Authentic Web.

ENTERPRISE DOMAIN MANAGEMENT FOR THE NEW TLD ERA

9 TLS AND DNS RISKS TO ENTERPRISE SECURITY AND COMPLIANCE

Eliminate known DNS and TLS problems that put your security and compliance at risk.

THE DIGITAL CHAIN OF TRUST IS BROKEN

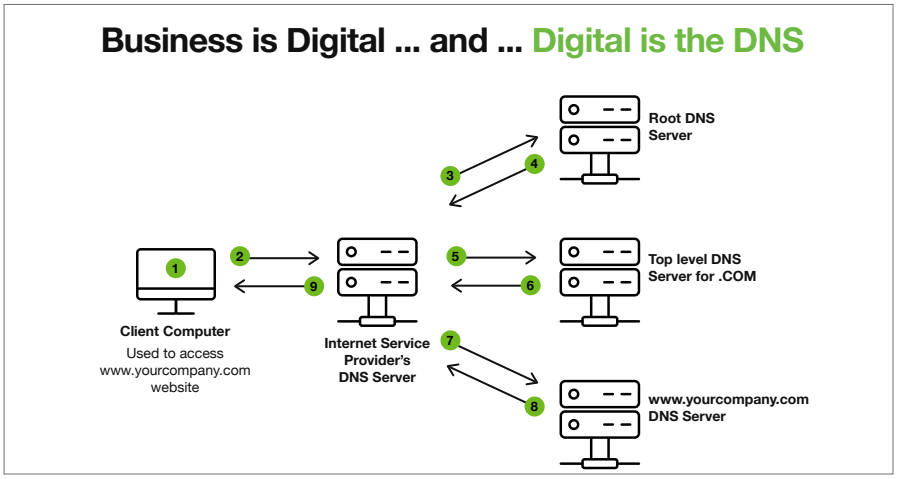
Digital transformation is driving unprecedented expansion of the enterprise digital attack surface. The number of network endpoints is growing exponentially. Deloitte cites the World Economic Forum Global Risks Report, 2017, saying:

> *"Digital technologies and innovation are growing exponentially, accelerating cyber risks, new attack vectors, and greatly expanding the attack surface that organizations must patrol and defend."*
>
> ***Deloitte, Take the lead on cyber risk. 2017*** ↳

The explosion of data volume and endpoints is creating significant challenges for enterprise network IT teams. Enterprise reliance on DNS and TLS integrity is critical as attack vectors proliferate. Security experts agree: **"BGP and DNS are the soft underbelly of the web,"** says Alan Woodward, Professor of computer science, University of Surrey.

Network endpoints are where proprietary enterprise and customer data is captured, processed and set in motion. For enterprise, data-in-motion security relies on flawless implementation and monitoring of DNS and TLS protocols to ensure the Chain of Trust is maintained.

Digital business services run on the Domain Name System (DNS), which is the network foundation for all digital communications, customer engagement and digital service delivery. Enterprises must secure it, or they will be dangerously exposed to compromise.

