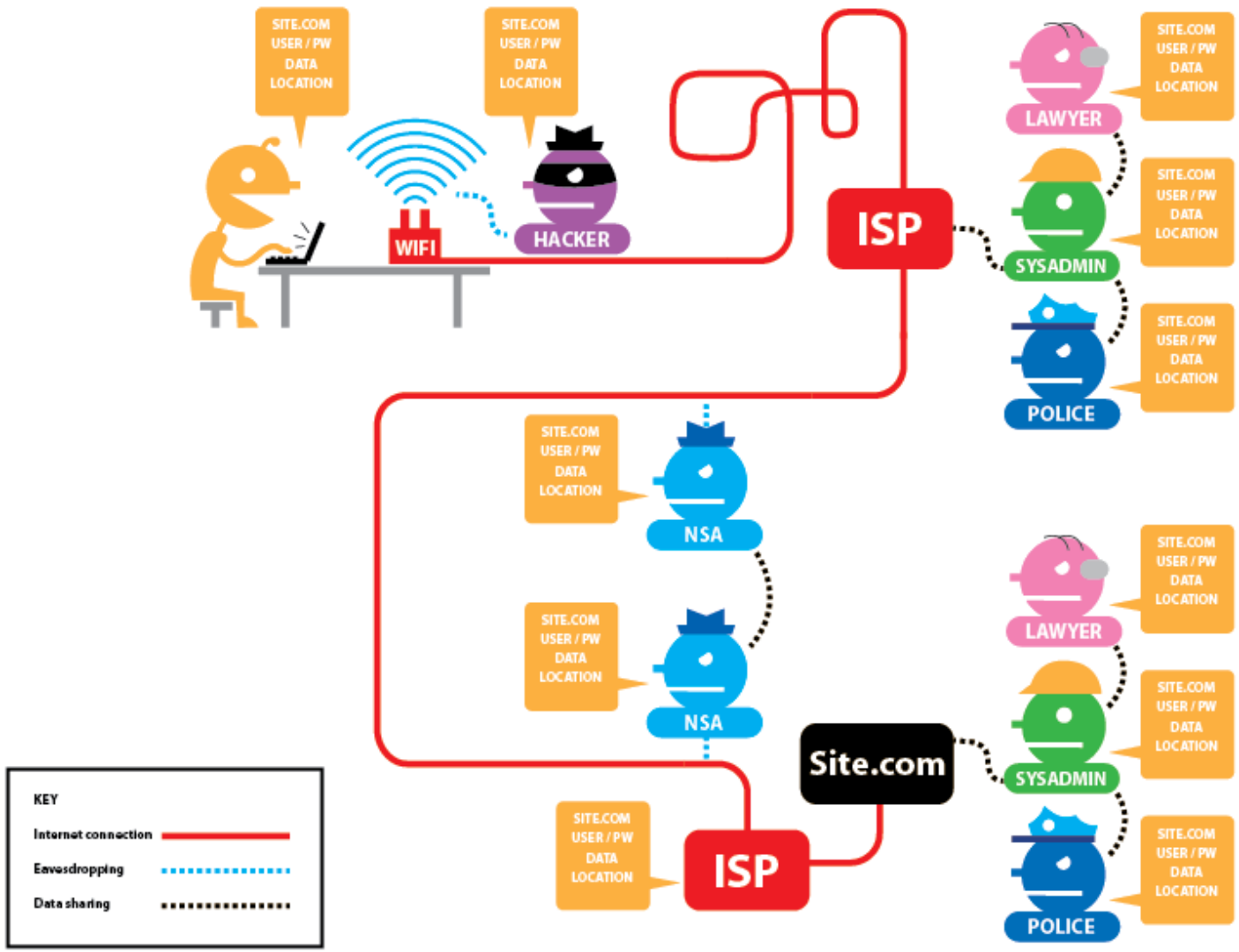
TLS: Today's Lite Security

Nov 2014

By @NullNode

Agenda

1. The Landscape
2. What is TLS?
3. The Chain of Trust
4. TLS Landscape
5. Technical Flaws
6. Known Vulnerabilities
7. Immediate Possible Protections
8. Conclusion



