The New New Internet

Johannes B. Ullrich Ph.D.

Dean of Research, STI

jullrich@sans.edu

SANS Technology Institute

The best. Made better.

About Me

- Dean of Research,
  SANS Technology Institute
- SANS Internet Storm Center
  https://isc.sans.edu
- Created DShield.org
- SANS Fellow
- Past: Physicist, Web Developer
- Living in Jacksonville, FL

SANS Technology Institute

What is the "Internet Storm Center"

- Global Network Security Information Sharing Community
  - Participants from dozens of countries
  - Automated as well as manual sharing of network security incident information
  - Many ways to share and consume data (always evolving)
  - Still a strong hobbyist base, but also many "commercial" users
  - Data made available via website in real time with little filtering. Often shared with researchers

Agile Honeypots

SANS Technology Institute

Myths About Participating

- My Data Isn't Important
  - In particular home / small business data is important. We are not looking for the latest APT. We are looking for attacks that matter
- My Employer Doesn't Let me
  - Submit your home network data ☺
- It is difficult to submit data
  - That is part of the fun!

SANS Technology Institute

The Good Old Internet ("The Web")

- Two (Three) Protocols dominate:
  - DNS: Helps you find stuff
  - HTTP: Delivers Exploits
  - (SMTP: Delivers Links to Exploits)

The New Internet

- Perimeters
- VPNs
- Private ”Internets”
- Encrypt important data

SANS Technology Institute

Privacy / Security Issues: DNS

- Weak authentication (QueryID)
  - Spoofing DNS possible
  - MitM trivial
- No confidentiality
  - Easy to profile users
  - Often used by Corporations/ISPs/Countries to analyze traffic patterns

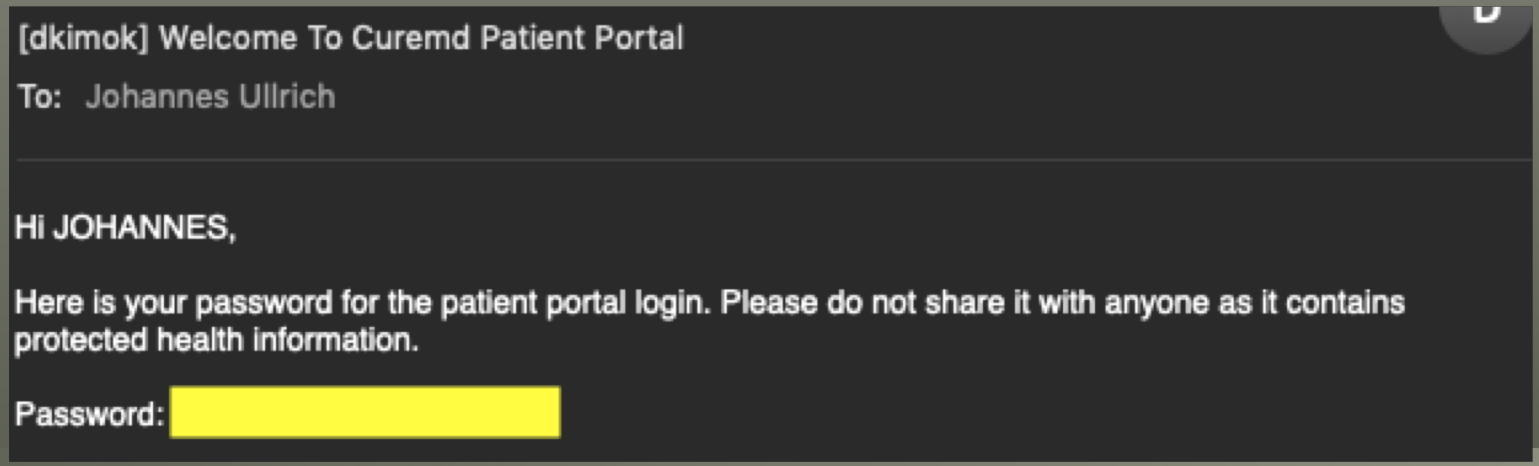
Privacy / Security Issues: HTTP

- Clear Text, not authenticated
  - Trivial MitM
  - Spoofing protection due to TCP
  - Very verbose: Referrer, Server, User-Agent header

```
POST /api/x?tVpmt3ZlJDExNzk0JDI3eDI5NA HTTP/1.1
Host: api-54-214-210-145.b2c.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10_14_1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/70.0.3538.102 Safari/537.36
```

