Oct 11th, 10:15 AM - 11:05 AM

Internet Core Functions: Security Today and Future State

Jeffrey Jones

Abstract
Never in the history of the world has so much trust been given to something that so few understand. Jeff reviews three core functions of the Internet along with recent and upcoming changes that will impact security and the world.

Location
KSUC 300

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Internet Core Functions : Security today and future state

Jeff Jones, CISSP GPEN

October 2019

I thought I understood the scope of this presentation. I was wrong.

End User Licensing Agreement

This is an agreement between the presenter, Jeff, and the audience, you. Jeff is not responsible for anything said, implied, gestured or presented in any way. You are responsible for incredibly undivided attention and loud rousing applause during and at the end of the presentation. Any semblance of this security presentation to an actual security presentation should be considered coincidental. Your silence will be considered as an acceptance of this agreement.

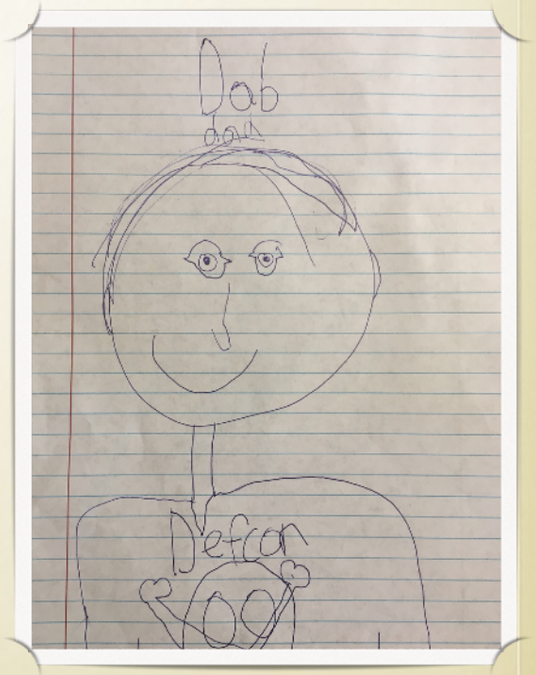
All opinions, beliefs, statements, and material in this presentation reflect my own personal beliefs and do not reflect the opinions or beliefs of my employer.

I don't read my slides.
My deck is more for those that see it without listening to me
I've put a lot sources for each slide in the notes.

Autobiography

Jones: Internet Core Functions: Security Today and Future State

- Emory University BA Sociology
- Southern Polytechnic State University BS CpET-Controls
- Recent Work History
  - Internal Consultant/Application Security and Project Review
  - Threat Intelligence/Level 3 Incident Response
  - Threat Hunter



Some of these slides are a wall of text. They are meant more to be like images showing the volume of the topic I'm discussing. The content is legitimate, but don't assume I'm going to review the details. If you are interested, please download and review later.

I have to leave after this presentation so I won't be around for questions.
My email is ……. Or you can get my contact info from Herb Mattord.

A Few Questions First

Who believes that at some point in the future there will be a great cyber war?

US destroying Iran's missile defense computers, NotPetya, Ukraine power station attacks, Iran centrifuges destroyed, Iran DDoSed banks

Who believes that this war will NOT be limited to only military targets and include civilian targets?

Who believes that if there were a great cyber war that critical infrastructure like electrical power, commerce, satellites, etc… will have limited or no functionality?

Could a satellite be directed out of orbit to bomb a city?

Who believes that during a great cyber war that civilians like Anonymous, cybercriminals, bot herders, and countless other civilian hackers will engage in rouge cyber attacks?

If most of us agree that this is an eventuality, what is being done to prevent it?

The people who write the software for the Internet are the most critical in preventing attacks.

