Einführung in die Informationssicherheit

Florian Mendel

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

http://www.iaik.tugraz.at/

L5 – Operating System Security

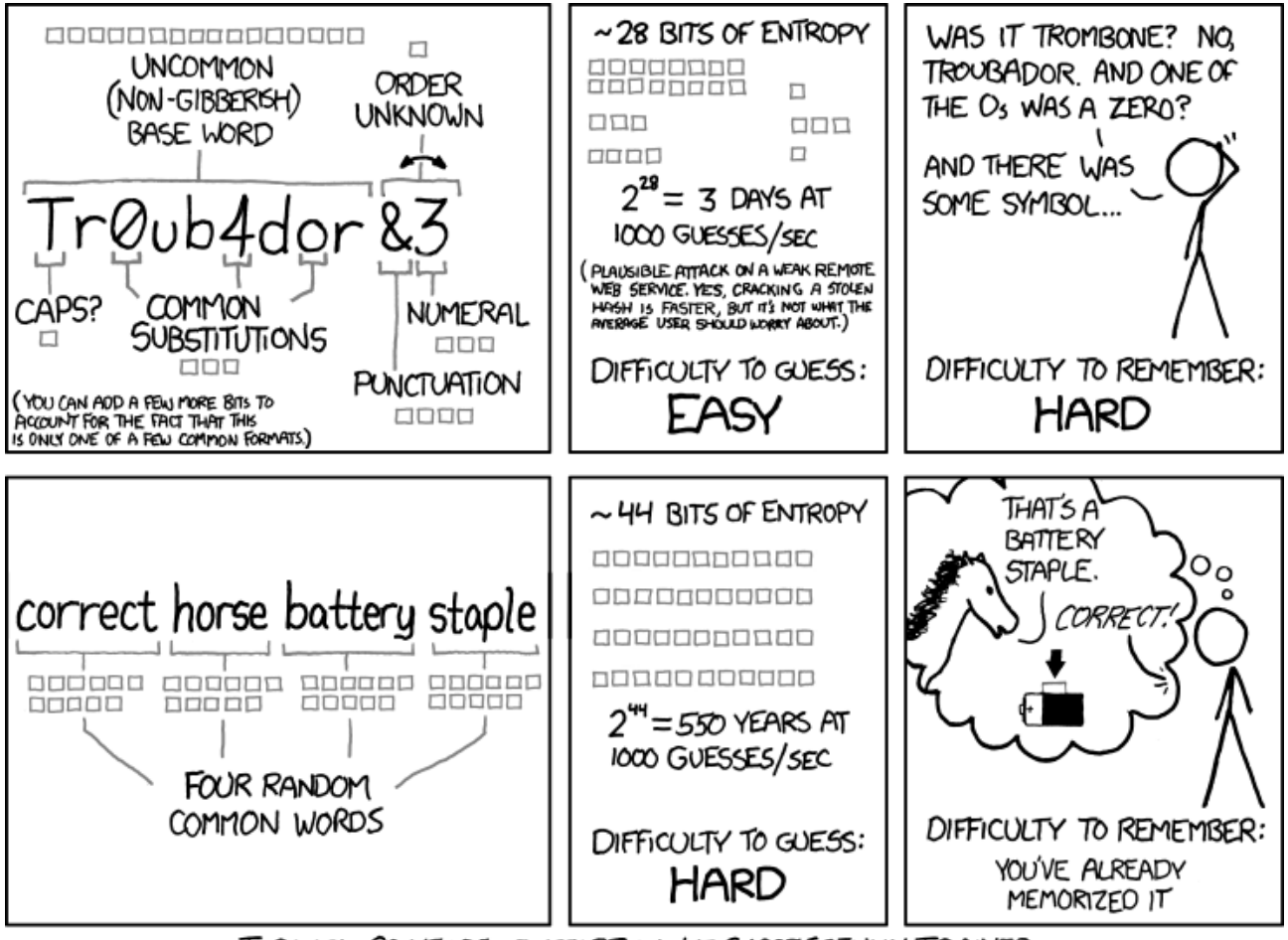
Einführung in die Informationssicherheit

Basierend auf den Folien von Mario Lamberger aus dem WS 12/13

Übersicht

- Authentication und Zugangskontrolle
- Windows Security
  - Authentication/Login
  - Access Control
  - Features und Probleme
- Unix/Linux Security
  - Authentication/Login
  - Access Control
  - Features und Probleme
- Security Enhancing Techniques

Motivation



source: http://xkcd.com/936/

Motivation

Your password must be at least 18770 characters and cannot repeat any of your previous 30689 passwords. Please type a different password. Type a password that meets these requirements in both text boxes

– Microsoft Knowledge Base Article Q276304

$\Rightarrow$ Es gibt Raum für Verbesserungen . . .

Entity Authentication

Authentication

Definition (HAC)

Entity Authentication (identification) is the process whereby one party is assured of the identity of a second party involved in the protocol, and that the second party has actually participated.

- Der erste Schritt wenn man einen Computer benutzt
  - Log in
- Authentication ist ein “real-time” Prozess
  - Die authentifizierte Partei ist aktiv beteiligt . . .

Prinzipien für Authentifizierung

- Ein Geheimnis, das man kennt:
  - PIN, Passwort
- Etwas, das man besitzt:
  - Smartcard, Passwort-Generator
- Etwas, das uns inherent ist:
  - Fingerabdruck, Stimme, Iris

$\Rightarrow$ In der Praxis benutzt man oft eine Kombination dieser Prinzipien!

Passwort-basierte Authentifizierung

- Passwort
  - Ein gemeinsames Geheimnis zwischen User und System
- Passwort-basierte Authentifizierung
  - User beweist Kenntnis des Passworts beim Login
  - System vergleicht das Passwort mit gespeicherten Werten
  - Es muss gewährleistet sein, dass das Passwort nicht für einen Angreifer sichtbar ist . . .

Wie werden Passwörter gespeichert

- Passwort-File
  - Passwörter werden im Klartext gespeichert
    (nur root hat r/w-Rechte)
- “Encrypted” Passwort-File
  - Hashwerte werden gespeichert anstatt des Passworts
- Salting Passwords
  - Im Encrypted Passwort-File wird noch ein t-bit Salt benutzt
    $\rightarrow$ gegen Wörterbuchattacken

Attacken

- Exhaustive Search
  - Durchsuchen aller Passwort-Kombinationen
- Wörterbuch-Attacken
  - Benutzen nur die “plausibelsten” Passwörter
    - Das Wörterbuch enthält die Hashwerte dieser Passwörter
  - Salting macht die (offline) Wörterbuch-Attacke erheblich schwieriger

Passwort-Policy

Eine gute Passwort-Policy die die User zwingt, gute/ sichere Passwörter zu wählen ist entscheidend für ein sicheres System!

Weak vs. Strong Authentication

- Schwache Authentifizierung
  - Replay-Attacken sind möglich
  - Einfache Passwort-basierte Systeme
- Starke Athentifizierung
  - Challenge-Response Prinzip
  - Wie schon in unserem ursprünglichen Beispiel der Authentifizierung Bankomat $\leftrightarrow$ Karte!

