# Network provider Security

Markus Peuhkuri

2005-04-28

## Lecture topics

- Basics of security
- Security threats
- Regulators and ISP security

## Some headlines

- Davie-Besse nuclear reactor control network was disabled by Slammer worm in 2002
- Blaster worm delayed power grid measurment information and was one component for North-East US blackout in 2003
- Panix.com[1] lost control for its domain resulting all emails of its customers to directed to third party in January 2005
- 30,000 personal records stolen from George Mason University
- Group stole USD 1.5 million worth from Wal-Mart using fake bar-codes
- A cracker had access to T-Mobile network for 7 months and had access to personal information, photos and FBI documents
- UK woman cannot sleep because someone stole remote control for her brain implant, possibly surgery needed to replace device.

## Key terms

**Security system** is designed to prevent unwanted events. This can be a preventive or one that has a deterrence effect.

**Intentional actions** are those that are of interest from security perspective. Unintentional actions are handled by safety systems. In some cases safety systems prevent also intentional attacks (and security systems some unintentional unanticipated events) but the evaluation principle is a different.

**Defender** is the one protecting assets.

**Attacker** performs intentional unwarranted actions. Note that this should not have any moral loading: for example the law enforcement may be the one that attacks on communications of organised crime.

**Attacks** are ways to break security system.

**Assets** are the objects that Defender wants to secure.

**Countermeasures** are security mechanisms the Defender implements to protect assets.

[1] Large ISP in NY

## Components of information security

**Confidentiality** is the concealment of information[2]

- patient records can be read only by those giving treatment

**Integrity** is trustworthiness of data[3]

- data integrity
- origin integrity (authentication)
- a bank must have integrity over it account records

**Availability** is the ability to use the information when desired[4]

- a stock broker must have access to trading system

## Threats in communications

- Disclosure — data is exposed
  - snooping
  - passive wiretapping
- Deception — invalid data is accepted
  - modification of information
  - active wiretapping
  - masquerading
    - delegation is authorised masquerading
  - repudiation of origin
  - denial of receipt
- Disruption — incorrect operation
  - delay, causing system to fail possibly more insecure system
  - denial of service
- Usurpation — resource is used by other entity

## Threat modelling

- Target: understand and document security threats
- Large number of possible threats
  ⇒ Ad-hoc treat searching incomplete
  ⇒ Must be methodological
- System threat profile described
- Characterisation of system security
- Threat is *not* vulnerability
  - vulnerability is unmitigated threat
  - attack classification important

[2] luottamuksellisuus
[3] eheys
[4] saatavuus

## Security is about tradeoffs

- Install a lock on a front door — have a risk forgetting key
- Install a burglar alarm — annoy your neighbourhood
- Use passwords on computers — forget it after vacation
- Use encryption for you photos — loss them for ever if you forgot the key pass phrase
- Have a low limit on credit card — have to spend nights in budget hotels
- Use encryption for a web site — need a faster computer

## Five-step evaluation of security mechanism[10]

1. What assets are you trying to protect?
2. What are the risks to these assets?
3. How well does the security solution mitigate those risks?
4. What other risks does the security solution cause?
5. What costs and trade-offs does the security solution impose?

## Threat tree [9]

- Goal as tree root
- An attack is decomposed to sub-goals

  **AND** all sub-goals must be meet

  **OR** any of subgoals is sufficient
- Attack costs or pre-requirements can be assigned
  - helps to determine seriousness
- Reuse of attack patterns

## Different assets

**Money** is traceable as long it is bits in computer systems; unmarked cash is anonymous

**Information** can be stolen[5], but most often it is just copied. Information that has leaked is impossible to get back with 100 % confidence.

**Reputation** of organisation is in many cases lost with defacement.

**Uninterrupted operation** of web site or network can be threatened by an extortionist, a competitor, or opposing group.

## Four different targets

**Any account on any system** to be used as step-stone for further attacks or just one resource for file storage and communications.

**Any account in one domain** to change external attack inside attack, possibly inside firewall perimeter.

**Any account in one system** that has proper protection makes possible to get desired information or a step closer for privileged account.

**Target account on target system** that has valuable assets.

[5] So that original owner does not have it anymore.

