Verteilte Systeme

...für C++ Programmierer

Security

by

Dr. Günter Kolousek

Sicherheit?

- Im Kontext verteilter Systeme…
- Unter (Computer)Sicherheit versteht man die Sicherheit eines Computersystems vor Ausfall und Manipulation sowie vor unerlaubten Zugriff.
- Datenschutz wird nicht betrachtet…

Überblick

- Konzept der Sicherheit
- Mechanismen
- Anwendungen

Konzept der Sicherheit

- Bedrohungsanalyse
- Schwachstellenanalyse
- Gefahrenanalyse
- Sicherheitsmanagement
- Sicherheitsmaßnahmen
- Mechanismen

Bedrohungsanalyse

- alle möglichen Bedrohungen und Angreifer identifizieren
- Ort der Gefahrenquelle
  - Datenübertragung
  - Datenspeicherung
- Art der Bedrohung
  - Allgemeine Bedrohungen
  - Grundbedrohungen
- Angriffe, wie z.B.
  - Man-in-the-middle

Allgemeine Bedrohungen

- ”Ausfall” … nicht nur bösartige Angriffe bedingt
- Äußere Einflüsse
  - Netzschwankungen und Netzausfall, elektrostatische Aufladungen, Magnetische Felder und Einstrahlungen benachbarter (Rundfunk)Sender
  - Übertragungsfehler und Fehlrouting (z.B. in Folge magnetischer Felder,…)
  - Überhitzung oder Brand, Blitzschlag, Explosion, Erdbeben, Wasser, Tiere,…
- Systemfehler: z.B. Programmierfehler, Konfigurationsfehler, Verschleißerscheinung der HW,…
- menschliche Fehler (ohne schädigende Absicht): z.B. Eingabe- oder Bedienfehler

Grundbedrohungen

- Verlust der Vertraulichkeit
  - Unberechtigter Dritter hat Zugriff auf Daten oder Service
- Verlust der Integrität
  - unerlaubt oder unabsichtliche Veränderung der Daten oder des Dienstes
- Verlust der Authentizität
  - behauptete Identität $\neq$ tatsächlicher Identität
- Verlust der Verbindlichkeit
  - bestandene Kommunikationsbeziehung wird geleugnet
- Verlust der Verfügbarkeit
  - Unterbrechung des Dienstes, Daten nicht mehr nutzbar oder zerstört

Passive Angriffe

- Abhören von Daten
  - Sammeln von ”Abfall” $\rightarrow$ physischer Zugang!
  - Illegales Kopieren von Daten $\rightarrow$ physischer Zugang, Zugriff auf gelöschte Daten, Zugriff auf Hauptspeicher, Zugriff auf GUI System,…
  - Abhören der Kommunikationsverbindung
  - Empfangen der Abstrahlung (Monitor, Kommunikationsweg)
- Abhören von Teilnehmeridentitäten
- Verkehrsflussanalyse
  - Zeit, Größe, Häufigkeit, Richtung
- Brute-force-Methode
- Wörterbuchangriff
- Seitenkanalattacke

Wörterbuchangriff

- Hashwert zu einem Passwort immer derselbe
- Vorberechnung möglich $\rightarrow$ Wörterbuchangriff (Rainbow Tables)
- Salt
  - Server erzeugt je Passwort zufällige Zeichenfolge und speichert diese (Salt)
  - Kombination mit Salt
  - Berechnung des Hashwertes
- Pepper
  - wie Salt, aber für alle Passwörter gleich
  - dafür wird dieser **nicht** in der Datenbank gespeichert sondern extern an einem sicheren Ort
  - $\rightarrow$ Auch wenn Angreifer Zugriff auf Datenbank erhält (z.B. mittels SQL-Injection) sind keine realistischen Angriffe auf die Passwörter möglich

Seitenkanalattacke

- Aus vorhandenen Daten wie
  - Dauer der Verschlüsselung
  - zeitlicher Verlauf des Stromverlaufs
  - Berechnungsfehler bei extremen Bedingungen
  - elektromagnetische Abstrahlung
  - Schallanalyse
    - Betriebsgeräusche bei Generierung von Schlüssel
- Informationen über Algorithmus, Implementierung, Schlüssel zu gewinnen

