M183 Applikationssicherheit Implementieren # 1

Herbst/Wintersemester 2017

Roman Thommen

roman.Thommen@gibz.ch

Web Application Security

«Web application security, is a branch of Information Security that deals specifically with security of websites, web applications and web services. At a high level, Web application security draws on the **principles of application security** but applies them specifically to **Internet** and **Web systems**»

https://en.wikipedia.org/wiki/Web_application_security

Internet & Web Systems?

(Stand 2017)

Internet & Web Systems

- Nodes:
  - Servers, Desktops, IoT-Devices, Printers, …
- Traffic
  - Data-Packets, Payloads, Streams
- Autonome Systeme
  - Bots, Malware, …
- Netzwerk
  - Architekturen
  - Topologien
- Protokolle
  - HTTP, HTTP2, I2P, TCP, Diffie-Hellmann, …
- Applikations Architekturen
  - GUIs, Webservices, …

Application Security Principles?

Application Security Principles 1

1. **Minimize attack surface area**
   - The search function may be vulnerable to SQL injection attacks. If the help feature was limited to authorized users, the attack likelihood is reduced
2. **Establish secure defaults**
   - Force Password refresh as default
3. **Principle of Least privilege**
   - Give a user at most the privileges for fulfilling the business case

Application Security Principles 2?

4 Principle of Defense in depth
5 Check at the gate
6 Fail securely
7 Don’t trust services and user input
8 Separation of duties
9 Avoid security by obscurity
10 Keep security simple
11 Fix security issues correctly

Motivation?

Motivation

Confidentiality

– only allow access to data for which the user is permitted

Integrity

– ensure data is not tampered or altered by unauthorized users

Availability

– ensure systems and data are available to authorized users when they need it (incl. archivation due to legal reasons)

Authorization

– It is the process that governs the resources and operations that the authenticated client is permitted to access

Motivation by example (tbc)

- Sensitive Daten dürfen jetzt und in Zukunft nur für authorisierte “Agents” zugänglich sein.
    - Bsp: E-Commerce-Tools, Notenverwaltung, Pharma-Rezepte

- Steuerung (Autonom / Remote) von Nodes im Web dürfen nur authorisierten “Agents” erlaubt sein.
    - Bsp: Self-driving Cars, Medizinische Überwachung

- Zugriff nur via autorisierte Kanäle
    -IP-Einschränkungen

- .

Importance?

Importance by example (tbc)

- Weiter fortschreitende Digitalisierung / Automatisierung
  - Medizin, Überwachung von Patienten
  - Smart-Shopping
- Anzahl, Standort und Typen von Nodes im Web nimmt zu
  - Mobile Geräte
  - Sensoren
  - Autos
- Traffic verändert sich
  - Total-Volumen und Kadenz
  - Form: Kleiner Payload, aber häufigeres Polling
  - Lokalität: Z.B. Parkplatzsensoren
- …

Consequences?

Consequences (tbc)

- Node-Lokalität kann Wahl über die Art der Authentifizierung beeinflussen:
  - Sensor sendet Payload oft (noch) unverschlüsselt. Einerseits um Strom zu sparen, anderseits schränkt die Reichweite den «Handlungsbereich» ein.
  - Im Gegensatz: google forciert https.

- Art des Traffics kann Wahl der Authentifizierung beeinflussen:
  - Häufiges Polling von kleinen Payloads -> Authentifizierungs-Token ist fix im Sensor eingebaut (“Token-Range”)
  - Im Gegensatz: Sessions

- Node-Typ kann die Art der Authentifizierung beeinflussen:
  - Retina-Authentifizierung für Geräte mit eingebauter Kamera
  - Im Gegensatz: Username & Passwort

-> Sehr Domain-Spezifisch & sehr schnellebig!