## Why bad security?

- Security implemented as add-on to completed system
  - system too complex to evaluate
- System purpose not one advertised
  - terrorist screening system helps for airline revenues
- Environment changes
  - closed system interconnected to other systems
  - system gets new functionality and becomes enticing target
  - technological advances
  - identifying token becomes authentication token, for example
- Wrong threat model
  - is fraud external or internal
- Security is not revarded
  - a shop does hand out revard money from CC companies to cash keepers
    $\Rightarrow$ no motive to risk question customer
- Designers or operators do not suffer on security failures
- Security system must be disabled to get work done

## Why adding more security measures may make systems less secure[8]

1. Common-mode problem: new items must be truly independent. If there is a common component, then a failure in it will result all dependet systems to fail.
2. Shirking problem:[6] someone or something other has checked it already. A strange email — but the antivirus software does not alert on it, so it must be safe to open.
3. Overcompensation problem: safer system enables more risks. Because we have firewall, we can decide not to deploy latest batches on computers before we have time to test that they do not cause any problems for our applications.
4. Dedicated worker problem: if security measure get in the way, they will be defeated

## Prevent — Detect — Recover

**Prevention** make attack to fail

- if the risk is an attack from Internet, disconnect machine
- access control, secure design, encryption

**Detecting** an attack or an attempt

- even if attack fails, detecting provides information
- monitoring, log analysis, traffic analysis

**Recovering** saves what is left or undoes damage

- stop attack, for example taking system off-line. In some cases it is not possible to take system off-line because of other risks.
- assess and repair any damage
- can be complicated if it is unsure when compromise took place
- reinstalling system from original install media, while truly paranoid does not trust even hardware anymore (BIOS, harddisk controller has malicious code?).

[6] Also known as "bystander apathy"

## Implementing security with people

- "Our system is secure, if no-one uses it"
- Outsiders can be detected at perimeter
- Insiders the difficult part: they
  - have *authority* to use the system
  - have *access* to the system
  - *know* details about the system
- Users must understand why each security measure exists
  - there are limits with user education
  - how to educate every Internet user?
- Social engineering age-old con man method

## Social engineering

- Computers are inflexible, humans adapt[7]
- Some common exploited scenarios
  - tit-for-tat helping (building trust)
  - authority over other party
  - pity, team player
  - greed
  - asking small amount of information at time
- Viruses use also social engineering: many email viruses have topical subject (celebrity pictures, messages from administration, crab CNN headlines) and trick users to open attachments
- Phishing is an automated con man. "Phishing" refers to collecting trustworthy information by masquerading to a trusted party, such as bank, eBay or PayPal. Word "phishing" comes from "fishing" with hacker lingo f⇒ph.

## Phishing: fishing for valuable information

- Trick users to reveal valuable information: credit card details, bank or website passwords, personal information
- Spam email messages
- Possibly malicious payload
  - or trick user to download some spy-ware
- Ever larger problem: December 2004
  - 1707 fake sites (24 % growth in 6 months)
  - 55 brands used (86 % financial institutions)
  - fake site on-line for 6 days on average (max 30)

[7]Note, that this is not just bad thing. A human can make judgement and act on situation that was not anticipated.

## Security policy

- Statement that bisects states to
  1. authorised, secure
  2. unauthorised, insecure
- Different policies can have different sets of states
- Secure system
  - starts in authorised state
  - cannot enter unauthorised state
    if this happens, *breach of security* occurs
- Security mechanism enfoces some part of security policy
  - entity
  - procedure
- Security model represents policy or set of policies

## How one authenticates

- What one *knows*
  - passwords, PIN
- What one *has*
  - keys, smartcards
- *What* one *is*
  - biometric identification
- *Where* one *is*
  - terminal restrictions

## Economics of authentication

- Software
  - for organisation, system
- Hardware
  - for site, user, workstation
- Enrolment costs
  - administration, per user costs
- Usage costs
  - time spent by user to authenticate
- Maintenance
  - time spent to maintain system: for system administration and user time to renew password.
- Problem recovery
  - lost devices, forgotten passwords, flu
- Availability
  - cost of lost access
- Revocation costs
  - removing rights from user, lost authenticators

## IPsec

- Provides
  - confidentiality
  - integrity
  - authentication
  - replay protection
- Two modes

