

2015
ZERO NIGHTS

Базовые приемы цифровой контрацепции и гигиены личных данных

- Интернет задумывался как доверенная среда для квалифицированных и ответственных пользователей: военных, ученых, университетов
- Снижение порога вхождения
удешевление доступа в интернет, дешевые компьютеры и смартфоны
- Проникновение в большинство сфер жизни со всеми последствиями
коммерция, банки, государственные услуги, социальные сети

Халатное отношение к приватности

- **Добровольное раскрытие подробностей частной жизни**
состав семьи и близкие, геометки с домашним адресом, интересы, хобби
- **Общедоступные базы информации**
позволяют найти полную информацию о личности, имея малую часть данных

Заблуждения

- **Мне нечего скрывать**
Почему неверно?
- **Угрожает не только вам, но и окружающим**
чтобы прочитать вашу переписку, достаточно взломать кого-то, кто с вами общается

Халатное отношение к приватности

★ «Наивность жертв определяется специальным скриптом»: злоумышленник рассказал о заработке сотен тысяч рублей на «угоне» айфонов

11 ноября нижегородский программист Артём Куликов [сообщил](#) о мошенниках, которые обманом заставляют пользователей сети ввести на айфоне чужие данные iCloud, удалённо блокируют смартфон и затем требуют деньги за его разблокировку. Взломавший друга Куликова мошенник рассказал TJ о том, как ведёт свой «бизнес».

«Программа ищет наивных людей. Наивность определяется по наличию на странице репостов различных розыгрышей и записей, сгенерированных приложениями «ВКонтакте».

злоумышленник

★ Американский чиновник потратил четыре года и 35 тысяч долларов, чтобы найти анонимного автора обидного комментария

Глава окружного совета из небольшого американского городка Фрипорт, избираясь на этот пост в 2011 году, был оскорблён анонимным комментарием в свой адрес на сайте местной газеты и решил найти обидчика. В течение почти четырёх лет он потратил 35 тысяч долларов и всё-таки узнал, кто оскорбил его, но оказался не удовлетворён результатом. Его историю рассказало издание [The Verge](#).

Халатное отношение к приватности



Анна Знаменская

20 сентября · отредактировано · 🌐

Вы еще не слышали про экшн "Преступная группировка #билайн?
Сегодня - вторая серия!

Месяц назад неизвестные лица получили мою симкарту в "Билайне" без документов. Попытались вскрыть Яндекс.Кошелек, хакнули все почты, пришлось поменять все банковские карты (Вы представляете, что это такое??)

Компания якобы провела расследование и заявила, что "нарушения устранены, виновные привлечены и это никогда не повторится". Мне даже зачислили 2000 рублей на счёт в качестве компенсации (!:))

Однако..

Позавчера в 18 часов вечера моя симкарта снова была выдана неизвестным лицам! И сразу были украдены деньги с Яндекса по одноразовому паролю. Проведя вечер субботы в офисе Билайна, и вспомнив всю ненормативную лексику, я заменила симкарту.

Наутро, вчера, в 12 часов дня моя сим-карта СНОВА была выдана посторонним лицам в городе Екатеринбурге!!

Я снова приехала в офис Билайна за новой симкой.

И ... Через 43 минуты (!!) после этого моя карта была вновь выдана в офисе Билайна кому-то, теперь уже в городе Омске!!!

Как обезопасить себя

- **Социальная гигиена и выбор друзей**
не рассматриваются в данном воркшопе

О чем воркшоп?

- О недопущении утечки данных с технической точки зрения
- О средствах для обеспечения сетевой безопасности и анонимности коммуникаций
- О типичных ошибках при использовании спецсредств

Уровни OSI

Транспортный и
прикладной

Сетевой

Физический
и канальный



Канальный уровень

- Трекинг беспроводных устройств по MAC-адресу



Сетевой уровень

- Публичный IP — звонок провайдеру, определение местоположения с точностью до города (особенно актуально на мобильных)
- Опасности IPv6: по умолчанию включен во всех ОС, приоритетнее, чем IPv4, получить можно в любой момент, вы его уже используете
- В середине 2014 года, 6 из 11 роутеров не блокировали IPv6.

