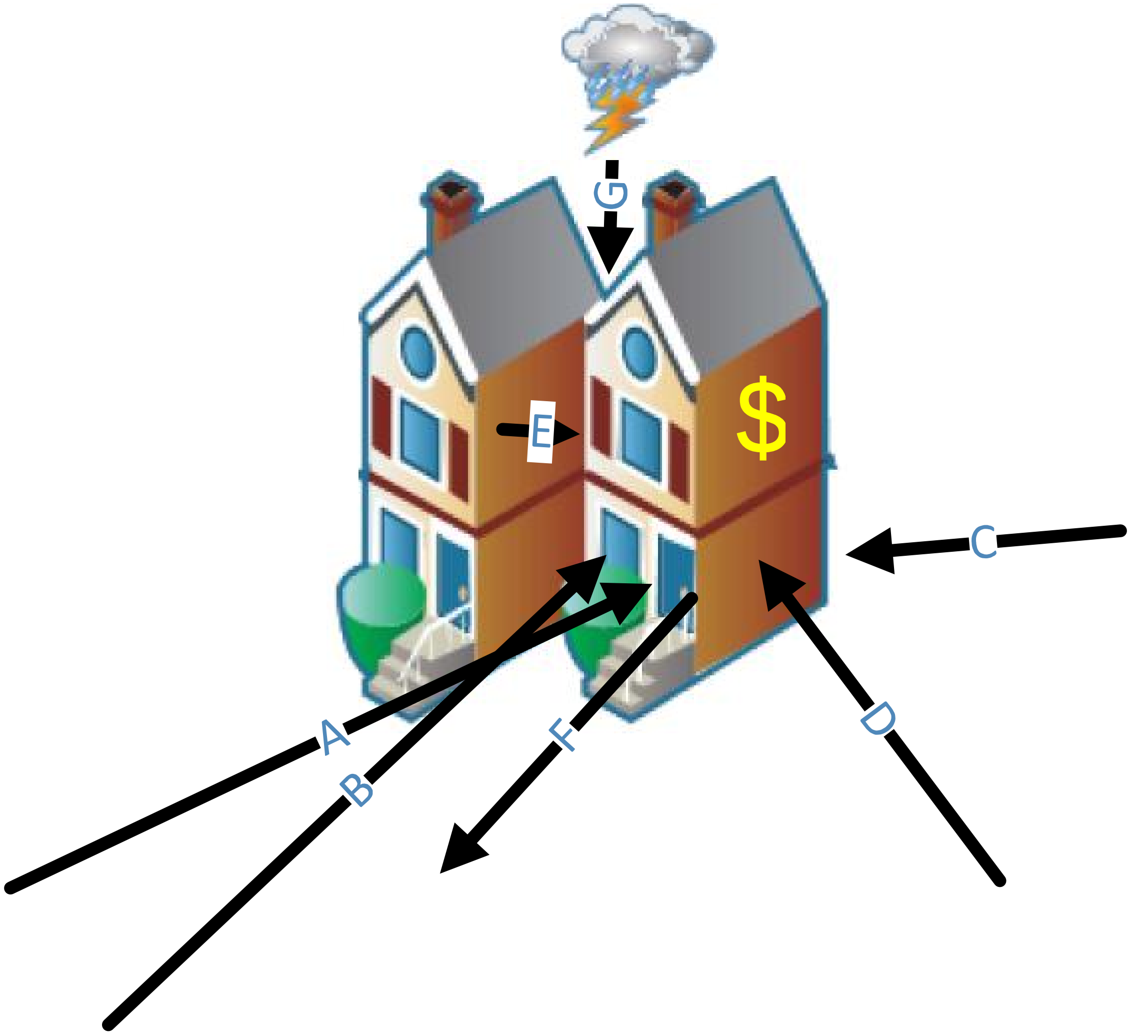
Defense in Depth

- Multiple overlapping mechanisms separate a valued resource from relevant threats
  – Mechanisms need not be all:
    - Technical (e.g. policies, procedures)
    - Preventative (e.g. monitoring, response)
    - Network oriented (e.g. OS policy, application authentication, patch management)

