Cybersecurity

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw-mannheim.de
Version: 1.0

Folien: https://delors.github.io/sec-cybersecurity/folien.de.rst.html

https://delors.github.io/sec-cybersecurity/folien.de.rst.html.pdf

Fehler melden:

https://github.com/Delors/delors.github.io/issues

Was ist Cybersecurity?

***Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks**. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.*

—July 4th, 2024 - Cisco

1

*[...] The security precautions related to computer information and access address four major threats: **(1) theft of data**, such as that of military secrets from government computers; **(2) vandalism**, including the destruction of data by a computer virus; **(3) fraud**, such as employees at a bank channeling funds into their own accounts; and **(4) invasion of privacy**, such as the illegal accessing of protected personal financial or medical data from a large database. [...]*

—July 4th, 2024 - Britannica

2

Das Ziel der IT-Sicherheit ist es Systeme vor:

- Ausfall
- Missbrauch
- Sabotage
- Spionage
- Betrug und Diebstahl zu schützen

3

1. Von praktischen und theoretischen Angriffen

Indonesia won't pay an $8 million ransom after a cyberattack compromised its national data center

[...] The attackers have held data hostage and offered a key for access in return for the $8 million ransom, said PT Telkom Indonesia's director of network & IT solutions, Herlan Wijanarko, without giving further details. Wijanarko said the company, in collaboration with authorities at home and abroad, is investigating and trying to break the encryption that made data inaccessible. [...]

—June 25th, 2024 - AP News

FAST 4.000 VERHAFTUNGEN: Interpol gelingt großer Schlag gegen Onlinebetrug

Die Einsatzkräfte haben nicht nur weltweit Tausende von Verdächtigen verhaftet, sondern auch Vermögenswerte im Umfang von 257 Millionen US-Dollar beschlagnahmt.

[...] Mit einem Gesamtwert von 135 Millionen US-Dollar besteht laut Interpol mehr als die Hälfte davon aus beschlagnahmten Fiat-Währungen wie US-Dollar, Euro oder Yen. Weitere zwei Millionen Dollar liegen in Form von Kryptowährungen vor. Hinzu kommen andere Vermögenswerte wie etwa Immobilien, Luxusfahrzeuge, teurer Schmuck und andere hochwertige Gegenstände und Sammlungen im Gesamtwert von 120 Millionen US-Dollar. [...]

—29. Juni 2024 - Golem.de

Hackers shut down heating in Ukrainian city with malware

For two days in mid-January, some Ukrainians in the city of Lviv had to live without central heating and suffer freezing temperatures because of a cyberattack against a municipal energy company [...]

[...], the cybersecurity company Dragos published a report with details about a new malware dubbed FrostyGoop, which the company says is designed to target industrial control systems [...]

—Juli 2024 - Techcrunch

Want to Win a Bike Race? Hack Your Rival's Wireless Shifters

Relatively inexpensive hardware can be used to hack the Shimano Di2 wireless gear-shifting systems used by cyclists [...]. They tested the eavesdrop-and-replay attack with a $1,500 USRP software-defined radio, an antenna, and a laptop but said the setup could be miniaturized. Attackers could spoof signals from up to 30 feet away, causing the target bike to shift gears unexpectedly or lock into the wrong gear.

—August 2024 - summary provided by ACM; full article: Wired

New RAMBO attack steals data using RAM in air-gapped computers

[...] A novel side-channel attack dubbed "RAMBO" (Radiation of Air-gapped Memory Bus for Offense) generates electromagnetic radiation from a device's RAM to send data from air-gapped computers.

[...] To conduct the Rambo attack, an attacker plants malware on the air-gapped computer to collect sensitive data and prepare it for transmission. It transmits the data by manipulating memory access patterns to generate controlled electromagnetic emissions from the device's RAM.
[...] The RAMBO attack achieves data transfer rates of up to 1,000 bits per second (bps) [at a distance of up to 7 meters], equating to 128 bytes per second, or 0.125 KB/s.

—September 2024 - Bleepingcomputer

Weitere Details

The emitted data is encoded into "1" and "0," represented in the radio signals as "on" and "off." The researchers opted for using Manchester code to enhance error detection and ensure signal synchronization, reducing the chances for incorrect interpretations at the receiver's end.

The attacker may use a relatively inexpensive Software-Defined Radio (SDR) with an antenna to intercept the modulated electromagnetic emissions and convert them back into binary information.

SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript

[Side-Channel Attack to circumvent privacy.]

