2017 Online Trust Audit Methodology Overview

Craig Spiezle
Executive Director & President

Jeff Wilbur
VP Research

Updated February 27, 2017

Summary of Clarifications

• DMARC policy with our RUA or RUF mechanisms receive no scoring (aka naked DMARC records) (slide 11)
• Added example of Vulnerability or Bug reporting (slide 26)
• Privacy scores reallocated; increased scores on privacy policy and reduce weighting on tracking (slide 27)
Background

- 9th annual Audit & assessment of adoption of best practices
- Methodology revised annually
  - Continually evolving
  - Reflects open Call for Public Comments
  - Incorporates evolving threats
  - Promotes norms for responsible and transparent privacy practices
- Leverage public lists and data for sites to audit
- Evolving practices and standards for “bonus points”

Online Trust Audit & Honor Roll

Objectives:

- Move from a “compliance” mindset to “stewardship”
- Recognize leadership brands, sites & apps that implement security and privacy practices protecting users’ data
- Incentivize businesses and developers to enhance their security, data protection and privacy practices
- Make security & privacy part of a brand’s value proposition
- Increase user awareness and preference
Honor Roll Overview – 2016

- **Audit of 1,000 web sites**
  - Internet Retailer Top 500
  - FDIC Banking 100
  - Top 100 Consumer Services
  - Top 100 News/Media
  - Top 50 Federal Gov’t
  - OTA Members

- **Scoring**
  - 100 baseline points for each category
  - Weighted composite analysis, ~50 criteria
  - Bonus points for emerging practices, demerits for poor practices

- **Honor Roll** = 80% or better, 55% or better in all categories

Honor Roll Recap

- Record achievement despite a bar that continues to rise
- 10% qualified for the “Top of the Class” (95%+)
Growth in All Sectors

- Nearly 3-fold increase in News, yet they still lag all sectors, primarily due to data sharing with limited controls

Underwriting Opportunities

- $20,000, limited to 4 Donors (existing members $16,500@)
  - Recognition in the report with logo and description
  - Inclusion in media and press releases
  - Participation in online briefings and webinars
  - Recognized on Audit landing page for 12 months
  - and more ....

2016 Donors included
Recognize Leadership

Ranked #1
of all sites across all sectors

Online Retailers  Consumer  Federal

Banking  News

© 2017 All rights reserved. Online Trust Alliance (OTA)

Audit Overview – 2017

- Audit of 1,000 web sites
  - Internet Retailer Top 500
  - FDIC Banking 100
  - Top 100 Consumer Services
  - Top 100 News/Media
  - Top 50 Federal Gov’t
    - Top 50 ISPs/Carriers-Mailbox Providers
  - OTA Members

- Scoring
  - 100 baseline points for each category
  - Weighted composite analysis, ~50 criteria
  - Bonus points for emerging practices
  - Penalty points for
    - Vulnerabilities, privacy practices, data loss incident & fines/settlement
  - Honor Roll = 80% of base points,
  - Possible shift from 55% or higher in each category to 60% or higher

© 2017 All rights reserved. Online Trust Alliance (OTA)
Consumer Protection – 2017

- **Base points**
  - Email authentication
    - SPF and DKIM at top-level and subdomains *(increased weight for TLD)*
    - DMARC record and policy
    - DMARC reject/quarantine *(Increased weight for reject)*
  - Bonus points
    - TLS for email
    - DNSSEC
    - IPv6
- **Penalty points**
  - Domain locking (not locked)

---

Email Authentication Overview

**SPF**
- Authenticates Message Path
- Authorized senders in DNS

**DKIM**
- Authenticates Message Content
- Public encryption keys in DNS

**DMARC**
- Consistency: A method to leverage the best of SPF and DKIM
- Policy: Senders can declare how to process unauthenticated email
- Visibility: Reports on how receivers process received email
- Aggregated Insights: Telemetry into mail streams (RUA)
- Failure & Spoofed email reports (RUF)

---

© 2017 All rights reserved. Online Trust Alliance (OTA)
https://otalliance.org/eaauthTool

SPF & DMARC Tools & Record Validator
Tool to validate if SPF and DMARC records have been "published" in a domain’s DNS zone file. The tool will query the DNS of the respective domains and present the records found. Up to 500 domains may be entered.