  **transport mode** transport protocol and payload encapsulated

  **tunnel mode** original IP datagram encapsulated
- Two protocols

  **ESP** Encapsulating Security Payload

  **AH** Authentication Header
- Three databases

  **SPD** Security Policy Database — contains policies for incoming and outgoing traffic

  **SAD** Security Association Database — established SAs

  **PAD** Peer Authorization Database — link between e.g. IKE and SPD
- Integrated into IP implementation or

  **BITS** bump-in-the-stack: additional software for host IP stack to implement IPsec

  **BITW** bump-in-the-wire: a gateway (router, firewall) in network implements IPsec on behalf of hosts

## WLAN security

- WEP protection weak
  - in many cases, not even used: the problem is that there may not be clear indicator if traffic is protected or not. If traffic is not protected, it works as well or even better than if protected.
  - invalid use of RC4, shared, manual secret (see lecture on cryptology for details)
- WPA and 802.11i will help (802.1X)
- Attacks on WLAN
  - war-driving: searching for (open) networks
  - passive attacks on encryption
  - fake access point
  - man-in-middle, ARP poisoning
  - traffic analysis: padding uses precious bandwidth
- Possible to eavesdrop from long distance
  - even bluetooth access to phone 1.6 km apart: bluetooth phone had transmission power less than 1 mW; WLANs have max. 100 mW.

## What is a firewall

- Divides network into two (or more) parts with *different security policy*
  - internal network ⇔ Internet
  - engineering ⇔ accounting: the other network must not be less secure that the other one. They just have different security policies or different assets to protect.
  - internal network ⇔ public servers ⇔ Internet
  - building automation ⇔ VoIP ⇔ surveillance system
- Enforces security policy
  - allowed traffic
  - prohibited traffic

  Refer to IPsec security policy database (SPD): traffic is bypassed, discarded, or bypassed as protected.
- May have additional roles, such as VPN endpoint

## Firewall types

**Packet-filtering** makes decision based only packet fields

- router ACL (access control list)
- TCP implicit state: for example to disallow incoming connections, firewall will drop any packet that has SYN flag set but no ACK and allows any packet with SYN+ACK.
- difficult with UDP, also some other TCP-based protocols such as FTP in active mode, where server establishes connection to client.

**Stateful** keeps track on connections

- maintains connection state
  - single point of failure
  - has to have some timeout mechanism as the state space is limited. Some attacks may exhaust state space.
    ⇒ random disconnections
- possible to accept related connections: for some protocols this needs application gateway.

**Application gateway** interpret connection on application level

- checks if application traffic is valid
- protects from simple port changes
- may provide payload inspection to detect malicious payload
- proxy servers
  - call-out
  - in-line (transparent)

**Address-translation** between internal numbering and external addresses

- using NAPT provides same as prohibiting incoming TCP
- internal topology can be hidden

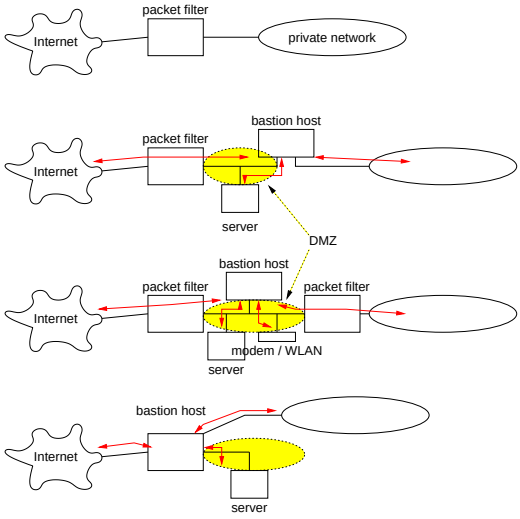
**Host-based** or software firewalls add on application security

- completes application security and access control
- possibly user- and application-level control

**Hybrid** use combination of different types for performance

- check start of connection with application gateway, switch to stateful filtering
  ⇒ better performance as bulk of traffic is handled by fast path.

