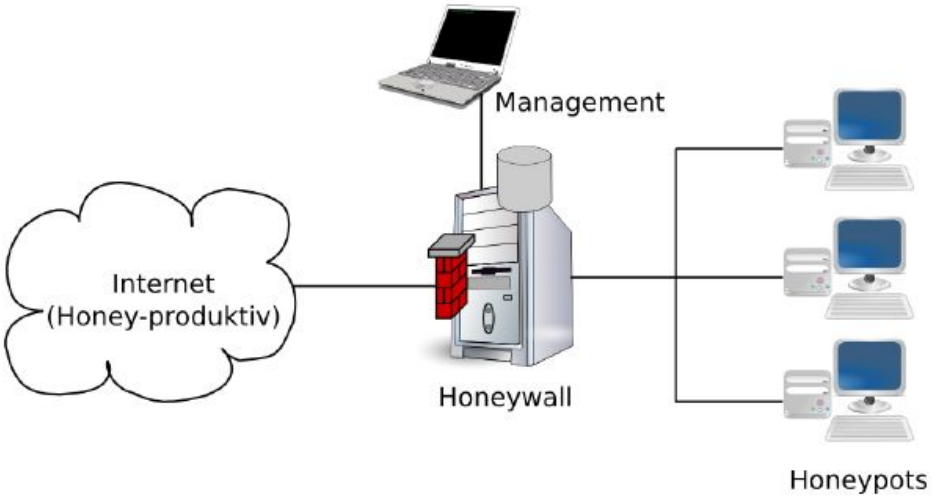
2017

Was ist ein Honeynet, woraus besteht es.

Honeynet = Netzwerk von Honeypots



Netz mit absichtlichen Schwachstellen, das benutzt wird um Angriffe zu analysieren und das Produktivnetz entsprechend vorbereiten zu können.

Müssen Apps bei einem Collusion Angriff die gleiche UID haben?
Antwort: Ja, müssen selbe UID haben (sharedUserId Attribut); erhält so mehrere Berechtigungen über verschiedene Apps (Jede App braucht eine andere Berechtigung zB Wetter-App: Internet und Text-App: Mikrofon)

Kann Gebäude-Sicherheit in einem Projekt vernachlässigt werden? +Begründung

Nein; wenn die Person direkt an den Rechner bzw. Server rankommt, kann sie Schadsoftware installieren

Was ist ein True-Positive bei IDPS?
Ein echter Angriff, der auch richtig aufgezeichnet wird

True-Negative → Kein Angriff und auch kein Alarm (→richtig als kein Angriff identifiziert)
False-Positive → Alarm obwohl kein Angriff
False-Negative→ Kein Alarm obwohl es einen Angriff gab

	Alarm JA	Alarm NEIN
Angriff JA	True-Positive	False-Negative
Angriff Nein	False-Positive	True-Negative

Security for Systems Engineers 2017SS Ausarbeitung

Nenne die 5 Schritte des IT-Grundschutzes.

■ Strukturanalyse
■ Schutzbedarfsfeststellung
■ Modellierung des Verbunds (Auswahl der Maßnahmen)
■ Basis-Sicherheitscheck (Soll-Ist-Vergleich)
■ Ergänzende Sicherheitsanalyse

Nenne 3 Arten wie mit Risiko umgegangen werden kann.

Akzeptanz (auf Management-Ebene)
Vermeidung
Verminderung/Mitigierung
Transferierung (Versicherung)

Beschreibe 2 UDP DoS Angriffe.

1. **UDP Packet Storm**: durch senden vieler Pakete an Broadcast- oder Multicast-Adressen wird ein hoher Netzwerk-Traffic erzeugt, welcher das Netz lahmlegen kann; dies wird noch verstärkt wenn das Netz Schleifen oder Redundanzen enthält
2. **UDP Flood Attack**: viele UDP Pakete werden an verschiedene Ports des Opfers gesendet. Opfer-Server muss nachsehen welche Applikation läuft und antworten (auch mit ICMP-Host Unreachable); häufig wird auch die Adresse gespooft und die Reply an falsche (oder nicht existente Adressen gesendet) → DoS Attacke

Nenne 3 Möglichkeiten für HTTP Sessions und Probleme damit (oder so ähnlich).