Defense in Depth

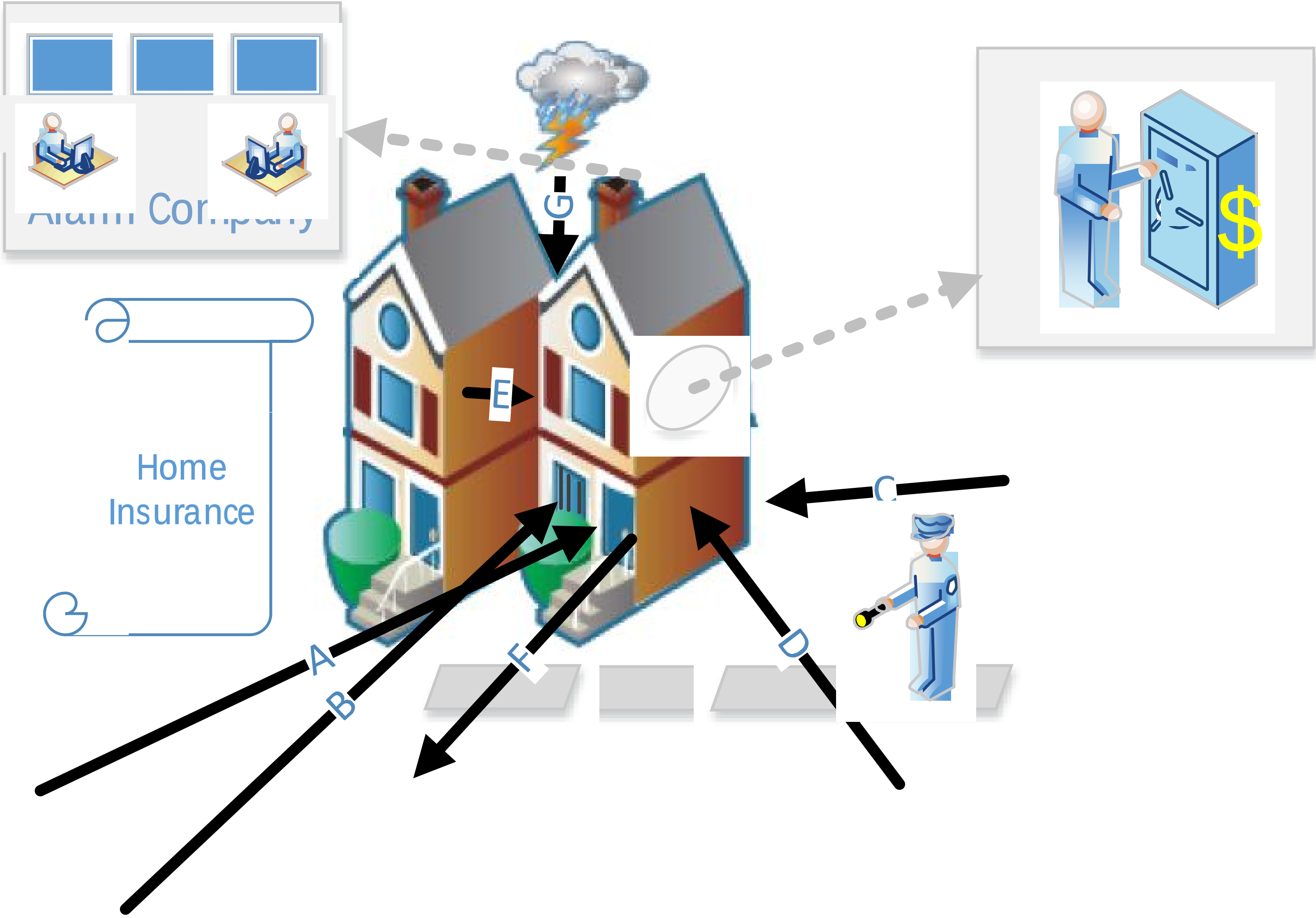
- In essence, it is a principle of defense diversity
  - Not relying on a single mechanism to protect what is valuable
- This approach guards against:
  - Loss of adequate protection due to mechanism maintenance, mechanism failure and an unexpected threat origin