Access Control

- Management von Usern und Prozess-Privilegien
  - Wer darf auf welche Files und Folders zugreifen?
  - Wer darf welche Applikationen (Prozesse) starten?
  - Wer darf das System konfigurieren?
- Access Control List (ACL)
  - Liste für Files (Prozesse), User und Privilegien
- Tickets

Security Mechanismen in Windows

Windows Login

- Einfache Folge von Schritten
  - Drücke `Ctrl+Alt+Del`
  - Eingabe von Username und Passwort
- Es gibt unterschiedliche Logins
  - Interactive, non-interactive
  - Batch, service
- Schutz vor Spoofing

Windows Login

- Spoofing
  - Angreifer schreibt ein Programm um das Login zu simulieren
  - Unachtsamer User gibt sein Passwort preis . . .
- Wird verhindert durch die Secure Attention Sequence (SAS)
  - `Ctrl+Alt+Del` ist die SAS
  - Die SAS wird vom Keyboard Treiber abgefangen
  - Der Treiber startet das Programm für den Windows-eigenen Login

Windows Authentifizierung

- Abgehandelt durch die Authentication Authority
  - Lokaler Login: Local Security Authority (LSA)
  - Domänen Login: LSA des Domain Controller (DC)
    - DC ist der zentrale Server der die Network Resourcen, security policies und User verwaltet
- Verschiedene Authentication-Protocols möglich:
  - NTLM (NT LAN Manager)
  - Kerberos $\rightarrow$ default
  - SSL, etc.

Interactive Login – Winlogon

- Startet wenn der User die SAS drückt
- Winlogon Service startet GINA (Graphical Identification aNd Authentication)
- GINA
  - Zeigt das Login Interface
  - Gibt die User Eingaben an die LSA weiter
- LSA führt die Authentifizierung durch

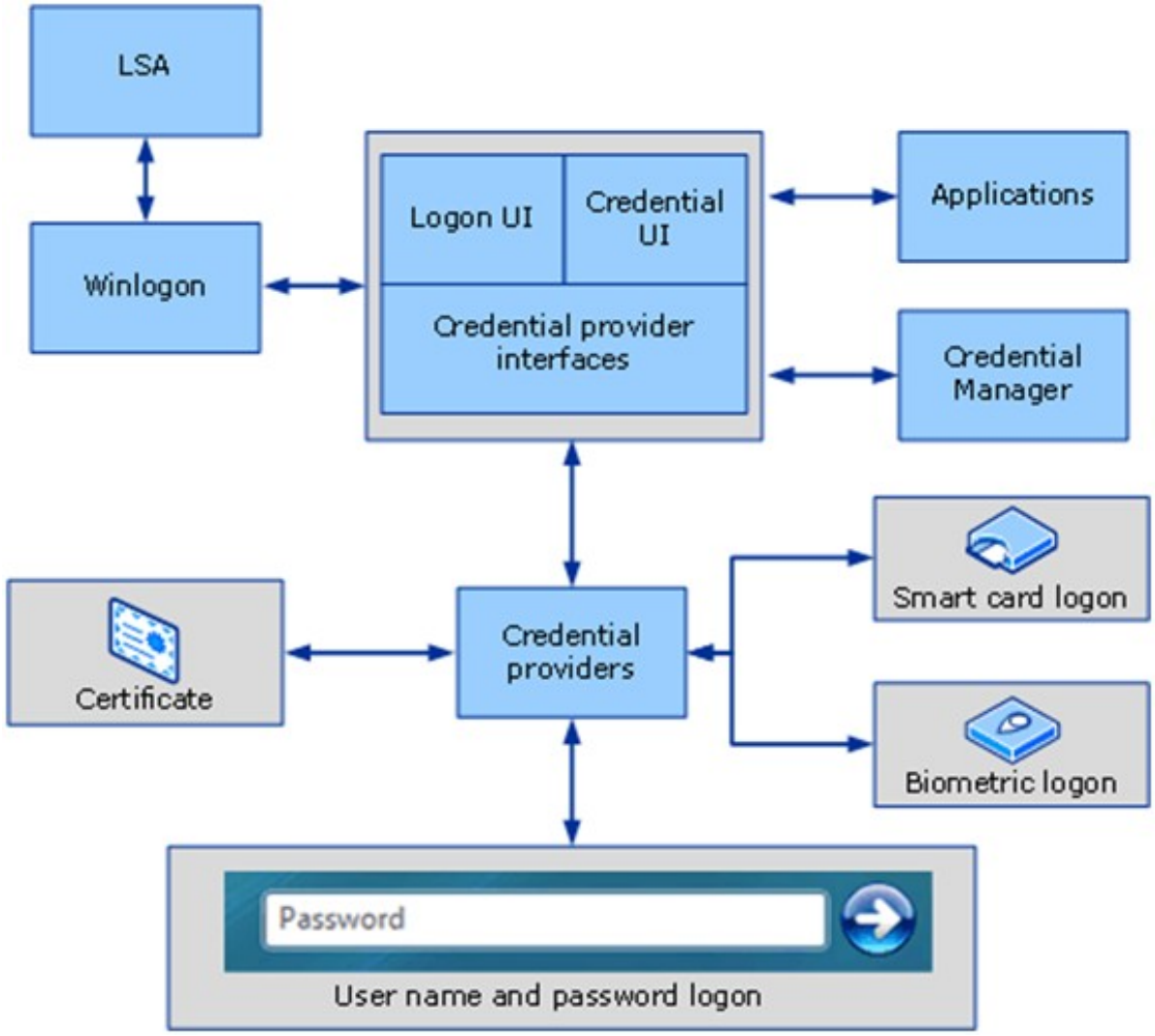
Authentication Packages

- MSV1_0 und Kerberos
  - Kerberos ist Netzwerk-basiert, es kann keine lokalen Logins behandeln
  - Kerberos benötigt ein Key Distribution Center (KDC) das normalerweise auf einem DC läuft
- User credentials werden am Domain Controller in einer Datenbank gespeichtert
  - Active Directory (SAM – Security Accounts Manager)
- Das System kann beliebig komplex werden:
  - Viele User wollen eine große Zahl an Netzwerk-Resourcen benutzen, auch aus fremden Netzen . . .

Credential Provider Architecture

- New: LogonUI + Credential Providers API
- Credential providers must be registered on a Windows computer and are responsible for:
  - Describing the credential information required for authentication
  - Handling communication and logic with external authentication authorities
  - Packaging credentials for interactive and network logon

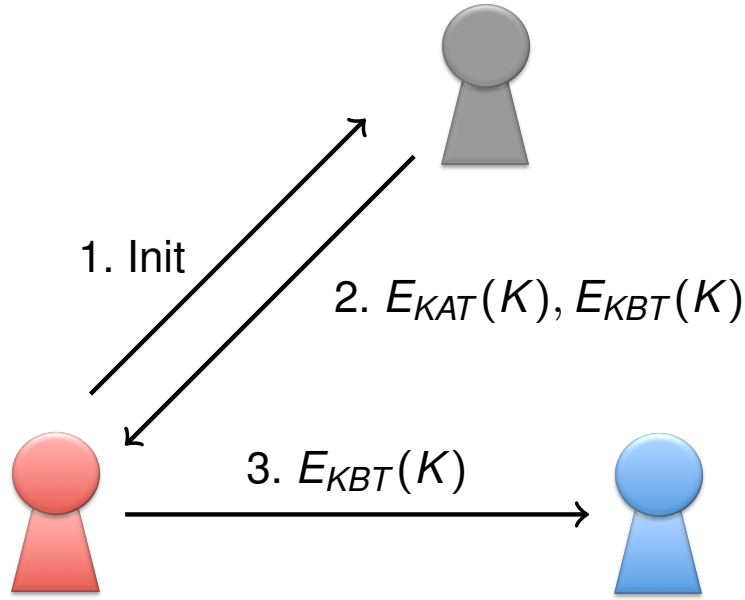
Credential Provider Architecture



source: http://technet.microsoft.com

Kerberos

- Symmetrische Kryptographie
  - Alice, Bob
  - KDC (Trusted third Party)
- Langzeit-Schlüssel
  - Alice, KDC: KAT
  - Bob, KDC: KBT