Enter a list of domains, one per line below. Then select a "Record type to query" (SPF or DMARC). The tool will query the DNS of the respective domains and present the records found. Up to 500 domains may be entered.

- SPF Records
- DMARC Records

Domains:

[Image of input fields for domains]

[Image of output fields for SPF and DMARC records]

lookup results:
- SPF Record for otalliance.org
- SPF Record for INTERNETSOCIETY.ORG
- SPF Record for apgei.com
- SPF Record for mail.com
- SPF Record for msn.com

Pipe Delimited Data Output
Submit Query
SPF & DMARC Tools & Record Validator

Tool to validate if SPF and DMARC records have been “published” in a domain’s DNS zone file. The tool will query the DNS of the respective domains and present the records found. Up to 500 domains may be entered.

Lookup Results

DMARC: Record for alliances.org
Domain: alliances.org, 800 IN TXT "v=DMARC1; p= spitf; a=enu; ; rua=mailto:security@alliances.org; ruf=mailto:security@alliances.org; rpa=mailto:security@alliances.org"

DMARC: Record for internetsociety.org
Domain: internetsociety.org, 800 IN TXT "v=DMARC1; p=sp; a=enu; ; rua=mailto:security@internetsociety.org; ruf=mailto:security@internetsociety.org; rpa=mailto:security@internetsociety.org"

DMARC: Record for agen.com
Domain: agen.com, 800 IN TXT "v=DMARC1; p=sp; ; rua=mailto:security@agen.com; ruf=mailto:security@agen.com; rpa=mailto:security@agen.com"

DMARC: Record for unifi.com
Domain: unifi.com, 800 IN TXT "v=DMARC1; p=sp; ; rua=mailto:security@unifi.com; ruf=mailto:security@unifi.com; rpa=mailto:security@unifi.com"

DMARC: Record for drasdac.org
Domain: drasdac.org, 800 IN TXT "v=DMARC1; p=sp; ; rua=mailto:security@drasdac.org; ruf=mailto:security@drasdac.org; rpa=mailto:security@drasdac.org"
Site Security – 2017

• Base points
  ▪ Server & SSL implementation

• Bonus points
  ▪ Extended Validation SSL Certs
  ▪ ASSL/HTTPS DDoS Mitigation
  ▪ Multi-factor authentication
  ▪ Vulnerability reporting mech

• Penalty points
  ▪ XSS / iFrame vulnerabilities
  ▪ Malware / Malicious links
  ▪ Malvertising
  ▪ Bot risk / Web app firewalls
  ▪ DV certificates

Best practices to secure data in transit and collected by websites, and prevent malicious exploits running against clients’ devices, including desktop, mobile and IoT devices.

High-Tech Bridge SSL Tool

https://www.htbridge.com/ssl
ota.ssllabs.com

https://SecurityScorecard.com
Malware, XSS, iFrames….

• Recommend OV or EV for increased trust/transparency
• Rise in fraudulent/lookalike sites that typically use DV certs
When We Discover Threats We…

- Contact the domain administrative / technical contacts
- E-mail security, security-alert, support, CEO, abuse & PR
- Use alternate channels & LinkedIn
- All ineffective, lack of “welcome mats”

Multi-Stakeholder Efforts

Vulnerability / Bug Reporting

• Bonus points
  ▫ Discoverable from home page link (maximum scoring)
  ▫ Discoverable from within the “site search function”

• Key search words (preliminary)
  ▫ Bug reporting
  ▫ Vulnerability reporting
  ▫ Security vulnerabilities
  ▫ Security reporting
  ▫ Bug bounty
  ▫ Vulnerability disclosure(s)
  ▫ Threat reports
  ▫ ………
Privacy – 2017

- **Base points**
  - Privacy policy (55+ pts)
    - Data sharing, retention
    - Third party sharing
    - DNT disclosure
    - Layered notices
    - Link on home page
    - Coppa
    - Date stamp on top of page
  - Third-party trackers on site (45 pts)

- **Bonus points**
  - Redline version archived
  - Use of Icons
  - Cross Device Tracking Disclosures
  - Honoring DNT / Multi-lingual policy
  - Tag mgmt or privacy solution

- **Penalty points**
  - WHOIS (if private vs public)
  - Data breach incidents
  - FTC / State settlements

Best practices providing users clear notice and control of the data being collected, tracked and shared with third parties.
Change History for Microsoft Privacy Statement

February 2017

- In Personal Data We Collect, we clarified additional details about the usage data we consider “Product use data.”

