Практические аспекты сетевой безопасности

Спецкурс кафедры АСВК ВМК МГУ

весенний семестр 2011 г.

Лекторы

- Денис Гамаюнов
  - м.н.с. ЛВК АСВК ВМК МГУ
  - соруководитель спецсеминара кафедры АСВК «Информационная безопасность и сети ЭВМ» с 2001 года
- Владимир Иванов
  - заместитель руководителя департамента эксплуатации «Яндекс»
- Андрей Петухов
  - сотрудник ЛВК АСВК ВМК МГУ

Информационная поддержка курса

- Wiki: http://course.secsem.ru/
- Список рассылки: course@secsem.ru http://lists.secsem.ru/cgi-bin/mailman/listinfo/course

Программа курса

- Два семестровых спецкурса:
  - «Введение в информационную безопасность» - осенний семестр
  - «Практические аспекты безопасности компьютерных сетей» - весенний семестр
- Допуск к весеннему спецкурсу по итогам сдачи экзамена по осеннему спецкурсу

Программа весеннего семестра – 1/2

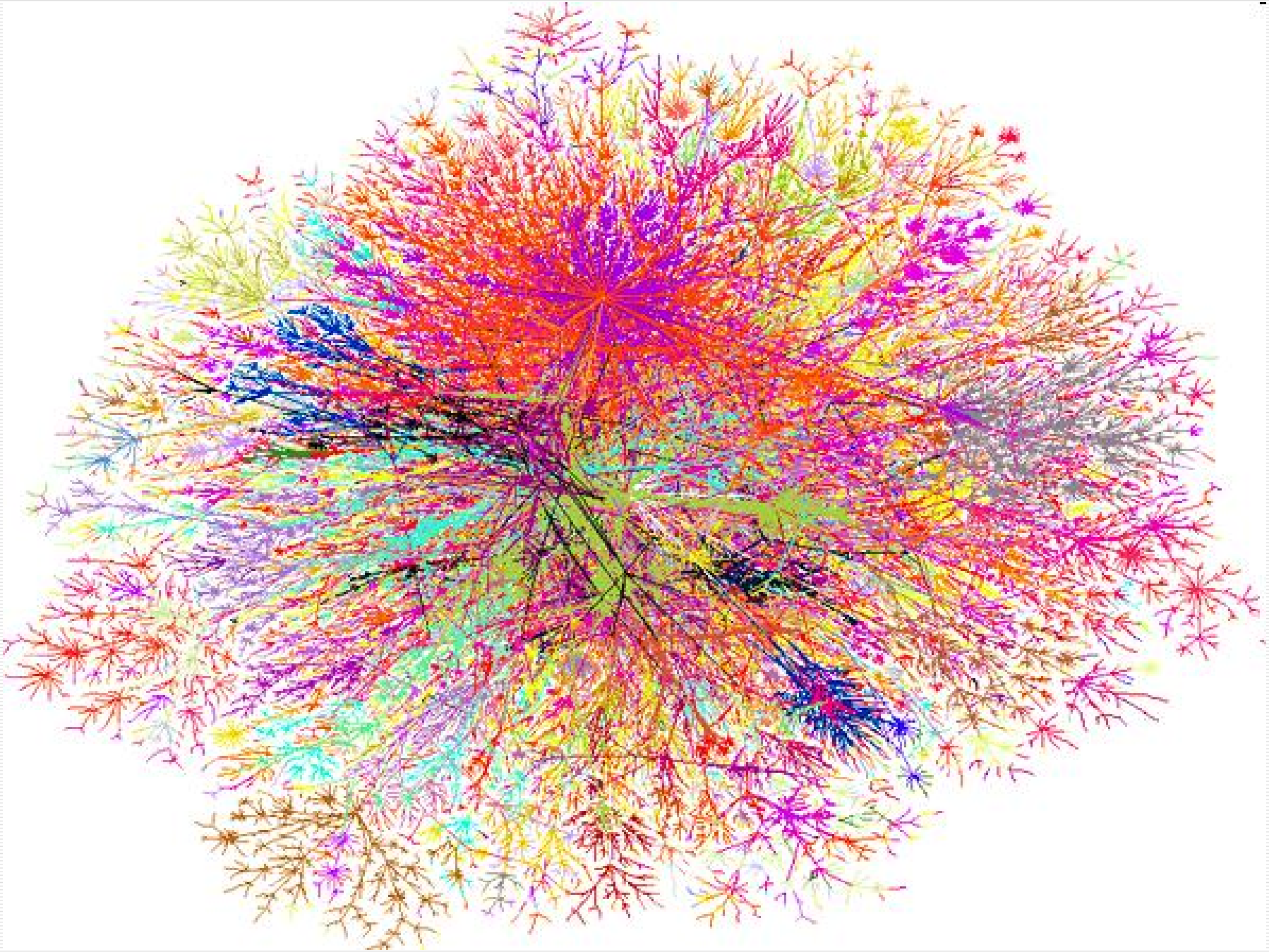
- **«Компьютер это сеть» - особенности защиты информации в сетях**
  - Введение в обеспечение безопасности в сетях
  - Стек протоколов TCP/IP
  - Настройка AAA в сетях Linux-машин.
  - Межсетевые экраны
  - Системы обнаружения атак
- **Анализ и контроль поведения программ**
  - Трассировка с помощью утилит strace, ltrace, netstat, lsof, procfs
  - Контроль поведения программ в Linux – SELinux, AppArmor, systrace