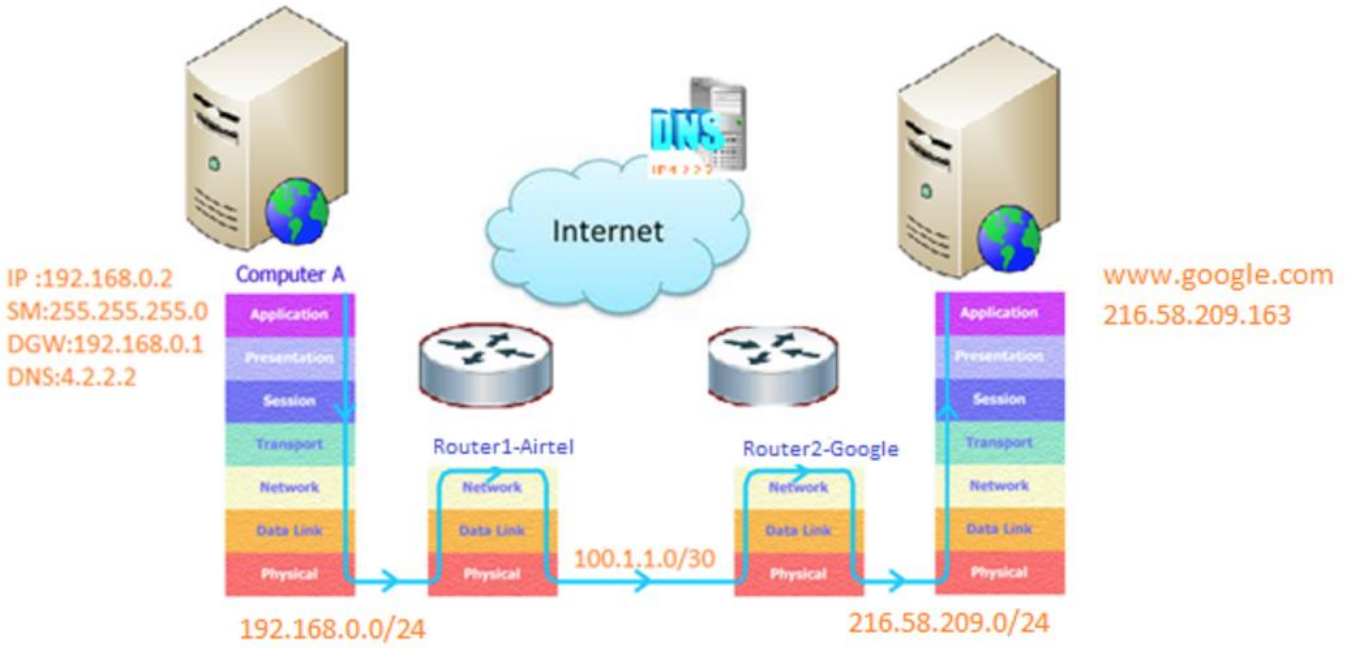
2 Webapplication scenarios

Machine to Machine (M2M)

&

Human to Machine (H2M)

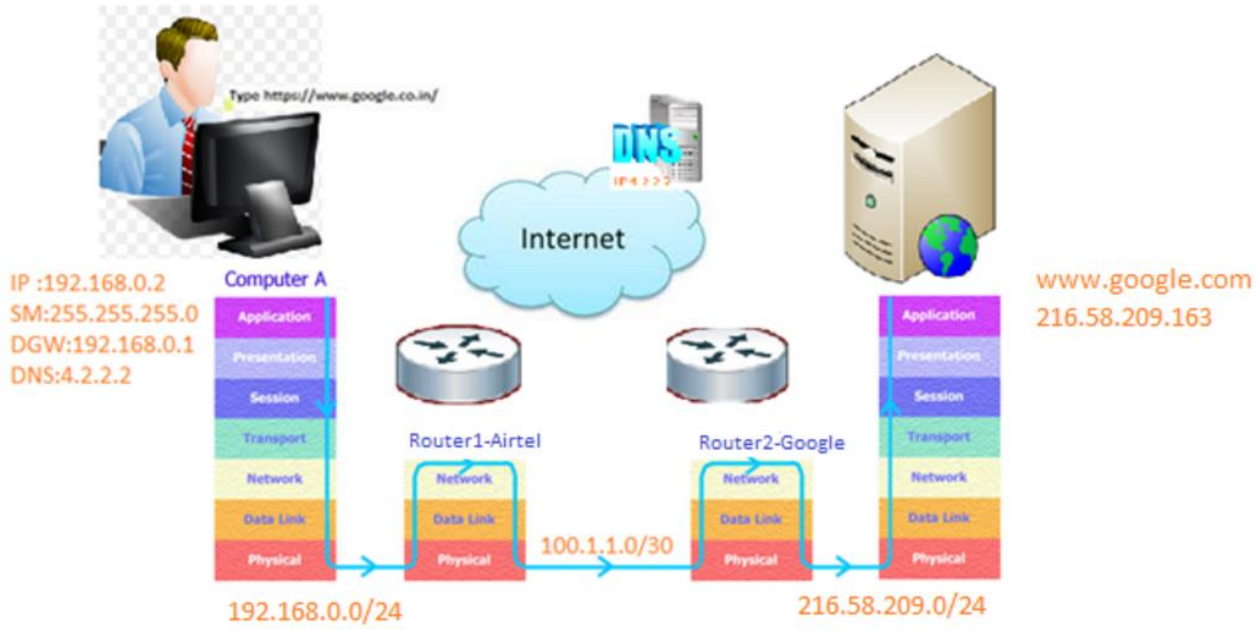
Web Application Scenario: M2M



Machine 1?: Native App, Sensor, Server

Machine 2?: Server, “Cloud”

Web Application Scenario: H2M



Human?: Native App, Browser

Machine?: Server, “Cloud”

Threats M2M/H2M-Scenario?