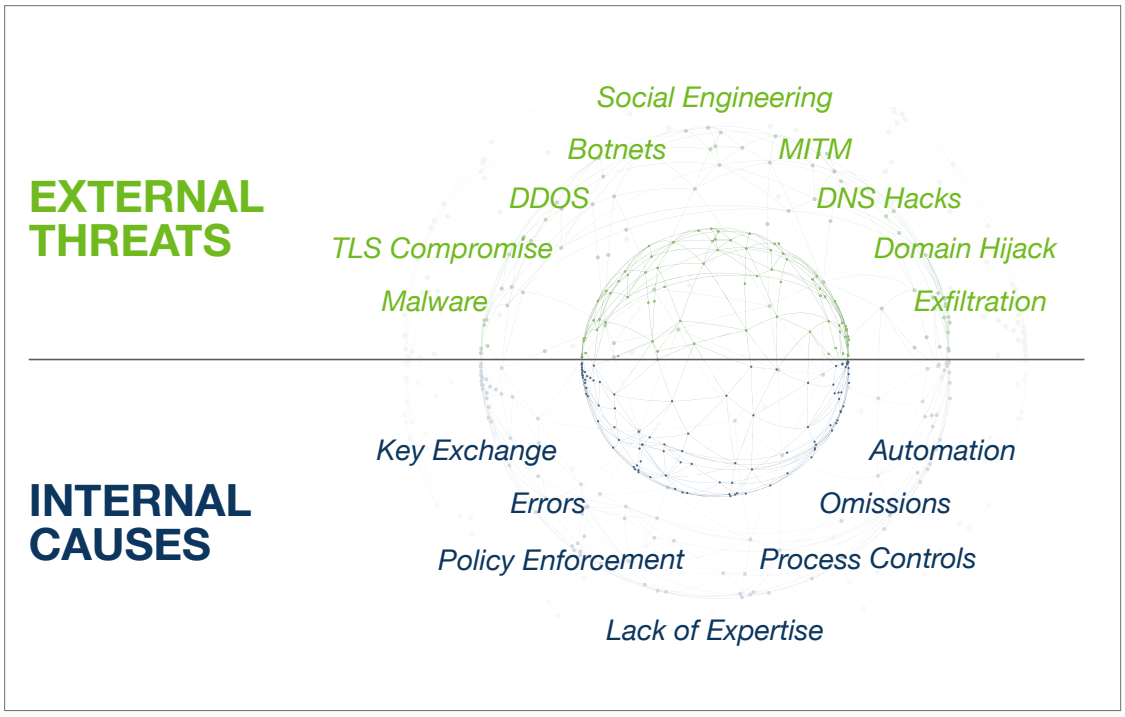


DNS AND TRANSPORT LAYER SECURITY (TLS)

The DNS is known to have security exposures due to under-utilization and enforcement of DNS security extensions (DNSSEC) and poor management controls over connections equipped with Transport Layer Security (TLS) encryption and authentication. While DNSSEC and TLS encryption promise a foundation of security, management shortcomings i.e. legacy tools, outdated processes and human actions create exposure. Data security and compliance need revisiting, particularly as DNS networks scale.

Enterprise DNS network security weaknesses largely exist due to processes, systems and operations where human error and omissions occur. Enterprise systems and management processes tend to operate in silos. Lack of visibility, control and compliance over the actions and inactions of personnel are the primary source of network security vulnerability. The lack of compliance over internal, partner, and supplier network parties creates weaknesses in the Chain of Trust, which expose the business.

Independent research validates that the biggest security risk to enterprise is the reliance on people, operating in silos with legacy tools, and inconsistent expertise and motivation, exposing the enterprise to TLS and DNS security risk.



TLS AND DNS: THE FRONTLINE OF ENTERPRISE DATA-IN-MOTION SECURITY

TLS and DNS technologies underpin enterprise digital infrastructure as the frontline for network data-in-motion security. Transport Layer Security is the trust protocol to authenticate communications between multi-party systems and to encrypt data in motion. The Domain Name System (DNS) is the addressing technology used as the address book of the Internet, directing/routing data between network endpoints.

> *"Silos between network edge, endpoint and data security systems can restrict an organization's ability to prevent, detect and respond to advanced attacks."*
>
> ***Gartner: Best Practices for Detecting and Mitigating Advanced Threats. 2016 Updated March 2016*** ↳

Enterprises utilize myriad third-party vendors for TLS relying on internal human resources and Certificate Authority (CA) employees to establish and maintain network security. With disparate employee groups, siloed systems and manual processes, it is practically impossible to maintain control and visibility over the risk factors that can compromise the Chain of Trust for data in motion. This represents a data security and compliance weakness.

