

PA197 Secure Network Design

6. Operational Security Management

How to design and manage reliable networks

Eva Hladká, Luděk Matyska

Faculty of Informatics

March 29, 2016

Content

- 1 Basic design principles
 - Access control
 - Limited management authorization
- 2 Critical infrastructure
 - Cyber-physical systems
- 3 Infrastructure security
 - Physical vs. digital security
 - Cost of higher security requirements
- 4 Software Defined Networks
- 5 Clean-slate design

Internet design principles

- Packet switched networks
 - no dedicated resources within the network
 - no fixed route between source and destination
 - accommodates links with different capacity
- Best effort service model
 - no strict guarantees provided
- End-to-end paradigm
 - any features (on top of the actual packet delivery) are to be provided by the higher level protocols at source and destination nodes only
- Implications:
 - **scalable** and **robust** network
 - no explicit security considerations
 - too open to malevolent exploitation

Network design example

- Paraphrasing from the CISCO Network Design principles
 - <http://www.pearsonhighered.com/samplechapter/1587132125.pdf>
- 1st step: **Network requirements**
 - 24/7 operation even if a node/service or link fails
 - data is transmitted in a timely manner
 - protect data transmitted and stored
 - allow for modifications and grows
 - fixing failures should be easy and fast
- 2nd step: Requirements translated into **Design goals**
 - scalability
 - availability
 - security
 - manageability

Network design example II

- CISCO proposes **Hierarchical design**
 - group devices into multiple networks
 - organize network in a layered approach
 - 1 core layer
 - 2 distribution layer
 - 3 access layer
- Advantages
 - local traffic remains local
 - encapsulation, different rules for different places (local networks)
 - this also increases reliability of different layers

Network design example III

- Roles of individual layers
- **Core layer**
 - 100 % uptime
 - maximizing throughput
 - facilitate network grows
- **Distribution layer**
 - filtering and managing traffic flows
 - enforcing access control policies
 - summarizing routes before advertising them
 - isolating core from access layer failures
- **Access layer**
 - controls user access to the network
 - QoS considerations
 - security policies enforcement

Internet architecture shortcomings

- No explicit security incorporated
 - no field in the packet is protected
 - easy to forge any identity
 - easy to forge source address
- No strict (hierarchical) structure of the management
 - local management “islands” without mutual influence
 - a robust solution
 - loss of control beyond islands' borders
- Problem of security of end nodes
 - holes in operating systems' security
 - devices (including the active elements on the network) with security holes and/or default passwords
 - easy to send “untraceable” packets
 - tracing beyond own management edge needs cooperation

Improvements of Internet architecture?

- Gradual improvements rather difficult
 - a complex interplay between protocols
- Adding a “security layer” is not sufficient
 - one layer will not be sufficient
 - attacker could use not-secured layer(s)
 - both transport and semantics of data must be secured
 - also end nodes can not be left unattended
- Nevertheless we must do what is possible
 - in parallel to more ambitious plans

Access control

- In Internet, if you have physical access to the network, you are in
 - no access control in standard Internet protocols
- Authentication
 - know who is speaking
 - know who is doing something
 - all not directly possible in the current Internet
 - but the necessary first step for access control
- Authorization
 - “another name” for **access control**
 - restricts what can be done by whom

Access control II

- Basic principle: **minimal rights**
 - start with an absolute minimum
 - rise access rights on request
 - and check repeatedly who is there
- Drawback: limited freedom
 - one of the major reasons why it is so difficult to make Internet more secure
 - remember the **control** part
 - you never know who will exert the control in the future

Limited management authorization

- Implementation of the restricted access right to the network management
- A very general concept
 - the general management theory
 - not restricted to networks or information technology only
 - **need to know** principle
 - split of decision rights among several players
- IT made the need for control more needed/explicit
 - remote decisions
 - no human check of the orders
 - extremely fast reaction time
- **Least privilege** principle
 - **abstraction layers**
 - start with the least privilege (access rights)
 - add more rights (increase the privilege) on the go as needed
 - usually requires repeated authentication