IPv6

- Router advertisement
- SLAAC
- DHCPv6

Сетевой уровень

```
valdikss@valaptop ~ % ping6 -c2 ff02::1%wlp3s0
PING ff02::1%wlp3s0(ff02::1) 56 data bytes
64 bytes from fe80::223:15ff:fe5b:240c: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from fe80::76d4:35ff:fe48:c561: icmp_seq=1 ttl=128 time=3.11 ms (DUP!)
64 bytes from fe80::96de:80ff:fe4b:3a6a: icmp_seq=1 ttl=64 time=3.16 ms (DUP!)
64 bytes from fe80::9eeb:e8ff:fe19:91d1: icmp_seq=1 ttl=64 time=3.18 ms (DUP!)
64 bytes from fe80::2c0:caff:fe82:1241: icmp_seq=1 ttl=64 time=130 ms (DUP!)
64 bytes from fe80::9e4e:36ff:fea1:5be4: icmp_seq=1 ttl=64 time=137 ms (DUP!)
64 bytes from fe80::3275:12ff:fedc:2a6e: icmp_seq=1 ttl=255 time=137 ms (DUP!)
64 bytes from fe80::5a12:43ff:fe17:15a4: icmp_seq=1 ttl=255 time=142 ms (DUP!)
64 bytes from fe80::3abc:1aff:fe24:f202: icmp_seq=1 ttl=64 time=153 ms (DUP!)
64 bytes from fe80::491e:b86a:2b2a:385c: icmp_seq=1 ttl=64 time=153 ms (DUP!)
64 bytes from fe80::6aa8:6dff:fe44:9842: icmp_seq=1 ttl=64 time=153 ms (DUP!)
64 bytes from fe80::4ca:de93:9d93:3df4: icmp_seq=1 ttl=64 time=157 ms (DUP!)
64 bytes from fe80::1849:8a21:3f46:2341: icmp_seq=1 ttl=64 time=180 ms (DUP!)
64 bytes from fe80::1438:b840:9330:aa93: icmp_seq=1 ttl=64 time=180 ms (DUP!)
64 bytes from fe80::4cf:87c0:5793:be20: icmp_seq=1 ttl=64 time=180 ms (DUP!)
64 bytes from fe80::7a31:c1ff:fed4:c600: icmp_seq=1 ttl=64 time=200 ms (DUP!)
64 bytes from fe80::a288:b4ff:febf:cfc0: icmp_seq=1 ttl=64 time=200 ms (DUP!)
64 bytes from fe80::20c:29ff:fe76:2cef: icmp_seq=1 ttl=64 time=200 ms (DUP!)
64 bytes from fe80::22c9:d0ff:fe7d:5a49: icmp_seq=1 ttl=64 time=203 ms (DUP!)
64 bytes from fe80::a288:b4ff:fe53:f548: icmp_seq=1 ttl=64 time=203 ms (DUP!)
64 bytes from fe80::104c:4424:c0f6:f34: icmp_seq=1 ttl=64 time=203 ms (DUP!)
64 bytes from fe80::1869:cbbe:b25f:4304: icmp_seq=1 ttl=64 time=225 ms (DUP!)
64 bytes from fe80::b9c3:3151:1cb8:9a27: icmp_seq=1 ttl=64 time=358 ms (DUP!)
64 bytes from fe80::52b7:c3ff:fe27:1399: icmp_seq=1 ttl=64 time=363 ms (DUP!)
64 bytes from fe80::223:15ff:fe5b:240c: icmp_seq=2 ttl=64 time=0.111 ms

--- ff02::1%wlp3s0 ping statistics ---
2 packets transmitted, 2 received, +23 duplicates, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.028/155.097/363.778/94.597 ms
```