## Firewall topologies




## What firewall protects and what not

- Protects
  - from known, vulnerable protocols
  - static network configuration
- Does *not* protect for / from
  - executable/active content
  - malicious insider
  - loopholes: modems, WLAN, mobile networks
  - carry-in attacks such as notebooks, mass storage
  - new attacks
  - most DoS attacks
- May result "hard perimeter, mellow inside"
  - failure to update internal systems
  - selecting insecure protocols and applications

## Intrusion Detection Systems

- How to make sure that firewall is not leaking
- How to detect internal attacks
- IDS is designed to
  - detect,
  - identify, and
  - report malicious activity
- IDS can be located different places
  - application
  - host
  - network

## What is Denial of Service

> The prevention of authorized access to a system resource or the delaying of system operations and functions[12]

- System is *unavailable* or *unusable*
- Unavailable
  - system crashed
  - route unavailable
- Unusable
  - responses too slow
    - protocol timers fire
    - users are impatient
  - high packet loss

## Why anybody wants to DoS

- Extortion
  - a large crime
  - aimed on bookies, online casinos and other e-Commerce sites
- Disabling some services
  - spam blacklist services
- Enabling other attacks
  - overloading firewall, IDS
- Revenge or hate
  - SCO, RIAA, ...
- Damaging competitors
- Last resort attack

## How to DoS

- Just send lots of packets
  - works best with distributed DoS
  - also amplification attacks
- Use protocol properties
  - TCP 3-way handshake, connection resets
- Use implementation vulnerabilities
  - send malformed data
- Use algorithmic complexity
  - exploit worst-case
- Attack on infrastructure
  - routers
  - support services (DNS, other directories, registries)
  - electrical power, air conditioning, physical cables

# Botnets

- What to use botnets for
  1. DDoS
  2. spamming
  3. traffic sniffing
  4. keylogging
  5. spreading new malware
  6. automated advertisisement clicks to get revenue on click-through adverisiment such as Google AdSense
  7. attacking on IRC networks
  8. manipulating polls and games
  9. large-scale identity theft by sending phishing spam and hosting phishing web sites; also computer user's information may be captured using keylogging or file search
- How to build a botnet
  - direct attacks (ports 445, 139, 137, 135, 5000)
  - browser, email exploits
  - p2p networks
- How much of bots
  - tens of active botnets
  - hundreds to tens of thousands bots in each net
    $\Rightarrow$ total *million bots*
  - 1000 bots with 256k upstream
    $\Rightarrow$ 256 Mbit/s attack speed: normal business have access speed a lot less
- Mostly controlled by IRC
  - provides quite scalable infrastructure
  - any communication possible, like using NNTP news
  - p2p networks
  - trin00, TFN: UDP-based (Tribe Flood Network)

# Routing attacks

- Blackhole
  - cause traffic directed wrong destination
  - drop packets
- Eavesdropping
  - receive data and record
  - resend data to right destination
- Network hijacking
  - steal network addresses
  - to send spam, other attacks

## Routing protocols

- Path vector protocols (RIP, BGP)
  - each router informs neighbours about its routing table
  - (destination, cost)
  - not possible to verify data
- Link state protocols (OSPF, IS-IS)
  - network topology flooded
  - independent verification of data (all neighbours must be evil)
- Attacks
  - compromised router
  - message injection
  - message modification
- May require physical access to link

## BGP security

- Internet runs on BGP4
- Should one trust for *ALL* ISPs?
  - small configuration error can lead to problems [1]
  - how about malicious user

  ⇒Use policy filters
- BGP connection resets
  - needs to establish a new session
    ⇒ uses router resources
  - use TCP MD5 extension to protect malicious resets [5]
  - TTL protection [4]
- Filter BGP (port 179) on edges

## Network administrator checklist

1. Check that your users cannot fake source address
   - ingress filtering [2]
   - `ip verify unicast reverse-path`

     It's better than a sharp stick in the eye, I'll tell ya, lad.

     Listen to me: It's called a "best current practice" for a reason – people should do it. Not sit and around and endlessly discuss it (we've already done that a thousand times).

     I wrote it, I stand beside it. I'm sick of hearing why people haven't implemented it yet – it's almost five years later and there's simply no excuse. It's sickening.

     - fergie[3]
2. Check source IP for forgery
   - don't accept local address from outside
   - packet filter or reverse-path verification
3. Do not accept directed broadcasts [11]

- `no ip directed-broadcast`

Note, that you cannot just drop any packet which destination address has low byte 255:

- it may be destined to /23 (or shorter prefix) network
- it does not help for /25 (and longer prefix) networks

4. Filter for bogons (unallocated or private-use address space) [6] `http://www.cymru.com/Bogons/`. Remember to follow lists for new allocations!

