Avoiding Gotchas! Patron Data Security in an Online World

TLA 2016 - Houston

Alexander Charbonnet, CTO, Biblionix

Biblionix

Sensitive Information

You have been entrusted with your patrons' secrets

Sensitive Information

You have been entrusted with your patrons' secrets

- Contact information (addresses, phone numbers, emails)
- Reading history
- Drivers license number
- Social Security number
- Password
- Date of birth

Secret Keeping

The primary rule of secret keeping:

Limit the number of people who are exposed to the secret.

“Three may keep a Secret, if two of them are dead.”

“If you would keep your secret from an enemy, tell it not to a friend.”

- Benjamin Franklin

Information Sharing

Avenues for the library to transmit sensitive information

Information Sharing

Avenues for the library to transmit sensitive information

- OPAC
- SIP2
- NCIP
- Staff interface
- Email/SMS notices
- Migrating
- Collection Agency/City Hall

Biblionix™

Threats

- Phishing
  - Stealing data
- Eavesdropping
  - Stealing data
  - Mass data collection
- Man-in-the-Middle “MitM”
  - Tampering

“Log in to your account at bankofamerca.com”

Solution

- Both encryption AND authentication
- TLS (aka SSL) handles both
  - But it has to be done well!
- “HTTPS” – HTTP with SSL

The Good News

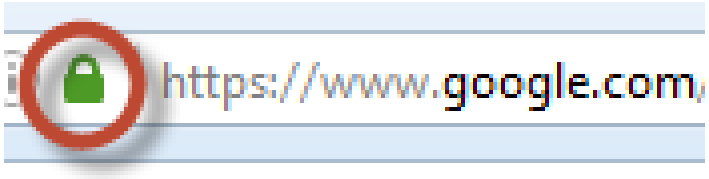
- Modern browsers are good about updates
- The unencrypted web is being deprecated
- There are now many features, protocols, and settings which can be used on the web to enhance security

The Bad News

- There are now many features, protocols, and settings which should be used on the web to enhance security.
- Protocols other than HTTP don't benefit from many of them.

The Web – Basics

- As a user: No logging in without a good padlock!



- As a provider: No enticing users to log in without HTTPS.

- Staff interface without padlock, especially if outside the building: CALL 911!!

The Web – Nitty Gritty

- Extended Validation

  – The Green Bar

- HTTP Strict Transport Security “HSTS”
- HTTP Public Key Pinning “HPKP”
- Certificate Stapling
- Whose certificate?

Beneath the Web – Nitty Gritty

- DNSSEC
- DANE

Horror Stories – Don’t be one!

- Staff interface – unencrypted.
- OPACs – unencrypted.
- SIP connections – unencrypted.
- 3rd party SIP clients which record patron passwords.
- Report modules – clear text.

Future Possibilities

- Logins by client certificate rather than password.
- Checkouts by hash – private even from the librarian.

Useful Tools

- HTTPS server tester:
  - https://www.ssllabs.com/ssltest/
- DNSSEC/TLSA Validator:
  - https://www.dnssec-validator.cz/
- Convergence:
  - http://convergence.io/

What did all that mean?

- …..


Biblionix™
POWER TO PUBLICS