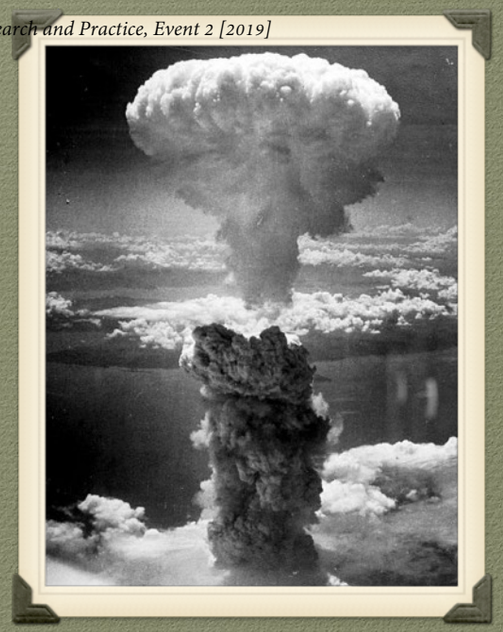
How many classes on writing secure code are required at your schools?

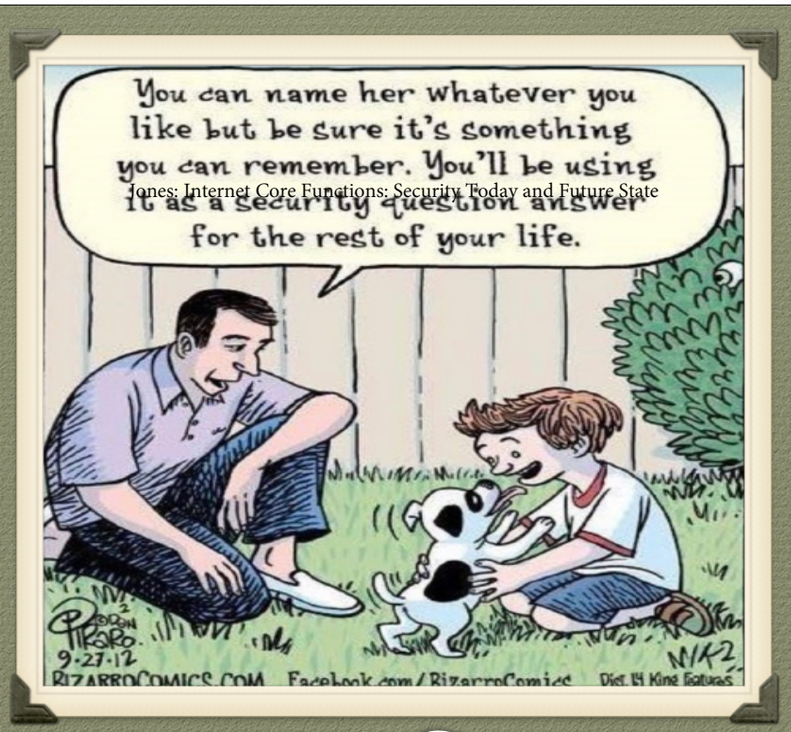
Why is an Introduction to Security not required for all students?

Is your university or college involved in the organizations that set the standards for Internet communications like the IETF and CA/B Forum?

