PA197 Secure Network Design
5. Security Architectures III

Eva Hladká, Luděk Matyska

Faculty of Informatics

March 17, 2020

Content

Resilience

- What is resilience?
  - *Resilience is the capacity to adapt to changing conditions and to maintain or regain functionality and vitality in the face of stress or disturbance. It is the capacity to bounce back after a disturbance or interruption.*
    - cited from `http://www.resilientdesign.org/what-is-resilience/`
    - *survivability* often used as an alternate term
- Design principles:
  - scale
  - diversity and redundancy
  - simplicity and flexibility
  - interruption and dynamism anticipation
- Resilience is not absolute

Scale

- Must be applicable to different physical scales (sizes)
  - local, regional or wide area networks
  - a floor, building, or a city
  - country-wide and international
  - DoS (single point) and DDoS (multi-point) attack
- Different time scales
  - fast reaction on an immediate threat
  - long-term sustainability to an extensive (long term) attack
  - incremental erosion (of security)

Diversity and redundancy

- Basic design principle
- Redundancy: way how to "bypass" faulty component
  - one-to-one
    - dual power supply
    - two (more) lines between the same points
  - alternative
    - a different route using different active elements and lines
- Perfect vs. degraded
  - not all functions (or full performance) may be available, but the system as a whole still functions (survives)
    - lower throughput backup line
- Diversity complicates an attack
  - a security hole in one system may not exist in the other

Simplicity and flexibility

- Simplicity as a design principle
  - more easy to analyze and verify
  - more easy to manage
    - more difficult to put a back door unnoticed
  - easy to recover in case of failure
- Flexibility to adapt
  - it's not sufficient to have redundant components, system must be able to recognize a failure and react appropriately

Anticipation

- Anticipates threats and failures
  - the most common mistake: this system cannot crash
- Expects problems and prepares to resolve (mitigate) them
- Interruptions of service
  - behaviour of the system in a presence of a failure
- System dynamism
  - high activity periods
  - regular maintenance tasks (e.g. backups)

ResiliNets Architecture

- An initiative of several US, Australian and EU institutions and companies
- See `https://wiki.ittc.ku.edu/resilinets/Main_Page`
- Resilience Axiom: IUER
  - Inevitability of faults
  - Understand normal operations
  - Expect adverse events
  - Respond to adverse events and conditions

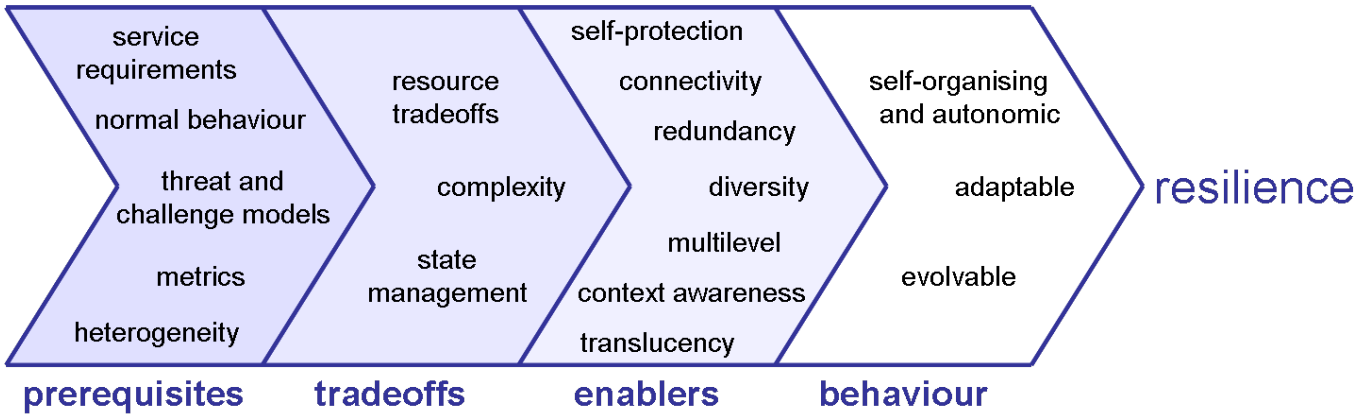
Resilience Strategy

- $D^2R^2 + DR$

  Real-time loop:
  - Defend against challenges and threats to normal operations
  - Detect when an adverse event or condition has occurred
  - Remediate the effects of the adverse events or conditions to minimise the impact
  - Recover to original and normal operations