- Cookies im Header (Header kann manipuliert werden)
- Hidden Form Field (kann im HTML Code ausgelesen werden)
- URL Parameter als Klartext (kann direkt aus der URL herausgefunden werden)

Nenne 3 HTTP-Methoden und die damit verbundenen Probleme.
(HTTP-Methoden)

1) GET → Parameter werden in der URL übertragen, sensible Daten können ausgelesen werden
2) OPTIONS → Abfragen am Server welche HTTP-Methoden unterstützt werden; kann verwendet werden um vom Server zu lernen bzw. um ihn auszuforschen
3) PUT → Datenupload; kann verwendet werden um Tabellen zu manipulieren
4) DELETE → Daten löschen

Weitere: POST (payload im message body), HEAD (nur head ohne message-body), TRACE (veränderungen nachvollziehen)

Generell: nicht benötigte Methoden abschalten (häufig PUT, TRACE, OPTIONS, DELETE)

Beschreibe TCP Poisoning und warum es möglich ist.
→ Pakete oder Header unbemerkt verändern???

Nenne 3 mögliche Ziele von Mobile-Malware.

1. Stehlen von Benutzerinformationen Kontaktdaten, Browserdaten, Download History (kann verkauft werden)
2. Premium Anrufe/SMS

3. SPAM versenden
4. Stehlen von Zugangsdaten (Bank, Facebook-Login, etc.)
5. Optimierung des Rankings von Suchmaschinen
6. Erpressung

Erkläre Unterschiede, VT/NT von anomaly- bzw. signature-based IDPS.

Anomaly-Based IDPS:
Es werden Regeln erstellt, welche Aktionen auf einem Host bzw. in einem Netzwerk als "normal" betrachtet werden. Abweichendes Verhalten wird als Angriff betrachtet.
Vorteile:

- Erkennung von unbekannten Angriffen

Nachteile:

- Oft hohe False Positive Rate
- "normales" Verhalten zu definieren sehr schwierig
- Angriffe mit "normalen" Systemverhalten werden nicht erkannt

Signature-Based IDPS:
Hier werden Signaturen von Events betrachtet und verglichen. Signatur ist ein Pattern, das einen Angriff identifiziert.
Vorteile:

- weit verbreitet und einfach zu implementieren

Nachteile:

- Signatur für jeden Angriff benötigt
- Unbekannte Angriffe werden nicht erkannt
- Viele False Positives und False Negatives, wenn Signatur nicht korrekt

Stateful-Based IDPS:
nur vordefinierte Events und Aktivitäten werden zugelassen

2016

Erkläre Low Rate TCP DoS Attacks.

Übliche TCP DoS Attacke - viele Pakete werden gesendet um den Server zu überfordern.

Low Rate TCP DoS: es werden nach der Zeit immer mehr "normale" Verbindungen geöffnet (mit kleinen, unauffälligen Datenmengen) und diese Verbindungen bleiben offen bzw. werden mit Keep-Alive-Paketen offen gehalten, bis der Server keine weitere Verbindung aufmachen kann und dadurch überlastet wird.

Erkläre Broadcast Theft Android + Beispiel für richtigen und falschen Einsatz

BroadcastReceiver: 2 Arten

1) Systemevents→ Battery Low, SMS Received, etc.
2) Custom Events

Broadcast Intents können von Applikationen empfangen bzw. abgefangen werden und nicht legitimierte Apps können auch Broadcast Intents senden (welche legitim aussehen und auch weiterverarbeitet werden) → Source immer checken und Rechte vergeben wer Broadcasten darf und wer nicht

Beschreibe den Schritt der Modellierung beim IT Grundschutz

■ Basis Strukturanalyse und Schutzbedarfsfeststellung

■ Abbildung des betrachteten/analysierten IT-Verbunds auf IT-Grundschutz-Bausteine

■ Zusammentragen der relevanten Sicherheitsmaßnahmen aus den Maßnahmenkatalogen

■ Ergebnis ist ein IT-Grundschutz-Modell des IT-Verbundes

Was sind Intents in Android? Wozu verwendet? Probleme?