At Some Point Securing the Internet will Become Very Important

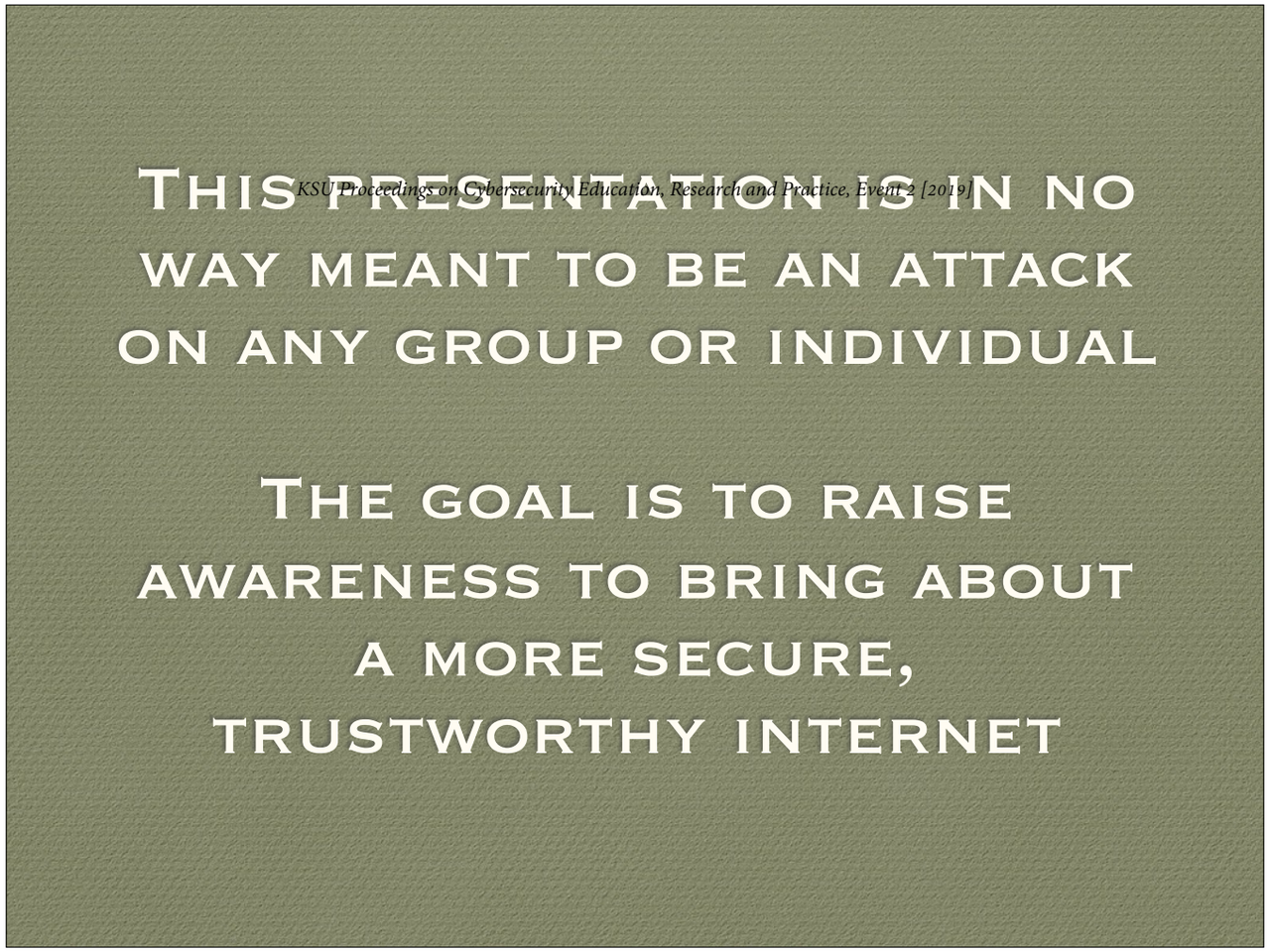
Are Students Being Prepared for this Eventuality?





Internet Security

Where are we and where are we going?



Making changes to the Internet now is like fixing a car with the engine running!

Internet Core Functions

- Domain Name System
- Digital Certificates
- Border Gateway Protocol

DNS

KSU Proceedings on Cybersecurity Education, Research and Practice, Event 2 [2019]

- Why was DNS created?
- How did it function in the 1987 RFC 1034 standard?

