Transport Layer Protection

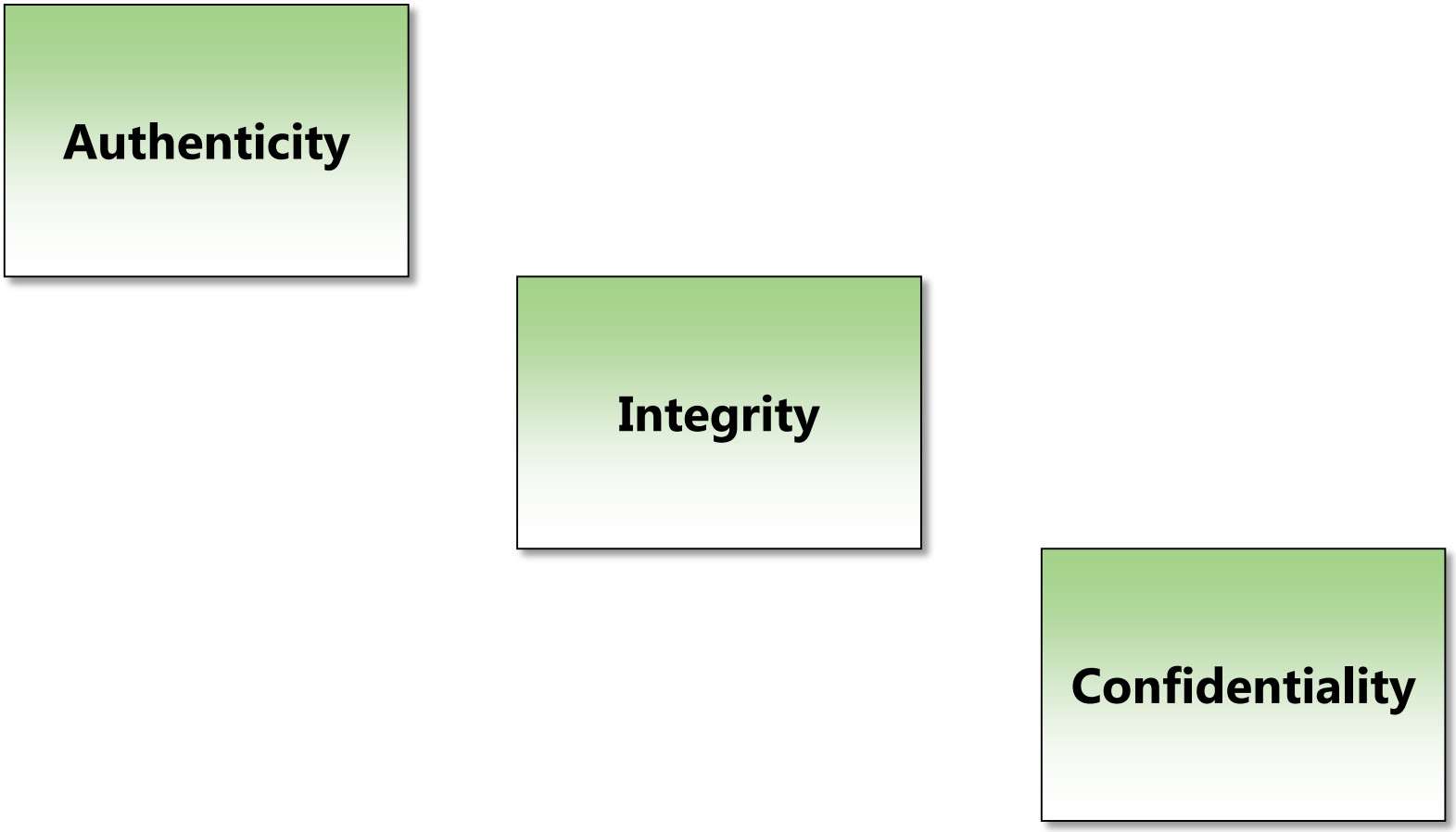
Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

Outline

- The three objectives of transport layer protection
- Understanding a man in the middle attack
- Protecting sensitive data in transit
- The risk of sending cookies over insecure connections
- How loading login forms over HTTP is risky
- Exploiting mixed mode content
- The HSTS header

The three objectives of transport layer protection



Authenticity

- Do we know who we're connecting to?
- What guarantees can be made as to their identity?