Aktive Angriffe

- Wiederholen oder Verzögern von Daten
- Einfügen und Löschen von Daten
- Modifikation von Daten
- Verweigerungsangriffe (Denial of Service)
- Vortäuschen einer falschen Identität (Masquerade)
  - Spoofing (Verschleierung, Manipulation): Täuschungsversuche in Netzwerken zur Verschleierung der eigenen Identität, z.B. ARP-Spoofing, DNS-Spoofing, IP-Spoofing, URL-Spoofing

Aktive Angriffe – 2

- Phishing (ursprünglich: password fishing): mittels gefälschten E-Mails,… an sensitive Daten zu gelangen
- Trittbrettfahrer (hijacking): Übernahme einer Login-Sitzung
- Erzeugung von Systemanamolien
  - Viren: selbstreproduzierend, kopieren sich in andere Programme
  - Würmer: selbstreproduzierend, eigenständig
  - Trojaner: geben vor eine Funktion zu erfüllen, aber eine andere
  - Bomben: stören Betrieb des Rechners nach Eintreten eines Ereignisses
  - Falltüren (backdoors): vom Programmierer zu Testzwecken,… eingebaut

Schwachstellenanalyse

- Untersuchung der konkreten Schwachstellen eines Systems
- Arten
  - Menschliche Schwachstellen: z.B. Fahrlässigkeit, Naiivität, Wissensmangel, Käuflichkeit, ehemalige Mitarbeiter
  - Organisatorische Schwachstellen: z.B. Vergabe von Zugriffsberechtigungen, Standort von Computersystemen,…
  - Technische Schwachstellen: z.B. ftp-Zugang,…

Gefahrenanalyse

- Gefahr = Bedrohung + Schwachstelle
- d.h. erkennen/finden von Gefahren und daraus Maßnahmen zur Risikominimierung ableiten und ergreifen

Sicherheitsmanagement

Sicherheitsmanagement führt, lenkt und koordiniert eine Organisation in Bezug auf alle Sicherheitsaktivitäten – Wikipedia

- technische Maßnahmen, betreffen
  - Netzwerk: Glasfaser vs. Kupferkabel, Firewall,…
  - Computer: Redundanz, Virenschutzprogramme, Betriebssysteme, Programmiersprachen,…
  - Brandschutz, Absperrungen, Wetterschutz,…

Sicherheitsmanagement – 2

- personelle Maßnahmen
  - Schulung, Förderung des Sicherheitsbewusstsein, Verbote
- organisatorische Maßnahmen
  - Sicherheitspolicy
    - Zutrittskontrolle, Zugangsberechtigungen, Schlüsselverwaltung, Backup, Brandschutz, Redundanzen,…
  - Audit-Trail Management
    - Überprüfung von sicherheitsrelevanten Ereignissen: Revision (sporadisch) und Controlling (regelmäßig)
  - Eventhandling: Tätigkeiten bei unerwarteten Ereignissen
  - Fehlermanagement: Tätigkeiten um Fehler zu entdecken, zu diagnosizieren und zu korrigieren

Sicherheitsdienste

- sind technische Maßnahmen im Rahmen des Sicherheitsmanagement
- 5 Arten von Sicherheitsdiensten, um auf mögliche Gefahrenquellen und Sicherheitsgefährdungen zu reagieren:
  - Authentifizierung
  - Geheimhaltung
  - Integrität
  - Zugriffskontrolle
  - Nicht-Zurückweisung

Authentifizierung

- Überprüfung der Identität eines Benutzers, Clients, Servers
- einseitige vs. zweiseitige Authentifizierung
- Methoden der Sicherstellung der Identität
  - Besitz einer geheimen Information: Passwort, Frage-Antwort Verfahren, One-Time-Passwords wie TANs), digitale Signatur, Challenge-Response Verfahren (Server überträgt Zufallszahl, Client verschlüsselt, sendet zurück und beweist…)
  - Besitz einer bestimmten Hardware
  - biometrische Verfahren