I E T F®

https://www.ietf.org/rfc/rfc1034.txt

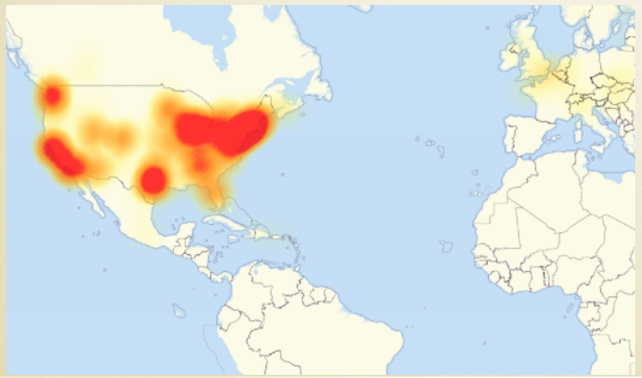
IETF Standardization Path:

- Draft
- RFC
- Proposed Standard
- Internet Standard

Security Issues with DNS

Jones: Internet Core Functions: Security Today and Future State

- Confidentiality
- Integrity
- Availability



https://www.networkworld.com/article/3134057/how-the-dyn-ddos-attack-unfolded.html
By flooding Dyn, the attack prevented traffic from reaching Dyn's customers, who include Amazon, Etsy, GitHub, Shopify, Twitter and the New York Times

http://techgenix.com/DNS-Security-Part-1/
- Zone file compromise
- Zone information leakage
- Compromised dynamic updates
- DNS denial of service
- Cache poisoning

https://www.dnssec.net/dns-threats

https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

DNS Security Extensions (DNSSEC)

- Published by IEFT in 2005 with first work started in 1993
- Origin authentication of DNS data
- Data integrity
- Authenticated denial of existence
- Does not protect against
  - Data confidentiality
  - DDoS attacks

https://www.dnssec.net/

DNSSEC adds four new resource record types:
- Resource Record Signature (RRSIG),
- DNS Public Key (DNSKEY),
- Delegation Signer (DS),
- Next Secure (NSEC).

It also adds two new DNS header flags:
- Checking Disabled (CD)
- Authenticated Data (AD).

https://www.rfc-archive.org/getrfc.php?rfc=3833

https://www.schneier.com/blog/archives/2008/07/the_dns_vulnera.html

Issues with DNSSEC

Jones: Internet Core Functions: Security Today and Future State

- RFC 3833 - Issues with DNSSEC
  - Published a year before the DNSSEC RFCs in 2004
  - Eight major issues identified
  - Debilitating requirements of DNSSEC design were all data would remain "public" and no authentication of clients or servers for access control
  - Extremely complex to implement and maintain
    - Time synchronization issues
  - Resource intensive
  - Key rollover is very hard
  - Not widely deployed due to issues

DNS Security Reboot

- DNS over TLS (DoT)
  - RFC7858 - Standards Track May 2016
  - Unique Port and Allows Inspection
- DNS over HTTPS (DoH)
  - RFC8484 - Standards Track Oct 2018
  - Uses Web Traffic and Supports an Open Internet
  - Overrides OS resolution for browser's choice
- DNS over DTLS
  - RFC8094 - Experimental Feb 2017
- DNSCrypt - Since 2011 Not IETF

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+-+The+Solutions

https://www.thesslstore.com/blog/dns-over-tls-vs-dns-over-https/

http://www.circleid.com/posts/20190906_dns_over_https_the_privacy_and_security_concerns/

https://www.theregister.co.uk/2019/09/09/mozilla_firefox_dns/

DNS-over-HTTPS

- DoH is the leading standard
- Firefox turned on DoH in late September 2019
  - Only works over Cloudflare for now
- Chrome has a Beta DoH and Already Exploited
  - ProofPoint found:

PsiXBot have now chosen Google's DoH service for routing their DNS queries to return the IP addresses of the C&C domains. By using Google's DoH service, it allows attackers to hide the DNS query to the C&C domain behind HTTPS.