SMTP

- No sender authentication
- No encryption. All clear text (S-MIME/PGP is NOT part of SMTP)
- Trivial MitM Attacks
- Verbose (mail client and server identification)



SANS Technology Institute

DNSSEC

- HTTP (and to a less extend SMTP) can use TLS. Not a great fit for DNS (more about that later)
- Very complex protocol
- Easy self inflicted DoS
- Enables some reflective DoS attacks
- Does not provide confidentiality
- Only offers (solid) message integrity protection

DEMO

DNSSEC

SANS Technology Institute

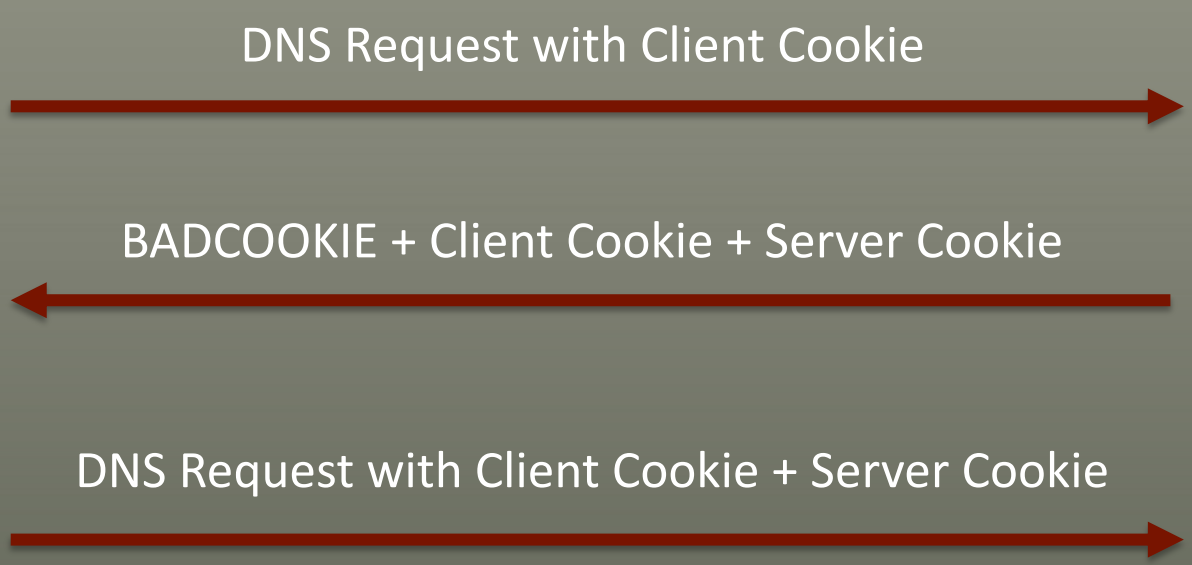
Introducing DNS Cookies RFC 7873

- Very simple security mechanism.
- Doesn’t solve all problems, but solves the important once
- Easy to enable, unlikely to break stuff
- Already in BIND

What are these cookies ?

- Implemented as a DNS Option (Option type 10)
- Client cookie: Hash(Client IP, Server IP, 8+ Bytes Secret)
- Included in first request to a server
- Server cookie: Hash(Client IP, Secret, Client cookie)

How is it supposed to work?



Other Options

- Client doesn’t send a cookie: Server will respond
- Malformed Cookies: FORMERR
- Only a client cookie is sent:
  - Discard the request
  - BADCOOKIE error
  - Respond as normal, but include cookie (in particular over TCP)
- Wrong server cookie: ignore.