Integrity

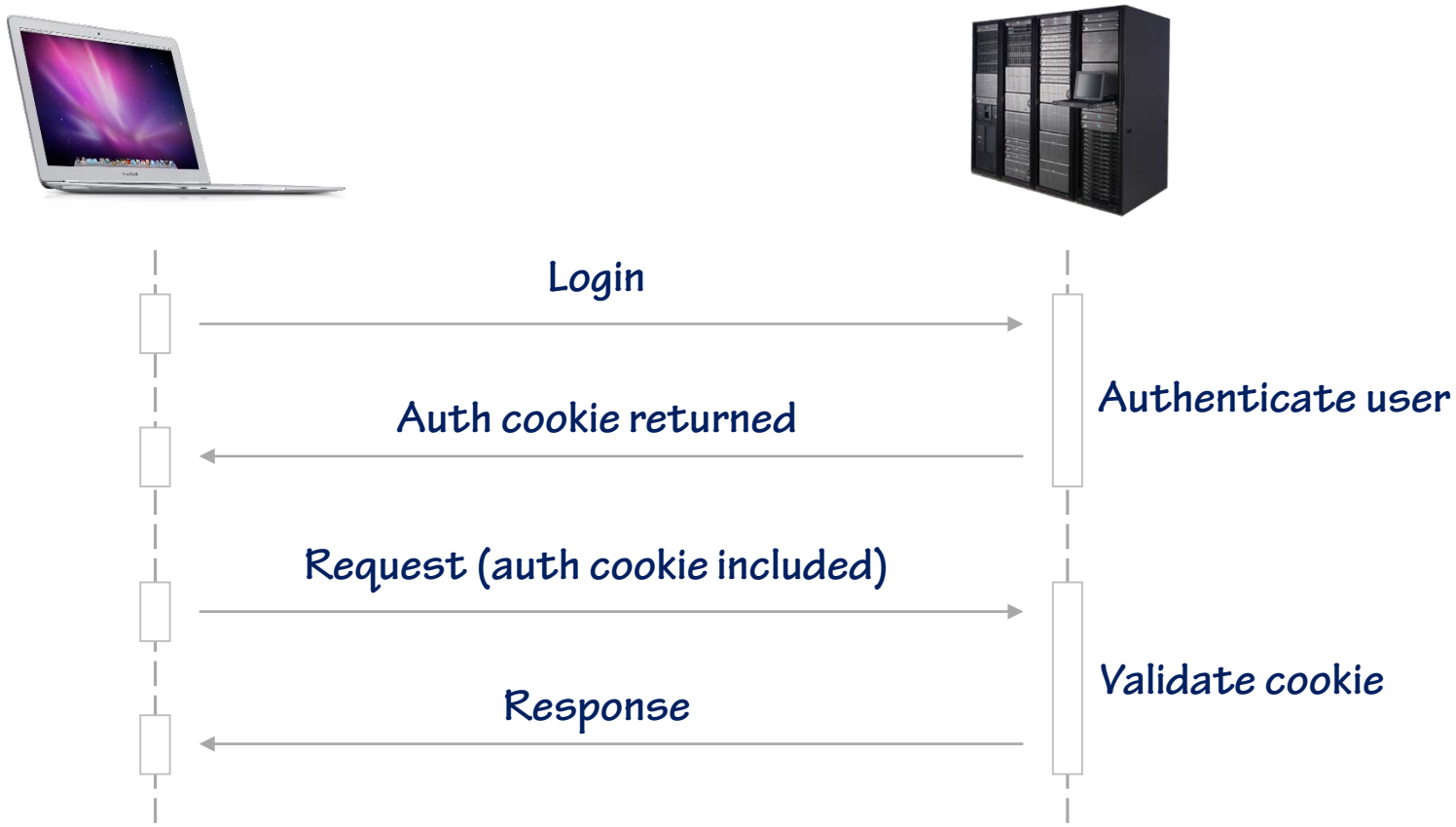
- Can we trust that our requests haven't been manipulated in transit?
- Conversely, can we be confident that the responses haven't been modified?