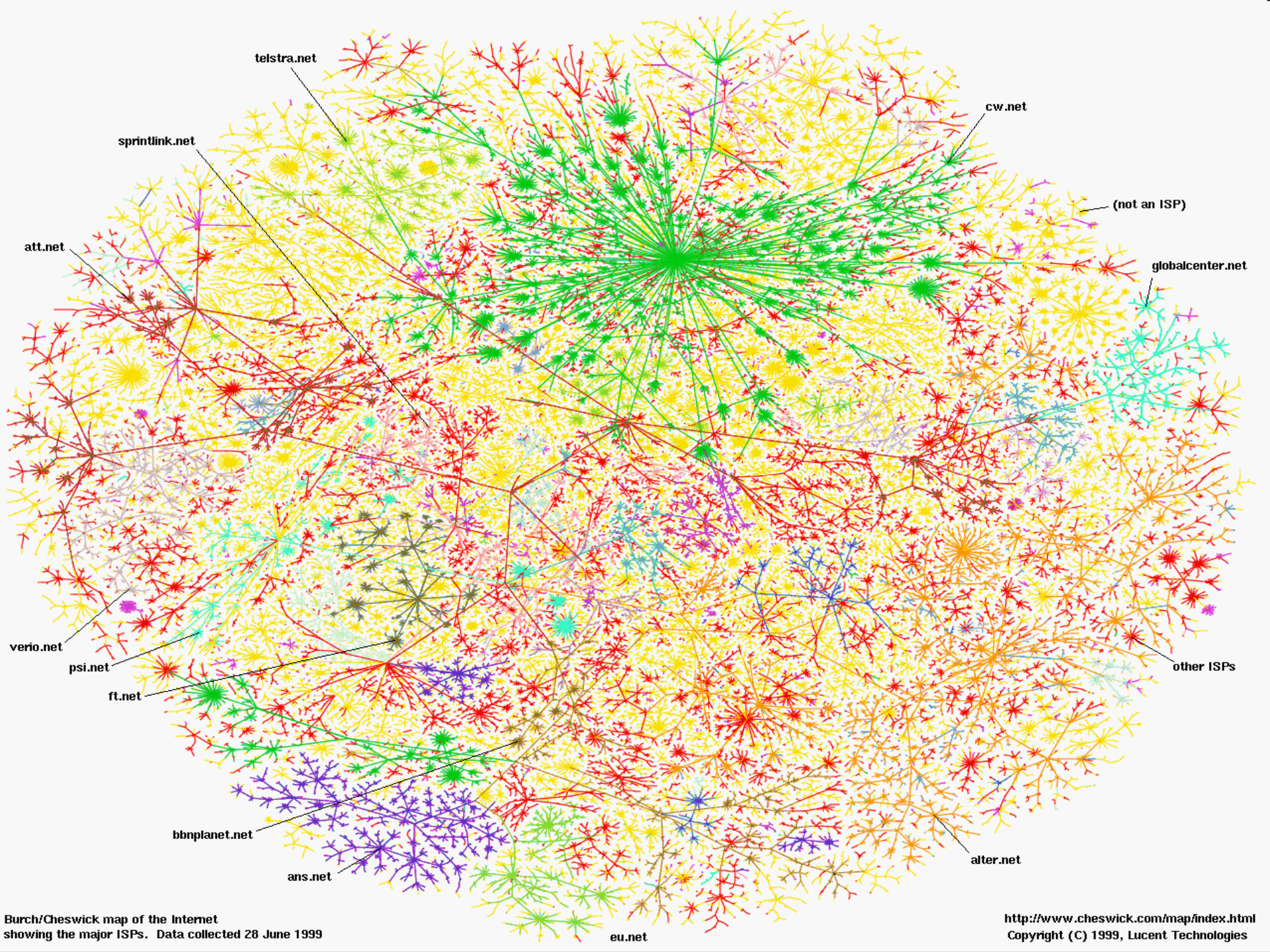
Программа осеннего семестра – 2/2

- **Безопасность веб-приложений**
  - Принципы работы основных веб-технологий: протокола HTTP, мехнизма реализации сеансов cookies, набора технологий HTML 4 (объектная модель документа + CSS + язык javascript)
  - Методы обнаружения и эксплуатации распространенных уязвимостей веб-приложений: XSS, SQL injection, CSRF, LFI/RFI
  - Обзор уязвимостей из OWASP Top 10 2010
- Примеры прикладных задач, связанных с информационной безопасностью

Введение

- Сеть – это компьютер?





Burch/Cheswick map of the Internet
showing the major ISPs. Data collected 28 June 1999

http://www.cheswick.com/map/index.html

2008 GLOBAL TRAFFIC MAP

TeleGeography

du — add life to life

ARCTIC OCEAN

ARCTIC OCEAN

RUSSIA

RUSSIA

CANADA

UNITED STATES

CHINA

INDIA

MEXICO

PACIFIC OCEAN

INDIAN OCEAN

BRAZIL

ATLANTIC OCEAN

CHINA

INDIA

INDIAN OCEAN

AUSTRALIA

ARGENTINA

AUSTRALIA

Where We Minutes Grow

The Hype about Skype