How Tor helped catch the Harvard bomb threat suspect

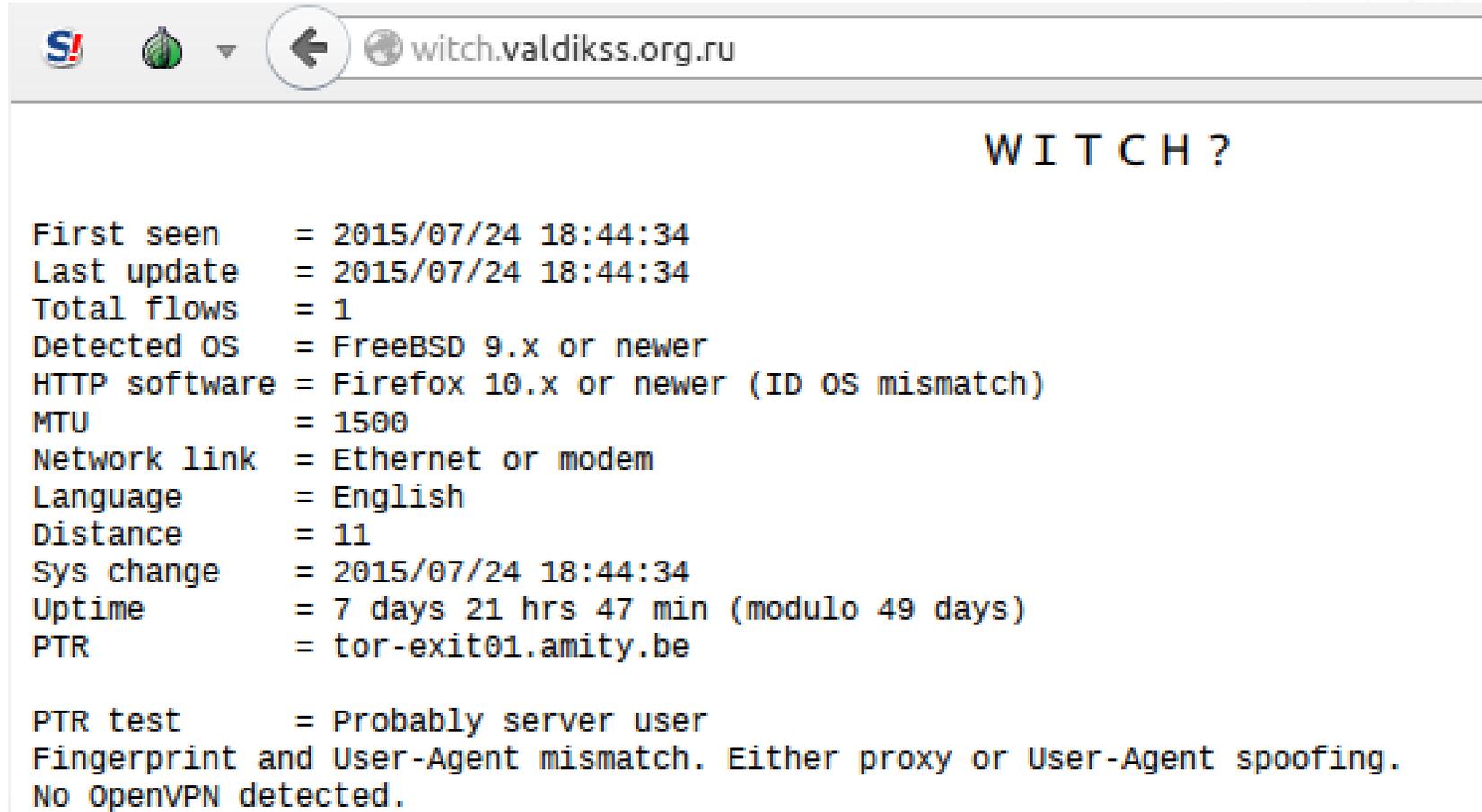
Dec 18, 2013, 10:26am CT | Last updated Dec 18, 2013, 10:29am CT

A Tor circuit is defined by the nodes that a message traverses and where it enters and exits, employing a concept called [onion routing](#). While the [list of Tor exit nodes](#) is publicly available, “relays” where connections enter are known as well. The IP address of the exit node used by the suspect was included in a header labeled ‘X-Originating-IP,’ which is tacked onto emails sent from GuerillaMail by default, and that IP also would have appeared in their access logs. On the other hand the address of the entry node, and the suspect's connection to it, could be observed by Harvard via [metadata](#) analysis of a traffic flow log on their network during the time in question. It’s trivial to correlate an IP address with Tor at either end of the equation.

Транспортный уровень

- Особенности реализаций TCP-стека
- TCP Timestamps (определение uptime)
- Разный MTU

Транспортный уровень



The screenshot shows a web browser window with the address bar containing `witch.valdikss.org.ru`. The main content area displays the output of a network analysis tool, titled "WITCH?". The output lists various connection details:

```
WITCH?  
  
First seen      = 2015/07/24 18:44:34  
Last update    = 2015/07/24 18:44:34  
Total flows    = 1  
Detected OS    = FreeBSD 9.x or newer  
HTTP software  = Firefox 10.x or newer (ID OS mismatch)  
MTU            = 1500  
Network link   = Ethernet or modem  
Language       = English  
Distance       = 11  
Sys change     = 2015/07/24 18:44:34  
Uptime         = 7 days 21 hrs 47 min (modulo 49 days)  
PTR            = tor-exit01.amity.be  
  
PTR test       = Probably server user  
Fingerprint and User-Agent mismatch. Either proxy or User-Agent spoofing.  
No OpenVPN detected.
```