November 2016

- In How We Use Personal Data, we updated Advertising to better clarify the use of your data by third parties to customize the ads you see.
- In How to Access & Control Your Personal Data, we updated Your Communications Preferences, clarifying how to modify your preferences.
- In Other Important Information, we updated the Where We Store and Process Personal Data section to reflect Microsoft’s participation in the EU-U.S. Privacy Shield program.
- In Bing, we removed the Bing Rewards Program section, as Bing Rewards has been replaced by Microsoft Rewards.
- We added a new Microsoft Cognitive Services section to explain how we collect and use data when developers use the services. We also clarified that Microsoft Cognitive Services are not Enterprise Products under this privacy statement.
- We added a new Microsoft Translator section, to explain how Microsoft Translator, Collaborative Translations Framework, and Microsoft Translator Hub collect and use data.
- In Windows, we revised the Telemetry & Error Reporting section to reflect that wireless network identifiers are collected at the optional “Enhanced” level of telemetry rather than at the “Basic” level.
- We added a new captioning section in Xbox to explain how Microsoft incorporates a voice-to-text feature to provide captioning of in-game chat for users who need it.
"Long Form" linking to short form

Localized Policy Site in Spanish
Cross Device Tracking

• Benefits
  ◦ Creates a seamless experience across devices
  ◦ Improved fraud detection and account security.
  ◦ Can enable marketers to provide consumers with an enhanced online experience.

• FTC recommends those engaged in cross-device tracking:
  a. be transparent about their data collection and use practices;
  b. provide mechanisms to give consumers control over their data;
  c. provide heightened protections for sensitive information, including health, financial, and children’s information;
  d. maintain reasonable security of collected data.
Layered with Icons

- Publishers Clearing House  
- Adds clarity, readability & transparency  
- Bonus points for icons

Tracking Tags / Calls

- Analysis of third party calls and site tracking  
- Does not apply to trackers used for anonymous site metrics  
- Focus on trackers who share, retarget  
- Use of multiple tools including but not limited to  
  - OTA tools  
  - Disconnect  
  - Ensighten
More Information

• Online Trust Audit [https://otalliance.org/TrustAudit](https://otalliance.org/TrustAudit)
• Follow OTA @otalliance
• Sign up for mailing list [https://otalliance.org/subscribe](https://otalliance.org/subscribe)
• Get Involved [https://otalliance.org/membership](https://otalliance.org/membership)

Resources

• Email Authentication [https://otalliance.org/eAuth](https://otalliance.org/eAuth)
• AOSSL [https://otalliance.org/AOSSL](https://otalliance.org/AOSSL)
• SSL Best Practices [https://otalliance.org/SSL](https://otalliance.org/SSL)
• EV SSL [https://otalliance.org/EVSSL](https://otalliance.org/EVSSL)
• Site Security Tools
  ▫ High-Tech Bridge SA [https://www.htbridge.com/ssl/](https://www.htbridge.com/ssl/)
    (SSL, Security, Domain Security)
  ▫ Security Scorecard [https://securityscorecard.com/](https://securityscorecard.com/)
  ▫ SSL Labs [https://ota.ssllabs.com](https://ota.ssllabs.com)
  ▫ Hardenize [https://www.hardenize.com/](https://www.hardenize.com/)
Vulnerability Reporting


Cross Device Tracking

- CDT [https://cdt.org/blog/from-televisionsto-telescreens-video-viewing-habits-are-sensitive-information/](https://cdt.org/blog/from-televisionsto-telescreens-video-viewing-habits-are-sensitive-information/)