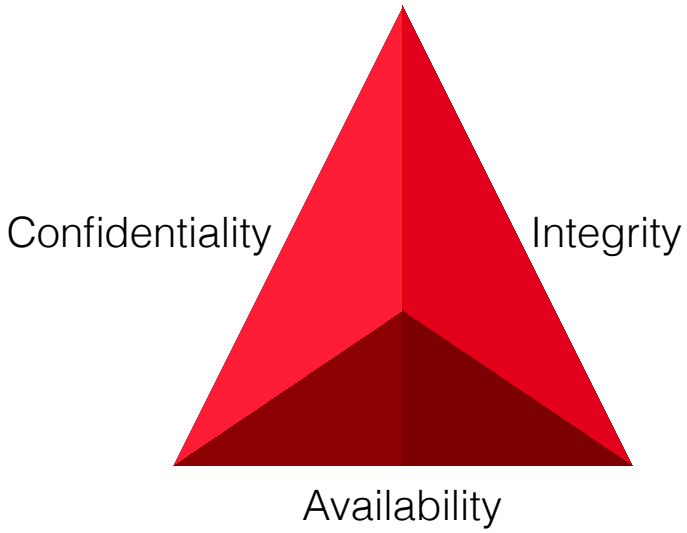
[...] The attack setup for SnailLoad. A victim downloads data from an attacker's HTTP server while it watches a video on a video-sharing platform, e.g., YouTube. Due to the network bottleneck on the victim's side, the attacker can infer the transmitted amount of data by measuring the packet round trip time. The round trip time traces are unique per video and can be used to classify the video watched by the victim. [...]

—28.6.2024 Snailload: Paper, Web

Ausgewählte Angriffe und Angriffsmethoden

- Backdoors (🇩🇪 *Hintertüren*)
- (Distributed-)Denial-of-service Angriffe
- Direct-access Angriffe
- Eavesdropping (🇩🇪 *Abhören*)
- Malware
- Man-in-the-middle (MITM) Angriffe
- Social engineering (z. B. Phishing)
- Privilege escalation
- Side-Channel attacks/🇩🇪 *Seitenkanalangriffe*
- Spoofing (z. B. IP-Spoofing)
- Advanced Persistent Threats (APT)

Schutzziele der IT-Sicherheit: CIA-Triade



Confidentiality ≙dt. Vertraulichkeit

Integrity ≙dt. Integrität

Availability ≙dt. Verfügbarkeit

2. Social-Engineering Angriffe

One Question Saved Ferrari from a Deepfake Scam

With one question, an executive at Ferrari stopped an effort to use deepfake technology to scam the company. CEO Benedetto Vigna (pictured) was impersonated on a call by deepfake software that, using a convincing imitation of Vigna's southern Italian accent, said he needed to discuss something confidential that required an unspecified currency-hedge transaction to be carried out. The executive started to have suspicions and asked, for identification purposes, the title of the book Vigna had recently recommended to him. With that, the call ended.

—Juli, 2024 - Zusammenfassung: ACM; Original: 'I Need to Identify You': How One Question Saved Ferrari From a Deepfake Scam - Bloomberg

Eigenschaften von Social-Engineering Angriffe

- **sind häufig die Ursache für erfolgreiche Angriffe**

  (Der Hacker Kevin Mitnick war praktisch immer aufgrund von Social Engineering erfolgreich.)
- stellen die größte Bedrohung für die Sicherheit von IT-Systemen dar
- es wird angenommen, dass die betroffenen Personen es in vielen Fällen nicht merken (Beispiel: Fake Bewerbungsgespräch)
- mittels OSINT kann die Vorbereitung von Social-Engineering Angriffen vereinfacht werden
- neue technische Möglichkeiten (z.B. KI generierte Stimmen) erweitern die Angriffsmöglichkeiten

Beispiel eines fortgeschrittenen Social-Engineering Angriffs

Ein vom Angreifer bewusst eingefädeltes Bewerbungsgespräch für eine Position als Administrator könnte zum Beispiel dazu genutzt werden, um Informationen über das Zielsystem zu erhalten, die für einen Angriff nützlich sind (z.B. welche Software wird eingesetzt, wie sieht die Architektur aus, ...). In diesem Fall ist davon auszugehen, dass ein Bewerber zum Beispiel durch ein Headhunter eine gutes Angebot gemacht wird und er dann im Rahmen des Gesprächs gebeten wird eine Sicherheitsarchitektur darzustellen, die er einführen würde. Es ist dann davon auszugehen, dass er auf seine bisherige Erfahrung zurückgreift und diese darstellt und er somit die Architektur des Zielsystems offenlegt.