Geheimhaltung

- Sicherstellung der Vertraulichkeit, dass nur beteiligte Partner die Kommunikation verstehen
- Methoden zur Sicherstellung der Geheimhaltung
  - Verschlüsselung
  - Verschleierung
  - Auffüllen mit Fülldaten in den Sendepausen $\rightarrow$ keine Struktur der Netzdaten erkennbar

Integrität

- Sicherstellung, dass Information nicht verändert wird
- Angriffe
  - Modifizieren, Löschen, Einfügen von Nachrichten
  - Wiederholung (replay attack) oder Verzögerung von Nachrichten
- Methoden zur Sicherstellung der Geheimhaltung
  - Verschlüsselung
  - Prüfsummen, Laufnummern, Zeitstempel
  - Wiederholung von gefälschten Nachrichten

Zugriffskontrolle

- Sicherstellung, dass nur berechtigte Benutzer Zugriff auf die Daten bzw. Dienste haben
- Methoden zur Sicherstellung der Zugriffskontrolle
  - Access Control Lists (ACL)
  - Schutzklassen (à la Unix)

Nicht-Zurückweisung

- Sicherstellung, das bestandene Kommunikationsbeziehung nicht geleugnet werden kann (non-repudiation)
  - d.h. Sender *hat* gesendet bzw. Empfänger *hat* empfangen
- Methoden zur Sicherstellung von Nicht-Zurückweisung
  - digitale Signaturen

Mechanismen

- dienen dazu die Sicherheitsdienste zu realisieren
- Mechanismen
  - Symmetrische Verschlüsselung
  - Asymmetrische Verschlüsselung
  - Message Digests
  - Message Authentication Codes
  - Digitale Signaturen
  - Zertifikate

Symmetrische Verschlüsselung

- Prinzip
  - Ein Schlüssel K zum Verschlüsseln (E … encrypt) und Entschlüsseln (D … decrypt) verwendet
  - Paket P
    - Verschlüsselung: $E(K, P)$
    - Entschlüsselung: $P = D(E(K, P), K)$
  - Grundbausteine: Substitution, Permutation
- Vorteile: schnell, Realisierung in HW, Schlüssellängen kurz
- Nachteile: Schlüsselverwaltung (# der Schlüssel, Schlüsselaustausch über sicheren Kanal)

Symmetrische Verschlüsselung – 2

- Arten: Blockverschlüsselung vs. Streamverschlüsselung
  - Modus (bei Blockverschlüsselung)
    - ECB (electronic code book)
    - CBC ()
    - CTR ()
- Verfahren
  - DES (Data Encryption Standard): Schlüssellänge 56 Bits, unsicher (wurde schon 1999 in 22 Stunden gebrochen, damals 100000 Rechner)
  - 3DES (Triple DES): Schlüssellänge je nach Modus bis zu 168 Bits
  - AES (Advanced Encryption Standard): Schlüssellänge 128, 192 oder 256 Bits
  - Blowfish, Twofish, Chacha20, IDEA, RC5 (Stromverschlüsselung)

Nonce und Padding

- Nonce
  - zufällige Zeichenfolge (wie Salt, siehe Folie Wöterbuchangriff), aber Sinn ist Einmaligkeit des Klartextes sicherzustellen, damit nicht zwei Klartexte den gleichen Geheimtext bewirken
- Padding
  - muss nicht zufällig sein
  - Sinn ist die Ermittlung der Länge des Klar- als auch des Geheimtextes zu erschweren bzw. auf Blocklänge aufzufüllen