NAT / Load Balancing

- The cookie is a pseudo random value unique to the client / server
- IP address doesn't really matter. Cookie just has to be consistent
- Typically, DNS server determines random secret on start. But a fixed secret could be configured for load balanced servers
- Cookies should be cached for up to 300 seconded (recommended 150 seconds)
- Secrets should be rotated 1 day-1 month.

Demo

DNS Cookies

SANS Technology Institute

Privacy in DNS

https://isc.sans.edu

Recursive Nameserver

Authoritative Nameservers

DNS over TLS (RFC 7858)

- Only works between stub clients and servers
- Substantial overhead in establishing TLS
- TCP Port 853
- TLS session is reused for multiple queries
- Only one session should be used

DNS over TLS Pros/Cons

- “Next Hop” (ISP) can not longer intercept DNS queries
- DNS queries are encrypted until they reach the resolver
- [insert all the TLS pros/cons here]
- Configuration isn’t difficult and starts to show up in various software
- DNS provider now becomes now single interception point

DNS over HTTPS (DoH)

- Experimental but starts to show up in browsers
- Uses a new MIME type: application/dns-message
- Particularly suited for HTTP/2, server push
- Data transmitted encapsulated in JSON and sent to

https://dns.google.com/resolve?

https://dns.google.com/resolve?name=isc.sans.edu&type=A

SANS Technology Institute

```
{
  "Status": 0,
  "TC": false,"RD": true,"RA": true,"AD": false,"CD": false,
  "Question": [
    {"name": "isc.sans.edu.","type": 1}
  ],
  "Answer": [{
      "name": "isc.sans.edu.",
      "type": 1,"TTL": 9,
      "data": "204.51.94.153"
    }],
  "Comment": "Response from dns31a.sans.org.(66.35.59.8)."
}
```


SANS Technology Institute

Pros/Cons

- Very similar to DNS over TLS
+ Additional anonymity. DNS traffic not distinguishable from HTTP traffic
+ More difficult to block
- Creates New Choke Points (DoH endpoints)
- Substantially more expensive if JSON is used, but can accept “UDP wire format”(still requires HTTP overhead)
- Removes insight into DNS traffic for operators (unless substantial investment is made to intercept all TLS traffic)

Paul Vixie on DoH

Paul Vixie
@paulvixie

Follow

Replying to @grittygrease

Rfc 8484 is a cluster duck for internet security. Sorry to rain on your parade. The inmates have taken over the asylum.

2:49 PM - 20 Oct 2018

DoH is an over the top bypass of enterprise and other private networks. But DNS is part of the control plane, and network operators must be able to monitor and filter it. Use DoT, never DoH.

SANS Technology Institute

Implementations

- See dnsprivacy.org
- For BIND: Use a proxy like “stubby”
- Linux/BSD based routers: unbound
- DoH is often implemented in the browser (e.g. Firefox)
- Android support for DNS over TLS

Demo

DNS Over TLS / DNS Over HTTPS

SANS Technology Institute

But What About HTTP(S)?

- TLS 1.3 is finally “done”!
- Improvements in speed and security
- Less fingerprinting (not really true yet)
- Less information leaked (not really true yet)

