Sec 101

Diego Pacheco

About me...

- Cat's Father
- Head of Software Architect
- Agile Coach
- SOA/Microservices Expert
- DevOps Practitioner
- Speaker
- Author

diegopacheco

@diego_pacheco

http://diego-pacheco.blogspot.com.br/

https://diegopacheco.github.io/

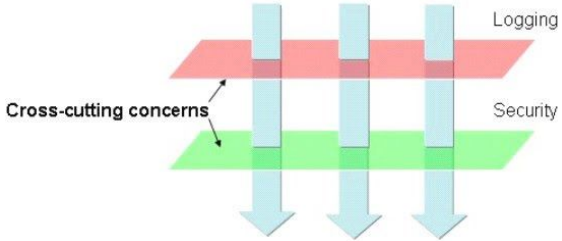
We are used to Security in the physical world

Software Security

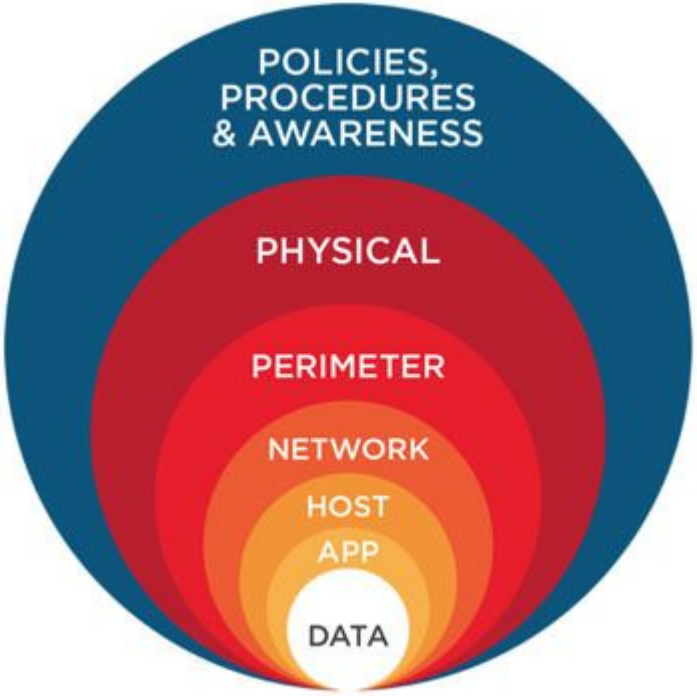
Why should we care?

- ❑ Ethics
- ❑ Customer Experience
- ❑ Brand Integrity
- ❑ Compliance

Defense in depth



- NSA
- Layers
- All IT systems
- It’s all about redundancy
- AV, Auth, Encryption, MFA, Sandboxes, DMZ, VPN, Firewalls, etc…

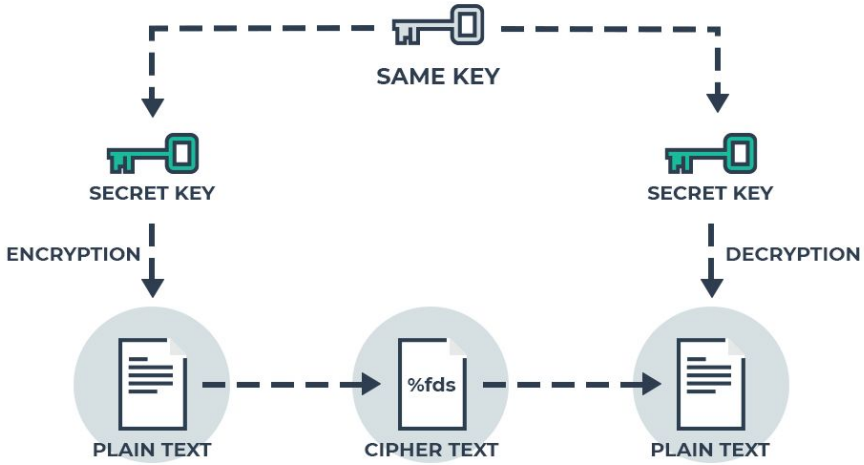


Least Privilege Principle

- ❏ Minimum level of access and privilege.
- ❏ Avoid wide open permissions like *
- ❏ Avoid Attacker Surface
- ❏ Spots malware spread