  Background loop:
  - Diagnose the faults that was the root cause
  - Refine future behaviour

Resilience Principles



Defense mechanisms

- What can we do with the current network architecture?
- Perimeter and internal defenses
  - Perimeter defenses: firewall, IDS
    - create a perimeter
    - protect local area network keeping external threats outside
  - Internal defenses: monitoring
    - virus scanning
    - normal and unexpected traffic/behaviour
  - Perimeter extension: DMZ and VPN
- Access and connectivity protection

Perimeter defenses

- Network conceptually split to two parts:
  - internal, considered secure ("being at home")
  - external, considered insecure
- Defenses on the edge between these two regions
  - nothing malicious will pass inside
  - nothing private will come out
- Analogy with a house ("my home my castle")
- Tools
  - firewalls—inspect/stop traffic passing through the edge
  - intrusion detection systems (IDS)—monitor network traffic within the internal perimeter

Perimeter extensions

- Problem with legitimate external (remote) access to systems within the perimeter
- Demilitarized zone (DMZ)
  - a "middle" layer
  - systems to be accessible remotely put into a specific region (zone) under specific surveillance
  - analogy of "presence chamber"
- Not covering all situations
  - just one system inside
  - remote access to all internal systems (e.g. for remote management)
- Virtual private network (VPN) as a secure lane to internal region
  - a single machine access
  - connecting two perimeter defended regions (creating a virtual one)

Internal defenses

- Admit that malicious "code" could get inside
  - do not assume absolute security within the defense perimeter
- Continuously monitor what is happening
  - network traffic
  - elements (active network elements, computers, . . .) inside the perimeter

Access and connectivity protection

- Network Access Protection
  - Microsoft technology
    - Network Policy and Access Services (NPAS)
  - access to the network is based on system health of the host computer
  - policy based: Network Policy Server (NPS) and Health registration authority (HRA)
  - checks the "health" of the host and authorization decision based also on the health status
    - updates
    - operation system version
    - specific features/add ons (presence, absence, ...)
- Connectivity protection for optical networks
  - SONET protocol and fast handover
    - automated protections switching schemes
  - subnetwork connection protection (SNCP) in synchronous digital hierarchy (SDH) networks

IP and NAT takeover

- A specific IP address a single point of failure
  - need a mechanism to take over the assigned IP by a backup system
- Shared link layer (shared LAN segment)
  - using broadcast nature
  - a backup "follows" the primary
  - if it fails, the backup advertises the same IP
    - a time penalty for ARP cache flush
- NAT takeover
  - load balancing
  - resilience through hiding the end-element IP

Floating IP Address

- IP address floats between instances
  - ARP requests served by a specific element
  - no permanent (fixed) assignment of IP address
- High availability or mobile environments
  - NAT support
  - smooth transition between interfaces
- Extensively used for dynamic address association with virtual machine instances

Connectivity overlay

- The goal: to use the overlay network to keep/restore connectivity
- Self-healing principle
  - react to link/node failure
  - re-establish as much connectivity as possible
- Internet routing protocols are self-healing
  - able to find new route in case of failure
  - redundancy essential

Connectivity overlay

- Resilient Overlay Network (RON) already discussed
  - usually smaller overlay networks (tens of nodes)
- Unstructured peer to peer networks
  - potentially much larger networks
  - concept of nodes with direct neighbours
    - followed by layers of 2nd, 3rd, . . . neighbours
  - keeps the number of direct neighbours constant
    - or within an interval
  - self-healing mechanism to reconstruct lost direct neighbours

Privacy

- Users don't want to be tracked through the network
- Technical and legal/organizational aspects
  - legal protection in old telecommunication (line phone) networks
    - a criminal offense to wiretap (without a warrant)
    - technically supported by limited access to the physical lines and low access to the necessary technology
  - telnet protocol
    - insecure transmission of login credentials over the network
    - protection through legal framework (telnet over phone lines)
- Network administration needs to track users
  - at least to some extent
- And the enforcement needs data, too
- A proper balance needed between privacy enhancements and operational and legal monitoring requirements

Isolation

- Segmenting network to security zones
- Physical isolation
  - use of separate cables/end stations
  - expensive, not always possible
  - multi-homed end-stations could compromise the design
- Virtual isolation
  - virtual networks (VLAN/PVLAN)
- Provides privacy through separate paths