The Landscape

-Data Oriented Society

-No Unified Regulations

-Lack of Oversight

-Lack of Foresight

-*"Web 2.0"*

-Legacy Technology

-No Systems Standards

-Modern Wild West?

to crypto #CryptoPartyTO

What is TLS? - Transport Layer Security

-Originally referred to as SSL (Secure Socket Layer)

-Most commonly used in secure HTTP sessions, HTTPS

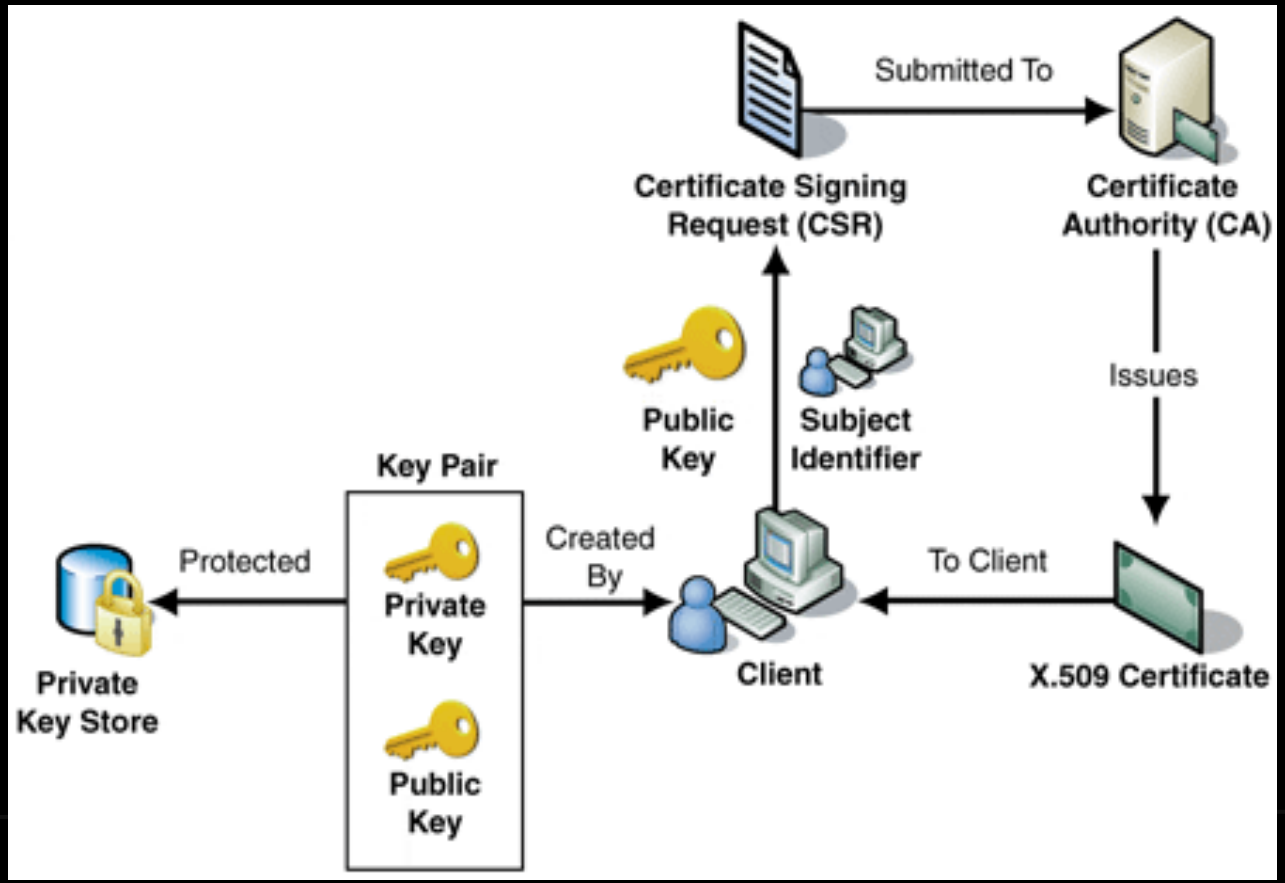
-Developed by NetScape in 1995 (first technical release)