- KDC erzeugt Schlüssel K für Alice und Bob

Kerberos version 5

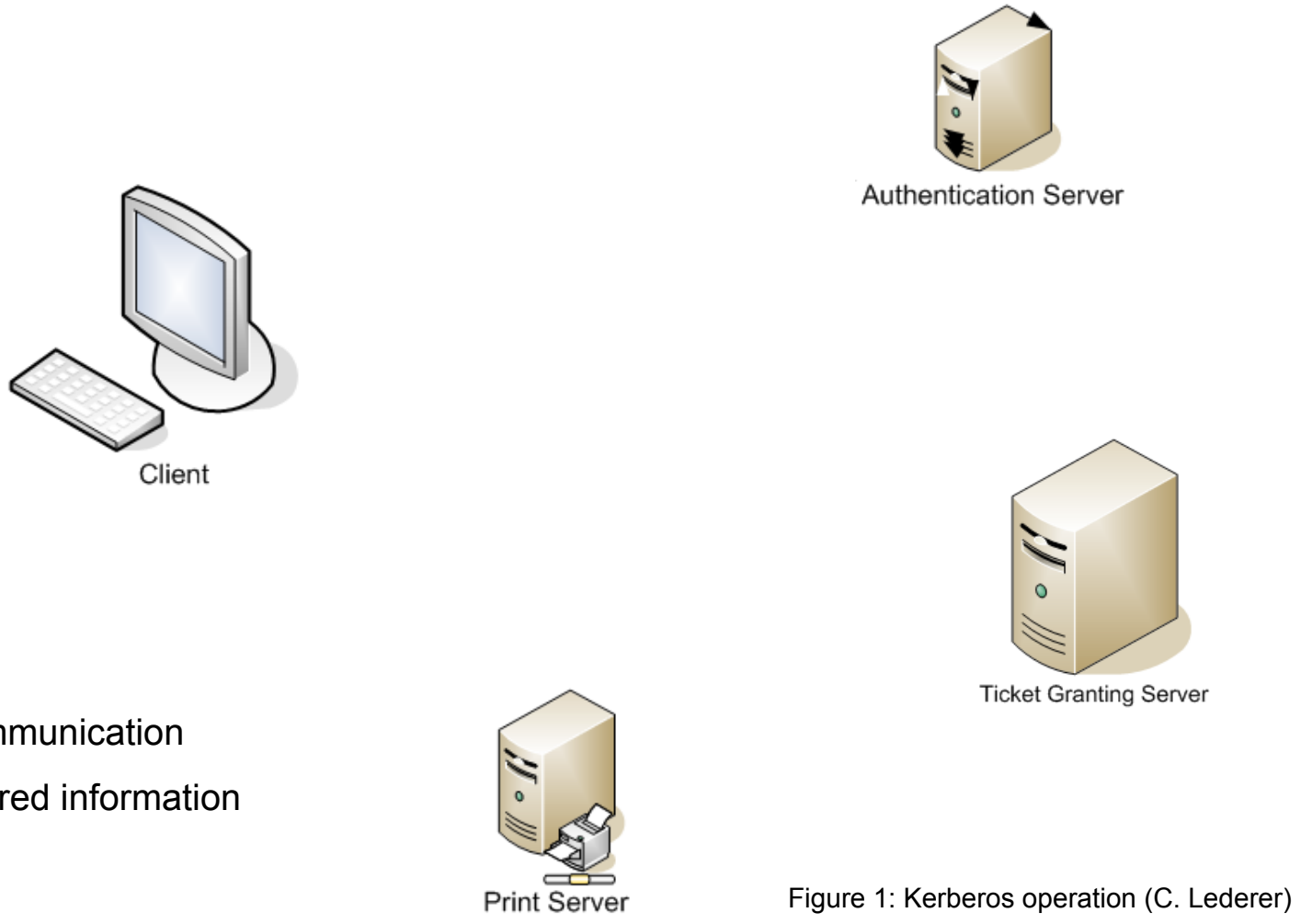


Figure 1: Kerberos operation (C. Lederer)

Kerberos version 5

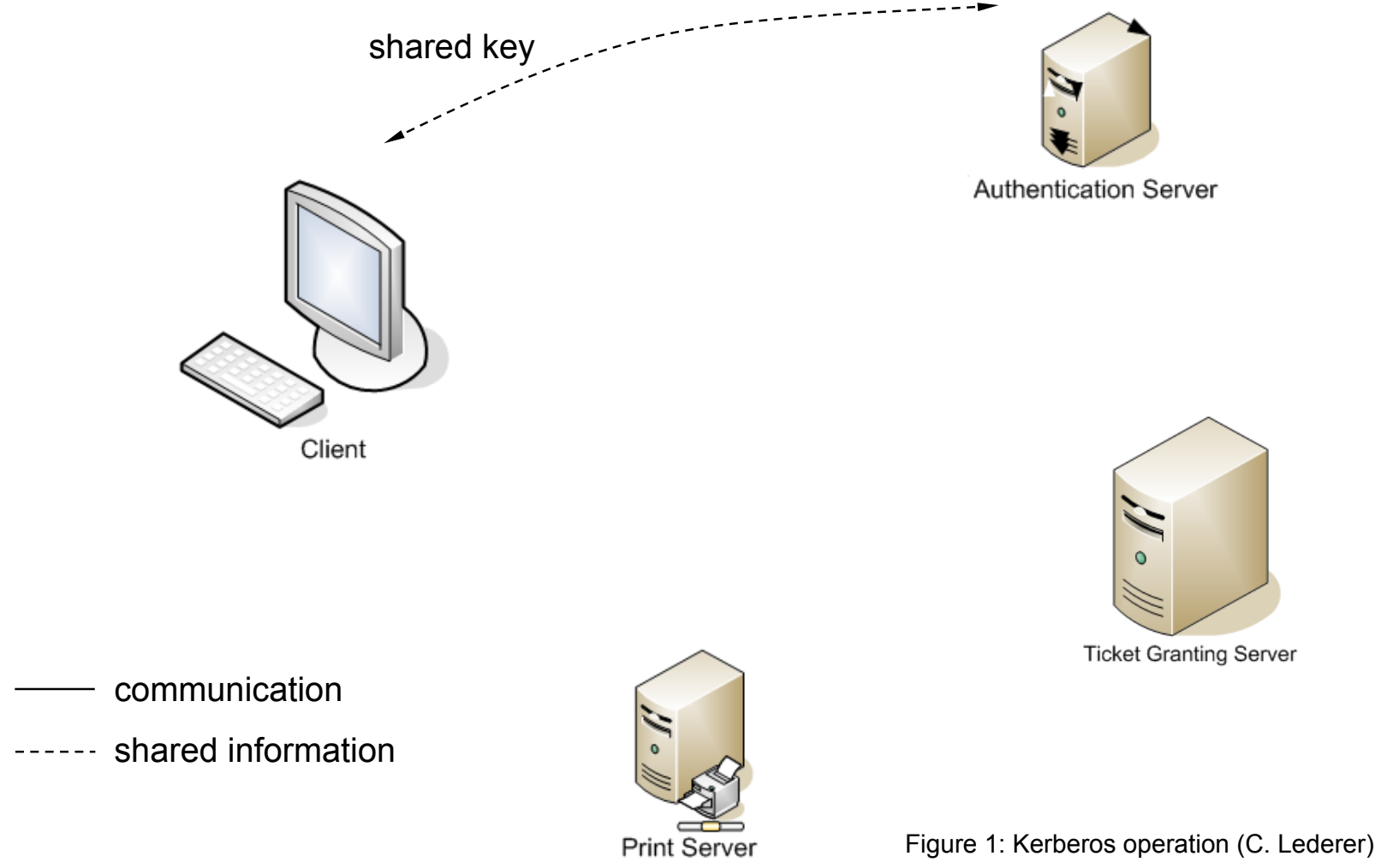


Figure 1: Kerberos operation (C. Lederer)