Inter Component Communication (ICC) → implizit (an bestimmte Komponente) vs. explizit (aktion wie z.B. action.send)

Message passing System → inter- und intra-App-Kommunikation

Confused Deputy Attack: Schadhafte App hat keine Berechtigung aufs Mikrofon zuzugreifen aber sendet Intent an z.B. Kontakte (welche diese Berechtigung hat) und verwendet Mikrofon

Injection Angriffe

Welche dieser Tools sind Decompiler? (Multiple Choice)

■ JD – Java Decompiler

■ JAD – Java Decompiler

■ JetBrains – .Net Decompile

Welche dieser Tools sind Obfuscator?

■ Proguard – Java Obfuscator

■ Eazfuscator – .Net Obfuscator

Nenne 3 Ziele von Code Encryption.

■ Zugriff auf Code einschränken

■ Code vor Manipulation schützen

■ Dekompilieren verhindern

Was kann trotz Code Encryption nicht gewährleistet werden?

VM Manipulation

Speicherung des Schlüssels nach wie vor ein Problem

Lademechanismus der VM ausnutzbar

Debugging

Wie vermeidet man Insufficient Transport Layer Security? (Multiple Choice)

TLS, VPN, White listing, Filtern von Hochkommas

Aufgrund des Android Sandboxing Systems soll man sensible Daten eher auf dem Client speichern. Richtig oder falsch? → Falsch

Erkläre XML Injections. Wie kann man diese verhindern?