# Malicious logic

**Trojan horse** user unintentionally executes program

- documented effect (what user expects)
- covert effect (malicious)
- Trojan in compiler [13]
- "free" software add-ons (spyware, adware)
- may replicate itself

**Virus** inserts itself to file

- may have malicious actions
  - corrupts files
  - destroys equipment
- loss of performance
- several subtypes by infection, implementation method

**Worm** propagates between systems

- may have an impact on network
- most current malicious logic
  - massmailers
  - chat
  - p2p networks

**Rabbits/bacteria** exhaust resources quickly
`main(){for(;;)fork();}` (*DO NOT* run code on public systems...)

**Logic bombs** event triggers malicious action

- disgruntled employee

# (Data) security governance in Finland

- Ministry of Transport and Communications[8]
  - FICORA (Finnish Communications Regulatory Authority[9])
- Ministry of Justice[10]
  - Office of the Data Protection Ombudsman[11]
- Ministry of Trade and Industry[12]
  - Consumer Agency[13] (Consumer Ombudsman[14])

[8] Liikenne- ja viestintäministeriö
[9] Viestintävirasto
[10] Oikeusministeriö
[11] Tietosuojavaltuutetun toimisto
[12] Kauppa- ja teollisuusministeriö
[13] Kuluttajavirasto
[14] Kuluttaja-asiamies

  - National Emergency Supply Agency[15]
- Ministry of the Interior[16]
  - Police

## Privacy

- Governed by multiple laws
  - Act on the Protection of Privacy in Electronic Communication[17] (516/2004)
  - Personal Data Act[18] (523/1999)
  - Communications Market Act[19] (393/2003)
- A message that is not intended to public, is confidential regardless of medium
  - unintended recipient may not disclose even existence of message
  - one may return to sender

## Who has right to handle identification data

- To realise services
  - even automatic handling for relaying is handling
- To implement data security
  - firewalls, virus scanners
  - must not infer with legal communication
- For charging
  - in most cases, no reason to reveal B-number
    $\Rightarrow$ aggregate information sufficient
- To improve technical implementation
  - only aggregate or anonymous information
- To resolve technical problems
- To resolve misuse
  - *not* to follow where a employee visits or what messages sends (unless identified as virus)
- Communicating parities
- If permission by one of communicating parties

## How to handle identification data

- Only when needed
- Only as much as needed
- Only those whose duties it belongs to
- Handing information over only to those that have right
- Service provider must have audit trail for two years
- Professional discretion must be maintained

[15] Huoltovarmuuskeskus
[16] Sisäministeriö
[17] Sähköisen viestinnän tietosuojalaki
[18] Henkilötietolaki
[19] Viestintämarkkinalaki

## Communications Market Act

Public communications networks and communications services and the communications networks and communications services connected to them shall be planned, built and maintained in such a manner that:

1. the technical quality of telecommunications is of a high standard;
2. the networks and services withstand normal, foreseeable climatic, mechanical, electromagnetic and other external interference;
3. they function as reliably as possible even in the exceptional circumstances referred to in the Emergency Powers Act and in disruptive situations under normal circumstances;
4. the protection of privacy, information security and other rights of users and other persons are not endangered;
5. the health and assets of users or other persons are not put at risk;
6. the networks and services do not cause unreasonable electromagnetic or other interference;
7. they function together and can, if necessary, be connected to another communications network;
8. terminal equipment meeting the requirements of the Radio Act can, if necessary, be connected to them;
9. they are, if necessary, compatible with a television receiver that meets the requirements of this Act;
10. their debiting is reliable and accurate;
11. access to emergency services is secured as reliably as possible even in the event of network disruptions;
12. a telecommunications operator is also otherwise able to meet the obligations it has or those imposed under this Act.

## Importance classification Ficora 27 E/2005 M[20]

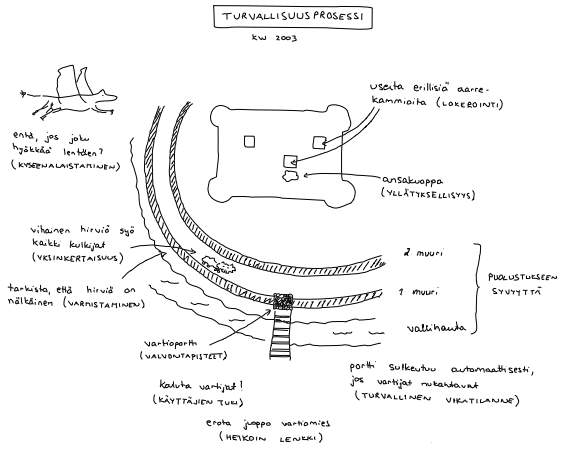
- It is not economical to protect all systems similarly
- Classification based on impact
- Important system[21]
  - serious risks of unauthorised access
  - difficult to replace
  - disruption has an effect on 1/3 of numbering area (based on number of subscribers or by area)
  - disruption has an effect on more than 10000 customer of public broadcasting network
- Very important system[22]
  - high importance to service continuity or during state of emergency
  - relays significant proportion of important community traffic
  - disruption covers whole numbering area
  - disruption covers all public broadcasting network
- Physical security, backup power