Kerberos version 5

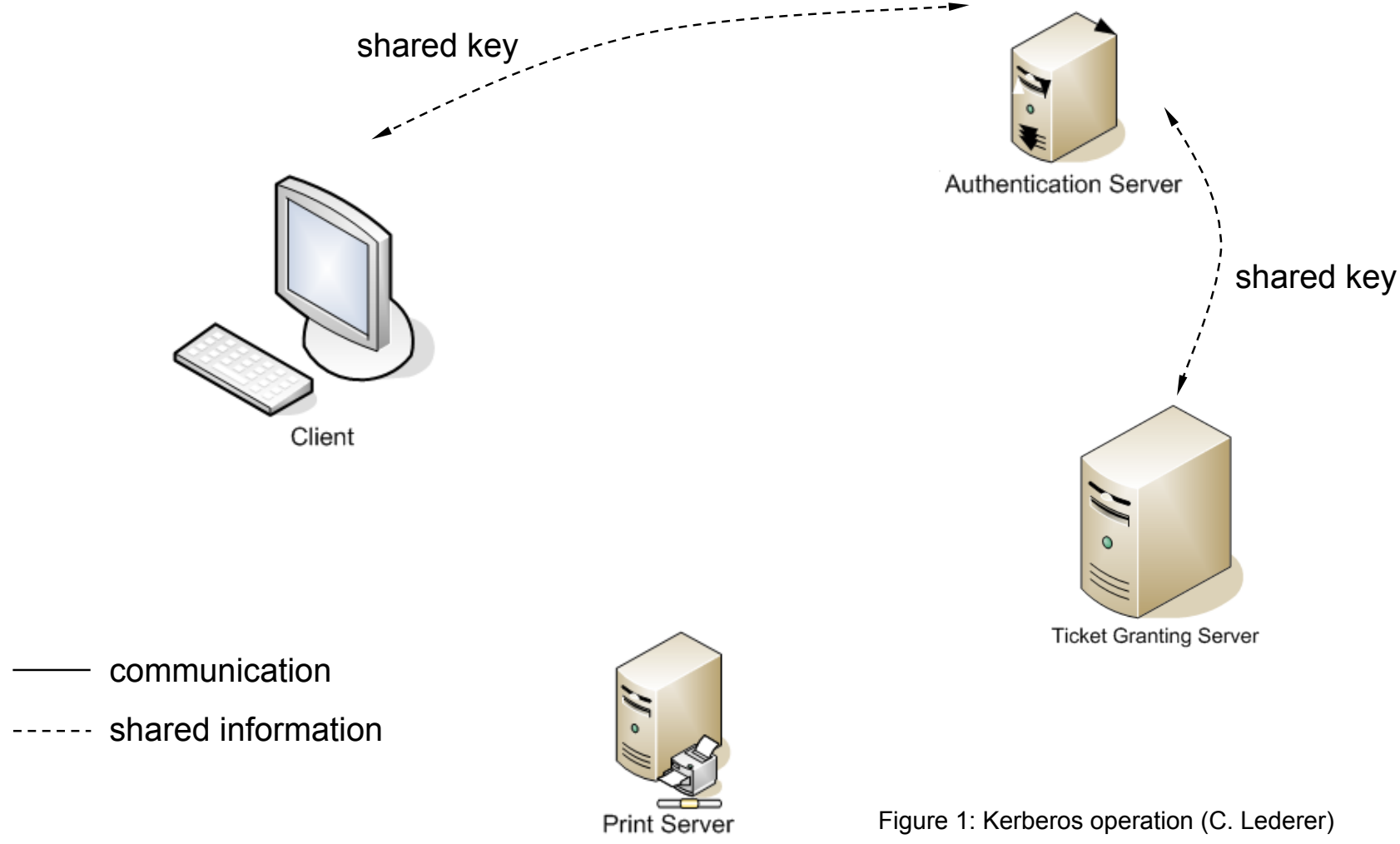


Figure 1: Kerberos operation (C. Lederer)

Kerberos version 5

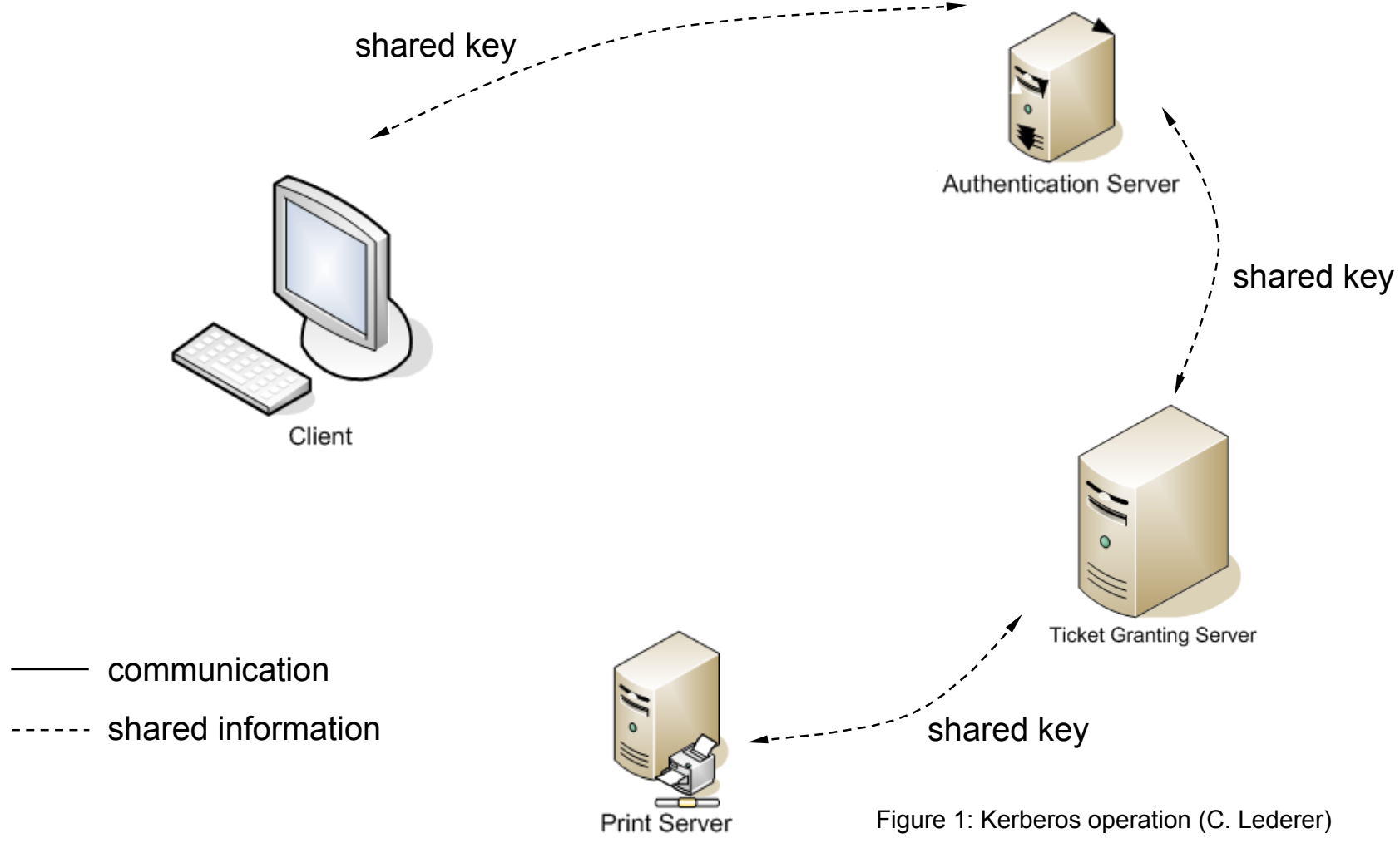


Figure 1: Kerberos operation (C. Lederer)