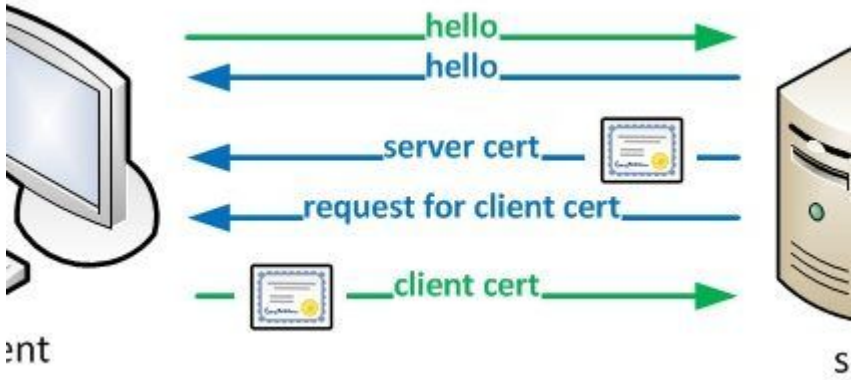
Encryption

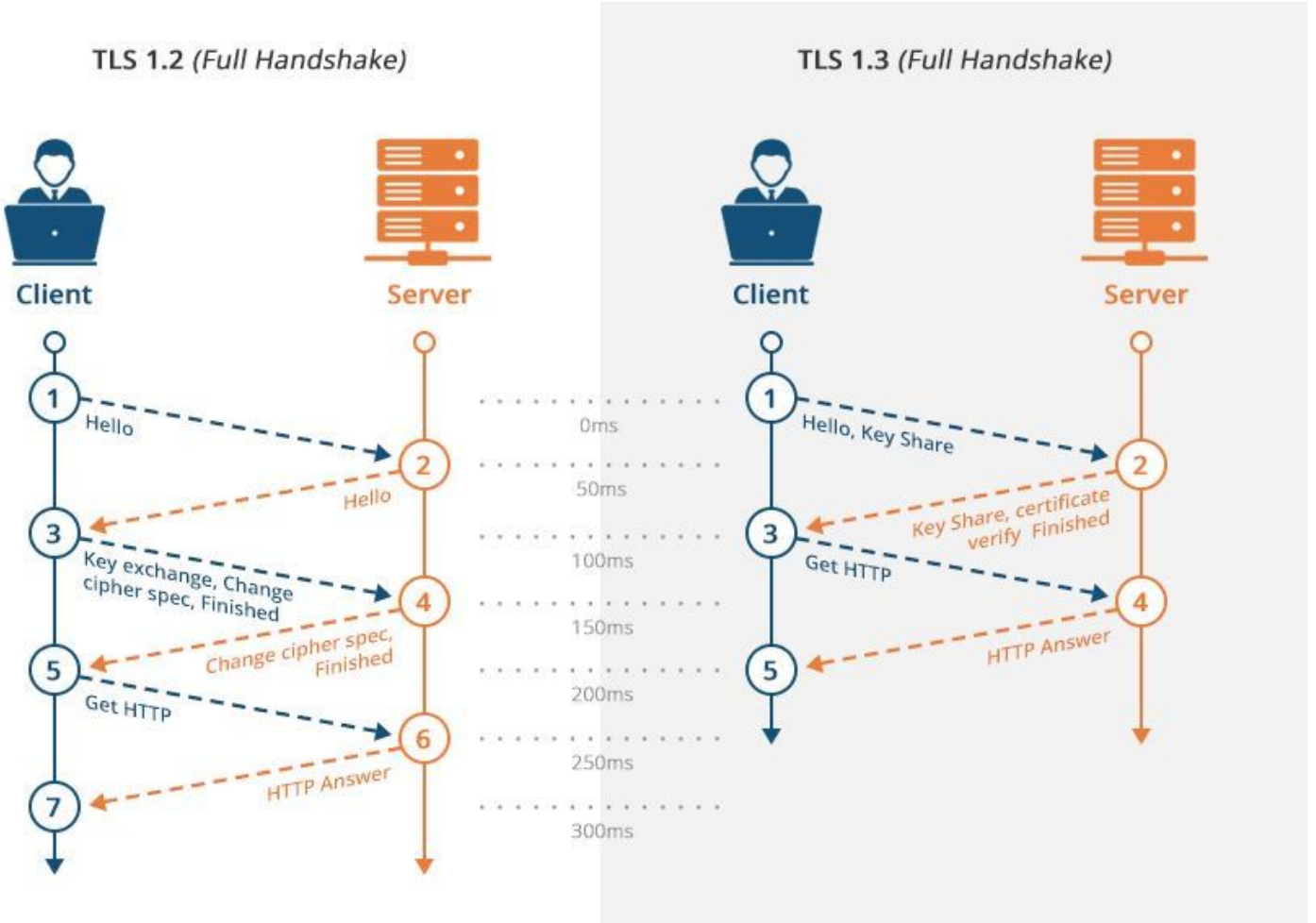
- ❑ Symmetric & Asymmetric
- ❑ Encoding Information
- ❑ AES Standard
- ❑ Key Diversity
- ❑ Envelope Encryption
- ❑ App vs Storage Encryption
- ❑ Rotations



