Analyse und Erfahrung mit Groove

Projektarbeit Telematik 2002

Betreuer: Dipl.-Inf. Thorsten Strufe

Vortragender: Eric Niedling

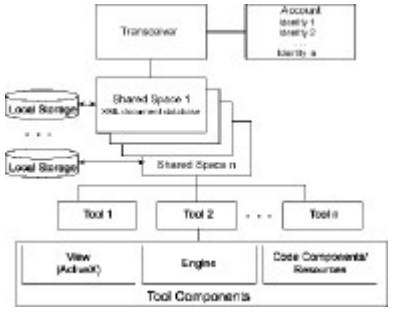
Motivation

- Internet: Nutzung von verteilten Ressourcen
- zunehmende Verwendung von Filesharing-Anwendungen im privaten Bereich (Napster,...)
- Sicherheit des „Intellectual Capital“ im Unternehmen bei dezentraler Speicherung?

→ Unterschiedliche Charakteristik der Daten

- Untersuchung einer Groupware-Anwendung und ihres P2P-Charakters
- Untersuchungsziele: Datenkonsistenz, Sicherheit, Erweiterbarkeit

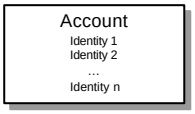
Wie sieht die Software-Architektur der Groove (Client) Software aus?



Mit einem Groove-Nutzerkonto können verschiedene Identitäten genutzt werden

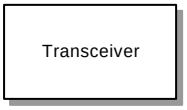
Account: durch eine Passphrase geschützter Zugang auf einen Groove Peer

Identity: Benutzeridentität, mit der an einer Arbeitsgruppe teilgenommen wird



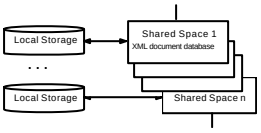
Der Transceiver ist die zentrale Softwarekomponente eines Groove Peers

Transceiver:
- Erledigen von administrativen und produktiven Aufgaben
- Zugriff auf Systemdienste (My Contact, My Accounts, My Space,...)
- Realisiert „Awareness“-Funktion



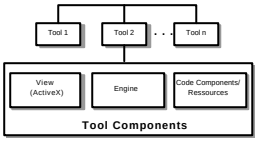
Die Objekte einer Arbeitsgruppe werden mit XML beschrieben und verschlüsselt

Shared Spaces = Arbeitsgruppen
- technisch: Kopie eines XML-Objekte Speichers
- funktional: Menge von Groove Anwendern, einer Auswahl an Werkzeugen und verwendete Daten



Diverse wählbare Werkzeuge stellen die flexible, technische Grundlage eine Arbeitsgruppe dar

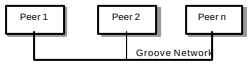
Tools = Werkzeuge
- Werden als Kopie einer Arbeitsgruppe hinzugefügt
- dadurch Versionsproblematik
- Nutzerrollen: Manager / Teilnehmer / Gast
- Verfügbare Werkzeuge:
  Kalender, Foren, „Document Review“, „Files“,
  3 Textwerkzeuge, „Sketchpad“, Browser,...



Kommunikation unter gleichen – Groove basiert auf einer P2P-Architektur

Groove als Peer-to-Peer Software

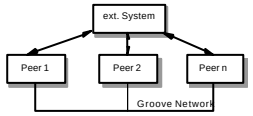
- hoher Grad an persönlicher Interaktion, wie Telefonsystem
- ermöglicht räumlich und zeitlich versetzte Zusammenarbeit
- Integration in „restliche“ IT-Landschaft?



Der „Multi Point Integration“-Ansatz erlaubt jedem Peer den Zugriff auf externe Systeme

„Multi Point Integration“

- jeder Peer kann Daten mit externen Systemen austauschen
- Beispiel „Gemeinsames Surfen“:
  Es wird lediglich die URL zwischen den Peers ausgetauscht, dies minimiert den Traffic im Peer-Netzwerk.

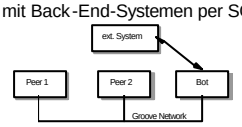


Bei dem „Single Point Integration“-Ansatz ist der Zugriff über auf ext. Systeme über Bots realisiert

„Single Point Integration“

Annahme: gleichzeitiger Zugriff von mehreren Anwendern auf eine ext. System aus Gründen der Performanz und Integrität eher nachteilig

- Bots = Software-Agenten
- Recherchieren in Datenbanken, verfolgen Diskussionen,...
- Werden zentral durch Groove Enterprise Integration Server verwaltet
- Kommunizieren mit Back-End-Systemen per SOAP, ADO und ODBC



Groove verwendet sowohl standardisierte Protokolle, also auch Proprietäre

Offene Standards und Protokolle:

- HTTP, UDP, TCP/IP
- XML (Beschreibung von Objekten und Nachrichten)
- SOAP, ADO, ODBC und XML-RPC zur anwendungübergreifenden Kommunikation
- vCard-Stand ← LDAP lesbar

Groove Protokolle:

- DPP (Device Presence Protocol) – wer ist online
- SSTP (Simple Symmetric Transport Protocol) – Datenaustausch zwischen Peers, egal ob direkt verbunden oder durch Firewall getrennt (Relaying)

Eine Passphrase beliebiger Länge ist der Ausgangspunkt für das Sicherheitskonzept

- alle Daten sind verschlüsselt (übertragene und gespeicherte)
- Daten + Binary Differentials
- Passphrase als schwächstes Glied
- Komplexes Schlüsselsystem zum Schutz lokal gespeicherter Daten
- Schlüssel zur Datenspeicherung werden von der Passphrase abgeleitet
- Verfahren: PBKDF2 und PBE-MARC4

Groove verwendet je nach Anwendungsfall unterschiedliche Verschlüsselungsalgorithmen

Anwendungsfall 1: Kommunikation zwischen zwei Anwendern außerhalb einer Arbeitsgruppe

- asymmetrische Verschlüsselung der Übertragung (ElGamal)
- Signatur der Verschlüsselung (RSA)
- jeweils 2048 Bit Schlüssellänge als default-Einstellung

Anwendungsfall 2: Kommunikation innerhalb einer Arbeitsgruppe

- Austausch eines symmetrischen Gruppenschlüssels nach dem Diffie-Hellman-Verfahren
- Verschlüsselung der Daten mit dem Gruppenschlüssel
- Unterschreiben der verschlüsselten Daten mit dem privaten Schlüssel (ESIGN)
- Neue Mitglieder erhalten aktuellen Gruppenschlüssel, bei Ausschluß eines Gruppenmitgliedes neuen Schlüssel erzeugen

Zusammenfassung

- Groove hat überwiegend P2P-Charakter
- Durch Funktionserweiterungen (Relaying, Bots) Übergang zu einer hybriden Architektur
- Gutes Sicherheitskonzept

Vielen Dank für Ihre Aufmerksamkeit