Kerberos version 5

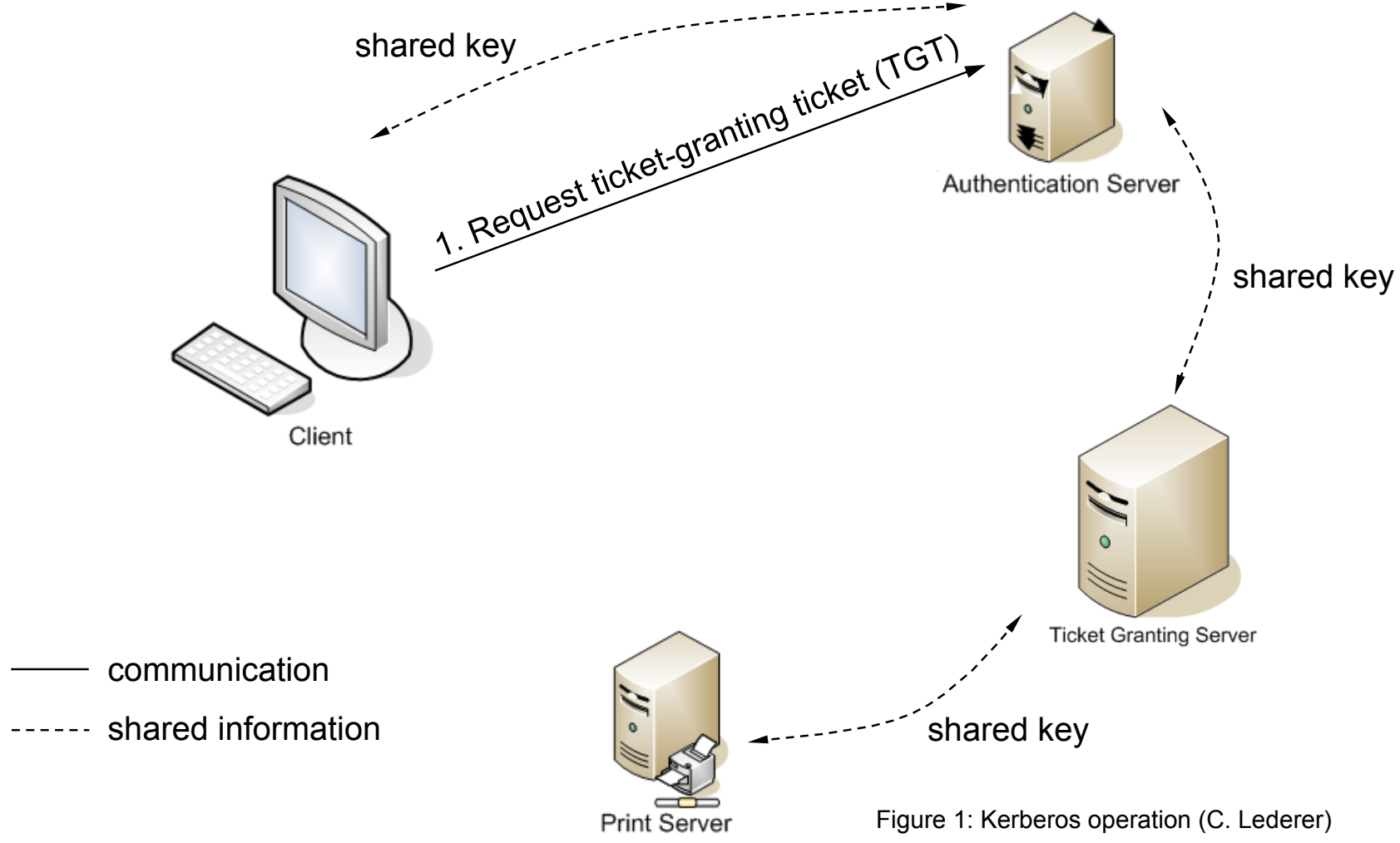


Figure 1: Kerberos operation (C. Lederer)

Kerberos version 5

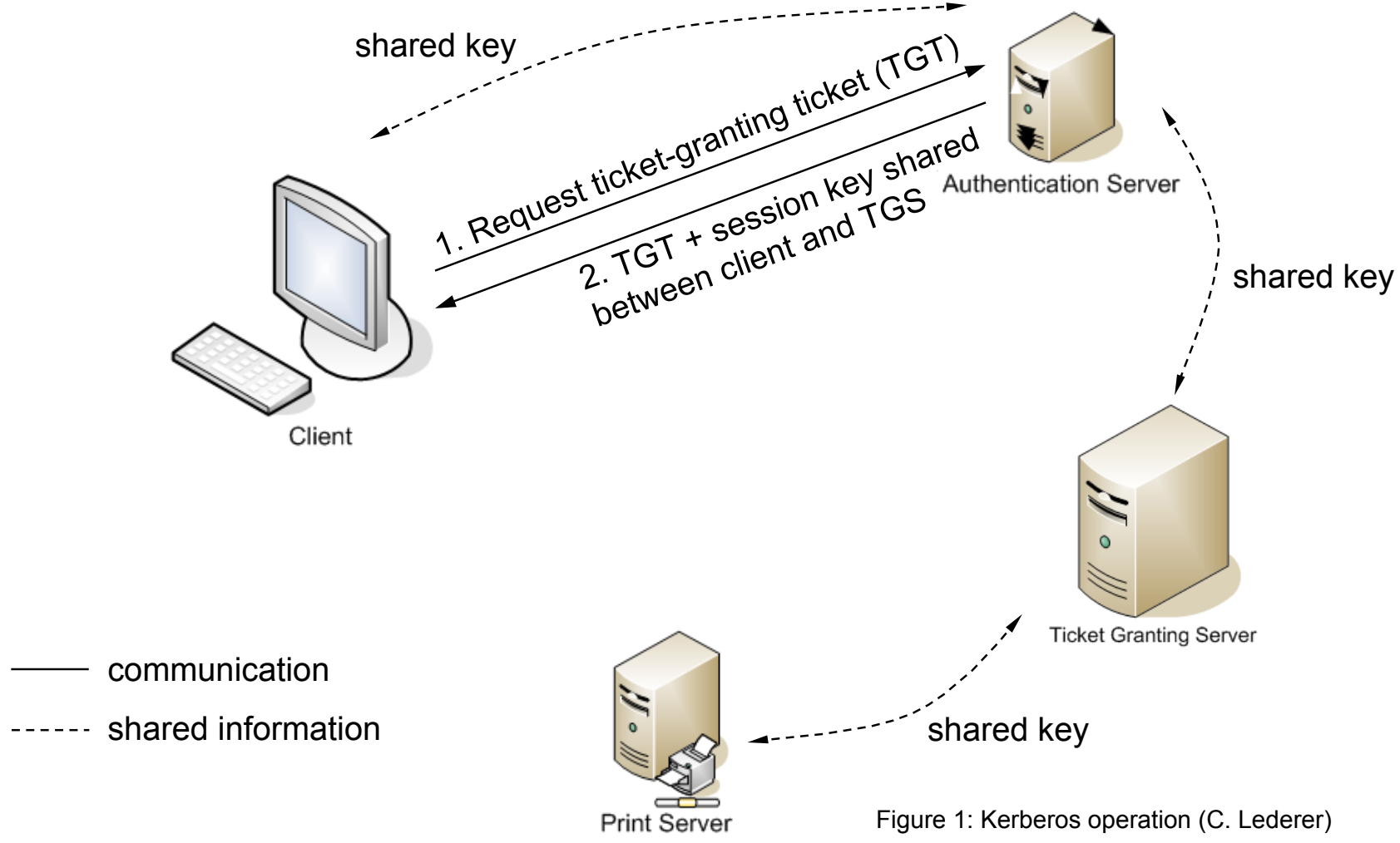


Figure 1: Kerberos operation (C. Lederer)