Adversarial View



Copyright 2013 Iowa State University

Defensive In Depth



Copyright 2013 Iowa State University

Perimeter

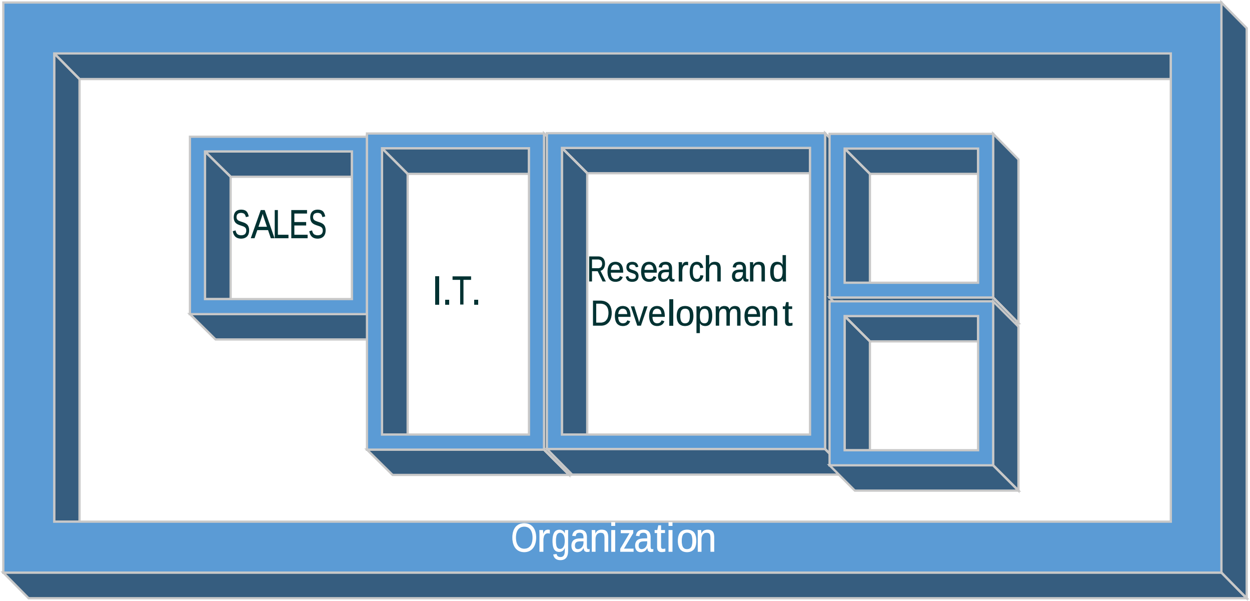
- The boundary between what is being protected and the likely source of threats.
  - Commonly associated with property lines or physical dimensions of a facility
    - Examples: Office building, manufacturing complex, military installation
- Although many cyber threats originate from the Internet, a good number do not.
  - An inside attack may eventually use the Internet after some level of success.

Perimeter

- Inside threats successfully breach the exterior perimeter
- Sources of inside threats:
  - Employees and Contractors
  - Visitors
  - Compromised portable devices
  - Poor worker security awareness and training
    - Victim of phishing
    - Drive by download

Perimeter

- Compartmenting resources (e.g. tools, technology and information) creates perimeters within the interior



Copyright 2013 Iowa State University

Perimeters

- Logically perimeters are the result of one or more controls maintaining confidentiality, integrity and availability of one or more resources (e.g. processes, people, information, systems).
- As the threat sources become more pervasive, so will the establishment of perimeters