- CobaltStrike utilizes DoH for controlling infected PCs

https://www.theregister.co.uk/2019/09/09/mozilla_firefox_dns/

https://www.proofpoint.com/us/threat-insight/post/psixbot-now-using-google-dns-over-https-and-possible-new-sexploitation-module

CobaltStrike:
https://github.com/SpiderLabs/DoHC2

https://community.checkpoint.com/t5/Access-Control-Products/How-to-deal-with-DNS-over-HTTPS-DNS-over-TLS-QUIC-and-PSOM/td-p/11528

Issues with DoH

According to ZDNet from 6 October 2019

KSU Proceedings on Cybersecurity Education, Research and Practice, Event 2 [2019]

- DoH **doesn't actually prevent ISPs user tracking**
- DoH creates havoc in the enterprise sector
- DoH **weakens cyber-security**
- DoH **helps criminals**
- DoH shouldn't be recommended to dissidents
- DoH centralizes DNS traffic at a few DoH resolvers

These browsers companies have some experienced and smart folks in then. Perhaps there is a Phase II for this. Perhaps there is another reason browser companies can’t discuss.

https://www.zdnet.com/article/dns-over-https-causes-more-problems-than-it-solves-experts-say/

WhoIs and GDPR

Jones: Internet Core Functions: Security Today and Future State

- General Data Protection Regulation is an EU regulation created to protect European citizens from unwanted personal data collection and potential misuse of this data.
- An unfortunate side effect of this regulation is Security's ability to identify, monitory, and stop threat actors.
- WhoIs is a standard developed to allow people on the Internet to see information about the owner of a DNS domain.

Historical Whois data

Domain Name: HOWTOINTERNET.NET
Registrar: TUCOWS INC.
Whois Server: whois.tucows.com
Referral URL: http://domainhelp.opensrs.net
Name Server: NS1.STARTLOGIC.COM
Name Server: NS2.STARTLOGIC.COM
Status: OK
Updated Date: 01-jan-2008
Creation Date: 01-jan-2008
Expiration Date: 01-jan-2009
Registrar results for howtointernet.net:
Registrant:
Contactprivacy.com
96 Mowat Ave
Toronto, ON M6K 3M1
CA
Domain name: HOWTOINTERNET.NET
Administrative Contact:
contactprivacy.com, howtointernet.net@contactprivacy.com
96 Mowat Ave
Toronto, ON M6K 3M1
CA
+1.4165385457
Technical Contact:
contactprivacy.com, howtointernet.net@contactprivacy.com
96 Mowat Ave
Toronto, ON M6K 3M1
CA
+1.4165385457
Registration Service Provider:
StartLogic, Inc., hostmaster@startlogic.com
1-800-725-8064
http://www.startlogic.com
Registrar of Record: TUCOWS, INC.
Record last updated on 01-Jan-2008.
Record expires on 01-Jan-2009.
Record created on 01-Jan-2008.
Registrar Domain Name Help Center:
http://domainhelp.tucows.com
Domain servers in listed order:
NS2.STARTLOGIC.COM
NS1.STARTLOGIC.COM
Domain status: ok

Threat actors would usually reuse the same contact info for their different attacks. WhoIs helped Security identify and stop attacks.

Current whois data


```
Domain name:
        marconi.co.uk

    Data validation:
        Nominet was able to match the registrant's name and address against a 3rd
party data source on 11-Jul-2017

    Registrar:
        GoDaddy.com, LLC. t/a GoDaddy.com, LLC. [Tag = GODADDYUK] [Tag = GODADDYUK]
        URL: ____________________

    Relevant dates:
        Registered on: 08-Sep-1998
        Expiry date:  08-Sep-2020
        Last updated:  22-Sep-2019

    Registration status:
        Registered until expiry date.

    Name servers:
        ns17.domaincontrol.com
        ns18.domaincontrol.com

    WHOIS lookup made at 17:57:18 28-Sep-2019
```

GDPR/WHOIS SECURITY IDEAS

- Use tokens to identify owner information
- Require verification of people making the requests
  - DNS would have different levels of verification like certificates

DNS Conclusions

Jones: Internet Core Functions: Security Today and Future State

- There are a lot of security issues with DNS
- The new standards and regulations favor privacy over security
- DoH is being deployed by browser organizations
  - Most people do not understand the difference or believe it matters
- Changing how DNS works involves a lot of complicated changes and effort