Kerberos version 5

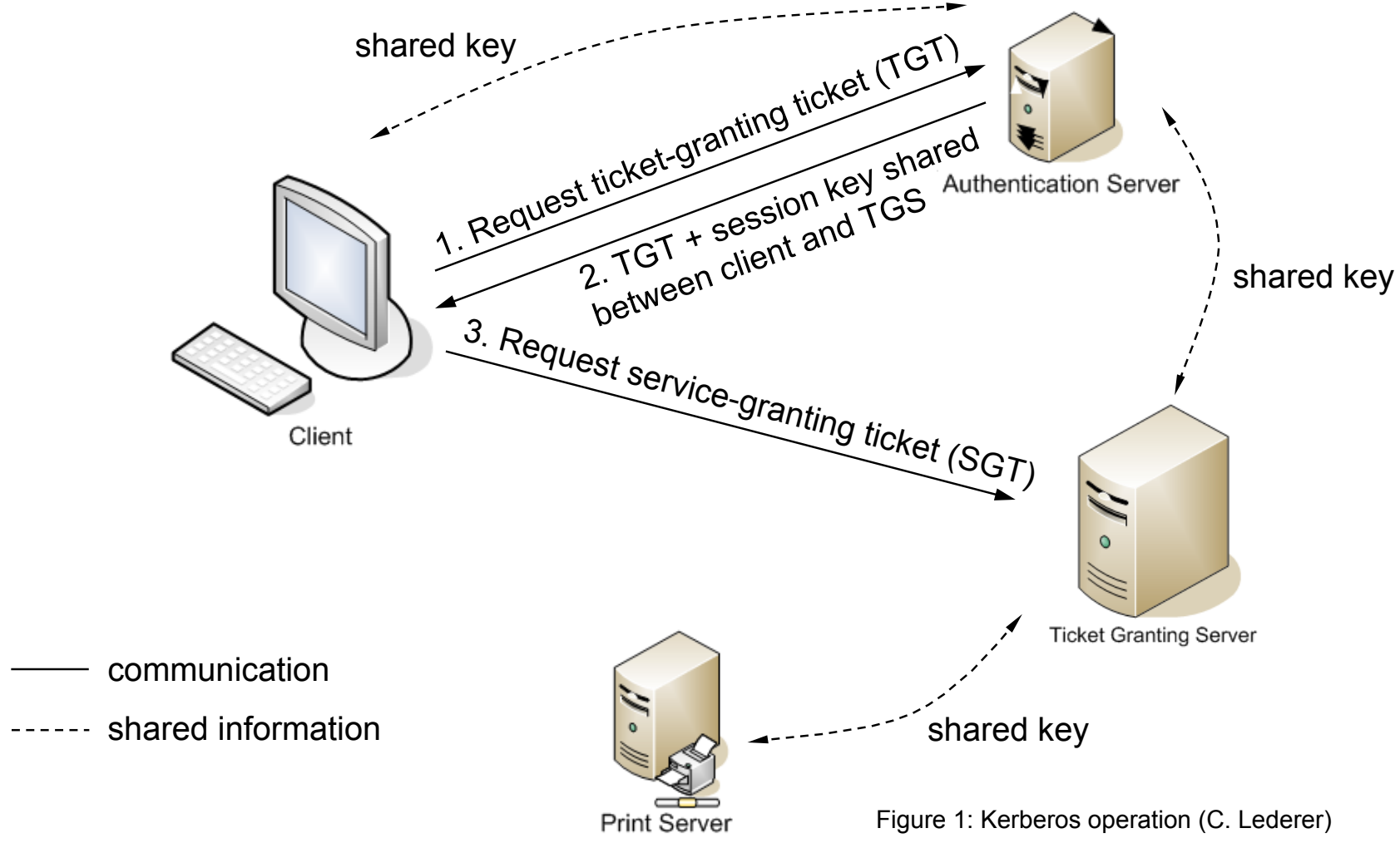


Figure 1: Kerberos operation (C. Lederer)

Kerberos version 5

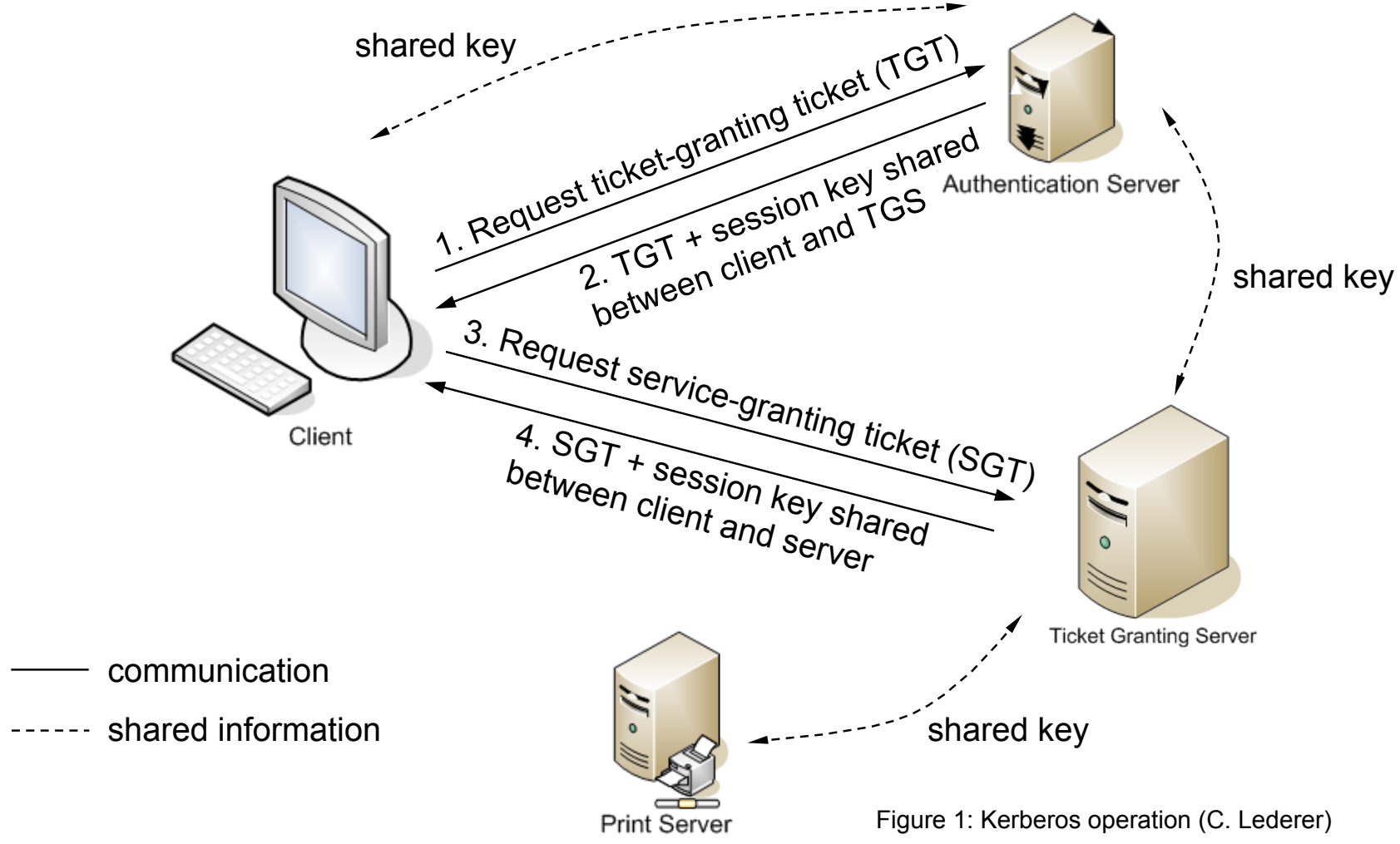


Figure 1: Kerberos operation (C. Lederer)