HTTPS CERTIFICATE PROCESS STEPS

16. RENEW CERTS
15. MANAGE & MAINTAIN CERTS
14. TEST THAT HTTPS IS ACTIVE ⚠ Errors can be missed without a final test. Don't forget to track the renewal date!
13. VERIFY HTTPS FIELDS ARE CORRECT ⚠ Errors can invalidate cert.
12. SELECT/UPLOAD CERT ⚠ Installation process varies by server type.
11. OPEN SSL MANAGER (OR SERVER) ⚠ Cert installation process varies by server type – your company may have several…
10. BACK UP EXISTING KEYS AND CERTIFICATES ⚠ Error in installing new cert(s) can invalidate existing certs.
9. RECEIVE SIGNED CERT AND DOWNLOAD
8. SPECIFY DOMAIN VALIDATION CONTROL METHOD
7. PASTE CA-ISSUED CSR INTO CERT ORDER FORM ⚠ Error will invalidate cert.
6. PREPARE HTTPS CERT ORDER ⚠ Incorrect cert type (shared, DV, OV, EV)
5. RECEIVE CONFIRMED CSR FROM CA
4. SUBMIT CSR TO CA ⚠ Poor choice of CA can invalidate cert
3. PREPARE CSR ⚠ Incomplete documents or errors – will prevent or invalidate CSR
2. STORE KEY SECURELY ⚠ Key security issue – invalidates CSR and HTTPS cert. Requires new key.
1. CREATE NEW PRIVATE KEY ⚠ Invalid key

TLS implementations are difficult to trust due to the manual steps, people-dependencies and lifecycle management required. Hence, the "Chain of Trust" is exposed to risk on numerous fronts.

TLS: MANUAL STEPS REQUIRED TO ESTABLISH A SINGLE NETWORK ENDPOINT WITH TLS

TLS deployments and administrative processes rely upon multiple business entities, systems and people. TLS security is easily compromised as a result. The complex sequence of steps required to secure a SINGLE server host or DNS endpoint is costly and difficult for teams to manage.

Now consider the increased complexity and personnel steps in securing hundreds or thousands of endpoint connections throughout their lifecycle. And all the while, vendors evolve and personnel throughout the ecosystem turn over.

DNS SECURITY: DNSSEC IMPLEMENTATION, MANUAL PROVISIONING AND MANAGEMENT

Like TLS implementation, the Chain of Trust in DNS route look-up requires proper implementation and maintenance of the DNSSEC protocol. DNSSEC protects against "Man-In-The-Middle" (MITM) compromises.

A paper published by MIT explains the value of DNSSEC with this summary and conclusion.

> *"DNSSEC allows transaction level authentication and secure zone transfers protecting all data in the zone during the transfer."*

Despite the universally acknowledged value of DNSSEC, organizations are woefully lax in adoption. Research from Farsight Security illustrates the poor state of enterprise deployment exposing data-in-motion to recursive server DNS cache poisoning.

6 Summary and Conclusions

DNS has major security issues that need to be addressed urgently. Threats such as Man in the middle attacks and cache poisoning arise because of the lack of authentication and integrity in the DNS transaction process. Inaccurate or nonexistent boundary checking and error handling conditions in BIND software lead to exploits such as buffer overflows. Usage threats are caused by a range of entities from misconfigured client resolvers to packet filters causing conditions similar to DDoS.

The Internet Engineering Task Force (IETF) has responded to the threats by developing DNSSEC, a secure DNS protocol, to address the data integrity and source spoofing issues. DNSSEC allows transaction level authentication and secure zone transfers protecting all data in the zone during the transfer. In DNSSEC, Name-based authentication attacks can be detected [7].

Source: Security Vulnerabilities in DNS and DNSSEC. ↳

Figure 8 DNSSEC Population

Source: www.farsightsecurity.com ↳

DNSSEC implementation is difficult. It requires technical expertise and diligence to establish and maintain integrity over the lifecycle of network endpoints. It must be configured at the Registrar/Registry level and at the Managed DNS level. DNSKEY management complexities and administrative oversights can cause loss of route look-up authenticity, often occurring without IT personnel's knowledge.

DNSSEC was established by the IETF to resolve data integrity risks. The operational challenge remains to equip enterprise IT and security teams with easy-to-use tools to ensure coverage.

Next, we will highlight 9 TLS and DNS risks facing enterprise IT security and compliance.