Asymmetrische Verschlüsselung

- Prinzip
  - Schlüsselpaar: privater Schlüssel K_pri und ein öffentlicher Schlüssel K_pub
    - privater Schlüssel kann mit Passwort verschlüsselt werden! $\rightarrow$ Verlust…
  - Paket P
    - Verschlüsselung: $E(K_pub, P)$ (K_pub vom Empfänger)
    - Entschlüsselung: $D(K_pri, E(K_pub, P))$
  - Grundbausteine: meist mathematische Probleme (z.B. Finden von Primfaktoren von sehr großen Zahlen oder Lösen algebraischer Gleichungen)
- Vorteile: Schlüsselverwaltung einfacher
- Nachteile: langsamer, Schlüssellänge lang

Asymmetrische Verschlüsselung – 2

- zu lösende Probleme
  - Identität des Benutzers muss geprüft werden, wenn öffentlicher Schlüssel veröffentlicht wird (d.h. Authentizität des Schlüssels)
  - der Instanz, die K_pub veröffentlicht, muss vertraut werden
  - diese Instanz ist besonders exponiert
  - Wie wird ein öffentlicher Schlüssel zurückgezogen?
- Verfahren
  - RSA (Rivest-Shamir-Adlman) $\rightarrow$ Primzahlenfaktorisierung
  - ElGamal
  - ECC (Elliptic Curve Cryptography) $\rightarrow$ Lösen von elliptischen Kurven in endlichen Körpern

Einweg- und Hashfunktionen

- Einwegfunktion
  - in eine Richtung leicht, in andere schwer
- Hashfunktion
  - Zeichenfolge beliebiger Länge in Zeichenfolge fester Länge
- Kollisionsresistenz
  - schwach: praktisch unmöglich für geg. x ein x' zu finden, sodass $h(x) = h'(x)$
  - stark: praktisch unmöglich zwei beliebige Werte x und x' zu finden, sodass $h(x) = h'(x)$
- Einweg-Hashfunktion:
  - Einwegfunktion
  - schwach kollisionsresistent
- kryptographische Hashfunktion
  - Einweg-Hashfunktion
  - stark kollisionsresistent

Message Digest

- Zweck: Sicherstellung der Integrität
  - kryptographische Hashfunktion
  - Hashwert wird separat übertragen oder hinten angehängt
- Verfahren
  - MD5: Message Digest 5, 128 Bits, nicht sicher
  - SHA-1: Secure Hash Algorithm, 160 Bits, nicht sicher
  - SHA-2: SHA-224, SHA-256, SHA-384 und SHA-512
  - SHA-3: variable Bitlänge, üblich sind 224, 256, 384, 512

Kryptoanalyse

- Analyse kryptologischer Verfahren $\rightarrow$ Ziel: *brechen*!
- Methoden
  - Ciphertext-only (oder *known ciphertext*)
    - Versuch aus bekannten Geheimtext den Klartext zu ermitteln
  - Known-plaintext
    - Aus bekannten Geheimtext samt zugehörigen Klartext den Schlüssel ermitteln
  - Chosen-plaintext
    - Klartext kann frei gewählt werden (sonst wie known-plaintext)
  - Chosen-ciphertext
    - Geheimtext kann frei gewählt werden und Entschlüsselung ist möglich (z.B. Zugriff auf HW)

Message Authentication Code (MAC)

- wie Message Digests aber mit Passwort
- Zweck
  - Verifikation der Integrität
  - Symmetrische Form der Authentifizierung
- Verfahren
  - HMAC

Digitale Signatur

- garantiert, dass Nachricht vom Signierer stammt und nicht verändert wurde
- Vorgang
  - Erzeugung eines Message Digest aus Nachricht
  - und verschlüsseln mit privatem Schlüssel
- Überprüfung
  - mit öffentlichem Schlüssel entschlüsseln
  - und mit berechnetem Message Digest vergleichen
- Eigenschaften
  - ist nicht fälschbar
  - ist einfach überprüfbar
  - ist nicht abstreitbar
- Verfahren
  - X.509, OpenPGP (PGP (Pretty Good Privacy) und GPG (GNU Privacy Guard))

Zertifikat

- stellt Zusammenhang zwischen öffentlichem Schlüssel und einer bestimmten Person (Identität) her
- Enthält Angaben
  - Name des Zertifikatsinhabers
  - öffentlicher Schlüssel des Zertifikatsinhabers
  - Name der Zertifizierungsinstanz
  - Gültigkeitszeitraum
- ist signiert mit privatem Schlüssel der Zertifizierungsinstanz
- Verfahren
  - X.509