Certificates

- Why were certificates created?
- Common Uses
  - Encrypt communications
    - Web
    - Email
    - Server to server
  - Sign software/documents

CA/BROWSER FORUM

https://www.ietf.org/rfc/rfc1034.txt

http://techgenix.com/DNS-Security-Part-1/

- Zone file compromise
- Zone information leakage
- Compromised dynamic updates
- DNS denial of service
- Cache poisoning

https://www.dnssec.net/dns-threats

Current Certificate Authority Issues

Jones: Internet Core Functions: Security Today and Future State

- Domain owner validation
  - (See next slides)
- Certificate impersonations
  - Original certificates
    - Symantec vs. Google example
  - Similar certificates
- Root certificates stolen
  - Diginotar example

https://securityaffairs.co/wordpress/91369/cyber-crime/digital-certificates-executive-impersonation.html

https://groups.google.com/a/chromium.org/forum/#!topic/blink-dev/eUAKwjihhBs%5B251-275%5D

https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/

https://blog.tinned-software.net/certificate-transparency-and-unauthorized-certificates/

https://blog.appsecco.com/certificate-transparency-the-bright-side-and-the-dark-side-8aa47d9a6616

In December, 2013, Google announced that they noticed unauthorized digital certificates issued for several Google domains by an intermediate CA linking back to ANSSI, a French Certificate Authority(that operates with French intelligence agencies). The ANSSI attributed the incident to “Human Error”. Google pointed out the importance of CT in that announcement.

In December, 2012, Google announced that they noticed unauthorized digital certificates issued for “*.google.com” domain by an intermediate CA linking back to TURKTRUST, a Turkish certificate authority. Google detected the issue using Chrome’s certificate pinning(Certificate Pinning is a mechanism by which applications indicate that only specific CAs are allowed to issue certificates on their behalf).

In August, 2011, Google announced that they noticed fraudulent SSL certificate issued by DigiNotar, a root certificate authority that should not issue certificates for Google. Attackers compromised DigiNotar’s infrastructure to issue hundreds of unauthorised digital certificates.

Types of Validation

Note: Validation methods must work in all countries

- DV - Domain Validation
  - Verifies the DNS owner
- OV - Organization Validation
  - Verifies the organization/business
  - Organizations are strictly authenticated by real agents against business registry databases hosted by governments.
- EV - Extended Validation
  - Extra validation steps
  - Solid green browser bar

https://www.ssl.com/article/dv-ov-and-ev-certificates/

https://www.sslsupportdesk.com/what-is-the-difference-between-domain-validated-dv-organization-validated-and-extended-validation-ev-ssl/

DV Certificate Validation Deep Dive

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

Validation of Domain Authorization or Control (Pick one)

~~3.2.2.4.1 Validating the Applicant as a Domain Contact*~~

3.2.2.4.2 **Email**, Fax, SMS, or Postal Mail **to Domain Contact**

3.2.2.4.3 Phone Contact with Domain Contact

3.2.2.4.4 Constructed Email to Domain Contact

~~3.2.2.4.5 Domain Authorization Document*~~

3.2.2.4.6 Agreed-Upon Change to Website

3.2.2.4.7 DNS Change

3.2.2.4.8 IP Address

3.2.2.4.9 Test Certificate

3.2.2.4.10. TLS Using a Random Number

*1 August 2018 the CA/B Forum modified validation methods

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.6.pdf

https://www.digicert.com/blog/new-cab-forum-validation-rules-go-into-effect-today/

EV Certificate Validation Deep Dive

- Verify Applicant's **existence and identity**
  - Verify the Applicant's **legal** existence and identity
  - Verify the Applicant's **physical** existence (business presence at a physical address)
  - Verify the Applicant's **operational** existence (business activity)
- Verify the Applicant is a registered holder, or has **control, of the Domain Name(s)** to be included in the EV Certificate
- Verify a **reliable means of communication** with the entity to be named as the Subject in the Certificate
- Verify the Applicant's **authorization** for the EV Certificate
  - Verify the **name, title, and authority** of the Contract Signer, Certificate Approver, and Certificate Requester
  - Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and **agreed to the Terms of Use**
  - Verify that a Certificate Approver has **signed or otherwise approved** the EV Certificate **Request**