Least privilege

- Several synonyms
 - least authority
 - minimal privilege
- A mitigation against both
 - bugs and faults (fault tolerance)
 - malicious use (security)

in both cases it increases **reliability** of the system
- More a principle than a precise set of rules
 - not easy do define the minimal privilege actually needed to perform an operation
 - more a human decision what is needed

Abstraction layers

- Abstraction layers in the active network elements
 - usually very limited set of layers in the standard elements
 - read vs. read/write access and user vs. administrator
 - even the read access can be dangerous
 - misuse of SNMP complex call requiring lot of processing power to get all the information
 - simultaneous read requests
- One source of interest for **Software Defined Networks**

US Critical infrastructure

- US definition:
 - Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Department of Homeland Security

www.dhs.gov/what-critical-infrastructure)

- many sectors, important for us are **Communications** and **Information Technology** ones
 - Office of Cyber security and Communications
 - responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure
- Understanding that attack on network (and cybersystems in general) could have very serious impacts on the whole national wellbeing (and its security)

Cyber-physical systems

- Computer systems (elements) controlling physical systems (entities)
 - *Embedded systems* a special (or predecessor) case
 - Examples in energy distribution, aerospace, autonomous automotive systems, process control systems in factories, (medical) monitoring etc.
- The major purpose is the physical expression, not computations (the digital part)
- More and more network connected
 - part of the **Internet of Things**
 - increased vulnerability

Connectivity adds value but also risks

Cyber-physical systems II

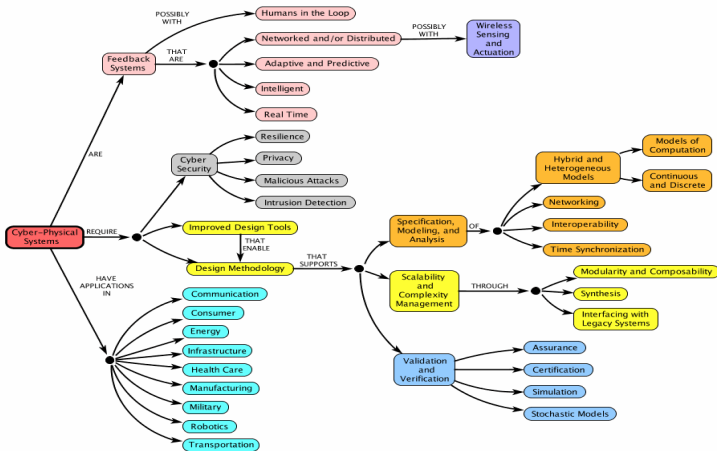
- For attacker, the physical manifestation is important
 - but the attack is led through the digital (cyber) part
 - the classical physical security may not be sufficient
 - the cyber part deserves equal (or even higher) protection
- See also <http://CyberPhysicalSystems.org>
 - the mental map on the next slide is taken from that source

Cyber-physical systems—Mental map

Cyber-Physical Systems – a Concept Map

See authors and contributors.

<http://CyberPhysicalSystems.org>



Control plane

- Two basic abstraction layers
 - **data plane**—all the users' traffic goes here; also called **forwarding plane**
 - **control plane**—the network management information
- Usually, the data and control plane share the same physical infrastructure
 - very convenient, easy to implement
 - opened to attacks
 - both passive and active attack modes

Control plane II

- Situation more confused when users' step in
 - VPN vs openVPN
 - VPN part of the network management, its control (management) messages) understood by network active elements
 - openVPN a software product, runs within the data plane, "hidden" from the network management
 - IDS systems looking both for data and control packets
- Don't mess with **physical** vs **digital** infrastructure
 - control plane part of the digital
 - however could run on a separate physical infrastructure

Physical security

- Physical layer the lowest layer of any communication network
- Security and reliability of the physical layer critical for all the above layers
 - however, with redundancy and fast recovery we may create more resilient networks even with not resilient physical layer
- Physical reliability
 - redundant **independent** connections
 - multihome nodes and multirouting protocols
- The physical security of critical nodes
 - limited access to the sites with
 - management systems
 - critical active elements