Threats M2M/H2M-Scenario

- OSI/Protocoll – Layers
  - Application: Trojans, Virus, Worms, etc.
  - Physical: Cutting Cables, Changing Pins, etc.
- “Traffic/Network”
  - “DNS”
  - Man in the Middle
  - …
- Web-Application
  - Authentication (Brute – Force, Rainbow Tables)
  - Injections
  - DOS
  - …
- Developer
  - Code Deployment
  - Versioning System
  - Error-Levels / -Handling
  - Development Environment
  - …
- Architecture
  - DB: Localhost / Server
  - Server (Non-SSL, IIS, Apache, nginx)
  - Local Sensor Networks
  - …
- User
  - Easy-to-guess Passwords
  - Physical Passwords (incl. RFIDs)
  - Old OS / Browser / Plugins
  - …

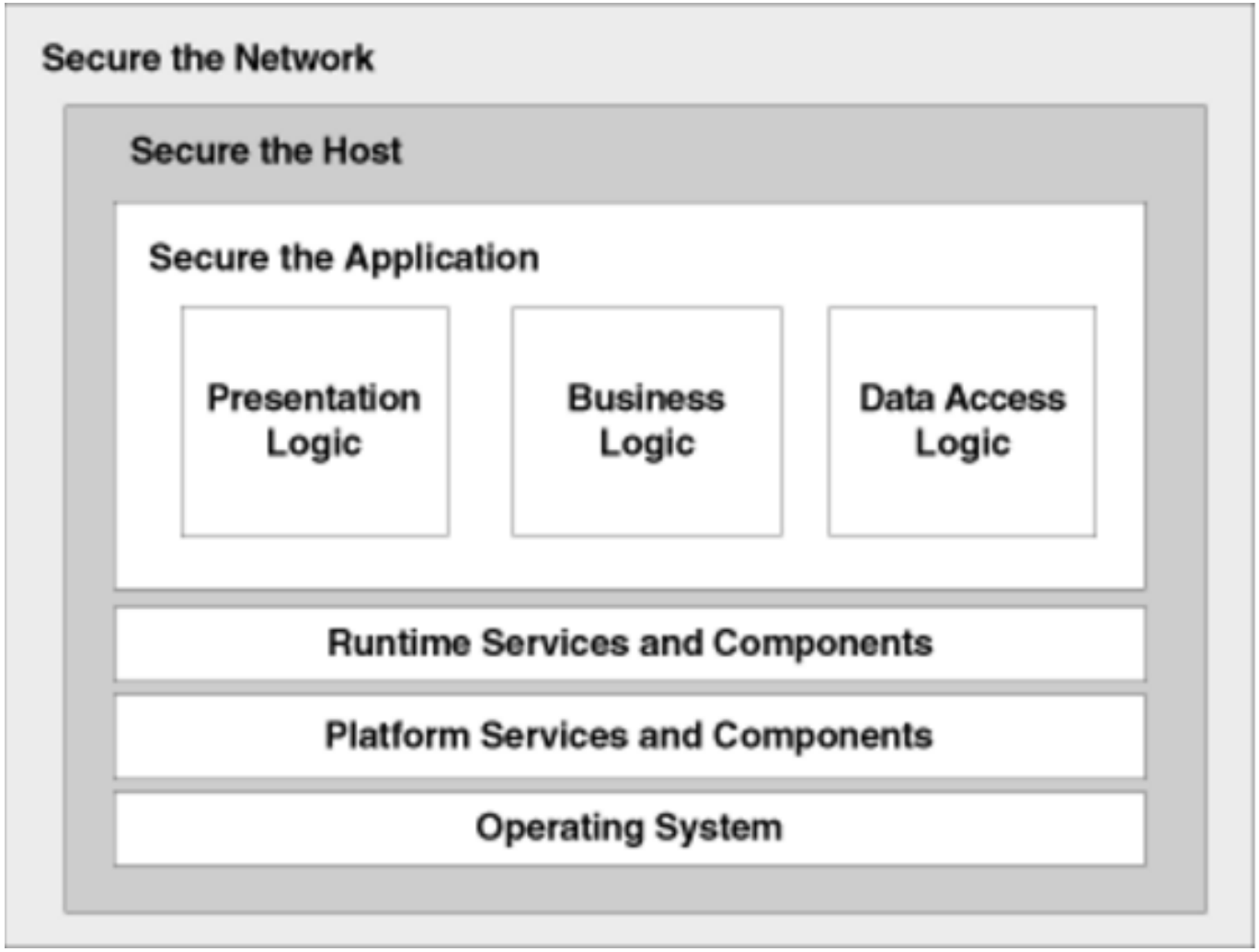
Threats of tomorrow?