TLS and mTLS

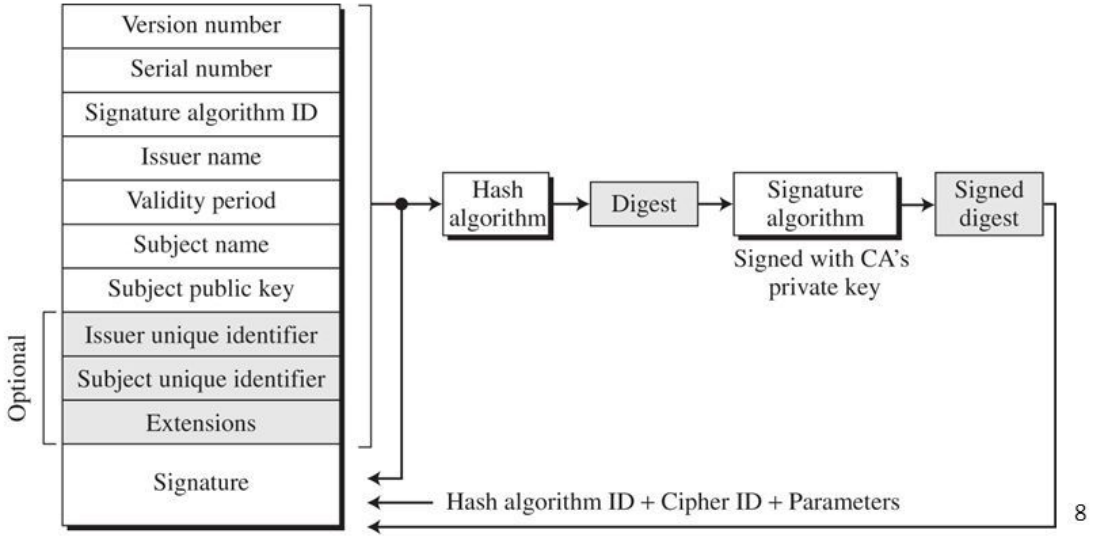
- Privacy and data integrity
- Secure Connections
- Asymmetric Encryption
- Email, Chats, VoIP, HTTPS
- mTLS - No Man in the Middle
- Rotations




TLS 1.2 (Full Handshake)
TLS 1.3 (Full Handshake)
Client
Server
Client
Server
1
Hello
2
Hello
3
Key exchange, Change cipher spec, Finished
4
Change cipher spec, Finished
5
Get HTTP
6
HTTP Answer
7
0ms
50ms
100ms
150ms
200ms
250ms
300ms
1
Hello, Key Share
2
Key Share, certificate verify Finished
3
Get HTTP
4
HTTP Answer
5

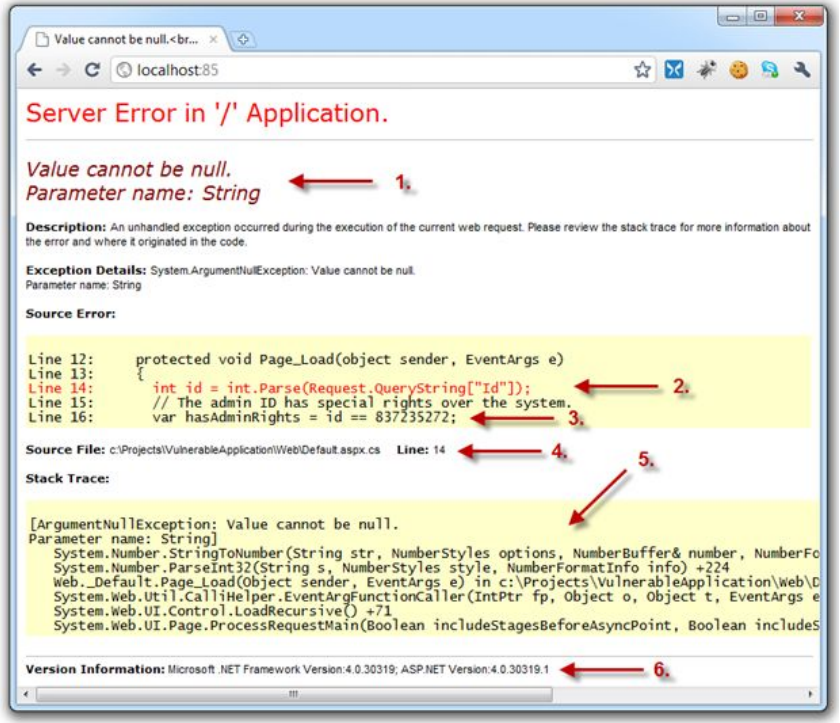
X.509 Standard

- Many known CA's (Verisign, Geotrust, Equifax, etc.)
- X.509 Standard provides common format for all certificates
  - Makes verification much simpler