Physical security II

- Impossible to control the whole network
 - redundancy, independent paths
 - wired (optical) and wireless networks
- Important to check whole paths for independency
 - e.g. a bridge aggregating all otherwise independent physical lines

Digital security

- Data and control plane
- Time critical information
 - esp. in the control plane
 - timeouts may lead to wrong conclusions about the state of the network
- Reliable protocols
 - both the architecture and the implementation
 - software engineering practices
 - Ada used for mission critical systems for the USA DoD

Digital security II

- Authentication and authorization
 - distinct requirements for data and control plane
 - essential for the control plane
 - no anonymous actions/users
 - strict access control with the least privilege principle applied
 - strong authentication (two factor, . . .) for some operations
 - organizational policies very important
 - a principle of “four eyes” (two persons) is forsaken if the same person keeps both digital credentials

Digital security III

- Encryption
 - both data and control packets
- Specific requirements for control plane
 - cross domain encryption
 - PKI vs. symmetric keys exchange
- Accounting
 - keep track of the actions taken
- Reliability of accounting data
 - remote data collection
 - size of the data/lossy aggregation over the time

Cost of higher security requirements

- Explicit
 - less easy access to the network
 - more complex protocols
 - high processing needs (authentication, encryption)
 - slower response time
 - for (repeated) authentication
 - for access right decisions
 - for continuous control of access privilege
 - higher management burden
 - must define, implement and control policies
 - higher operational costs
 - keys, policies, accounting, . . .

Cost of higher security requirements

- Implicit
 - higher control could mean less freedom
 - in strictly hierarchical systems, compromising the highest layer could be disastrous
 - in too complex systems people start to bypass the rules and policies
 - a conflict between “have things done” and “check every step”
 - the natural world is imperfect and does not fully fit into strict mechanical rules

SDN principles

- A network with clear separation between control and forwarding plane, where the control plane spans/controls several devices
- Features:
 - makes control plan directly programmable
 - abstracts the underlying infrastructure
- SDNs present a reaction to
 - limits of vendor based solutions
 - requirements of more dynamic access patterns (mobile, remote, ...)

SDN advantages

- **directly programmable** and forwarding independent control
- **programmatically configurable** not vendor locked
- **central management** of several devices: the concept of **network controllers** that
 - maintain a (global) view of the network
 - provide a single interface to applications and services
 - mimic a single active element (switch)
- **flexible** allow fast (programmed) reaction to events and changing environments
 - including profound changes in traffic flow (routing)

SDN architecture

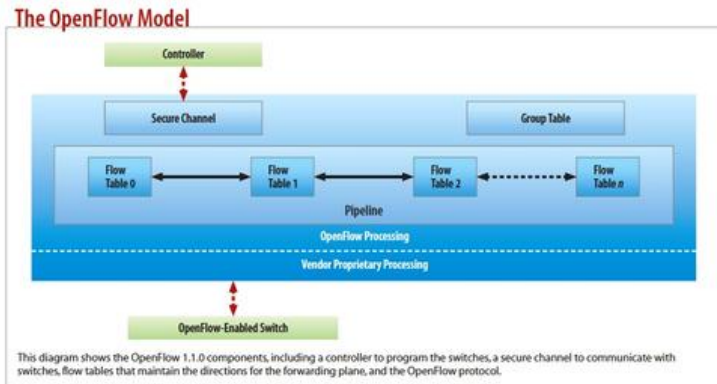
- Three different layers
 - the major difference is in the interaction, not the layers themselves
- **Application and orchestration layer**
 - focuses on expansion of network services
 - examples are cloud orchestration network virtualization, QoS, ...
- **Control plane layer**
 - logically-centralized SDN controller
 - exposes clearly defined APIs to Application layer
 - performs consolidated management and monitoring of network devices
- **Data plane layer**
 - physical network equipment
 - programmable

