P2P - Sicherheit

Georg Lukas

2003-12-03

Seminar "Kommunikation in P2P-Netzen"

Ziele des Vortrags

- Sicherheit auf Konzept-Ebene
  - Kommunikationsprotokolle
  - Datenspeicherung
  - Resistenz gegen Störungen, Angriffe, Zensur
- Nicht Sicherheit konkreter Implementierungen
  - Bugs
  - Abstürze
  - Ad-Ware, Würmer, Trojaner

Gliederung

- Sicherheitsziele
- Störer und Störungen
- Sicherheitskonzepte
- Zusammenfassung
- Diskussion
- Quellen

Was ist Sicherheit?

- safety + security
- Ziele
  - Integrität
  - Verfügbarkeit / Verlässlichkeit
  - Vertraulichkeit
  - Authentizität
  - Anonymität
- Mögliche Konflikte
  - Vertrauen vs. Anonymität
  - Vertraulichkeit vs. Verfügbarkeit und Integrität
  - effiziente Suche vs. anonymer Speicherort

Störer und Störungen

Störerklassen, Angriffsziele, Angriffsebenen

Klassifizierung von Störern

- Ungezielte Störung
  - Hardware-Ausfall
  - Störungen der Netzwerkinfrastruktur
  - Vandalismus

Klassifizierung von Störern

- Ungezielte Störung
  - Hardware-Ausfall
  - Störungen der Netzwerkinfrastruktur
  - Vandalismus
- Laienhafte Angreifer
  - Cracker, Firmen
  - begrenzte Ressourcen
  - Kenntnis der Infrastruktur

Klassifizierung von Störern

- Ungezielte Störung
  - Hardware-Ausfall
  - Störungen der Netzwerkinfrastruktur
  - Vandalismus
- Laienhafte Angreifer
  - Cracker, Firmen
  - begrenzte Ressourcen
  - Kenntnis der Infrastruktur
- Professionelle Angreifer
  - Sicherheitsdienste, Großkonzerne
  - Bündelung großer Ressourcen
  - Finanzielle Übermacht

Klassifizierung von Störern

- Ungezielte Störung
  - Hardware-Ausfall
  - Störungen der Netzwerkinfrastruktur
  - Vandalismus
- Laienhafte Angreifer
  - Cracker, Firmen
  - begrenzte Ressourcen
  - Kenntnis der Infrastruktur
- Professionelle Angreifer
  - Sicherheitsdienste, Großkonzerne
  - Bündelung großer Ressourcen
  - Finanzielle Übermacht
- Behörden
  - Einfluß durch Gesetze, Verordnungen, Gerichte, Polizei
  - Zensur, Unterdrückung

Angriffsziele

- Netzbetrieb stören
- Zugang zu Daten verhindern
  - für alle zu bestimmten Daten
  - für jemanden zu allen Daten
- Daten aus dem Netz entfernen
- Daten manipulieren
- Zugang zu vertraulichen Daten erhalten
- Erfahren, wer bestimmte Daten sendet/empfängt

Angriffsebenen

- Physikalische Ebene
  - Zerstörung von Leitungen, Rechnern
  - Beschlagnahmen von Datenträgern zur Analyse
- Protokoll
  - Man-In-The-Middle korrumpiert Suchanfragen
  - Mißbrauch konkreter Implementierungen
  - Routing-Manipulation (GNUnet)
- Anwendung
  - Einschleusen sinnloser Daten
  - Überlastung von Knoten durch Suchanfragen
  - (D)DoS

Umsetzung der Sicherheitsziele

Schwerpunkt verteilte Datenspeicherung

Integrität

- Kryptographische Checksummen (MD5, SHA-1)
- Hashwert als Identifikator für Daten
- Suche und Sortierung im Netz (Freenet)
- Manipulationserkennung auf Protokollebene
  - Hash-Überprüfung vor und nach Transfers
- Erkennung unzutreffender Daten
  - Verknüpfung von Hashwert und Beschreibung über dig. Signatur
  - Zuverlässigkeit von Suchergebnissen anhand der Hash-Häufigkeit

Verfügbarkeit

- Physikalische Sicherheit
  - Verteilte Speicherung vieler Kopien
  - Keine zentralisierte Infrastruktur
  - Verschleierung des Speicherorts
    - gezielte Angriffe nicht möglich
    - Suche und Routing weniger effektiv
- Protokollebene
  - gleichzeitige Verbindung zu möglichst vielen Knoten
  - dezentrale, parallele Suche
  - nicht identifizierbares Netzwerkprotokoll
- Anwendung
  - lokale Priorisierung von Anfragen
  - Reputation