Misconfiguration & Error Handler

- ❑ Unnecessary enable ports
- ❑ Stacks Traces
- ❑ Default Passwords
- ❑ Software Out of Date
- ❑ Missing Sec configs

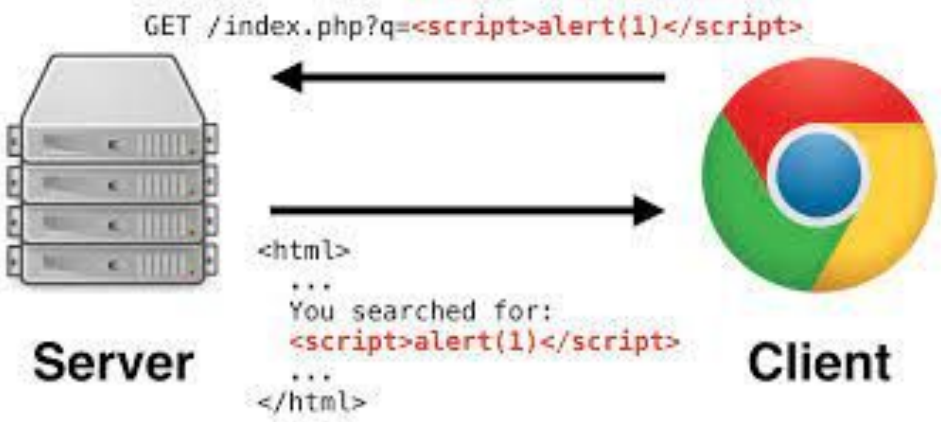


Input Sanitization

- SQL Injection
  - Prepared Statements
- Remote File Inclusion
  - Paths / Sequences
- Always clean user inputs
- Use UUIDs

XSS (Cross Site Scripting)

- ❑ JavaScript Injection
- ❑ Storage (view by admin)
- ❑ Reflected (back to user)
- ❑ Latest Browser versions
- ❑ Requires Sanitization



Insecure Serialization/Deserialization

- XXE - External XML Entity SAML(SSO), < SOAP 1.2
- XML Upload from untrusted sources
- Disable XML external entity and DTD processing
- Validate XML with XSD

Know Vulnerabilities

- ❑ OWASP top 10
- ❑ CVE/CWE
- ❑ Code Analysis
- ❑ Keep Software up to date

Logging & Audit Trail

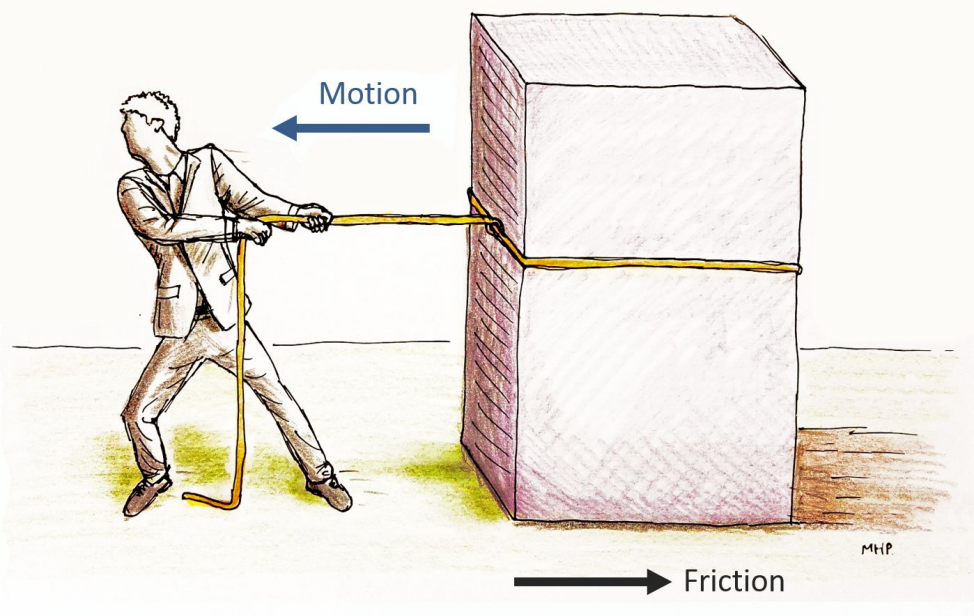
- ❑ Local / Unmonitored logs
- ❑ Audit trail on high-value transactions
- ❑ Monitoring on suspicious activities

Threat Analysis

- All models are wrong but some are useful for us
- Allow us to see the Threats
- Help figure out priorities
- Democratize security
- https://threagile.io/

Engineering Friction

- Tests, DevOps, ...
- Security might cripple engineering capabilities
- Security is a Refactoring enabler force
- Security is Everybody's jo



Sec 101

Diego Pacheco