[20] Yleisen viestintäverkon tärkeysluokittelu
[21] Tärkeä järjestelmä
[22] Erittäin tärkeä jäjrestelmä

## Reporting responsibility

- Telecommunications provider must report to FICORA
  - security violations
    - break-ins to provider systems
    - sensitive information disclosure
    - degenerated performance because of attack (DOS, SPAM)
    - malicious software in provider system
    - social engineering
    - unauthorised wiretapping equipment
  - security threats
    - serious break-in attempts
    - anomalous traffic
    - new security problems in provider systems
  - serious system malfunction or disruption
    - breaks longer than one hour affecting many subscribers
    - very important system malfunction more than 30 minutes
- Customers must be informed
  - customer education
  - information about implemented protection measures like email filtering

## Security in organisation




## Summary

- Security is ever-moving target
- KISS[23] is a good principle for security too
- Operator has lots of responsibilities towards
  - clients
  - other operators
  - authorities
- If somebody can mess with your routing, it is not network anymore

[23] Keep It Simple and Stupid

# References


[1] Vincent J. Bono. 7007 explanation and apology. Nanog mailing list, April 1997. URL:http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html.

[2] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Request for Comments RFC 2827, Internet Engineering Task Force, May 2000. (Best Current Practice) (Updated by RFC3704) (Obsoletes RFC2267) (Also BCP0038). URL:http://www.ietf.org/rfc/rfc2827.txt.

[3] Paul Ferguson. Re: Bcp38 making it work, solving problems. Nanog mailing list, October 2004. URL:http://www.merit.edu/mail.archives/nanog/2004-10/msg00121.html.

[4] V. Gill, J. Heasley, and D. Meyer. The Generalized TTL Security Mechanism (GTSM). Request for Comments RFC 3682, Internet Engineering Task Force, February 2004. (Experimental). URL:http://www.ietf.org/rfc/rfc3682.txt.

[5] A. Heffernan. Protection of BGP Sessions via the TCP MD5 Signature Option. Request for Comments RFC 2385, Internet Engineering Task Force, August 1998. (Internet Proposed Standard). URL:http://www.ietf.org/rfc/rfc2385.txt.

[6] IANA. Special-Use IPv4 Addresses. Request for Comments RFC 3330, Internet Engineering Task Force, September 2002. (Informational). URL:http://www.ietf.org/rfc/rfc3330.txt.

[7] G. Meyer. The PPP Encryption Control Protocol (ECP). Request for Comments RFC 1968, Internet Engineering Task Force, June 1996. (Internet Proposed Standard). URL:http://www.ietf.org/rfc/rfc1968.txt.

[8] Don Norman. Why adding more security measures may make systems less secure. *RISKS-LIST: Risks-Forum Digest*, 23(63), December 2004. URL:http://catless.ncl.ac.uk/Risks/23.63.html.

[9] Bruce Schneier. *Secrets and Lies: digital security in a networked world.* Wiley Computer Publishing, 2000.

[10] Bruce Schneier. *Beyond Fear.* Copernicus Books, 2003.

[11] D. Senie. Changing the Default for Directed Broadcasts in Routers. Request for Comments RFC 2644, Internet Engineering Task Force, August 1999. (Best Current Practice) (Updates RFC1812) (Also BCP0034). URL:http://www.ietf.org/rfc/rfc2644.txt.

[12] R. Shirey. Internet Security Glossary. Request for Comments RFC 2828, Internet Engineering Task Force, May 2000. (Informational) (Also FYI0036). URL:http://www.ietf.org/rfc/rfc2828.txt.

[13] Ken Thompson. Reflections on trusting trust. *Commun. ACM*, 27(8):761–763, 1984.