Kerberos version 5

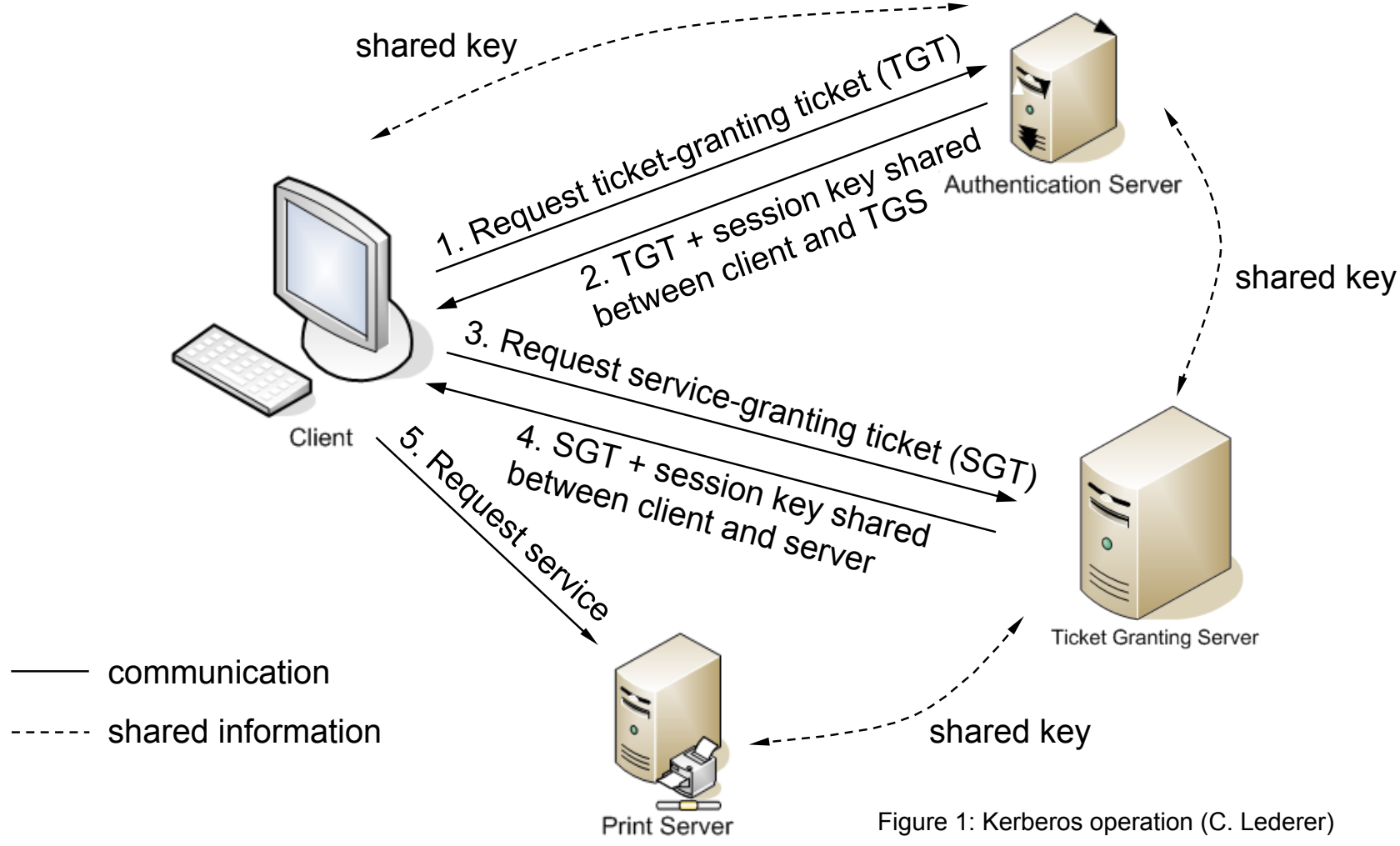


Figure 1: Kerberos operation (C. Lederer)

Kerberos version 5

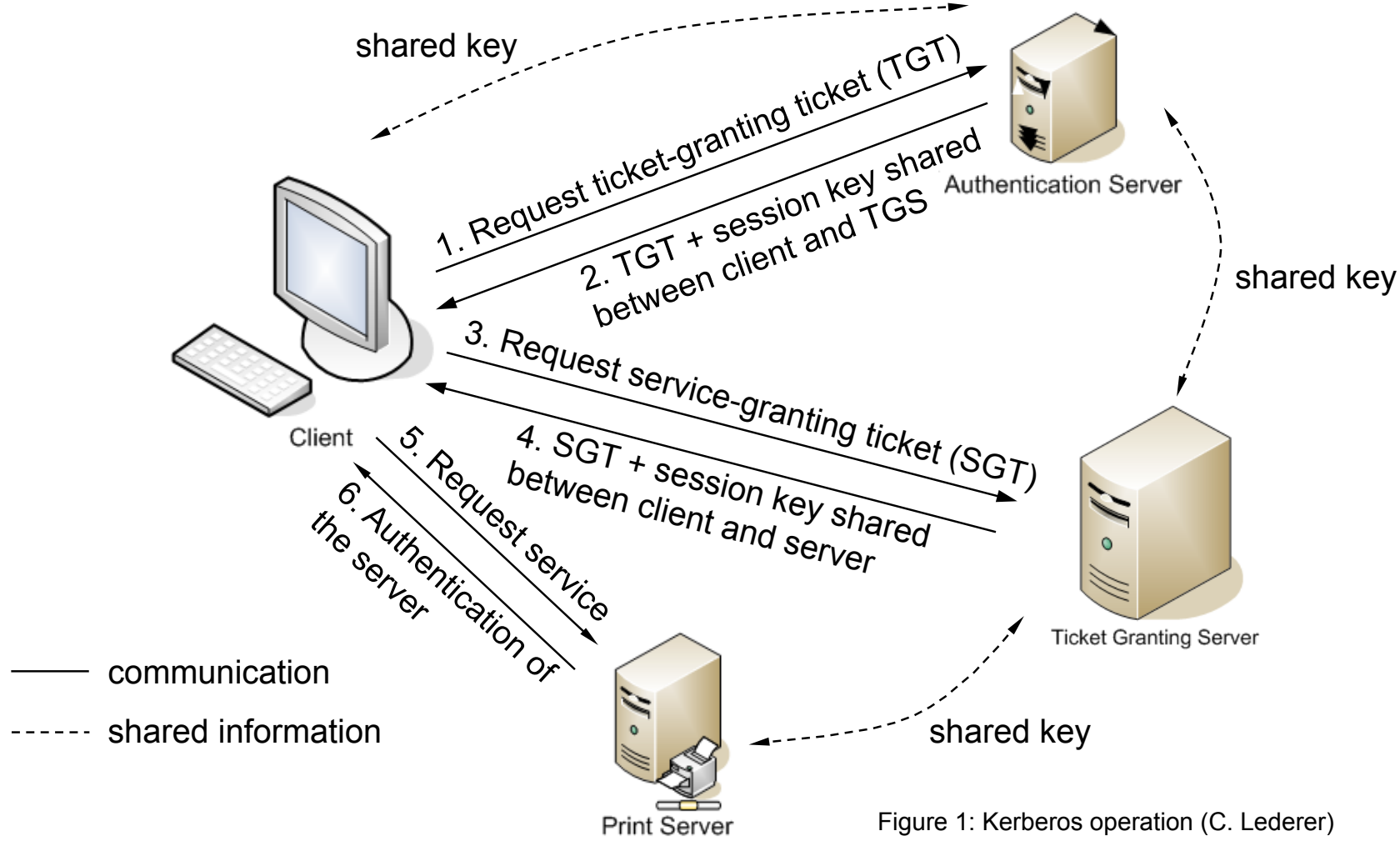


Figure 1: Kerberos operation (C. Lederer)

Kerberos in Windows Login

- Offensichtlich komplexer als lokales Login
- Erlaubt “single-sign on”
  - User authentifiziert sich nur einmalig:
    - Erhält ein “Ticket” um Resourcen zu benutzen beim Login
  - Kann diese Resourcen für die Dauer der Gültigkeit des Tickets behalten