Прикладной уровень

- Спонтанные утечки данных через мобильные приложения
- Утечки DNS
- Раскрытие IP при использовании Skype, браузеров (WebRTC), почты, открытия офисных документов и PDF
- UPnP

Прикладной уровень

Viber, a mobile messenger app that allows users to make phone calls and send text messages and images for free, also gives up plenty of free user data to anyone who wants to listen.

According to researchers from the University of New Haven (UNH) in Connecticut, US, Viber's app sends user messages in unencrypted form – including photos, videos, doodles, and location images.

All of that rich data from users is also stored unencrypted on Viber's servers, rather than being deleted immediately, and is accessible without credentials, just a link, the [UNH researchers said](#).

It's the second cryptographic blunder exposed by UNH researchers in as many weeks – the *UNH Cyber Forensics Research & Education Group* disclosed on 13 April 2014 that the [WhatsApp](#) messenger app also gives away user location data in unencrypted form.

Using a Windows PC as a Wi-Fi access point, the UNH team was able to capture data sent by an Android smartphone with regular traffic sniffing tools, the same approach taken by UNH in their experiments with WhatsApp.

Прикладной уровень

Capturing from 2 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.102.20	192.168.102.1	DNS	65	Standard query 0x2753 A ya.ru
2	0.00021300	192.168.102.20	192.168.102.1	DNS	65	Standard query 0x9a3e AAAA ya.ru
3	-0.0003800	192.168.5.198	192.168.5.1	DNS	65	Standard query 0xaf9 A ya.ru
4	0.00553200	192.168.5.1	192.168.5.198	DNS	244	Standard query response 0xaf9 A 213.180.193.3 A 213.180.204.3

Командная строка

```
C:\Users\vboxten>ping ya.ru

Обмен пакетами с ya.ru [213.180.193.3] с 32 байтами данных:
Ответ от 213.180.193.3: число байт=32 время=15мс TTL=58
Ответ от 213.180.193.3: число байт=32 время=16мс TTL=58
Ответ от 213.180.193.3: число байт=32 время=19мс TTL=58
Ответ от 213.180.193.3: число байт=32 время=16мс TTL=58

Статистика Ping для 213.180.193.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 15мсек, Максимальное = 19 мсек, Среднее = 16 мсек

C:\Users\vboxten>
```

Прикладной уровень

```
./log.txt.2015-04-11:11:17:12 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:11:17:13 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:11:26:23 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:11:26:26 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:11:37:45 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:11:38:16 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:11:38:19 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:11:41:00 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:11:54:29 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:12:04:10 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:12:05:30 lekcjoner 46.39.229.16 22522 192.168.1.40 22522
./log.txt.2015-04-11:12:05:30 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:12:05:31 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:12:35:08 lekcjoner 46.39.229.16 22522 192.168.1.40 22522
./log.txt.2015-04-11:12:35:08 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:13:10:17 lekcjoner 46.39.229.16 22522 192.168.1.40 22522
./log.txt.2015-04-11:13:10:17 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:13:13:34 lekcjoner 46.39.229.16 22522 192.168.1.40 22522
./log.txt.2015-04-11:13:13:34 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:13:13:34 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
./log.txt.2015-04-11:13:13:35 lekcjoner 81.23.13.2 65231 192.168.136.136 65231
```

Прикладной уровень

```
Message-Id: <1511f5d00b7-4bff-36b4@webprd-a10.mail.aol.com>  
In-Reply-To: <564DA897.8000501@[REDACTED]>  
Subject: =?UTF-8?Q?Re:  
MIME-Version: 1.0  
Content-Type: multipart/alternative;  
    boundary="-----=_Part_17740_1438786202.1447930167478"  
X-MB-Message-Source: WebUI  
X-MB-Message-Type: User  
X-Mailer: JAS STD  
X-Originating-IP: [188.162.64.[REDACTED]]  
x-aol-global-disposition: G  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mx.aol.com;  
    s=20150623; t=1447930168;  
    bh=bR9Ws9Sp0699oDQPhdo03vjfal1iy0mcqN+2j70m3dY=;  
    h=From:To:Subject:Message-Id:Date:MIME-Version:Content-Type;  
    b=RlE518MBqdzXXIaKn1Y/R0ga+W6KcgU6owR4cLqdvEhpPe1rPIagx5JPWS3ExQJt+
```