Schlüsselverwaltung

- manuelle Verteilung symmetrischer Schlüssel
  - bei n Partnern $O(n^2)$ verschiedene Schlüssel notwendig!
  - sichere Kanäle notwendig
- Schlüsselaustauschprotokolle
  - ”mehrfaches Versenden einer verschlossenen Kiste”
  - ”Farbmischen” $\rightarrow$ Diffie-Hellmann
  - Diffie-Hellmann
- Hybride Verschlüsselung
- Public Key Infrastructure (PKI)
- Web of trust

Versenden einer Kiste

1. A erzeugt ein Geheimnis
2. A gibt dieses Geheimnis in eine Kiste und versperrt diese mit einem Vorhangschloss (nur A hat Schlüssel)
3. A versendet diese Kiste an B
4. B hängt noch ein Vorhangschloss an diese Kiste
5. B versendet diese Kiste an A
6. A nimmt eigenes Vorhangschloss ab
7. A versendet Kiste nochmals an B
8. B nimmt eigenes Vorhangschloss ab und hat Zugang zu dem enthaltenen Geheimnis

Farbmischen

1. A denkt sich eine öffentliche Farbe aus und sendet diese an B
2. A denkt mischt öffentliche Farbe mit (geheimer) privaten Farbe und sendet das Ergebnis an B
3. B denkt mischt öffentliche Farbe mit (geheimer) privaten Farbe und sendet das Ergebnis an A
4. A mischt erhaltene Farbe mit geheimer Farbe
5. B mischt erhaltene Farbe mit geheimer Farbe
6. Beide haben jetzt Zugriff auf einen geheimen Farbwert!

Voraussetzung: Mischen von Farben ist eine Einwegfunktion!

Diffie-Hellmann Schlüsselaustausch

- basierend auf Exponentialfunktion in GF(p), vereinfacht: $f(x) = g^x \bmod p$
- A denkt sich große Primzahl p sowie eine Primitivwurzel[1] g aus und teilt B mit (wie gemeinsame Farbe)
- A und B denken sich jeweils jeweils eine private Zahl x_A und x_B aus ($x_{A,B} \in \{1, ..., p-1\}$)
- A sendet $y_A = g^{x_A} \bmod p$ an B und B sendet $y_B = g^{x_B} \bmod p$ an A
- A berechnet $z_{BA} = {y_B}^{x_A} \bmod p = g^{x_B x_A} \bmod p$
- B berechnet $z_{AB} = {y_A}^{x_B} \bmod p = g^{x_A x_B} \bmod p$
- aber… nicht sicher gegen MITM Angriffen!

[1] jedes Element von GF(p) kann als Potenz von g dargestellt werden

Hybride Verschlüsselung

- Kombination aus symmetrischer und asymmetrischer Verschlüsselung
- A wählt einen symmetrischen Schlüssel, verschlüsselt diesen mit dem öffentlichen Schlüssel von B und sendet diesen an B
- B entschlüsselt mit privaten Schlüssel
- $\rightarrow$ Sessionschlüssel!
  - Wird oft mittels Langzeitschlüssel (master key) zwischen Kommunikationspartnern ausgetauscht
    - was wenn Langzeitschlüssel kompromittiert wird?