Speaking in Volumes

Chatter Box

Who are You Going to Call?

Pipe Dreams

How We Connect

Minute by Minute

Dinner Margins

Going Mobile

Minutes are Our Business

Staying on Top of the Curve

Госпрограмма РФ «Информационное общество (2011 - 2020 годы)»*

	2008	2011	2012	2013	2014	2015	2020
Число домашних хозяйств, имеющих широкополосный доступ в сеть Интернет, в расчете на 100 домашних хозяйств	26%	45%	47%	48%	52%	55%	80%
Доля федеральных государственных услуг, которые население может получить в электронном виде	-	39%	93%	98%	100%	100%	100%
Доля электронного документооборота между органами государственной власти в общем объеме документооборота	-	10%	15%	20%	35%	70%	70%

* выдержка

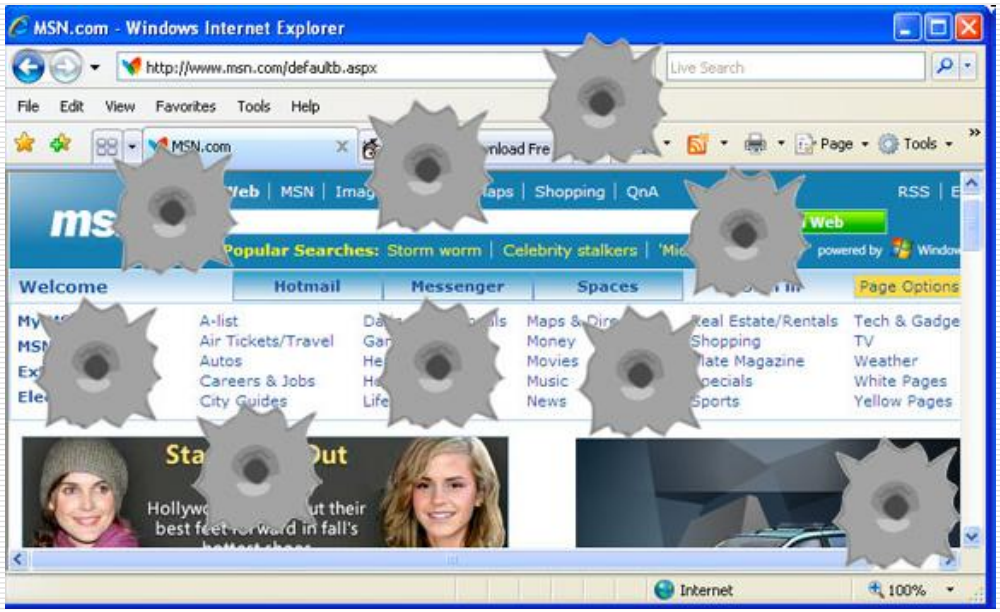
Факторы роста

- Миграция приложений в сеть – снижает расходы на безопасность
  - SaaS – Software as a service
  - PaaS – Platform as a service
  - IaaS – Infrastructure as a service
- Доступность стойкой криптографии – ограничения со временем ослабляются