Confidentiality

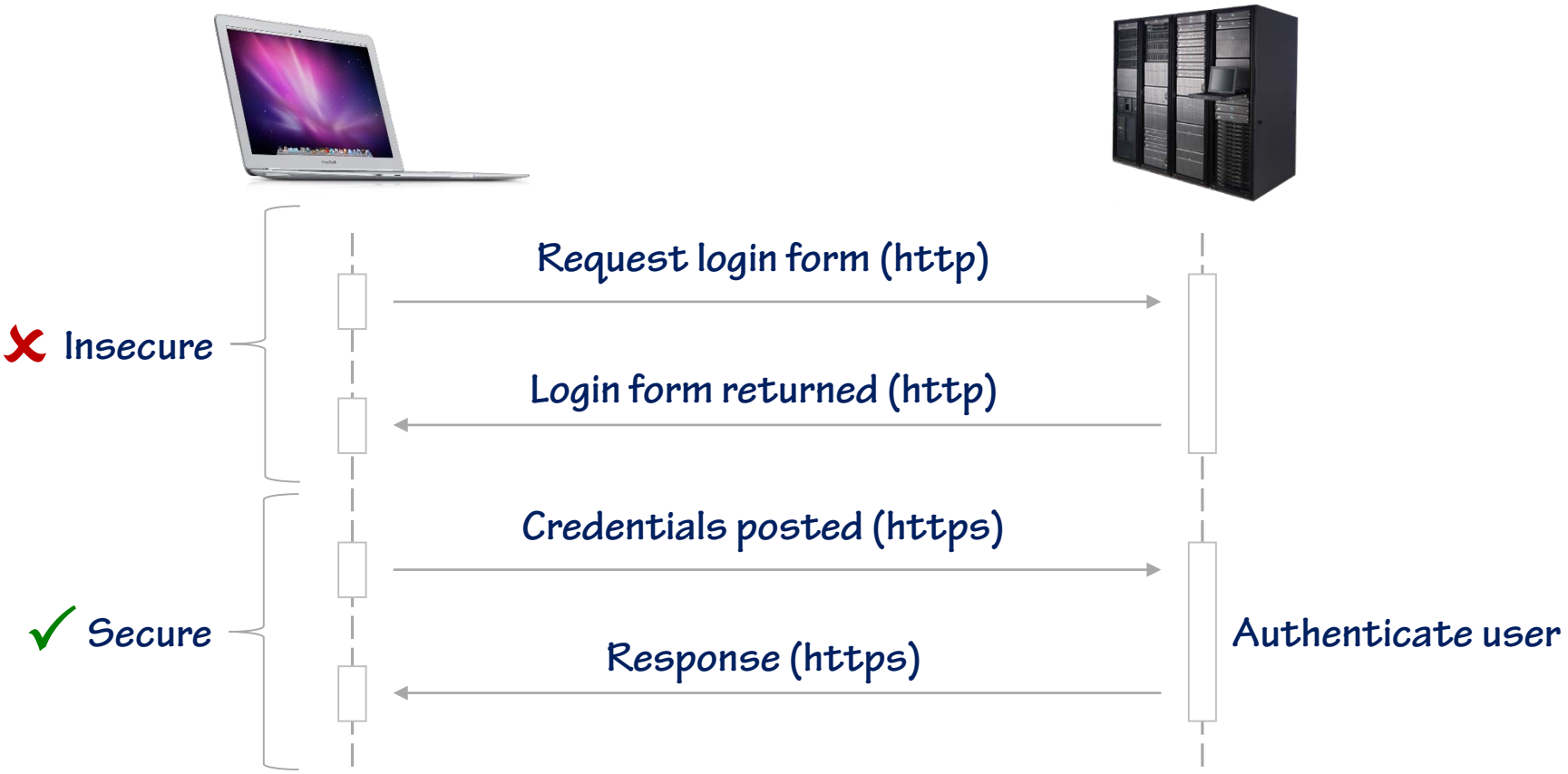
- Can we be confident the data we're sending to the website is kept private in transit?
- And again, conversely, are the responses sent to our browser being kept away from prying eyes?

Understanding a man in the middle attack

Persisting authentication state via cookies



Loading login forms over HTTP



Loading a secure page

All assets must be loaded securely

Summary

- **Always remember that SSL is about more than just encryption**
  - Authenticity, integrity, confidentiality
- **There are many, many points where an MitM attack can occur**
  - Wireless networks, proxies, ISP, internet nodes
- **If you acknowledge the need for SSL, then you must also acknowledge the need to implement it correctly**
  - Don't send sensitive cookies over HTTP
  - Don't rely on HTTP to load forms that deal with sensitive data
  - Don't embed insecure content in secure pages
- **Use HSTS as an additional safety net**
  - Unfortunately though, you can only rely on it in Chrome and Firefox