

Summing up: How the Internet Works

- Important protocols we haven't got time for
 - We haven't said nearly enough about security
- How things fit together
- Guiding principles
- Questions?

1

314 s2c Exam, 2010

- Exam Date: Thursday 28 October 2010
- Time: 2:15 - 4:30 p.m.
- 11 short-answer questions
 - 100 marks total
 - 20 for part 1, 40 each for parts 2 and 3
- Material covered includes
 - All the lecture slides
 - Assignments

2

Other infrastructure topics

Background slide

- | | |
|---|----------------------------------|
| • PPP (point-to-point protocol) | • Multicast (Shay 11.2) |
| • EAP, RADIUS, DIAMETER <ul style="list-style-type: none"> – Authentication, authorisation | • Mobile IP, mobility in general |
| • IPSec, IKE (Shay 11.3) <ul style="list-style-type: none"> – Applies to IPv4 or IPv6 | • SASL (simple auth & security) |
| • VPN (virtual private networks) | • SLP (service location) |
| • NAT <ul style="list-style-type: none"> – Network address translation | • RSVP (Shay 11.2) |
| • Firewalls | • ROHC (header compression) |
| • SOCKS (firewall traversal) | • iSCSI (SCSI over IP) |
| | • RDMA (remote DMA) |

3

Other application topics

Background slide

- | | |
|---|---|
| • MIME (multimedia formats) | • NFS, AFS <ul style="list-style-type: none"> – Remote file systems |
| • SIP, ENUM <ul style="list-style-type: none"> – standards for voice over IP | • NNTP (network news) |
| • Video over IP | • RSS, ATOMPUB (feeds) |
| • PGP, S/MIME (secure email) | • Instant messaging |
| • Internationalised email | • Language tags |
| • Anti-spam solutions | • Web Services <ul style="list-style-type: none"> – XML-based distributed computing over SOAP+HTTP |
| • LDAP (directory) | • Peer to Peer protocols |
| • NTP (network time protocol) | • Grid computing protocols |
| • IPP (Internet printing protocol) | |

4

Background slide

- | | | | |
|---------------------|--------------------|------------------------------|----------------------|
| CAP | TN3270 | MANET(AUTOCONF | NETCONF |
| APEX | URI,URL,URN issues | MobileIP | POLICY |
| ATOM | VoIP | NEMO | SNMP |
| BEEP | WEBDAV | NETLMM | Traffc Engineering |
| CALSCH | WIDEX | OSPF | DIAMETER |
| CIP | FECFRAME | PPP | EAP |
| DKIM | iSCSI, iFCP | PTOWAINE | IDX |
| DNS | MIDCOM, STUN | PWE | IEPREP, ECRT |
| EDIINT | ONCRPC | RIP | INCH |
| Email and MIME | RDDP | Router Discovery | IPSEC, IKE |
| ENUM | ROHC | RSVP, Integrated Services, | KERBEROS and GSS-API |
| FAH | RMT | NSIS | KEYPROV |
| FTP | RTSP, RTSP, SDP | SOFTWIRES | LTANS |
| GEOPRIV | SCTP | UDLR | NEA |
| HTTP | TCP | VRRP | OPENPGP |
| Instant messaging | UDP | ZEROCONF | OPSEC |
| IPP | BEHAVE | 16ag (IP over IEEE 802.16) | OTP |
| LDAP | BFD | 6lowpan (IPv6 over 802.15.4) | PANA |
| Language Tags | BGP | GWPLS | PKI |
| Multimedia | DHCP | IP over X | RADIUS |
| NFS | DIFFSERV, PCN | IPoB | RPSec, SDR |
| NNTP | FORCES | IMSS | SACRED |
| NTP | GROW | MPLS | SASL |
| OPES | HIP | TRILL | SEND |
| RSERPOOL | ICMP | ANCP | SOCKS |
| SEAMOB | IPv4 | BWWG | SSH |
| SIP, SIPPING, PPSIP | IPv6 | CAPWAP | SSL/TLS and HTTPS |
| SLP | IPMTUD discovery | COPS | SYSLOG |
| TELNET | IP multicast | GSMF | SIMIME |
| TFTP | IS-IS | IPFIX, PSAMP | XMLDSIG |
| TIP | L2VPN, L3VPN | IPM | |
| | | WIRs | |

The diagram illustrates a multi-layered network architecture. At the top, various application and transport protocols are shown as stacked boxes, categorized into three main groups: yellow (left), orange (middle), and light blue (right). Arrows from these boxes point down to a large blue horizontal band representing the network core. This core band is divided into several horizontal sections, each containing specific protocols. The bottom of the diagram is a purple band representing the physical link layer.