Firewalls

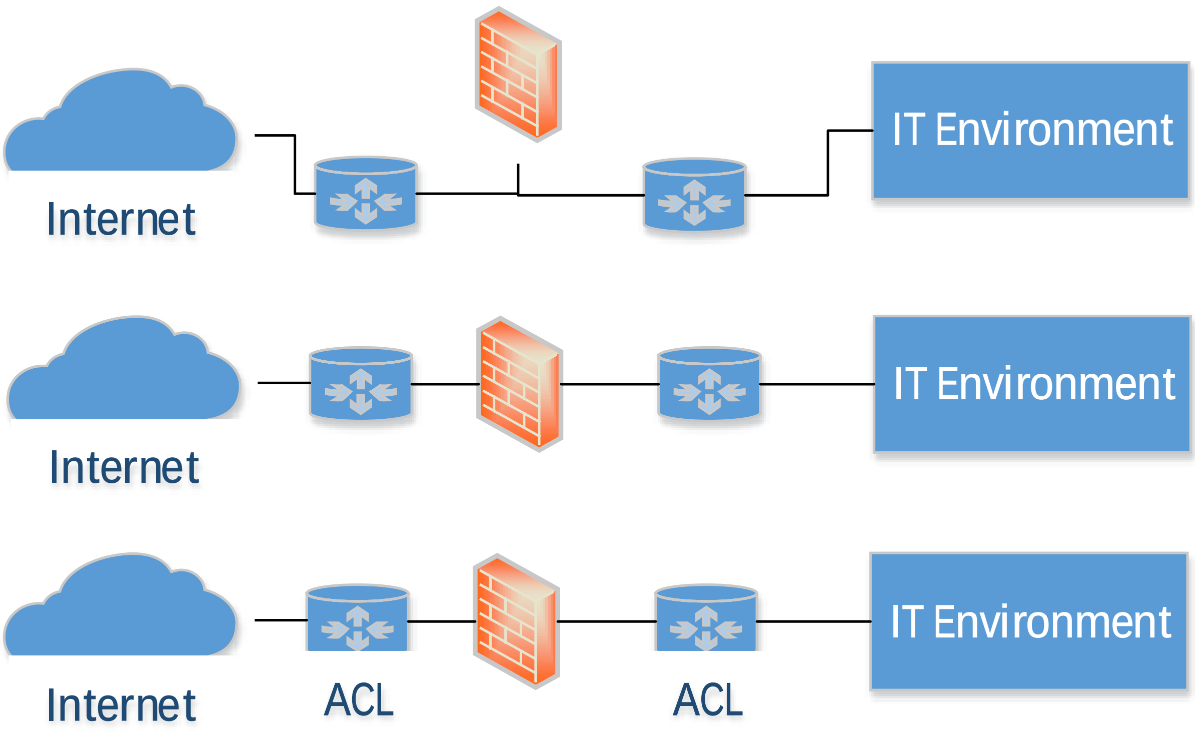
- Information flow is needed between parties even though:
  - The parties may not be fully trusted
  - The method of communication is not trusted
    - Example: Internet
- Firewalls are intended to limit exposure
  - Control which parties may communicate across it
  - Control the type of communication flowing through it

Firewalls

- Firewalls Product Types
  - – Dedicated devices
  - – Multi-function security devices
    - Unified Threat Management – AV, FW, IDS, etc.
  - – Software application running on generic computer
  - – Routers with access control enforcement

Firewalls

- Some deployment configurations



Internet — IT Environment — Single Homed Firewall

Internet — IT Environment — Dual Homed Firewall

Internet — ACL — ACL — IT Environment — Screened Subnet Firewall

Firewalls

- Firewall logical types
  - Based on what layers of the protocol stack the policy enforcement takes place
  - Layer 3 – IP Networking Layer
    - Enforces rules regarding IP addressing and IP protocol parameters
    - Commonly enhanced to be "stateful"
      - TCP protocol is stateful and many firewalls of this type are aware of the beginning, end and middle of a TCP connection

Firewalls

- Layer 5 (TCP/IP model) or Layer 7 (OSI model) – Application Layer
  - Logic ensures protocol (e.g. HTTP, FTP, SMTP) is being used properly
  - Logic is able to restrict protocol options
  - Logic is able to inspect more of the application payload
  - A common implementation method is through proxies

Intrusion Detection & Prevention

- Firewalls permit a restricted flow of traffic
  - Traffic that does flow may have malicious intent
- Intrusion detection systems (IDS) inspect traffic looking for suspicious behavior
- Originally this technology was meant to be a detection not a prevention technology

Intrusion Detection & Prevention

- Suspicious traffic is determined by:
  - Signatures or patterns of known suspicious behavior
    - A new threat may not be detected
  - Anomalies within traffic
    - Anomalies may not be malicious, so related alerts may not be useful
- Intrusion Prevention System (IPS)
  - Stop suspicious traffic using mentioned detection techniques
    - Instruct firewall to change policy
    - Block traffic at the IPS device

IDS and CDC

- Cyber Defense Competitions have by design an abnormally high rate of threats.
  - You know you are under attack
  - It may help identify the type of attack, but it may not!