9 SECURITY RISKS WITH TLS AND DNS

There are multiple, known problems inherent to DNS and TLS networks that routinely expose enterprise to network security issues and failures. They are:

1. *TLS Version Control Vulnerabilities and Compromises*
2. *Chain of Trust Vulnerabilities: Key Exchanges and Implementation Practices*
3. *Certificate Authority (CA) Compromises: Market Disruption and Uncertainty*
4. *Certificate Authority: Endpoint or Entity Verification Weaknesses*
5. *Expanding Top Level Domain Spaces: Confusion and Lack of Trust*
6. *DNSSEC: Lack of Use; Man-In-The-Middle; DNS Cache Poisoning*
7. *Compliance: Monitoring and Remediation*
8. *Manual Processes: Errors and Omissions*
9. *Digital Transformation and Cloudification: The Network Scaling Cost Constraint*

1

TLS: VERSION CONTROL

Old versions of SSL and TLS (pre-Version 1.3) have numerous, known security weaknesses. Failure to track and correctly update legacy versions of TLS exposes data-in-motion to serious security and compliance risks. TLS version control enforcement and best-practice implementation to improve the Chain of Trust mitigates these risks.

Reference: SSL, TLS and PKI History ↳

2

CHAIN OF TRUST KEY EXCHANGE PRACTICES

Trusted key exchange and storage processes depend on human resources including: internal, third party Certificate Authority (CA) and third-party endpoint server administrators. The Chain of Trust assumption requires all parties to act professionally, without error and without exception.

Silo operational and systems controls, separate business entities, and disparate systems make it practically impossible to guarantee the Chain of Trust over the lifecycle of even a single TLS-enabled network endpoint, much less hundreds or thousands of endpoints.

Reference: The Chain of Trust is Broken

3

CA COMPROMISES: MARKET DISRUPTION AND UNCERTAINTY

Certificate Authority (CA) compromises are frequent and ongoing. When a CA is compromised, fraudulent or exposed certificates are issued and in use, abrogating the trust that parties universally place in SSL certificates. Any entity can establish itself with a browser firm to be included in the CA bundles. Further, TLS protocol standards set out in the CA Browser Forum are arguably difficult to fully enforce.

Exacerbating the trust question, the market is being disrupted by new CA business models e.g. Let's Encrypt's free SSL certs. The Certificate Authority Chain of Trust has been challenged by large-scale CA compliance control breakdowns according to browser firms that have flagged non-compliant CA practices. For example, Google declared certain Symantec certificates untrustworthy due to chain of trust failures. SSL reseller Trustico was exposed when a company executive reportedly emailed 23,000 private keys, rendering the affected certificates of Symantec, GeoTrust, Thawte and RapidSSL untrustworthy.

The conclusion: Trusted SSL coverage is increasingly uncertain.

4

CA: ENDPOINT OR ENTITY VERIFICATION IS WEAK

Endpoint entity verification is weak. A Domain-validated certificate can be obtained where the CA only requires verification that the entity requesting the certificate has control of a web server or the DNS of the domain name. This is insufficient to prevent malicious parties from accessing servers to show control, hack a DNS service, gain access via social engineering or execute a Man-in-the-Middle attack. While standards are slowly changing to address this vulnerability with initiatives such as the Google TLS Transparency Project, verification remains a weak link in the Chain of Trust. Extended Validation certifications may be more effective, however, the difference may not be noticeable. Moreover, their high cost and manual, labor-intensive administration requirements make them impractical for broad use as a scaled network TLS solution.

Reference: Google TLS Transparency Project. ↳

5

EXPANDING TOP LEVEL DOMAIN SPACES

The massive expansion of new Top-Level Domains has created trust and brand identity challenges for enterprise web or server endpoints. The noisy and largely unregulated expanding name space means that signed TLS certificates don't hold much inherent trust. Still, Internet users simply consent to trust SSL certificate enabled properties assuming the owner is verified. This creates increased opportunity for actors to register domains for malicious purposes that appear to be brand-authentic and TLS-enabled.

The exception is the Brand Top Level Domain or Brand Registry, where authority, authenticity and control are verifiable by ICANN and can act as an anchor of digital TRUST.

6

DNSSEC: LACK OF USE AND UNDERSTANDING

Under-deployment of DNS Security Extensions (DNSSEC) exposes enterprise to several security risks. Data transport verified by DNSSEC is required to address 'Man-In-The-Middle' (MITM) attack vectors. Without DNSSEC, DNS cache poisoning allows for MITM rerouting of valid queries to fraudulent destinations. Network operators have not widely implemented DNSSEC for various reasons that include: lack of knowledge and lack of integrated control systems to implement and maintain DNSSEC provisioning, and related DSKey management.