Прикладной уровень

Demo for: <https://github.com/diafygi/webrtc-ips>

This demo secretly makes requests to STUN servers that

Your local IP addresses:

- 172.20.32.255
- 10.10.10.45

Your public IP addresses:

- 94.155. [REDACTED]
- 95.158. [REDACTED]

- Правильная настройка зашифрованного туннеля по протоколам IPsec IKEv1/IKEv2 и OpenVPN
- Использование PGP на примере GnuPG для сохранения секретности переписки и подтверждения авторства написанного

IPsec IKEv2 vs OpenVPN

IPsec IKEv2	OpenVPN
Встроен в большинство десктопных и мобильных ОС (Windows, OS X, iOS, Android, Windows Phone, Blackberry), не требует установки сторонних программ	Необходимо установить OpenVPN. Работает на Windows, Linux, OS X, Android, iOS.
Аутентификация по сертификатам и/или EAP (Расширяемый Протокол Аутентификации). Использует системное хранилище ключей.	Аутентификация по сертификатам и дополнительно по логину и паролю.
Использует свой сетевой протокол, возможна инкапсуляция в UDP по фиксированным портам	Используется инкапсуляция в TCP или UDP на любом порту
Различные (плохие) реализации	Почти нет сторонних реализаций, работает одинаково хорошо на всех платформах с незначительными отличиями
Фиксированные стандартизированные группы DH	Любые группы DH
Быстрое переключеение при смене сети (MOBIKE)	Нет быстрого переключеения в текущей стабильной версии

- Два подхода с IPsec: аутентификация с использованием сертификатов (RSA, ECDSA) и аутентификация по логину и паролю (EAP-MSCHAPv2)
- <https://github.com/ValdikSS/easy-rsa-ipsec> — удобный генератор сертификатов для OpenVPN и IPsec
- Необходимо:
 - Настроить VPN так, чтобы не было утечек через Wi-Fi хакера
 - Настроить VPN в режиме VPN-only

«Говорить красным»

суббота

-  привет 19:02
- Привет, Паш 19:06
-  слушай, Макс
у меня просьба 19:06
- ну 19:07
-  у тебя есть деньги, на карте,занять? 19:09

суббота

-  до вторника 19:09
- смотря сколько 19:11
-  хотя бы 7 т.р. нужно
в идеале, больше(19:11

да не вопрос, куда кидать? 19:12

я убегаю через 10 минут, так что не тормози) 19:14

 на киви смож? 19:15

можно 19:16

 немного больше 7 сможешь?
тебе вернуть на карту? или если тоже на киви, то пойдет?
мне без разницы, в принципе 19:17

ну 10 от силы смогу 19:17

 мне 9 хватит
займешь? 19:17

вернуть можешь лично потом)
9 ок 19:18

«Говорить красным»

[5:17:49 PM] **ValdikSS:** Короч, у меня ж украли все карты, есть только одна карта киви

[5:17:50 PM] **Pavel Zhovner:** я могу пополнять киви с вебмани

[5:17:54 PM] **ValdikSS:** Вот мне на киви нужны деньги

[5:17:56 PM] **Pavel Zhovner:** чооооо

[5:17:58 PM] **ValdikSS:** Можешь? У тебя привязано?

[5:18:02 PM] **Pavel Zhovner:** украли?!

[5:18:12 PM] ... а ну-ка красным

[5:18:15 PM] **ValdikSS:** Ну я в бункере писал

[5:19:02 PM] ... / -----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

У меня украли деньги ночью. Кошелек. Из общаги. Там налички было всего рублей 300, но, блин, все банковские карты и водительское удостоверение.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v2

Comment: <https://keybase.io/valdikss>

iQIcBAEBCAAGBQJVHqFQAAoJEFzXIC7viPdyw38P/jk4rEiaBeHl7mpNqpK7de0b
3f/4754pFx/cDATSA053Yck9BbHp0mYK/LAJp2VH0a9WCz9WQmcwyUD0i5fxE+YB

- Генерация сертификатов
- Публикация сертификатов на key server
- Подпись ключей проверенных людей
- Передача зашифрованных сообщений и файлов
- Подпись открытых сообщений

Подтверждение OTR