- Controllers
 - keep the **network intelligence**
 - allows to provide a central (global) view on the whole network
 - in contrast to the current distributed approaches
 - controller provides a programmatic API to the network
- Security
 - benefits of a central controller for distributed attacks
 - DDoS attack, botnet or worm propagation
 - controller's global view allows collecting traffic information that could be fed to a specific IDS for attack recognition
 - controller's central role allows for fast reaction at the or near real sources of attack

OpenFlow protocol

- A communication protocol
 - gives programmable access to the switch forwarding plane
 - enables to determine a path of packets through a network of switches
- Function: remote administration of packet forwarding tables (layer 3)
- Routing decisions taken by the controller
 - translated into rules and tables
 - implemented at wire speed by the device
- Properties
 - uses TCP, port 6653
 - TLS mandatory
- Security implications
 - central controller a central point of attack/failure
 - TLS faults susceptible

OpenFlow Model



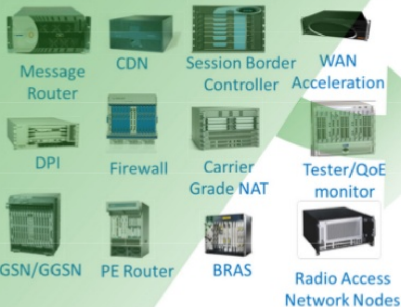
Data: InformationWeek Reports

Network Functions Virtualization

- A complementary activity to SDN
 - not dependent, but beneficial
- Aim is to consolidate network equipment types
 - leveraging virtualization technology
 - reducing the number of network device types
 - exposing their functionality through clearly defined APIs
- NFV support to SDN
 - standardized programmable network interfaces
 - use of commodity servers and switches

NFV Approach

Classical Network Appliance Approach



- Fragmented non-commodity hardware.
- Physical install per appliance per site.
- Hardware development large barrier to entry for new vendors, constraining innovation & competition.



Why clean-slate design?

- Need for fundamental changes in Internet architecture
 - flaws in the current Internet architecture
 - incremental changes may not be sufficient (see IPv6 example)
- A research activity
 - to investigate options
- RINA as an example
 - <http://www.cs.bu.edu/fac/matta/Papers/rina-security.pdf>
 - <http://irati.eu/wp-content/uploads/2013/01/6-Security130123.pdf>

RINA

- Recursive InterNetwork Architecture (Boston University)
- Basic premise: *Network is only Inter-Process Communication (IPC)*
- IPC a function to allow two processes (sender and receiver) to communicate
 - process names are identifiers
 - IPC function examples: process location, permissions determination, passing information, . . .
- Security by **isolation**
 - hosts can not address any element of the ISP
 - no hacker can compromise ISP assets
 - unless ISP is **physically** compromised

RINA II

- *Distributed IPC Facility (DIF)*
 - an organizing structure
 - “medium” for communication
 - processes can communicate only if they belong to the same DIF
 - a **layer** in a standard architecture
 - allows processes to allocate flow between them
 - providing names for the processes
 - and flow characteristics (bounds on data delay, jitter, loss, reliability, ...)
 - supports recursivity
 - a group of processes connected through DIF could play a role of a process in a different DIF

RINA III

- Security mechanisms
 - mandatory authentication before joining DIF
 - a process does not know any addresses nor “well known ports”, all is provided after authentication by the appropriate DIF
 - node addresses are internal to DIF, not exposed to the applications
 - data connections are dynamically assigned connection-endpoints IDs
 - bound to dynamically assigned ports
 - DIFs are securable containers, so no need for firewalls
- Security implications
 - resiliency to transport attacks
 - clear security borders
 - complexity of RINA security is lower than the security of the current Internet
 - much lower number of protocols and security mechanisms

Summary

- Secure network design
 - access control and the least privilege principle
 - redundancy
 - clear role separation
- Critical infrastructure and cyber-critical systems
 - attack through the digital, not physical components
 - physical and digital security recapitulation
- Software defined network
 - overcoming many current drawbacks
 - incremental changes to the network design
 - centralized control
- Clear slate design and RINA
 - far reaching vision
- Next session: Network monitoring and defense