



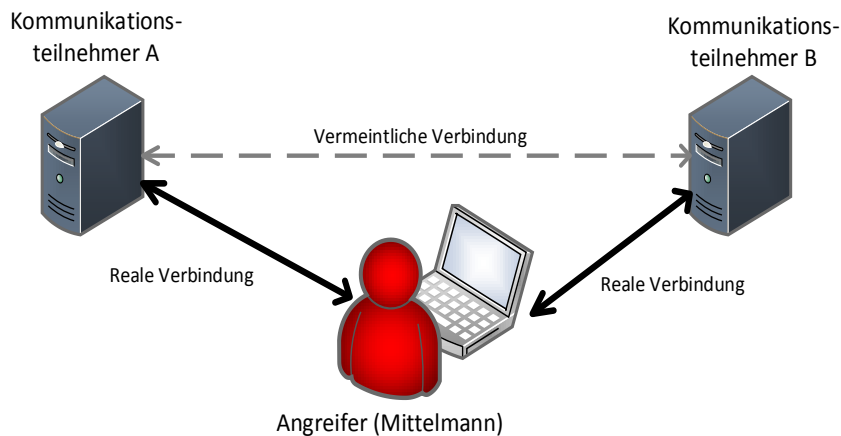
openHPI – Sicherheit im Internet Man-In-the-Middle Angriffe

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Man-in-the-Middle Angriffe (1/2)

Man-in-the-Middle-Angriff (kurz: **MitM**, dt. Mittelmannangriff), besteht in dem unberechtigten Zwischenschalten in eine Kommunikation, um diese abzuhören oder zu manipulieren

- Meistens bleiben MitM unbemerkt – **transparent** – von den betroffenen Kommunikationsteilnehmern
- Es gibt **verschiedene MitM-Varianten** auf der Ebene verschiedener Kommunikationsprotokolle und Dienste, z.B.
 - DNS – Domain Name System
 - SSL/TLS – Secure Socket Layer / Transport Layer Security
 - HTTP – Hypertext Transport Protocol
 - Darstellung der Web-Seite (im Web-Browser)



DNS-Man-in-the-Middle

Erinnerung

- **DNS – Domain Name Service** – sorgt für die mit dem Internet verbundenen Systeme für die Zuordnung von Domänenname und Internetadresse

Beim **DNS-Man-in-the-Middle – DNS-MitM** – sorgt Angreifer dafür, dass der Domänenname des Opfers seiner eigenen IP Adresse zugeordnet wird, so dass sämtliche an das Opfer versendete Nachrichten an den Angreifer ausgeliefert werden

Angriffsszenarium

- Angreifer sorgt für DNS-Spoofing der Opferdomäne
- Alle Datenpakete, die an die Opferdomäne gesendet werden, werden dann an die IP Adresse des Angreifers ausgeliefert
- Angreifer liest mit oder manipuliert Daten und leitet sie dann an echte IP Adresse des Opfers weiter

Beim **Man-in-the-Browser**-Angriff setzt sich ein Schadprogramm im Browser fest, so dass die Ansicht von Webseiten im Browser manipuliert werden und eingegebene Daten abgefangen werden können

- Ist spezielle Form des Man-in-the-Middle-Angriffs auf Anwendungsebene
- Sehr verbreitete Funktionalität in vielen Trojanern, insbesondere in Banking-Trojanern, z.B. bei
 - Zeus,
 - SpyEye,
 - Caberp

Beim **SSL-Man-in-the-Middle – SSL-MitM** – manövriert sich der Angreifer in (die Mitte einer) abgesicherte(n) Verbindung

- Besonders problematisch, das SSL/TLS die Sicherungsschicht betrifft, also die für die Ende-zu-Ende Verschlüsselung und sichere Authentifizierung verantwortliche Protokollschicht
- Nutzt einen zuvor etablierten **Man-in-the-Middle**-Kanal auf unterer Protokollebene, z.B. vermittelt von DNS-MitM
- SSL bietet Kommunikationspartnern die Möglichkeit, sich über digitale Zertifikate auszuweisen
 - erschwert MitM-Angriffe
- Funktioniert also nur im Fall von **Konfigurationsfehlern** bei SSL-Verbindungen und **menschlicher Unachtsamkeit** bei Akzeptanz von falschen Zertifikaten

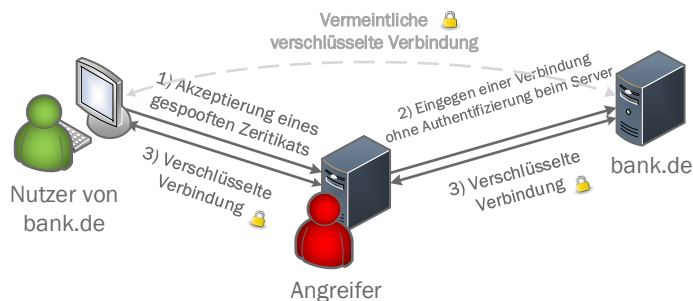
SSL-Man-in-the-Middle (2/3)

- Angreifer erstellt falsches digitales Zertifikat mit dem Namen „bank.de“
 - wird auf Grund der Dopplung des Namens von vertrauenswürdiger Stelle **nicht** signiert
- Opfer akzeptiert Zertifikat, obwohl Warnung über nicht vertrauenswürdiges Zertifikat erscheint



SSL-Man-in-the-Middle (3/3)

- Wenn (falsches) Zertifikat akzeptiert wurde, wird verschlüsselte Verbindung zum Angreifer (nicht zum gewünschten Kommunikationspartner) aufgebaut und vom Nutzer unwissentlich genutzt
- Zur Weiterleitung baut sich Angreifer eine Verbindung zur wahren Bank auf



Man-in-the-Middle-Angriffe sind oft **schwer zu entdecken**

Wichtigstes Gegenmittel: Starke Authentifizierung

- Verwendung von digitalen Zertifikaten

Trotzdem: SSL-Man-in-the-Middle ist auch mit (nicht von vertrauenswürdiger Stelle bestätigten) Zertifikaten möglich

- Zertifikate durch vertrauenswürdige Dritte bestätigen lassen
- Genaue Beachtung von Zertifikatswarnungen
- Zusätzlich für Betreiber: Nutzung von statischen Zertifikaten
 - echtes Zertifikat wird bei erster Kommunikation gespeichert
 - danach immer mit neu angelieferten Zertifikaten vergleichen und ggf. Warnung bei Abweichungen