SKIP

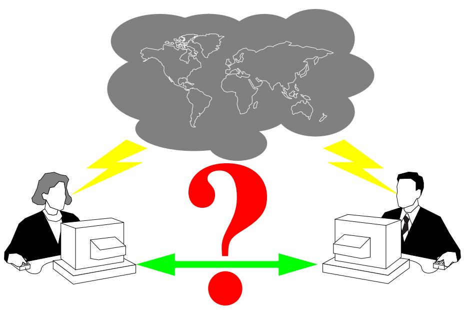
Proliferation von Sicherheit im Internet

Germano Caronni

Institut für Technische Informatik und Kommunikationsnetze
ETH Zürich

Themengebiete

- Schwachpunkte der aktuellen Infrastruktur
- Sicherheit auf Netzwerkebene: SKIP
  (SKIP = Simple Keymanagement in Internet Protocols)
- Mögliche Einsatzformen von SKIP



Teil I: Sicherheit – wieso?

Zunahme der Bedeutung offener Systeme

Firmenübergreifende Kommunikation

E-Mail

Verteilte Datenbanken

Desktop Conferencing

Telebanking

Schutz geistigen Eigentums

Typische Nutzungsarten des Internets

- Client–Server Anwendungen
- Peer-to-Peer Kommunikation
- Virtuelle (Firmen-)Netze

Klassische Bedrohungsformen

- Hacker
- Missbrauch durch Insider
- kriminelle Organisationen
- (Wirtschafts-) Spionage

Fundamentale Anforderungen

Vertraulichkeit der Daten

Authentizität von Partnern und Daten

Beweisbarkeit von Vorgängen (non-repudiation)

Schutz vor böswilligem Wiederholen

Verfügbarkeit der Systeme

Kosten der Sicherheit

Behindert Arbeitsprozesse

Verschlechterung der Dienstgüte
- Rechenleistung
- Bandbreite

Teil II: Mögliche Lösungen

1. Sicherheit in jedem Programm
2. Gesicherte Verbindungen
3. Sichere Netzwerkschicht

Application	FTP/SMTP/RPC
Presentation	XDR
Session	
Transport	TCP/UDP
Network	IP
Link	Ethernet /ATM
Physical	

Sicherheit auf der Anwendungsschicht

+ Datentypen bekannt
+ Integrierte Zugriffskontrolle
+ Kein Vertrauen in tiefere Layer

– Jede Applikation muss aktiv gesichert werden
– Interoperabilität kann verloren gehen
– Schlüsselverwaltung in jeder Anwendung resultiert in Overhead

Sicherung der Verbindungen (Link-Layer, resp. Hardware)

+ hoher Durchsatz (dedizierte Hardware)
+ Sicherheit durch Betreiber erzwingbar

– Wächst nicht ‘einfach’ mit dem System
– In der Regel teuer und proprietär
– Sicherheit pro Maschine, unabhängig vom Kanal

Sicherung der Kommunikation durch die Netzwerkschicht

+ Nur einmal pro Maschine vorhanden
+ Für die Applikation transparent
+ Besser durch den Administrator wartbar

– Applikation muss Netzwerkschicht vertrauen
– Kontextsensitive Behandlung der Daten geht verloren

Sicherheit auf der Netzwerkebene

Betriebssystem kontrolliert Applikation

Sicherheit pro Kanal machbar

Interface zur Applikation möglich

Netzwerkschicht ist die zentrale Schaltstelle

Sichert Interoperabilität

Teil III: SKIP

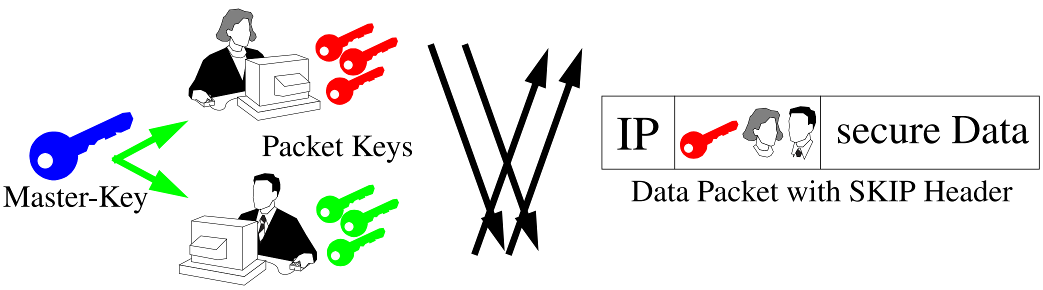
Simple Keymanagement for Internet Protocols
Suns Vorschlag für Sicherheit in IP
(IETF Working Group IPSEC)

Stellt Schlüsselmaterial zur Sicherung von IP, UDP und TCP zur Verfügung.

Erlaubt dem Sender die Auswahl der zu verwenden-den Algorithmen.