Features Added/Removed

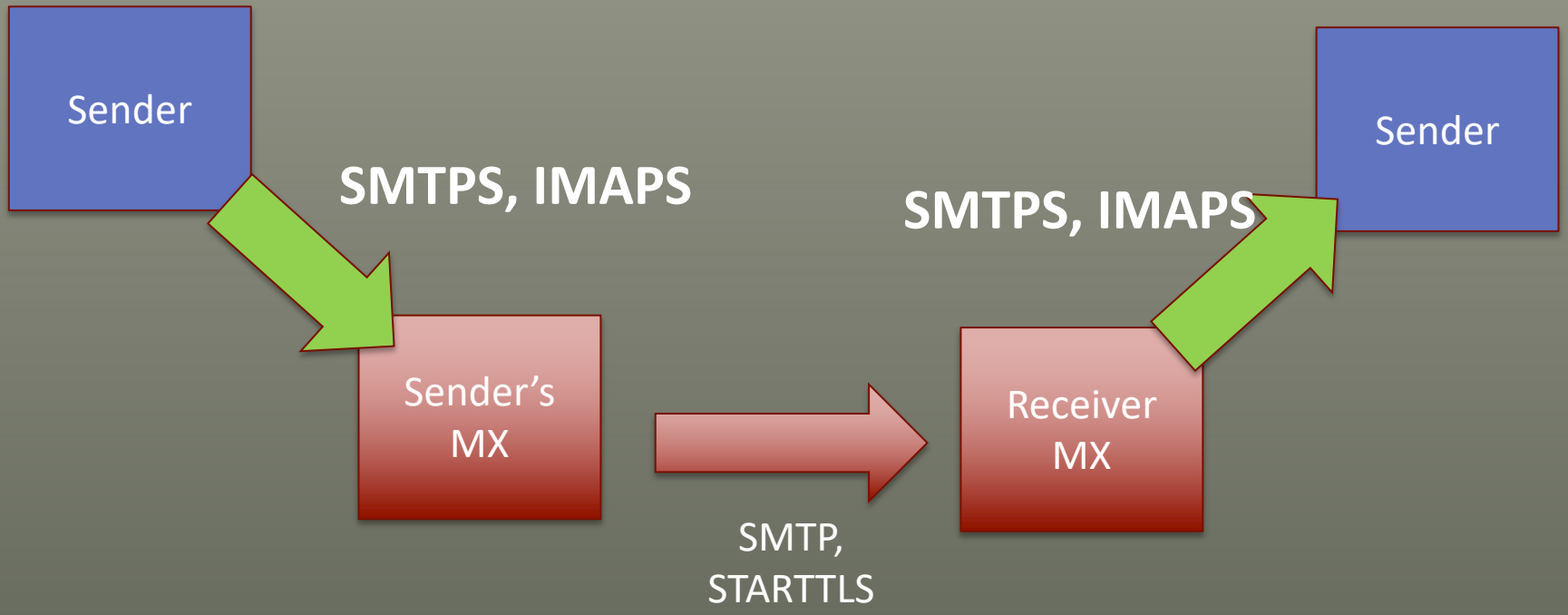
Removed	Added
• Static RSA handshake • CBC MtE modes • RC4 • SHA1, MD5 • Compression • Renegotiation	• Full handshake signature • Downgrade protection • Abbreviated resumption with optional (EC)DHE • Curve 25519 and 448

Faster Handshake

TLS 1.2	TLS 1.3
Client Hello	Client Hello
Server Hello (Certificate)	Server Hello (Key Share, Certificate..)
Client Key	**HTTP Request**
Change Cipher Spec	
HTTP Request	

Any hope for SMTP?

- Clients are moving to HTTPS
- Some web clients now implement end-to-end encryption that is transparent to the user
- But even current end-to-end encryption schemes assume the integrity of the web server
- Email is often forwarded from server to server providing for frequent opportunities to intercept and email



What's STARTTLS?

- Optional SMTP security
- Upgrades existing (port 25) connection using TLS
- However: Initial negotiation happens in the clear
- Attacker may modify / remove STARTTLS message

EFF STARTTLS Everywhere

https://www.starttls-everywhere.org/

SANS Technology Institute

MTA STS

- Mail Transport Agent Strict Transport Security” (HSTS like. There is also SMTP STS)
- RFC 8461
- Uses mix of DNS and HTTPS to discover policies
- Simpler than DANE (does not require DNSSEC)

SANS Technology Institute

MTA STS Policy discovery

- DNS TXT Record:
- _mta-sts.example.com. IN TXT "v=STSv1; id=20160831085700Z;”
- https://mta-sts.example.com/.well-known/mta-sts.txt

SANS Technology Institute

```
version: STSv1
mode: enforce
mx: mail.example.com
mx: *.example.net
mx: backupmx.example.com
max_age: 604800
```

SANS Technology Institute

Thank You!

Questions?

jullrich@sans.edu

http://isc.sans.edu

Daily Updates * Daily Podcast * Data Feeds

Twitter: @johullrich / @sans_isc

SANS Technology Institute