Security Skills for Sysadmins

Wieviel Kryptografie muß im root Account stecken?

René 'Lynx' Pfeiffer

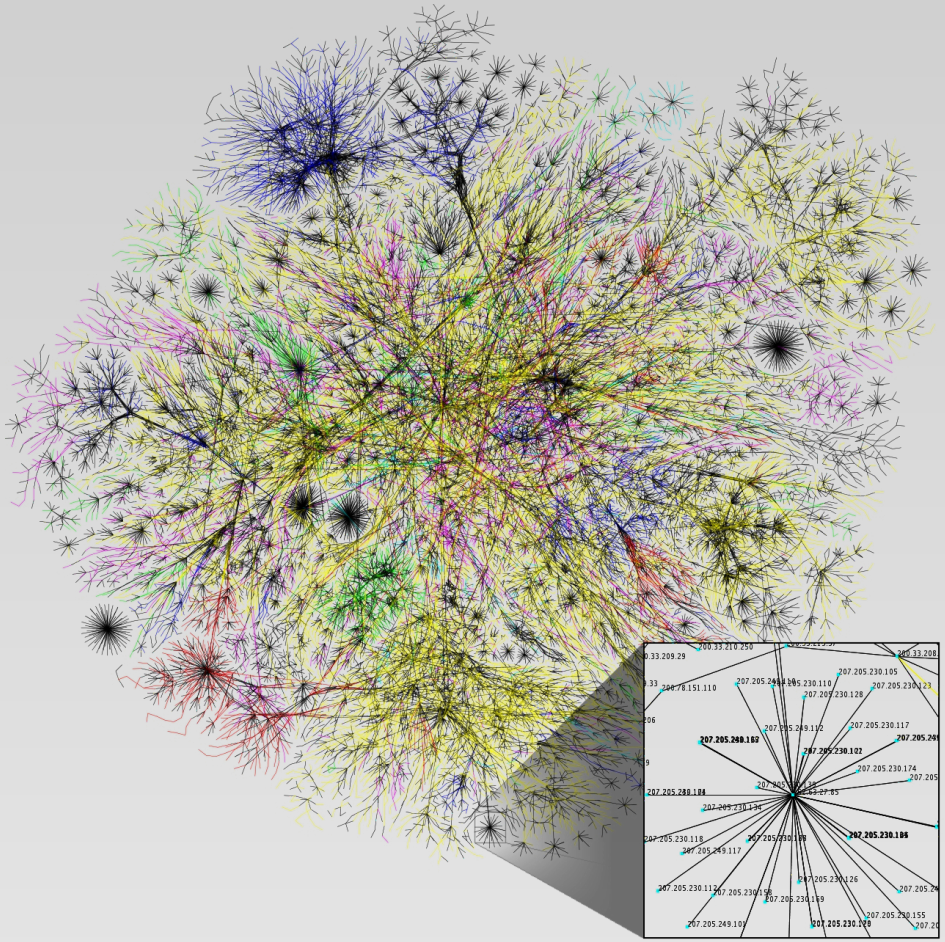
Crowes Agency OG
http://www.crowes.eu/, rene@crowes.eu

Linuxwochen Wien
FH Technikum Wien, Wien, Österreich.

Table of Contents I

Table of Contents II

Systemadministration



Geschichte

- (digitale) Hausmeierei
- existiert seit es Infrastruktur gibt
- „Sysops kümmern sich um Computer“
- tatsächliches Berufsbild viel komplizierter
- Studienfach *theoretisch Systemadministration*

Typische Tätigkeiten

- Integration neuer Technologien in bestehende Infrastruktur
- Sicherstellung von Betrieb von Systemen und Software
- Wartungen/Upgrades/Migrationen
- Verwaltungsaufgaben (Konten, Resourcen, Betriebsmittel)
- Sicherheitsaufgaben
- (technische) Dokumentation
- Unterstützung von Anwendern/Entwicklern
- Datensicherung/-wiederherstellung
- Performance Verbesserungen
- . . .