-Based on X.509 certificate standard (certificate authorities / public key infrastructure)

-Reliant on chain of trust governed by industry giants

-Swappable/modular cipher suites

Chain of Trust



-Certificate exchange

-Centralized in nature

-Legacy trust model

-Universal concept

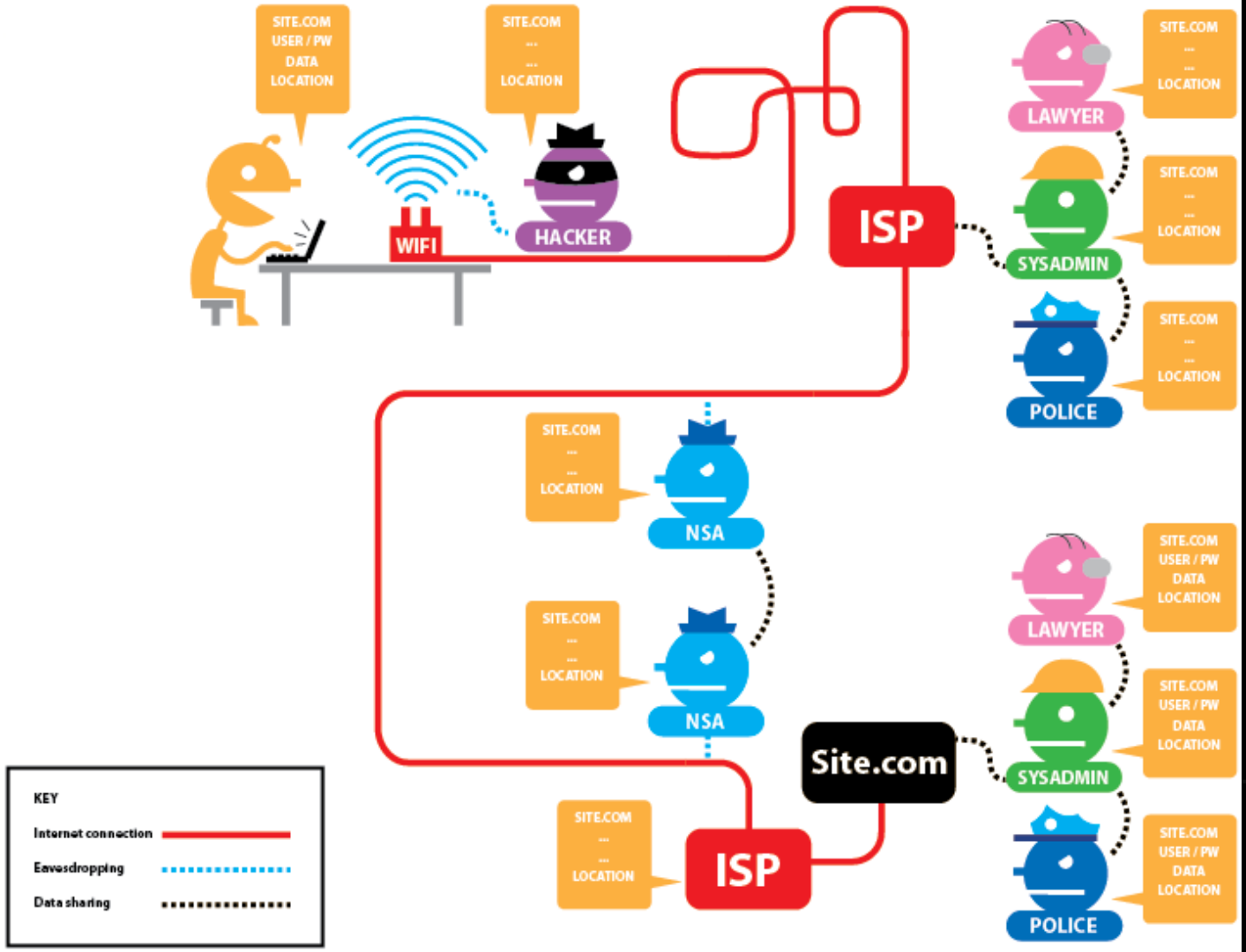
-Modular implementation

-Many implementations

-Stable model

-"Set in stone"

-Legacy support



TLS Landscape

-Industry view of TLS

-Encrypted in transit

-Need to know basis

-Metadata

-Still dependent on sites

-Lack of verification

-Not the whole picture

to crypto #CryptoPartyTO

Technical Flaws

-Built for a different generation and industry

-Centralized authority model

-Modular isn’t always good

-Fragmentation

-Legacy support

-Dependency support (RNG: Random Number Generator)

-Lack of consensus

Past Vulnerabilities

-Most have KNOWN exploits been patched/fixed

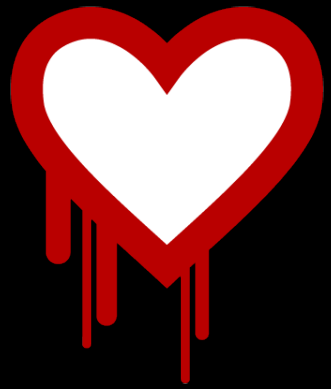
-At least 0.5% of all sites still vulnerable

-Most vulnerabilities can't be fully mitigated because of legacy support

-Library specific (sometimes)

-Public disclosure

-Is your data secure?



Top 10 Greatest Hits!

-Renegotiation attack
-Version rollback attacks
-BEAST attack
-CRIME attack
-BREACH attack
-Padding attacks
-POODLE attack
-RC4 attacks
-Truncation attack
-Heartbleed Bug

Immediate Possible Protections

-[Hard] Certificate Pinning

-[Hard] Manually distrust CAs