Network Virtualization

- Logically isolated network partitions
  - sharing the same physical infrastructure
- Each behaves as a separate independent network
  - independent set of policies
- Path isolation
  - independent logical traffic paths
- Unencrypted payload does not guarantee privacy
  - "sniffer" can read packets
  - physical security of network important

Anonymization

- Protects identity/data association
  - hides who is doing what
  - through group of identities
- Benefits
  - Internet censorship
  - freedom of speech
    - whistleblowers, journalists, dissidents, ...
  - privacy protection
    - financial and medical records
    - marketers
- Threats (malicious use)
  - (cyber)attacks
  - money laundering
- Anonymous mailers, routing

The Onion Router (TOR)

- Provides low latency anonymous Internet connections
  - `http://www.torproject.org`
  - clients use an overlay network of TOR routers
- Routers
  - distributed overlay network with virtual circuits
  - info stored in directory servers
- Clients
  - transport layer (TCP)
  - applications: web browsing, IRC, instant messaging
  - sender chooses random sequence of routers
- Layered cryptography
  - encryption related to the path

TOR security issues

- Out of band leaks
  - DNS traffic
  - errors in the application layer
- Traffic analysis
  - global passive adversary (government)
    - monitors entry/exit nodes
  - timing (entry vs. exit)
  - volume analysis (follow the bulk of data)
- Anonymity is not security
- Eavesdropping at exit nodes

Covert channels

- Security attack through channel that bypass access control mechanisms and policies
  - information transfer between processes/entities that are not allowed to communicate
  - bypass firewalls and not detected by IDS
- Basic characterization
  - storage channels
    - modify some "storage location"
  - timing channels
    - modify response time of a legitimate communication
- Properties
  - detectability: only recipient can measure the signal
  - indistinguishability: no identification
  - bandwidth: how many bits are transferred per use of covert channel

Covert channels in network

- LAN environment
  - covert communication between regular data transmitter and eavesdropper over LAN
  - frame size selection: a particular size selected is the covert message
  - LAN address selected can also be a covert message
- Transport layer
  - use of some control fields of IP or TCP packet
  - covert_tcp code developed by Craig Rowland
    - IP packet identification field
    - TCP initial sequence number field
    - TCP acknowledge sequence number field "Bounce"
  - compromised server that detects covert channel
    - variant of eavesdropper
  - can be identified ("unnatural sequence numbers")

Covert channels—summary

- Covert channels are not equivalent to steganography
  - they use illegitimate channles
  - while steganography uses legitimate communication channels to transfer hidden message
  - however, steganography could be used in a way that is practically equivalent to covert channel
    - no direct connection between sender and receiver
- Needs a modified system
  - installed receiver/sender
  - identifiable by covert channel analysis
- Communication is obscured, bypassing current security tools
- The fact of communication between parties is hidden

Censorship resistance protocols

- Censorship definition: *Internet censorship is the intentional suppression of information originating, flowing or stored on systems connected to the Internet where that information is relevant for decision making of some entity*
- The goal of censorship resistance protocols: To circumvent the censorship
  (i.e. to allow communication between two parties even in the presence of a censor who can check source, destination and content of the message and and is able to block the communication)
  - do you see similarities with a firewall?
  - this time we are on the "other side" (trying to circumvent the network "protection")

Censorship resistance protocols

- Basic principle: Disguise the traffic
- Censorship decision based on
  circumstances
    - addresses, timing, data transfer, services

  content
    - deep packet inspection
    - kind, properties, type, value

Censorship resistance protocols

- Hiding the content within other protocols
  - steganography
  - VoIP, http, e-mail, ...
- VoIP/Skype:
  - SkypeMorhp: shapes the traffic of ToR communication to look like Skype video call
  - Freewave: converts data into sounds and then sends them as a Skype voice call
  - CensorSpoofer: Decoupled communication channels
- ImagesInfranet
  - data hidden inside pictures on accepted image servers (standard steganography)
  - users "share" images

Censorship resistance protocols

- Rendezvous point
  - a seemingly innocent (from censor's point of view) site that helps connect the users
  - ToR routers as an example
- For more information see bibliography at `http://www.cs.kau.se/philwint/censorbib/`

Summary

- Design principles for resilient network architectures
- Defense against attacks on individual addresses
- Dual position in privacy
  - privacy protection
  - defense against unwanted traffic
- ToR and anonymization
- Censorship protection as the "other side" view
- Next lecture: Operational security management
  - how to design reliable networks
  - software defined networks