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE accounts SYSTEM "accounts.dtd">
<accounts>
    <account>
        <username>e123456</username><pwd>hash(deem*ohG1oor)</pwd>
            <perms>rw</perms></account><account><username>e654321
        </username>
        <pwd>deem*ohG1oor</pwd>
        <perms>r</perms>
    </account>
</accounts>
```

verhindern durch Codierung der Zeichen oder nicht zulassen von “<” und “/>”

Was ist der Unterschied zwischen Network Layer Firewall und Application Layer Firewall?

Application Layer auf höherer OSI-Ebene; betrachtet Input, Output, Access etc.

Network Layer Firewall: auf OSI Ebene 3 betrachtet Traffic, einzelne Pakete, etc.

Nenne zwei Beispiele für Google Hacking.

■ Websites mit potenziellen MySQL SQL Injection

→ inurl:"php?id" "You have an error in your SQL syntax"

■ Oracle-Applikationen ermitteln

→ intitle:iSQL intitle:Release inurl:isqlplus

■ Fehlerhafte Konfigurationen

→ filetype:inc intext:mysql_connect

■ Webcams
→ intitle:axis intitle:"video server"

■ Jenkins mit offener Admin-Schnittstelle

→ intitle:"Dashboard [Jenkins]" intext:"Manage Jenkins"

Erkläre "Failure to Restrict URL Access"

Angreifer hat Zugriff auf Funktionen (über URLs), für welche er nicht berechtigt ist (z.B. asdf.com/[user|admin]/getAccessData

Was macht die Monitor- und Aktionskomponente in IDPS?

Aufbereitung und Durchführung von Aktionen

Man hat aus verschiedenen Gründen nur HTTP zur Verfügung. Ist es sicher das Passwort am Client mittels SHA512 zu hashen und nur diesen + Username an den Server zu übertragen?

man sollte zusätzlich noch mindestens einen Salt verwenden ???

Nenne 3 Wege mobile Malware zu verbreiten.

Repackaging: Runterladen vom App-Store, modifizieren, Upload auf nicht legitimen Plattformen

Update Angriff: Neue Update Routine wird hinzugefügt

Drive-By-Download: “stealth” download

manuelle Installation/Fake Apps

Nenne zwei Dinge, die aus Security Sicht beim Logging zu beachten sind. Nenne zwei Probleme die auftreten können.

Einheitlicher Aufbau der Log-Files

Logging Frameworks verwenden

Muss geloggt werden: Datenmanipulation, Anmeldeversuche, Authorization Requests, Session-Terminierung

Probleme:

- Detailgrad des Logs
- Speicherort der Logdateien
- Größe und Lebensdauer von Logdateien
- Sensible Informationen
- Intrusion Detection System (IDS) und Intrusion Prevention System (IPS)
- Nichtabstreitbarkeit / Nachvollziehbarkeit

Warum ist Security und Usability wichtig? Nenne 3 Gründe.

1. Security wird nur benützt bzw. angewendet, wenn sie auch vom User verstanden wird
2. Schlecht Designte oder nicht aussagekräftige Fehlermeldungen werden ignoriert oder “weggeklickt”
3. User umgehen Security weil zu komplex oder aufwändig

2015

welche Maßnahmen gehören zum Bereich transport layer security?

verschlüsseln und signieren der Daten vor der Übertragung
Setzen der Secure-Flags bei Cookies

welche Arten von Honeypots gibt es? (geringe, hohe, mittlere, schwankende interaktivität?)

2 grundlegende Arten:
geringe Interaktivität → Simulation (wenige Dienste) → eher zum erkennen von automatischen Angriffen
hohe Interaktivität → reale Systeme → erkennen von manuellen Angriffen (aber auch schwieriger zu Verwalten und aufzubauen)

welche dieser Aussagen über das Maximumprinzip sind richtig?

maximumprinzip: das System hat immer den Schutzbedarf der Komponente mit dem höchsten Schutzbedarf; zB 3 Applikationen mit niedrigem Schutzbedarf und eine mit hohem Schutzbedarf → System hat hohen Schutzbedarf

wie kann man ein drahtloses Netzwerk absichern?

- WPS ausschalten
- admin name+passwort ändern
- wlan ssid ändern (wenn netzwerk “ThomsonXXX” heißt, weiß der Angreifer, welches Modell der Router hat)
- Verschlüsselung aktivieren
- Firmware Updaten
- standard-passwort ändern

- mac-adressen whitelisten (es können sich nur eingetragene mac-adressen verbinden)
- dhcp ausschalten

Beschreiben Sie die Fragment Overlap Attack.

IP Fragmente überlappen einander und beim zusammensetzen dieser Fragmente werden Exceptions geworfen oder ähnliche Systemfehler treten auf

Was ist Split DNS?
In einer Split DNS Infrastruktur werden 2 Zonen für die gleiche Domäne verwendet; eine wird vom internen Netzwerk und die andere vom externen Netzwerk verwendet (Normalfall: Benutzer im Internet). Interne Hosts werden zum internen DNS weitergeleitet (kann auch auf Unternehmensressourcen oder sensible Daten zugreifen) und externe Hosts werden auf den externen DNS Server weitergeleitet
→ verstecken von internen Unernehmensressourcen für Außenstehende

Was ist Certificate Pinning und warum ist es für mobile App-Entwickler wichtig?

Zertifikate werden normalerweise über die Hierarchie bestätigt. Beispiel: Das Zertifikat "asdf" soll überprüft werden. Das Zertifikat ist von Google signiert. Da man Google vertraut, vertraut man auch "asdf".