-[Easy] HTTPS Everywhere! (browser plugin)

-[Easy] EFF SSL Observatory! (community project)

-Practice Perfect Operational Security (PPOS)

    -Limit data you give out

    -Combine current technology and best practices

-Test your configurations and learn!

Conclusion

-The current model is broken

-Redefinition of secure needs to take place

-Encryption or trust?

-Centralized vs decentralized?

-Internet of things?

“It is in the admission of ignorance and the admission of uncertainty that there is a hope for the continuous motion of human beings in some direction that doesn't get confined, permanently blocked, as it has so many times before in various periods in the history of man.”

Richard P. Feynman

Questions?

Sources:

- http://tools.ietf.org/html/rfc6176
- https://www.eff.org/observatory
- https://www.eff.org/HTTPS-EVERYWHERE
- https://www.ibm.com/developerworks/library/ws-ssl-security/
- http://msdn.microsoft.com/en-us/library/ff647097.aspx
- http://technet.microsoft.com/en-us/library/cc785811.aspx
- https://eprint.iacr.org/2013/049.pdf
    - “Lessons Learned From Previous SSL/TLS Attacks A Brief Chronology Of Attacks And Weaknesses”
- https://www.isecpartners.com/media/106031/ssl_attacks_survey.pdf
    - “ATTACKS ON SSL A COMPREHENSIVE STUDY OF BEAST, CRIME, TIME, BREACH, LUCKY 13 & RC4 BIASES”
- http://news.netcraft.com/archives/2013/06/25/ssl-intercepted-today-decrypted-tomorrow.html

To learn more visit the TorontoCrypto.Org