Neue Gefahren

Durch KI generierte Stimmen kann es Angreifern gelingen, z. B. durch das Vortäuschen einer Notlage einer nahestehenden Person, an Informationen zu gelangen.

Ausgewählte Social-Engineering Angriffe

Phishing and Spear Phishing:

Phishing nutzt elektr. Kommunikationswege um an Informationen zu gelangen (z.B. E-Mail oder SMS).

Spear phishing ist Phishing, bei der der Angreifer auf eine bestimmte Zielgruppe oder Person abzielt.

Smishing:

Phishing mit Hilfe von SMS.

Vishing: Phishing mit Hilfe von Telefonanrufen.
(Z.B. Anrufe von Europol)

Whaling: Phishing, dass sich gegen hochrangige und sehr ausgewählte Personen richtet (z.B. den CEO eines Unternehmens).

Pharming:

Manipulation des DNS-Servers, um den Nutzer auf eine gefälschte Webseite zu leiten, um dann sensitive Informationen zu erlangen.

Spam / Spam over Internet messaging (SPIM):

Unerwünschte und nicht angeforderte E-Mail-Nachrichten oder Nachrichten in sozialen Medien bzw. Instant Messaging-Diensten.

Dumpster Diving:

Durchsuchen von „Müllcontainern" nach Informationen, die für einen Angriff nützlich sein könnten.

Shoulder Surfing:

Beobachten von Personen, die sich an einem Computer anmelden, um das Passwort zu erfahren oder die sensitive Informationen auf dem Schreibtisch liegen haben.

Tailgating:

Ein Angreifer nutzt die Zugangsberechtigung einer Person, um sich Zugang zu einem Gebäude zu verschaffen ohne dass die Person dies bemerkt oder gar zustimmt.

Dies kann z. B. durch Zugangsschleusen verhindert werden, die immer nur einer Person den Zugang gewähren.

Identity Fraud:

Identitätsdiebstahl. Der Angreifer gibt sich als jemand anderes aus, um an Informationen zu gelangen oder um eine Straftat zu begehen.

Invoice Scams:

Versenden von Rechnungen, für Dienstleistungen und Produkte die man nicht gekauft hat (z.B. Rechnungen für Postzustellung.)

Credential Harvesting:

Sammlung von Zugangsdaten, die durch Sicherheitslücken in Systemen oder durch Phishing erlangt wurden.

Hoax: Eine bewusste Falschmeldung, die Menschen dazu veranlasst etwas falsches zu glauben.

Impersonation oder Pretexting:

Vorgabe einer falschen Identität (z.B. als Mitarbeiter des IT-Supports); d.h. der Angreifer gibt sich persönlich als jemand anderes aus, um an Informationen zu gelangen und nutzt dafür keine elektronischen Hilfsmittel.

Eavesdropping:

Abhören von Gesprächen, um an relevante Informationen zu gelangen.

Eliciting Information:

Der Angreifer versucht durch geschicktes Fragen an Informationen zu gelangen, die für einen Angriff nützlich sein könnten.

Baiting (*Ködern*):

Der Angreifer bietet etwas an, um an Informationen zu gelangen (z.B. ein USB-Stick mit einem Virus, der sich beim Einstecken des USB-Sticks auf dem Rechner installiert.)

Watering Hole Attack:

Der Angreifer infiziert eine Webseite, die von der Zielgruppe häufig besucht wird, um dann die Besucher der Webseite anzugreifen.

Typo Squatting:

Ausnutzen von Tippfehlern durch das Registrieren einer Domain, die der Domain eines Zielunternehmens ähnelt, um dann Besucher der Webseite auf eine gefälschte Webseite zu leiten. (z.B. *www.gooogle.com*)

Ein Beispiel eines nicht-harmlosen Streichs (Hoax) ist die Falschmeldung vom 1. April 2003, dass Bill Gates gestorben sei. Diese Falschmeldung wurde von vielen Menschen geglaubt und hatte relevanten Einfluss auf den Aktienmarkt.

Credential harvesting

In der Anfangszeit von Github und Bitbucket wurden häufig Zugangsdaten und Zertifikate in öffentlichen Repositories gefunden, da die Nutzer diese im Quellcode hinterlegt hatten oder sogar als Ressourcen direkt eingebunden hatten.

Typische Phishing E-Mail

„Motivationstechniken” von Angreifern

- Autorität: Der Angreifer gibt sich z.B. als Mitarbeiter des IT-Supports aus.
- Einschüchterung (🇺🇸 *Intimidation*)
- Dringlichkeit
- Konsens (*"Alle machen das so."*)
- Knappheit (*"Nur noch Heute im Angebot."*)
- Vertrautheit
- Vertrauen