Факторы риска

- Отличия сетевой защиты от физической
  - Небольшое изменение в защите может сколь угодно сильно повлиять на стойкость
    - Debian RAND()
  - Сложность программ препятствует их анализу
  - Возможности по анализу сильно отстают от скорости смены версий ПО

Разнообразие задач



- Строгие механизмы…
  - Разграничение доступа, аутентификация, авторизация
  - Обеспечение конфиденциальности
  - Управление доверием
- … из-за обилия дыр
- … становятся не такими строгими
  - Intrusion Detection & Prevention Systems
  - Web Application Firewalls
  - AV software…

…подчёркивают процессную сущность обеспечения информационной безопасности

Разнообразие средств

- Сканеры безопасности
- Анализаторы исходного кода
- Межсетевые экраны
- Системы обнаружения атак
- Виртуальные частные сети (VPN)

Стек протоколов TCP/IP

- Иерархия протоколов, как средство борьбы со сложностью
- Открытые системы
  - многоуровневость
  - интерфейсы
  - правила взаимодействия и композиции
- Назначение каждого уровня
  - обеспечить определенный сервис верхним уровням
  - сделать независимыми верхние уровни от деталей реализаций сервиса на нижних уровнях
- В сети уровень n на одной машине отвечает за установление и поддержку связи с уровнем n на другой машине.
- Протокол – правила, соглашения, структуры данных, для установления, поддержки связи и передачи данных между **одинаковыми** уровнями на **разных** машинах

Стек протоколов TCP/IP

Стек протоколов TCP/IP

- ***Физический уровень*** отвечает за передачу последовательности битов через канал связи. Вопросы кодирования битов физическими сигналами в соотв. среде.
- Основная задача ***канального уровня*** - превратить несовершенную среду передачи в надежный канал, свободный от ошибок передачи.
  - разбиение на кадры
  - определение границ кадров
  - исправление ошибок при передаче на физическом уровне
  - уничтожать дубликаты кадров
  - минимизировать затраты на служебные кадры (piggy backing)
  - регулировать доступ к каналу с множественным доступом (MAC подуровень)

Стек протоколов TCP/IP

- ***Сетевой уровень*** отвечает за функционирование транспортной подсети
  - Основная задача маршрутизировать пакеты от отправителя к получателю
    - два вида протоколов
      - по вектору расстояния
      - по состоянию канала
    - policy routing
      - автономные системы, BGP
  - глобальная адресация – IPv4, IPv6
  - Internet Exchange Points

Стек протоколов TCP/IP

- Проблемы безопасности уровня IP
  - Не обеспечивает надёжную идентификацию отправителя и получателя
  - Не защищает данные от перехвата
  - Не контролирует целостность данных
  - Отправитель и получатель не контролируют маршрут
- Виды атак на уровне IP:
  - ARP spoofing
  - MITM
  - Атаки на маршрутизацию (BGP poisoning)