Certificate Pinning umgeht diesen Prozess, das heißt es wird einfach dem Zertifikat speziell vertraut/nicht vertraut, ohne Hierarchie-Überprüfung.

Dient zur Verhinderung von Man-In-The-Middle-Attacks

Erklären Sie vier Aufgaben in der Strukturanalyse der IT-Grundsicherung

- Erfassung der Anwendungen und der zugehörigen Informationen; z.B. Personaldatenverarbeitung
- Netzplanerhebung; z.B. Switches, Router
- Erhebung der IT-Systeme; z.B. Server f¨ur Personalverwaltung
- Erfassung der Räume; z.B. Serverraum
- Komplexitätsreduktion durch Gruppenbildung (zB alle Mitarbeiter außerhalb der IT haben selbe Gruppe "User")

Erklären Sie den allgemeinen Ablauf im (Risiko-)Managementprozess (gemeint war, denke ich, Plan - Do - Check - Act mit Erklärungen).

PDCA

Risikoidentifikation
Risikobewertung

Risikobehandlung/-steuerung
Risikokontrolle

Beschreiben Sie drei Ziele von IDS.

- **Unterstützung** der **Aufrechthaltung** der **IT-Sicherheit** während des Betriebs
- Möglichst frühe und genaue **Erkennung von möglichst vielen Angriffen/böswilligen Aktivitäten**, d.h. Verletzungen der Security Policies, mit guter Darstellung der Incidents
- Dadurch **Schadensreduzierung** bei Angriffen
- Erkennung von **Fehlkonfigurationen** (z.B. von Firewalls)
- **Abschätzung** der Gefahrenlage für ein Unternehmen
- **Abschreckung** von AngreiferInnen, aber auch MitarbeiterInnen

Nennen Sie drei Injection Flaws.

= Möglichkeiten für Injections

1. SQL-Injection,
2. Command-Injection
3. XML-Injection
4. XPath-Injection

Können HTTP Header Pakete einer Anwendung auf einem Internet-Zugangsrouter gesehen werden, wenn diese an eine nicht existente Domäne von einer Webapplikation gesendet werden. (+ Begründung schreiben)

Zusätzliche Recherche und Notizen:

01- Netzwerk Sicherheit

- IP
  - **Fragment Overlap Attack**: IP Fragmente überlappen einander und beim zusammensetzen dieser Fragmente werden Exceptions geworfen oder ähnliche Systemfehler treten auf
  - **Ping of Death**: IP Pakete, welche laut Spezifikation zu groß sind und deshalb den Empfänger zum Absturz bringen können oder hohe Server-Last erzeugen (spezielle DoS-Attacke)
  - **Tiny Fragment Attack**: IP-Paket Filterregeln können dadurch umgangen werden, dass Pakete „zu klein“ sind, um von einem TCP-Header Filter gefiltert werden zu können
- **IPv6**
- **UPD**
  - **UDP-Flood:** viele UDP Pakete werden an verschiedene Ports des Opfers gesendet. Opfer-Server muss nachsehen welche Applikation läuft und antworten (auch mit ICMP-Host Unreachable); häufig wird auch die Adresse gespooft und die Reply an falsche (oder nicht existente Adressen gesendet) à DoS Attacke
  - **UDP Packet Storm:** durch senden vieler Pakete an Broadcast- oder Multicast-Adressen wird ein hoher Netzwerktraffic erzeugt, welcher das Netz lahmlegen kann à dies wird noch verstärkt wenn das Netz Schleifen oder Redundanzen enthält
- DNS
  - **Name Chaining:** DNS Eintrag von vertrauenswürdigem Server leitet weiter zu unsicherem Server
  - Erraten ID für DNS Request
  - Mitlesen/Verändern von Requests/Replies
- TCP
  - **Low Rate DoS**: nicht wie übliche DDos Attacke – Pakete werden in längeren Abständen gesendet und sehen wie legitime TCP Pakete aus
  - **Christmas Tree Packing:** TCP Attacke bei der im TCP Header alle Options gesetzt sind und daher aufwändig vom Server überprüft werden müssen (jede Option vorstellbar als Glühbirne in einer anderen Farbe à wenn alle leuchten, Weihnachtsbaum)
  - **Session Poisoning:** Session-Daten modifizieren
  - **Session Hijacking:** Session eines anderen übernehmen

02- Sichere Programmierung

- **Checked vs. Unchecked Exception (z.B. RuntimeException):** bei einer Checked Exception möchte man, dass der User mitdenkt und mithilft aus der Exception wieder zu einem „normalen“ Zustand zu kommen – Unchecked bedeutet, dass das System vom Programmierer wieder in einen sicheren Zustand geführt werden muss

03- Web Application Security

- **Same Origin:** Policy die Abfragen oder Daten von anderen Servern nicht zulässt (nur same origin allowed)
- **Sandboxing:** Isolierter Bereich in einem Programm, bei der keine Aktion auf die Auswirkung der Umwelt halt

04- IT Risiko MGT & IT-Grundschutz

05- Gastvortrag
06- Mobile Security
- **Side Channel Angriff**: kryptoanalytisches Verfahren; Bestimmte Verschlüsselte Programme werden angegriffen und es wird versucht Korrelationen herzustellen, um den Schlüssel zu finden

07- Usability & Security

08- Capture the Flag

09- Datenspuren im Internet
- **CEO Fraud:** eine Betrugsmasche, bei der Firmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden.
- **Vorschussbetrug:** das Opfer überweist Geld und erwartet zukünftig Geld zurück zu bekommen (oder gar Gewinn zu machen) – dies war jedoch nicht beabsichtigt und das Geld wird veruntreut (häufig bei Schneeballsystemen mit versprochenen Provisionen)

.