Hybride Verschlüsselung

- Kombination aus symmetrischer und asymmetrischer Verschlüsselung
- A wählt einen symmetrischen Schlüssel, verschlüsselt diesen mit dem öffentlichen Schlüssel von B und sendet diesen an B
- B entschlüsselt mit privaten Schlüssel
- $\rightarrow$ Sessionschlüssel!
  - Wird oft mittels Langzeitschlüssel (master key) zwischen Kommunikationspartnern ausgetauscht
    - was wenn Langzeitschlüssel kompromittiert wird?
    - Speicherung des gesamten Verkehrs und entschlüsseln im nachhinein…
  - perfect forward secrecy (PFS) dann, wenn Sitzungsschlüssel aus Langzeitschlüssel nicht ermittelt werden kann
- Vorteile
  - Schlüsselverteilungsproblem…
  - Geschwindigkeit der symmetrischen Verschlüsselung

Public Key Infrastructure (PKI)

- Idee: PKI wird vertraut
- Zertifikate ausstellen, verteilen, prüfen
- Zertifizierungsstelle (engl. certificate authority, CA)
  - stellt CA-Zertifikat zur Verfügung und signiert Zertifikatsanträge
- Registrierungsstelle (engl. registration authority, RA)
  - bearbeitet Zertifikatsanträge: prüft Angaben auf Richtigkeit
- Zertifikatssperrliste (engl. certificate revocation list, CRL)
  - enthält Angaben zu allen zurückgezogenen Zertifikaten
- Hierarchie von CAs
  - Wurzelzertifizierungsinstanz (Root-CA)
    - Zertifikat der Root-CA oft in Anwendungen integriert
    - privater Schlüssel muss besonders geschützt sein!!!
  - Zertifikatskette!

Web of trust (WOT)

- Idee: keine zentrale PKI $\rightarrow$ ”Vertrauen durch das Netz”
- Prinzip
  - A signiert Schlüssel von B (und vertraut Schlüsselsignaturen von B)
    - z.B. A trifft B persönlich
    - z.B. B übermittelt A den Fingerprint des öffentlichen Schlüssels über einen sicheren Kanal (z.B. per Telefon)
    - Zertifikat $\equiv$ Signatur & öffentlicher Schlüssel
  - B signiert Schlüssel von C
  - A betrachtet somit den Schlüssel von C als gültig

Web of trust – 2

- Problem
  - Vertrauen, dass B nur wirklich bekannte Schlüssel signiert kann eigentlich nicht sichergestellt werden
  - Lösungsansatz: Mehrere Signaturen u.U. notwendig
  - speichern in öffentlichem Schlüsselbund
- öffentlicher Schlüsselbund (public keyring)
  - eigene und fremde öffentliche Schlüssel samt Zertifikate
  - Zuordnung und Berechnung von Vertrauenswerten
  - je mehr Signaturen ein öffentlicher Schlüssel hat, desto vertrauenswürdiger $\rightarrow$ Schlüsselserver
- privater Schlüsselbund (private keyring)
  - eigene private Schlüssel

Anwendungen

- Sicherheitsprotokolle
  - TLS (siehe Folien `tls`)
  - OpenVPN
  - IPSec
- Firewalls (siehe Folen `firewalls`)
- Intrusion Detection Systems (IDS)
- Audit Tools

OpenVPN und IPSec

- OpenVPN
  - ein VPN auf Basis von TLS
  - kann auf Schicht 2 oder Schicht 3 arbeiten
  - einfacher zu konfigurieren als IPSec
  - geringere Performance als IPSec
- IPSec
  - integraler Bestandteil von IPv6
  - eigenständig auch für IPv4 verfügbar

IDS

- Einbruchserkennung
- Unterschieden wird
  - HIDS … Host Intrusion Detection System
    - oft auch mit Firewalls kombiniert
    - wird nur versucht Veränderungen an Dateien zu erkennen → System Integrity Verifier, z.B. OSSEC, tripwire, Samhain, Snort
  - NIDS … Network Intrusion Detection System
- Einbruchsabwehr → Intrusion Prevention System (IPS)

Audit Tools

- Verwendung im Zuge des Audit-Trail Managements
- Beispielhaft:
  - Anwendungsschicht: Schwachstellenscanner, Brute Force Tools, Virenscanner
  - Transportschicht: Scanner, OS-Fingerprinting (wie z.B. nmap)
  - Vermittlungsschicht: ICMP-Packet-Injectors
  - Sicherungsschicht: ARP-Spoofer (z.B. Ettercap)
  - Bitübertragungsschicht: Sniffer (wie z.B. Wireshark)