Netflow

- What is it?
  - A proprietary protocol designed by Cisco
  - Multiple variants exist, such as: sFlow, NetStream, IPFIX, J-Flow
  - Network activity recording technique
    - Record is an “IP flow”
      - Concept is not native to IP protocol definition
    - For Cisco, a unique “IP flow” is designated based on 5 to 7 packet attributes

Netflow

- Cisco’s selected attributes are:
  - IP Source Address
  - IP Destination Address
  - Source Port (Transport protocol)
  - Destination Port (Transport protocol)
  - Layer 3 protocol type (e.g. ICMP,TCP,UDP,OSPF)
  - Class of Service
  - Router or switch interface

Netflow

- A new record is opened for each unique combination
  - A timer is set for each record
    - If a new packet arrives matching an existing attribute combination the counters for packet count and number of bytes transferred are updated for the “IP Flow”
    - Timer is reset
    - If timer expires, the “IP Flow” is considered terminated
  - TCP SYN and TCP FIN, RST help designate the begin and end of a TCP connection

Netflow

- Additional information recorded in each “IP Flow” record
  - Timestamps
  - Next hop address
  - Subnet mask of source and destination addresses
  - TCP flags

Netflow

- Uses:
  - Application and network usage
  - Impact analysis of network changes
  - Unusual network activity patterns and network threat tracking
  - Network productivity and utilization

Netflow in the Playground

- Netflow support is greatest among network devices, which can not be virtualized
- Pfsense, FreeBSD and OpenBSD are platforms that support Netflow
- As of vSphere 5, VMWare supports Netflow on virtual switches.
  - Requires additional licensing, not available

Netflow

- Configuration
  - Need to establish a Netflow collector
    - Receives exported Netflow records
    - Loads records in a database
  - A reporting and/or monitoring tool
    - Dynamic views of Netflow require a monitoring tool
      - Tool retrieves updates from collector
      - Renders information in various visual formats

Malware Defenses

- Primary vector of malware is the network
  - Worms
  - User web browsing
  - Email
  - File transfers
- Physical transfer of malware still occurs
  - Infected USB thumb drive
  - Infected portable computing device attaching to network

Malware Defenses

- Methods of Detection:
  - Signatures – content of a file is compared to a list to determine if the file is present on a list of known threats
  - Heuristics – a “generic” signature that is able to identify multiple variations of malware that have characteristics in common
  - Isolated testing – suspected file is executed in an isolated and instrumented environment to determine its nature

Malware Defenses

- Firewalls, Patch Management, Configuration Management, Security Awareness
  - Limit exposure to vulnerabilities that malware exploits
- Defense in Depth
  - Anti-virus engine at the perimeter
  - Anti-virus engine on email servers
  - Anti-virus engine on file servers
  - Anti-virus engine on endpoints (PCs, tablets, smartphones)

Malware Defenses

- Signature Updates
  - Anti-virus is not effective if signatures are not maintained by organization or vendor
  - Enterprise anti-virus products provide centralized monitoring and control
    - It can be determined which hosts are not current
    - It is possible to push signatures and initiate AV scans
      - AV is a useful tool to corroborate or confirm indications of possible infection on a host

Malware Defenses

- Weakness of AV:
  - Relies heavily on vendors having a sample to analyze
  - Can be disabled or rendered ineffective if host compromise is severe
    - Malware with access to the kernel can block detection
    - Solution is to reboot host with a clean OS and scan the hard drive contents.
      - Disruptive and labor intensive

Malware Defenses

- Vendor Diversity
  - Not knowing the delay a vendor may have in preparing and distributing signatures to the newest threats
  - Deploy different vendor for:
    - Malware that is missed by one engine type will be caught by the next type.
    - Perimeter protection
    - Email server protection
    - File server protection
    - Endpoint protection

Malware Defense

- Downsides to Vendor Diversity
  - Costs
    - Licensing tends to be volume oriented
      - Fewer licenses bought results in higher per license costs
    - Labor efficiency
      - More products to manage separately
        - » Unified management interface is unlikely
      - More products to train on
- Uncertain security benefit in the long run
- Multiple engines on one host may not function and will consume more CPU time and generate more I/O

Public Key Infrastructure

- Certificates
  - The binding of public key to an identity
    - Service
    - Person
    - Organization
  - Trust in the binding is necessary
    - You want to know with whom or what you are sharing sensitive information
    - Public keys are distributed to strangers by strangers

Public Key Infrastructure

- Asymmetric or public key cryptography provides the literal security services of:
  - Encrypting/decrypting information
  - Integrity
- These basic services can be extended to provide:
  - Authentication
  - Non-repudiation

Public Key Infrastructure

- Encrypting sensitive information for use by another is great so long they were the recipient you intended
- Authentication relies on at least one factor
  - Private key could be either “what you have” or “what you know” (you have good memory)
  - But whose key is it really?
    - Are we letting in a stranger?
- Non-repudiation relies on involved parties not being able to wiggle out of something they did or said
  - Did we accept a digital signature from the wrong person?
    - Could a party legitimately claim that the digital signature was not theirs?