Application and Transport Protocols (Top Layer):

- Yellow Boxes (Left):** SLP, DNS, DHCP, and a large box for Routing (OSPF, BGP4, IS-IS, RIP).
- Orange Boxes (Middle):** SIP VoIP, LDAP, FTP, Email (SMTP, POP3, IMAP, PGP, S/MIME), SNMP, and SSH Login, telnet.
- Light Blue Boxes (Right):** etc., etc., Web Services, SOAP, NFS, and HTTP HTTPS.

Network Core (Blue Band):

- Socket interface, secure transports (SSL, TLS, SSH, SASL):** The top section of the blue band.
- RDMA:** A small yellow box on the left side of the blue band.
- TCP, UDP, SCTP, DCCP, RTP:** The middle section of the blue band.
- QOS: Diffserv, RSVP:** A yellow box on the right side of the blue band.
- ROHC:** A small yellow box on the left side of the blue band.
- Mobile IP, multicast:** A yellow box on the left side of the blue band.
- Security: IPsec, IKE:** A yellow box on the right side of the blue band.
- RADIUS, DIAMETER:** An orange box on the left side of the blue band.
- IPv4, IPv6, ICMP, ARP:** The bottom section of the blue band.
- Layer 3 VPNs, SOCKS, NAT:** A yellow box on the right side of the blue band.

Link Layer (Bottom Layer):

- EAP authentication:** A yellow box on the left side of the purple band.
- Link layer encapsulation, packet drivers IP over X, PPP, MPLS, Layer 2 VPNs:** The main section of the purple band.

The diagram illustrates a network topology where a Site OSPF network is connected to three Autonomous Systems (ASes) via BGP4. The Site OSPF network is divided into two regions: Area and Back bone. The Area region contains routers A and B, and the Back bone region contains routers R1 and R3. R1 is connected to R3, and R3 is connected to R21 in ISP1. R1 is also connected to R99 in the Local ISP. The Local ISP contains DNS, DHCP servers, R99, NAT+firewall, and ADSL user components. The Site OSPF network also contains DNS, DHCP servers and a Firewall. The three ASes (ISP1, ISP2, and Local ISP) are connected to each other via BGP4. The Site OSPF network is connected to ISP1, ISP2, and the Local ISP via BGP4. The Site OSPF network is also connected to the Local ISP via BGP4. The Site OSPF network is connected to the Local ISP via BGP4. The Site OSPF network is connected to the Local ISP via BGP4.

Background slide

- 8

The end-to-end principle* (2)

Background slide

- Certain required end-to-end functions can only be performed correctly by the end-systems themselves
- Any network, however carefully designed, will be subject to failures of transmission at some statistically determined rate. The best way to cope with this is to give responsibility for the integrity of communication to the end systems. A similar argument applies to intrusions
- No solution buried inside the network can give the same level of assurance as the end systems
 - For example, *end-to-end* encryption is intrinsically safer than *router-to-router* encryption

* see References

9

Other principles (1)

Background slide

- Heterogeneity by design
- Avoid duplicate solutions
- Scalable designs
- Performance and cost must be considered as well as functionality
- KISS (keep it simple, stupid!)
- Modularity is good
- Good enough is enough (don't seek perfection)
- Minimise use of options
- Be strict when sending and tolerant when receiving

10

Other principles (2)

Background slide

- Be parsimonious with unsolicited packets, especially multicasts and broadcasts
- Circular dependencies must be avoided
- Objects should be self-describing (type and size)
- Nothing gets fully standardised until there are multiple instances of running code
- Avoid design that requires hard coded addresses
- Addresses must be unambiguous (NAT breaks this!)
- Designs should be fully international
- All protocols need strong security (early ones didn't!)

11

References

Background slide

- RFC 1958: Architectural principles of the Internet
 - End-to-end principle paraphrased from "End-To-End Arguments in System Design", J.H. Saltzer, D.P.Reed, D.D.Clark, ACM TOCS, Vol 2, Number 4, 1984
- "Why the Internet only just works" by Prof. Mark Handley, University College London

<http://www.cs.ucl.ac.uk/staff/M.Handley/papers/only-just-works.pdf>

12

Questions?

- What haven't you understood in this course?