Access Control in Windows

- DACL (Discretionary ACL)
  - Für jedes File (Resource) wird eine Liste von Usern und Rechten gespeichert
  - Der Besitzer des Objekts vergibt die Rechte
- SID (security identifier)
  - Datenstruktur die User/Group/Computer-Accounts identifiziert
- Access token eines Prozesses
  - Beinhaltet SID und zusätzliche Info (Privilegien)
- SACL (System ACL)
  - Gibt an, welche Zugriffe auf ein Objekt mitgeloggt werden

Encrypted File System (EFS)

- Unterstützt vom NTFS
- Seit Win2000:
  - Default Algorithmus: DES (56 bit key)
  - 128-bit Encryption pack: DESX wird benutzt
- WinXP
  - Default Algorithmus ist AES-256
  - 3DES kann benutzt werden
- Bis WinXP: Nur Microsoft Cryptographic Providers können für EFS benutzt werden

Encrypted File System (EFS)

- Verschiedene Schlüssel:
  - Für jedes verschlüsselte File, legt die LSA einen File Encryption Key (FEK) an
  - Diese Schlüssel werden wiederum verschlüsselt auf der Festplatte abgelegt
- Schlüssel-Verschlüsselung
  - Basiert auf Asymetrischer Kryptographie
  - Der FEK wird mit dem EFS Public Key des Users verschlüsselt
  - Zum Entschlüsseln muss der korrespondierende private Key vorhanden sein

Encrypted File System (EFS)

- Sicheres Speichern des privaten EFS-Keys
  - Auf Smartcard (seit Vista möglich)
  - Wiederum verschlüsselt
    (und wo speichern wir nun den Encryption Key?)
- Passwort-basierte Verschlüsselung
  - Definiert in PKCS#5
  - Encryption Key wird (mit einer Einweg-Funktion) von einem Passwort abgeleitet
  - `www.emc.com/emc-plus/rsa-labs/standards-initiatives/`

EFS Probleme

- Windows gibt “Hinweise” darauf, ob User EFS benutzen (oder benutzt haben)
  - Registry Einträge
- Windows ermöglicht Datenwiederherstellung
  - Die Security Policy legt fest, ob das auch von anderen Usern für die eigenen Daten passieren kann
- Verlorene Passwörter (reset)
  - Daten sind weg (ohne Data Recovery)

Disk Encryption

- Full (whole) disk encryption
  - Software basiert
  - Hardware-basiert innerhalb / außerhalb des Devices
  - Alles ist verschlüsselt (Swap, temp files)
- Boot key problem
  - Die Datenblöcke, die das OS enthalten müssen entschlüsselt werden, um zu booten.
  - Pre-Boot Authentication (mini-OS, integrity protected)
    - Usr/Pwd, PIN/Smartcard, USB-Dongle, . . .
    - MS Bitlocker benutzt z.B. TPM Modul
- Data recovery mechanisms

Attacken auf Disk Encryption

- Cold boot attack (Keys bleiben im SRAM, DRAM)
  - Unmounten von Vaults
  - Two-factor authentications
- Watermarking-Attack
  - CBC mode anfällig (mit vorhersagbaren IVs)
  - NIST: AES-XTS mode

Disk Encryption

- Tools:
  - Bitlocker (Windows)
  - dm-crypt (Linux)
  - MacOS FileVault
  - ...
- Smartphones
  - Hohe Mobilität $\rightarrow$ Schutz der Daten noch wichtiger!

Security Mechanismem in Unix/Linux

Unix User Authentication (Historisch)

- Login-Prozess fragt nach Username und Passwort
  - Früher wurden Encrypted Passwort-Files benutzt
  - Login “verschlüsselt” das Passwort und vergleicht es mit dem Eintrag für den jeweiligen User
- “Encryption” – crypt
  - User Passwort wird als Schlüssel
  - Plaintext = ’00. . . 0’
  - Modifizierte Version des DES wurde oft benutzt
  - Mit Salt!

Unix Login

- Login-Prozess läuft mit SETUID root
- Nach erfolgreicher Verifikation des Passworts
  - Login ändert die User ID (UID) und Group ID (GID) auf die UID und GID des Users
  - Login aktiviert Standard IO (Keyboard, Monitor)
  - Login öffnet Shell und terminiert

Linux – PAM

- Pluggable Authentication Modules for Linux
- Eine Suite von shared-libs
  - Admin/System Setup legt fest, wie App. einen User authentifiziert
  - Der Auth-Mechanismus kann gewechselt werden, ohne die Applikation (z.B. login/ssh) neu kompilieren/installieren zu müssen
- Große Flexibilität
  - Smartcard, passwd-check, etc.

Access Control in Unix

- User, Prozesse, Resourcen haben
  - UID
  - GID
- UID und GID werden vom Owner übertragen
- Resourcen haben auch Permissions (vom Owner gesetzt)
  - Read, Write, Execute (Search)

Access Control in Unix

- Root (Superuser)
  - User mit hohen Privilegien
- SETUID
  - Prozess läuft mit den Privilegien seines Owners statt mit denen des Users, der ihn gestartet hat
  - Real UID (owner), effective UID (access control), saved UID (previous UID)
  - UIDs ändern sich kurzzeitig, damit Prozesse mit höheren Privilegien laufen können (Bsp. lpd)

Angriffe auf Betriebssysteme

- Weniger “large scale” Vulnerabilities seit 2005
  - vgl. Blaster, etc.
  - Mehr Antivirus-Schutz
- Starker Anstieg in Client-Vulnerabilities:
  - Browsers, office software, media players, desktop apps.
- Web-Applikationen
  - $\approx$ 50% der Vulnerabilities in 2007
  - PHP, SQL, Cross Site Scripting, Cross Site Req. Forgery

Angriffe auf Betriebssysteme

- Default Konfiguration von OS
  - Weiterhin viele schwach
  - Default Passwörter (brute force, Wörterbuch-Attacken)
  - Würmer/Viren die Passwort-Cracker inkludieren!
- SmartPhones: Attacken am Vormarsch!

Security Enhancing Technologies

Security Enhancing Techniques

- Windows Update (daily updates)
  - Wenn man das Problem nicht umgehen kann, dann zumindest den Schaden begrenzen!
- Sandboxing
  - Restricted execution environment
  - JVM ist ein Bsp.
- Code Signing
  - Authentizität des Codes durch Public-Key Cryptography
  - Vertrauen in welche CAs?

Security Enhancing Techniques

- Data Execution Prevention
  - non-executable stack
- SELinux (NSA/RedHat)
  - Mandatory Access Control
  - AppArmor
- grsecurity
  - Web servers mit Linux
  - Role Based Access Control (viel mehr “Rollen” für User/Prozesse)

Trusted Computing

- Trusted Computing
  - User vertrauen ihrem OS?
  - Vertraut OS (Hersteller) den Usern?
- User vertraut OS
  - Grundsätzlich nützlich
  - Voraussetzung für Verlässlichkeit, Produktivität, ...
- OS Hersteller kontrollieren User
  - DRM

Trusted Computing

- TCG (Trusted Computing Group)
  - Unter anderem: AMD, HP, IBM, Intel, MS, Sony, Sun, Atmel, Ericsson Mobile, Nokia, ...
- TPM (Trusted Platform Module)
  - Microcontroller für das sichere Speichern/Behandeln von krypto. Schlüsselen, Passwörter, Zertifikaten, ...
  - Spezifikation ist öffentlich
- Open TC (EU Project)

Zusammenfassung

- Unsichere OS führen zu unsicheren Computern
  - OS ist einer der Kern-Bereiche für sichere Systeme
  - Login und Access Control sind wichtige Teile bei OS Sicherheit
- Immer mehr Zugänge zur Verbesserung von OS Sicherheit

Vielen Dank für Ihre Aufmerksamkeit!