Public Key Infrastructure

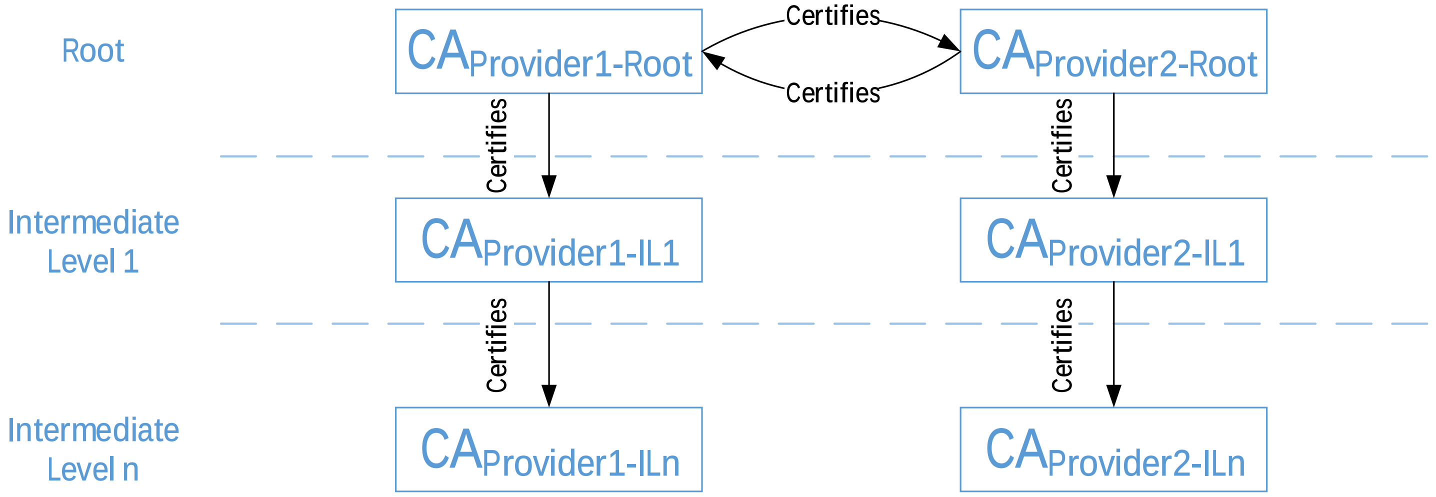
- Those issues are the reason for certificates
- But, who do we trust to bind public keys to identities?
  - Anybody?
    - Do they know what they are doing?
    - Are they who they say they are?
      - I, Frank, certify that public key DAF23D is Sally's
      - Who is Frank? Do you know and trust him?

Public Key Infrastructure

- Certificate Authority (CA)
  - – An entity that issues, distributes, verifies and manages certificates
    - Certificate lifecycle – issuance, use, expiration
      - – Revocation may be necessary if public-private key pair is compromised or control of it was lost
  - – Has the necessary technology, people and procedures to perform certificate services, users can trust

Public Key Infrastructure

- Certificate authorities can issue certificates for other CAs
  - Users do not trust CA_1 but trust CA_2
    - User may trust CA_1 if and only if CA_2 trusts CA_1
- CAs can be deployed in a hierarchical fashion



Public Key Infrastructure

- Registration Authority (RA)
  - Performs a subset of CA services
    - Verifies the identity of the entity requesting a certificate
    - Acts a liaison between entity requesting a certificate and the CA
    - Could assist an entity by accepting requests to revoke an issued certificate

Public Key Infrastructure

- Self-Signed Certificates
  - Certificate is issued by the person or organization that generated the key pair
    - CA’s certificate needs to be added trusted list used by applications like a web browser to avoid warnings and mistaken trust
- Commercial Certificates
  - Certificate is issued by a CA that is recognized
    - Typically application developers provide an initial list of “root certificates”