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.7.0.pdf

User Verification of Certificate

Jones: Internet Core Functions: Security Today and Future State

- Most people do not understand the difference between DV, OV, or EV
- Most people click through certificate error messages
- The URL bar has started showing green, but do people notice when it is not green

Certificate Solutions

- Certificate pinning
- Certification Authority Authorization (CAA)
- Certificate Transparency (CT)
  - But who is checking?
- Have certificates expire quickly

https://thenewstack.io/heres-caa-dns-record-https-website/

About the new TLS 1.3 standard

Jones: Internet Core Functions: Security Today and Future State

- Utilizes unique encryption for every connection.
  - PFS - Perfect Forward Secrecy in Diffie-Hellman
    - Ephemeral-Mode
    - Elliptic-Curve
  - The private certificate keys cannot be utilized to break the encryption
  - Good: Limits the ability of repressive countries from monitoring and controlling people
  - Bad: Organizations cannot utilize their own certificates to inspect traffic to protect themselves
  - Bad: DDoS filtering in the cloud cannot be utilized for application layer traffic

https://tools.ietf.org/html/draft-green-tls-static-dh-in-tls13-01

Digital Certificate Conclusions

- There has been a lot of progress recently
- There are still some large and very complicated challenges
- Any solution must work and be accepted worldwide
- The combination of TLS 1.3 and DoH creates new attack vectors for Security organizations

Border Gateway Protocol

Jones: Internet Core Functions: Security Today and Future State

- Why was BGP created?
- What is BGP used for?
- BGPv4 in use since 1994
  - RFC 4271 in 2006

IETF®

BGP Issues

Attacks according to NIST 800-54:

- Peer Spoofing and TCP Resets
- TCP Resets Using ICMP
- Session Hijacking
- Route Flapping
- Route Deaggregation
- Malicious Route Injection
- Unallocated Route Injection
- Denial of Service via Resource Exhaustion
- Link Cutting Attack