Reference: ICANN 2019 ↳

"Full deployment of DNSSEC will ensure the end user is connecting to the actual web site or other service corresponding to a particular domain name. Although this will not solve all the security problems of the Internet, it does protect a critical piece of it – the directory lookup – complementing other technologies such as SSL (https:) that protect the conversation and provide a platform for yet-to-be-developed security improvements."

7

COMPLIANCE: CHAIN OF TRUST MONITORING AND REMEDIATION

Automated monitoring and remediation is not widely deployed to manage TLS and DNS network security policies. Organizations may monitor server and end-point connections, data flow, and/or active status. Even with DNS threat detection tools, however, connections are rarely monitored for compliance with TLS and DNS security policy protocols.

Monitoring and remediation automation for non-compliance is critical to ensure lifecycle Chain of Trust integrity.

8

THE HUMAN FACTOR: OPERATING ERRORS AND OMISSIONS

Organizations rely on internal and 3rd party team members to ensure security compliance over DNS and TLS networks. Despite the use of various tools to maintain security posture integrity, enterprise operations depend largely on people, who are expected, unrealistically, to perform flawlessly at all times. Even the most stringent best practice policies and procedures are not good enough. People make mistakes, forget, and are overworked, don't know, don't care and in some cases intentionally do not act to protect the business. They also turn over which diminishes institutional knowledge.

The human factor is the single greatest enterprise risk for which system-based automation is required.

Reference: The SANS Incident Response Survey 2017 ↳

9

NETWORK SCALING: DIGITAL TRANSFORMATION COMPLEXITY

Exacerbating all these factors is the increase in scale and complexity of the enterprise digital attack surface. There is increasing pressure on Infrastructure and Operational teams to efficiently scale while ensuring continuing data security compliance integrity. Applying current TLS and DNS practices involves a complex set of manual processes and dependencies. Scale issues create a practical impediment to ensuring trusted network authentication and data-in-motion security. It is simply too costly and inefficient to maintain compliance with largely manual, legacy practices.

Reference: Growth in Attack Digital Surface Area ↳

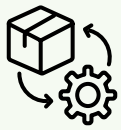
SUMMARY AND CONCLUSION

Network communications largely rely upon the Domain Names System (DNS) using Transport Layer Security (TLS). The 9 RISKS discussed above show a fragile ecosystem for securing increasing numbers of endpoints. Known process flaws compromise the Chain of Trust for data-in-motion. Human resources – people - using antiquated legacy processes are the main source of these flaws. Lacking systems that economically scale, teams cannot be trusted to ensure adequate security compliance.

Ensuring secure authentication and TLS certificate-based (HTTPS) encryption across all end-points has proven challenging to IT teams. The widespread failure to deploy DNSSEC despite oft-repeated calls to action by security and regulatory agencies underscores the vulnerabilities and exposures of the enterprise DNS and TLS environment.

IT security and network infrastructure managers need an easier, more scalable way to ensure authentication and encryption over enterprise data-in-motion.

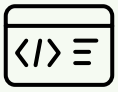
USE CASES



SUPPLY CHAIN

CLOUD

IOT



APPLICATIONS

EDI

THE BRAND REGISTRY CAN SOLVE CHAIN OF TRUST ISSUES

Security and compliance challenges for data-in-motion can be effectively mitigated with a new, sytems-based approach anchored on the trust authority of a Brand Registry. Brand Registries are highly securable assets with superior encryption and authentication capabilities over generic TLD-based DNS networks.

Authentic Web has incorporated the trust and control strengths of the Brand Registry into a system to secure the DNS Chain-of-Trust solving the problems inherent to DNS and TLS implementations. The management and provisioning system automates, monitors and remediates network connections. TLS security and application authentication are assured with remediation and auditability over the lifecycle of all endpoints.

Contact us to learn more how this new systems-based approach with your Brand Registry can ensure regulatory compliance is fully addressed across your network use cases, at scale.

AUTHENTICWEB.COM
info@authenticweb.com
NA 1.855.436.8853 | International +1.416.583.3770