- HTTP2
- IoT
- Docker
- …

Bei neuen Technologie eröffnen sich neue Falltüren.

-> **Security Models**, **Threat Detection and Monitoring**, **Best Coding Practices** und **Security Recommendations** je Domäne regelmässig checken (Twitter, Mailing-Listen, Webseiten)

Security Models (Microsoft)



Security Models (Wikipedia)

Ebene		Inhalt (Kurzfassung)	Verantwortlich	Fachkenntnisse
5	Semantik	Schutz vor Täuschung und Betrug	Zentrale	Corporate Identity und Unternehmenskommunikation
4	Logik	Absicherung von Prozessen und Workflows als Ganzes	Auftraggeber	Kenntnisse der Geschäftsprozesse
3	Implementierung	Vermeiden von Programmierfehlern, die zu Schwachstellen führen	Entwickler (Umsetzer)	Softwareentwicklung
2	Technik	Richtige Wahl und sicherer Einsatz von Technik	Fachentwickler, IT-Betrieb	Allgemeine IT-Security
1	System	Absicherung der auf der Systemplattform eingesetzten Software	IT-Betrieb	Netzwerk- und Systemadministration

Threat Detection & Prevention

Detection:
- Analyzing User & Attacker behavior (via Logs)
- Aktivitäten Überwachen (Monitoring)
- Eintrittsfallen stellen
- Hackathons organisieren (Defense & Offence Teams)
- …

Prevention:
- Source Code Security Analysis (SAST)
- Dynamic Application Security Testing (DAST)
- Penetration Testing
- Security Checklists
- …

Best Practices und Security Recommendations

Offizielle Quellen

- Open Web Application Security Project (OWASP) https://www.owasp.org/
- ISO – Standards
- W3C
- “Per Technology”: IIS, nginx, SSL, C#, Browsers

Bücher

- Writing Secure Code: Practical Strategies and Proven Techniques for Building Secure Applications in a Networked World (Developer Best Practices). ISBN-13: 978-0735617223

-http://www.cl.cam.ac.uk/~rja14/book.html (Gratis)

-https://www.owasp.org/index.php/Category:OWASP_Training & Bookstore: http://www.lulu.com/spotlight/owasp

Praktische Quellen

- https://security.stackexchange.com
- https://stackoverflow.com/questions/tagged/security
- https://msdn.microsoft.com/en-us/library/ff648636.aspx

Focus in M183

Category	Threats / Attacks
Input Validation	Buffer overflow; cross-site scripting; SQL injection; canonicalization
Software Tampering	Attacker modifies an existing application's runtime behavior to perform unauthorized actions; exploited via binary patching, code substitution, or code extension
Authentication	Network eavesdropping ; Brute force attack; dictionary attacks; cookie replay; credential theft
Authorization	Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
Configuration management	Unauthorized access to administration interfaces; unauthorized access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
Sensitive information	Access sensitive code or data in storage; network eavesdropping; code/data tampering
Session management	Session hijacking; session replay; man in the middle
Cryptography	Poor key generation or key management; weak or custom encryption
Parameter manipulation	Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
Exception management	Information disclosure; denial of service
Auditing and logging	User denies performing an operation; attacker exploits an application without trace; attacker covers his or her tracks

Exkurs: Professional Hacker «Pablos Holman»

https://www.youtube.com/watch?v=FtYW4sPefhY

http://www.intellectualventureslab.com/

https://twitter.com/pablos

Übungen

1. Youtube Video: Welcher Threat wird da angetönt? Wie funktioniert dieser? (Informeller Beschrieb).

2. Vervollständigen Sie die Liste der Threats je OSI-Layer. (Je Layer ein oder mehrere Threats).

3. Vervollständigen Sie Beispiele zu den Application Security Principles.

4. Youtube Video https://www.youtube.com/watch?v=8Kga-CHf-pU schauen.

5. Youtube Video https://www.youtube.com/watch?v=GHmkuv69PQE schauen.