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-54.pdf

BGP Security Vulnerabilities Analysis
https://www.ietf.org/rfc/rfc4272.txt

https://www.schneier.com/blog/archives/2018/10/chinas_hacking_.html

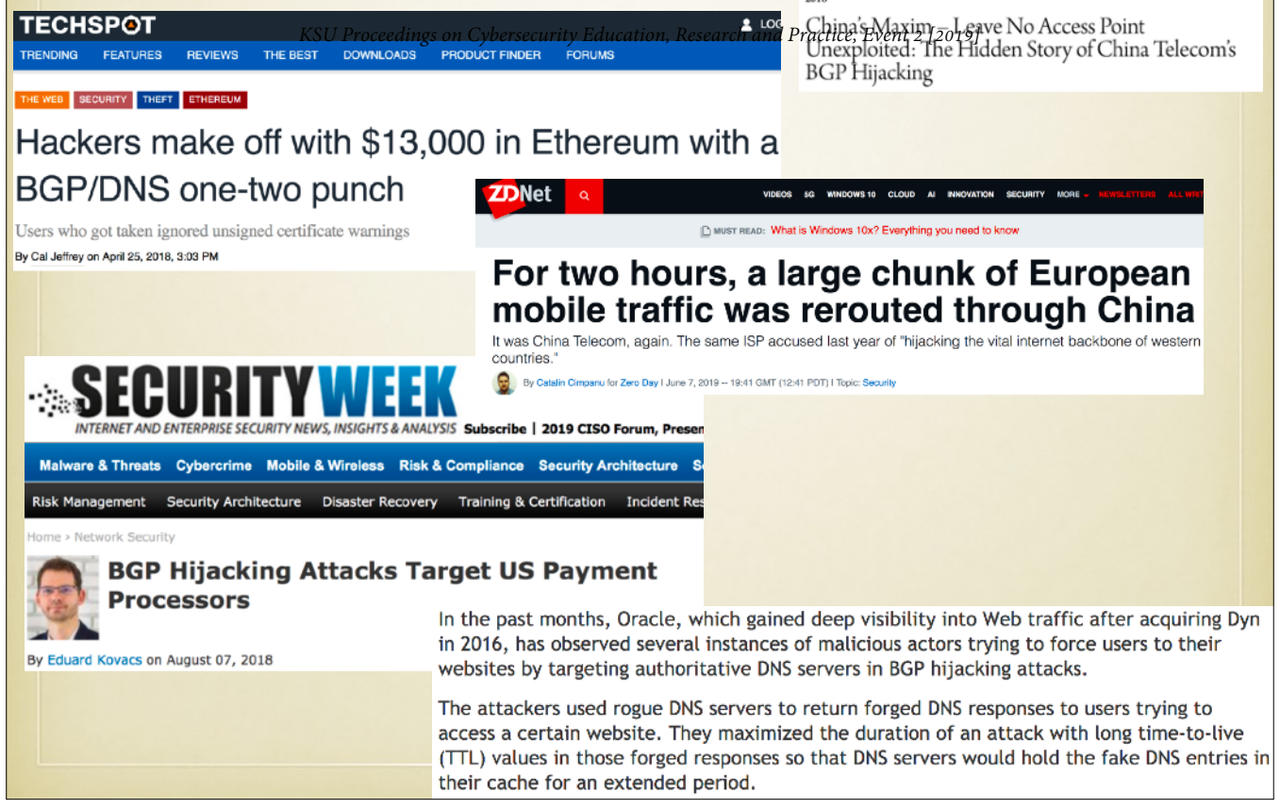
GBP Summary

Jones: Internet Core Functions: Security Today and Future State

Natively BGP is…

- "Open"/Trusting/Not Centralized
- Quick to reconverge
- Falt tolerant
- Not country specific i.e. "borderless"
- Passively monitored. Not policed.
- Only deeply understood by very few people.
- Classic case of fast and easy vs. security dichotomy.

BGP Attacks in News



https://observatory.manrs.org/#/overview

https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca

https://www.techspot.com/news/74318-hackers-make-off-13000-ethereum-bgpdns-one-two.html

https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/

https://www.securityweek.com/bgp-hijacking-attacks-target-us-payment-processors

BGP Solutions

Jones: Internet Core Functions: Security Today and Future State

- BGPsec - RFC 8205 Proposed Standard Sept 2017
  - Resource intensive - not well supported
- TCP MD5 Password - RFC 2385 (1998)
  - Mitigates BGP session hijacking
  - Not widely implemented
- Route Origin Validation - NIST 800-14 June 2019
  - New and shows promise
  - More of a best practice document
- BGP Communities for filtering

http://bgpexpert.com/

https://tools.ietf.org/html/rfc8205

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-14.pdf

https://www.potaroo.net/ispcol/2019-09/secbgphard.html

Summary

- Security needs to become more involved in the standardization process
- Non-security people need to learn about security
  - Security needs to become more proactive and not reactive
  - Think more strategically than tactically
- Security needs to focus more than just on how things break
  - Security needs to be part of creative solutions

https://www.ietf.org/rfc/rfc1034.txt

http://techgenix.com/DNS-Security-Part-1/

- Zone file compromise
- Zone information leakage
- Compromised dynamic updates
- DNS denial of service
- Cache poisoning

https://www.dnssec.net/dns-threats

Topics of Discussion

- Why do people trust a car mechanic more than Security people?
- There is no CISO for the whole world
  - What is the largest group that speaks for Security?
- If everyone knew what Security people knew, would they behave differently?
- **What can universities do to train the next generation of cyber warriors?**
  - Blockchain classes?

AMA, ADA, Bar Association,