Стек протоколов TCP/IP

- Сетевой уровень – стандартные утилиты
  - ping – клиент к протоколу ICMP (Internet Control Message Protocol)
  - traceroute (tracert для win*) – анализ маршрутов

```
~> ping -s 10000 secsem.ru
PING secsem.ru (158.250.17.104) 10000(10028) bytes of data.
10008 bytes from redsecure.lvk.cs.msu.su (158.250.17.104): icmp_req=1 ttl=63
time=1.03 ms
…
--- secsem.ru ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 1.003/1.062/1.184/0.063 ms
~> ping -s 10000 kremlin.ru
PING kremlin.ru (195.208.24.91) 10000(10028) bytes of data.
^C
--- kremlin.ru ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3007ms

~> traceroute whitehouse.gov
traceroute to whitehouse.gov (95.101.0.110), 30 hops max, 60 byte packets
 1  gate.lvknet (192.168.128.254)  0.758 ms  0.734 ms  0.725 ms
 2  cmc-cmc.dept-vl171.cmc.msu.net (193.232.127.33)  1.390 ms  1.508 ms  1.553 ms
 3  msu-cmc-core-vl501.leo.msu.net (193.232.127.93)  26.469 ms  26.513 ms  26.506 ms
 4  m9-leo-core-vl350.sphinx.msu.net (193.232.127.13)  1.687 ms  2.004 ms  2.080 ms
 5  m9-1-gw.msk.runnet.ru (194.190.255.233)  2.053 ms  2.051 ms  2.041 ms
 6  m9-1-gw.msk.runnet.ru (194.85.40.213)  47.719 ms  47.064 ms  47.055 ms
 7  b57-1-gw.spb.runnet.ru (194.85.40.134)  44.957 ms  44.640 ms  44.839 ms
 8  kt12-1-gw.spb.runnet.ru (194.85.40.154)  44.838 ms  44.828 ms  44.833 ms
 9  tug11-1-gw.sth.runnet.ru (194.85.40.142)  44.856 ms  45.113 ms  45.108 ms
10  hikhef-1-gw.ams.runnet.ru (194.85.40.241)  45.178 ms  59.956 ms  59.970 ms
11  amsix-ams6.netarch.akamai.com (195.69.145.208)  45.193 ms  44.969 ms  44.938
ms
12  * * *
```

Стек протоколов TCP/IP

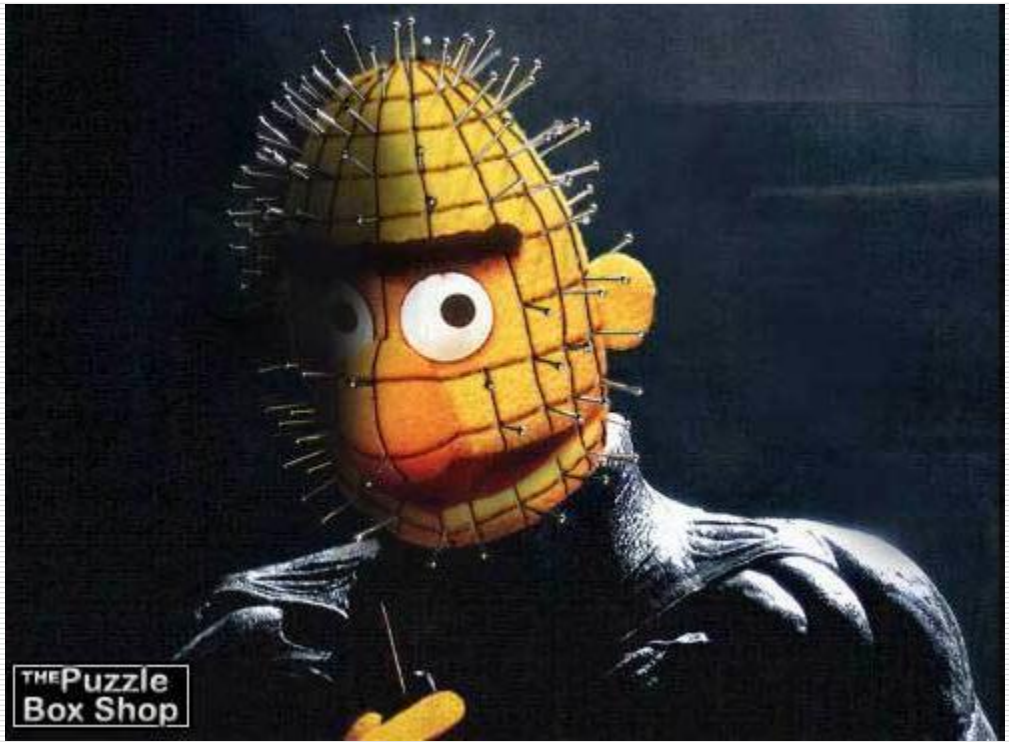
- Основная функция ***транспортного уровня*** это: принять данные с уровня приложений, передать на сетевой уровень и позаботиться, чтобы все они дошли до адресата в нужном порядке и целиком
- Основные протоколы:
  - TCP – Transmission Control Protocol
  - UDP – User Datagram Protocol

Стек протоколов TCP/IP

- Проблемы безопасности на транспортном уровне:
  - ресурсоёмкость TCP – основа для DDoS-атак
  - нет контроля целостности и конфиденциальности данных
  - ранние реализации уязвимы к подбору ISN и реализации MITM

Стек протоколов TCP/IP

- Уровень приложений



...это ужас