Vertraulichkeit

- Verschlüsselung der Daten (lokal / netzweit / extern)
- Verschlüsselte Kommunikation zwischen Knoten (SSL)
- Vermeiden unbekannter / unsicherer Knoten
  - Reputationsmechanismen manipulierbar?
- Verschleiern der Kommunikation
  - Steganografie
  - Übertragung von zufälligem Rauschen
  - zufällige Readressierung
  - Überlistung "omnipräsenter" Überwacher

Authentizität

- Widerspruch zur Anonymität
- Verwendung von Pseudonymen
- Schlüsselpaare identifizieren Nutzer
- Signierung von Daten
- lokale oder globale Reputation an Public Key gebunden
- Nachteil: jederzeit neue Identität erzeugbar

- PKI für hierarchische Strukturen
  - Zugriffsrechte werden mit abgedeckt

Anonymität

- "Unmöglichkeit, aus einer Menge von Teilnehmern identifiziert zu werden"
- Arten der Anonymität
  - Autor-Anonymität
  - Herausgeber-Anonymität
  - Leser-Anonymität
  - Server-Anonymität
  - Dokument-Anonymität
    - isolierter Server
    - netzwerkweit
- Teilnehmer-Anonymität nur auf Protokollebene möglich
  - Verwendung von Mix-Netzen
  - Quelle und Ziel für Zwischenstationen nicht sichtbar
  - kein Austausch von Routing-Informationen

Verteiltes Rechnen

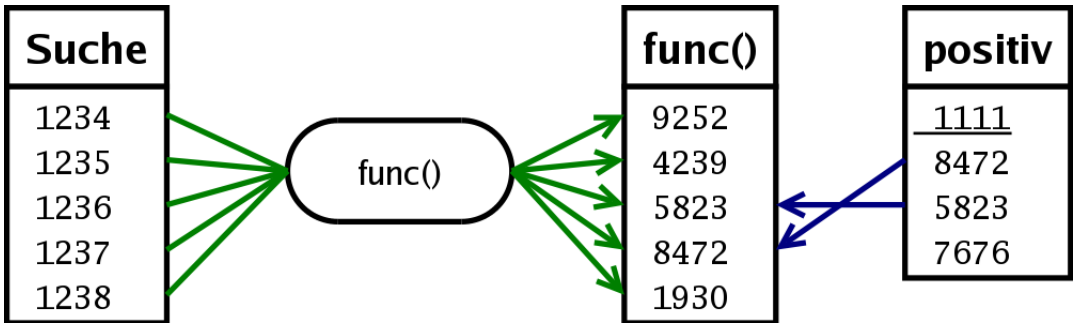
- Analogie: Suche nach Daten - Suche nach Ergebnis
- Integritätsüberprüfung komplexer
- Cheaten: maximaler Gewinn bei minimalem Aufwand
  - Preisgeld
  - Ressourcen
  - Bewertung (psychologische Aspekte)
- Auswirkungen von Angriffen
  - Verwendung falscher Ergebnisse
  - unerkannte korrekte Lösung
  - Denial of Service
- Bestrafung über Reputation

Sicherheit von Rechenergebnissen

- Ehrliche Teilnahme effizienter als Cheaten
- Ideale Sicherheit:
  - selbstständiges Nachrechnen aller Ergebnisse
  - verteiltes Berechnen unnötig
- Überprüfung von Stichproben
  - Speicherung aller Ergebnisse auf Client nicht immer sinnvoll
  - Umgehung möglich

"Magic Numbers"

- für Bruteforce-Suche in Einwegfunktionen
- vom Veranstalter eingestreute "false positives"
- zufällig über individuellen Suchbereich verteilt
- weitere Werte außerhalb des Suchbereichs



Zusammenfassung

- Sicherheitsziele
  - Integrität
  - Verfügbarkeit
  - Vertraulichkeit
  - Authentizität
  - Anonymität
- Störer und ihre Ziele
  - Verhinderung von Kommunikation
  - Löschung
  - Manipulation
  - Aushebeln von Anonymität
- Konzepte der Sicherheit
  - Kryptographie
  - Reputationsmechanismen
  - Mix-Ketten
  - Magic Numbers

Diskussion

- Urheberrecht und sichere Datenspeicherung kombinierbar?
  - Freie Meinungsäußerung erfordert Anonymität
  - Durchsetzung von Urheberrechten erfordert Verfolgbarkeit von Daten
- Bündeln Systeme gegen Überwachung ebendiese auf sich?

Quellen

- http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html
- http://www.freehaven.net/anonbib/cache/strong-eternity.pdf
- http://www.cl.cam.ac.uk/users/rja14/eternity/eternity.html
- http://crypto.stanford.edu/~pgolle/papers/distr.pdf
- http://freenet.sourceforge.net/papers/freenet-ieee.pdf

- Präsentation (incl. Source): http://op-co.de/p2psec/