Funktionsweise

Erzeugung gesicherter Pakete



Sicheres IP

Proposed Standards und Internet Drafts

Sicherheitsarchitektur: RFC1825

Authentisierung in IP: RFC1826, 1828

Vertraulichkeit in IP: RFC1827, 1829, esp-stream

Key-Management: **skip** (cdp, adp, pfs, ...)
Alternative Vorschläge: oakley, isakmp, photuris

DRAFT		STANDARD		
Individual	WG	Proposed	Draft	—

IP Header (ein Beispiel)

IP	S	AH	SPI	MAC	ESP	SPI	IV	opaq: IP, TCP, ...

AH: Authentication Header

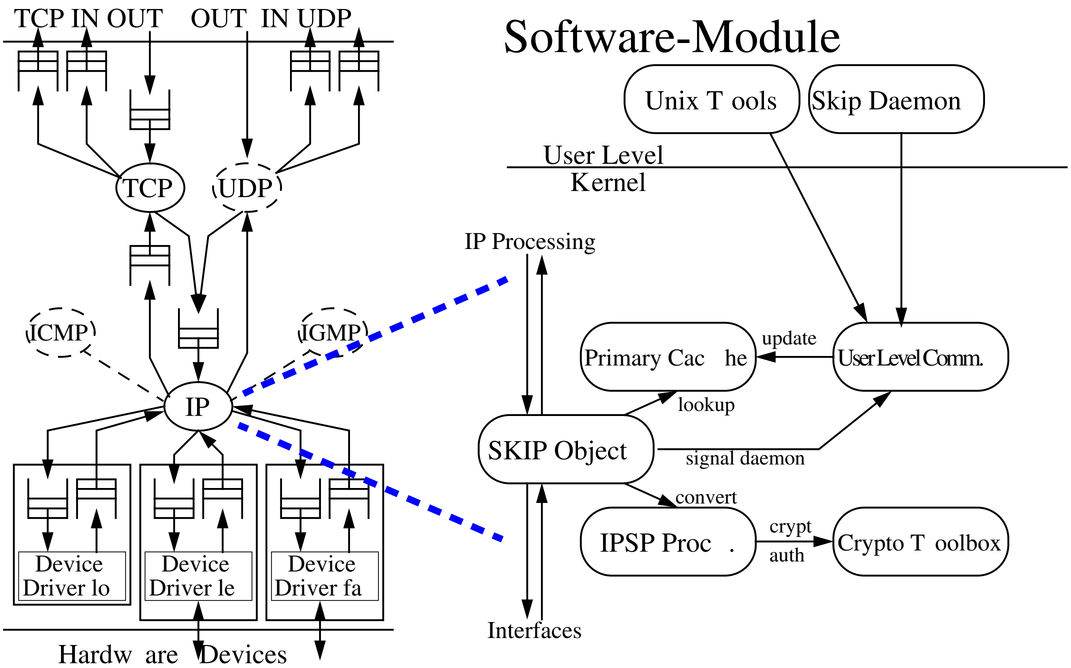
SPI: Security Parameter Index

MAC: Message Authentication Code

ESP: Encapsulating Security Payload

IV: Initialisation Vector

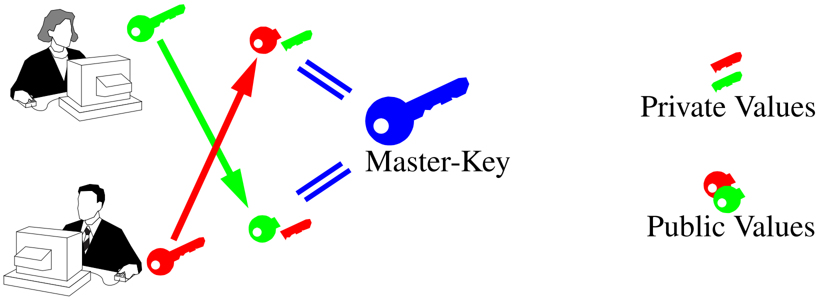
Einbettung ins Betriebssystem



Teil IV: Schlüsselverwaltung in SKIP

Wofür eine Schlüsselverwaltung?

Ermittteln des gemeinsamen Geheimnisses:



Public Key Verfahren

Rivest-Shamir-Adleman (RSA)

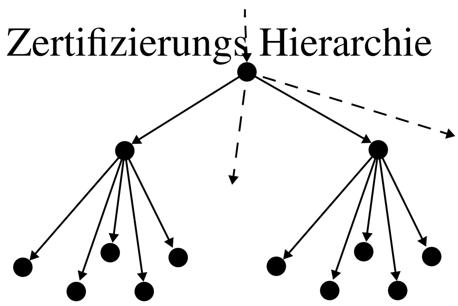
Diffie-Hellman (DH)

Quellen für Public Values

- Datenbanken (z.B. lokale Daten, DNS, PGP)
- SKIP-internes Certificate Discovery Protocol
- Dynamische Erzeugung und Zertifizierung von Public Values
- Alternativen: NIS+, Kerberos, Chipkarten

Vertrauen in Public Values

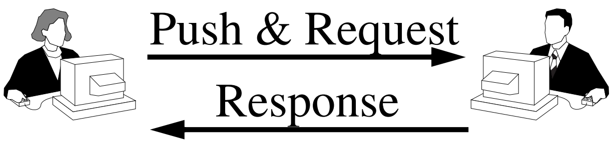
Public Value
DH Parameter
Lebensdauer
Besitzer-ID
Certifier-ID
Signatur



Zertifikat bindet Identität an Public Value

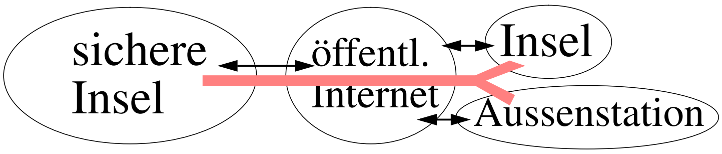
Nur sinnvoll in hierarchischer Organisation

Certificate Discovery Protocol

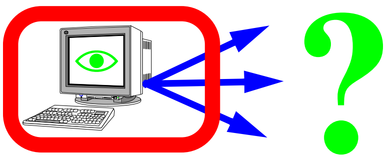


Die Einsatzszenarien

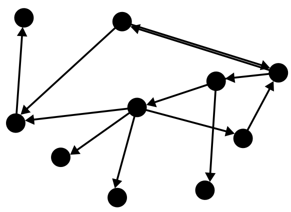
Trusted Environment (Virtual PrivateNetwork)



Halb authentisierter Verkehr (Client–Server)



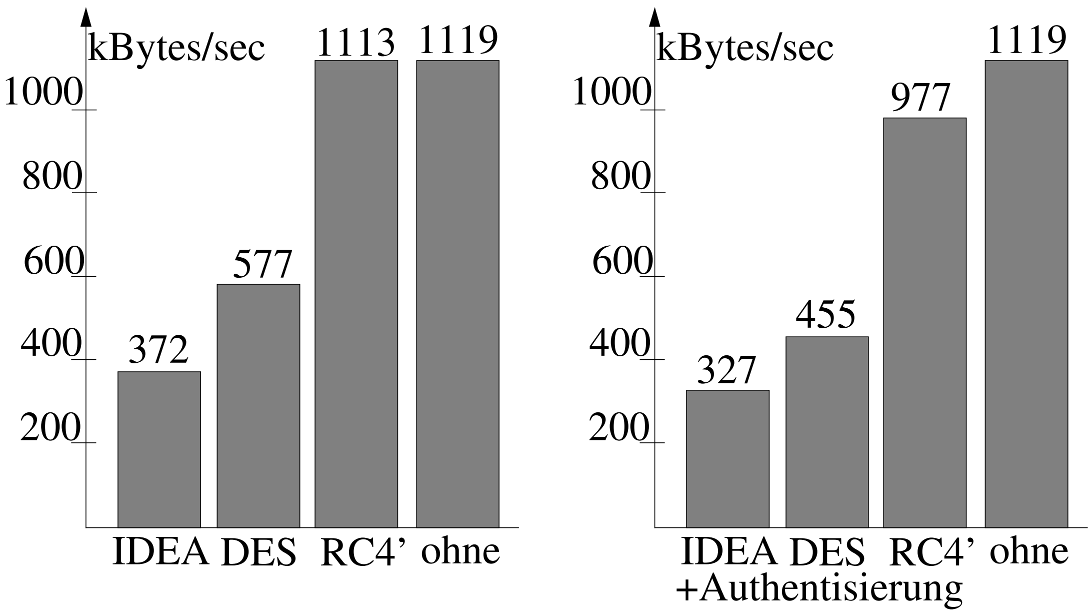
Freie Umgebung (Peer-to-Peer)



Verschiedene Formen von Public Values

- Klassische Zertifikate
  (authentisiert durch Certification Authority)
- Dynamisch generierte, authentisierte Zertifikate
- Unzertifizierte Public Values

Performance



Zukünftige Entwicklung von SKIP

Schnittstelle zur Applikation

Integrierter Paketfilter, Adresskonsistenz

Multicast-Support

IPv6

■ SKIP: Proliferation von Sicherheit im Internet ■

Sicherheit in Zukunft?

Einheitliche Module für
- Datenspeicherung
- Datenübermittlung,

Einheitliches, flexibles Keymanagement

In OS integriert, dedizierte Hardware wird genutzt,
Steuerung der Stärke der Sicherheit
- durch Administrator
- durch Applikation

Kontaktadresse

skip@tik.ee.ethz.ch

Unterlagen

http://www.tik.ee.ethz.ch/~skip
ftp://ftp.tik.ee.ethz.ch/pub/packages/skip