Verhältnis zur Sicherheit

- betreute Systeme sind meist exponiert
  - Netzwerke
  - Interaktion mit anderen Systemen
  - Benutzereingaben
- Systemadministration trifft Sicherheitsprobleme zuerst
- Systemadministration muß Schaden
  - verringern oder
  - abwenden

Table of Contents I

Table of Contents II

Bedrohungen

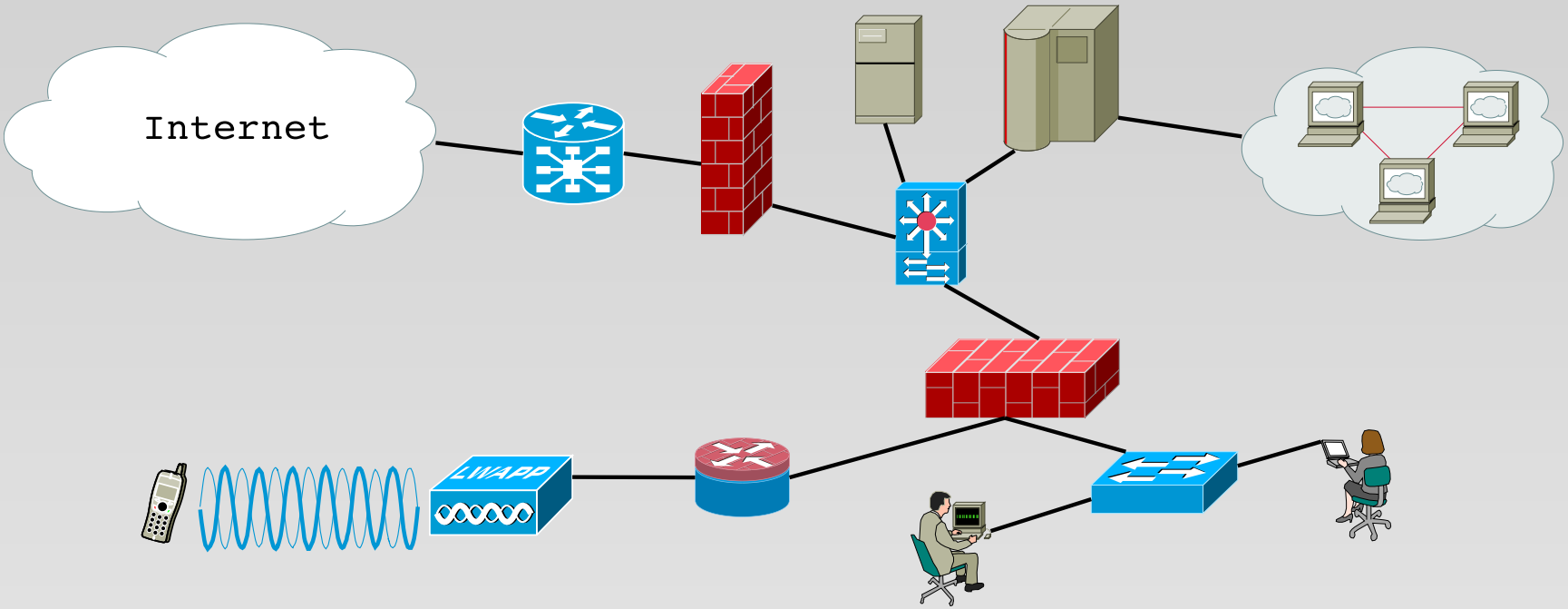
Digitale Nachbarschaft

- “normale” Menschen (sprich “Privatpersonen”)
- Firmen, Industriebetriebe
- Regierungen, Behörden, Militär, Polizei
- Kriminelle (“Cybercrime”)
- technische Begabte (Hacker, Hacktivists, H4x0rS/Script Kiddies)
- Organisationen (beliebiger Art)
- Geräte (ebenso beliebiger Art, “Internet der Dinge”)

IT Security 101

- Snowden Affäre hat nichts verändert
  $\longrightarrow$ endlich öffentliche Quellen zu Vermutungen
- Grundprinzipien bleiben aufrecht
  - *Principle of Least Privilege* / *Prinzip der minimalen Rechte*
  - *Compartmentalisation* / *Abschottung*
  - *CIA* $=$ *Confidentiality*, *Integrity*, *Availability*
- Systemadministration hat/pflegt Werkzeuge dafür

Werkzeuge



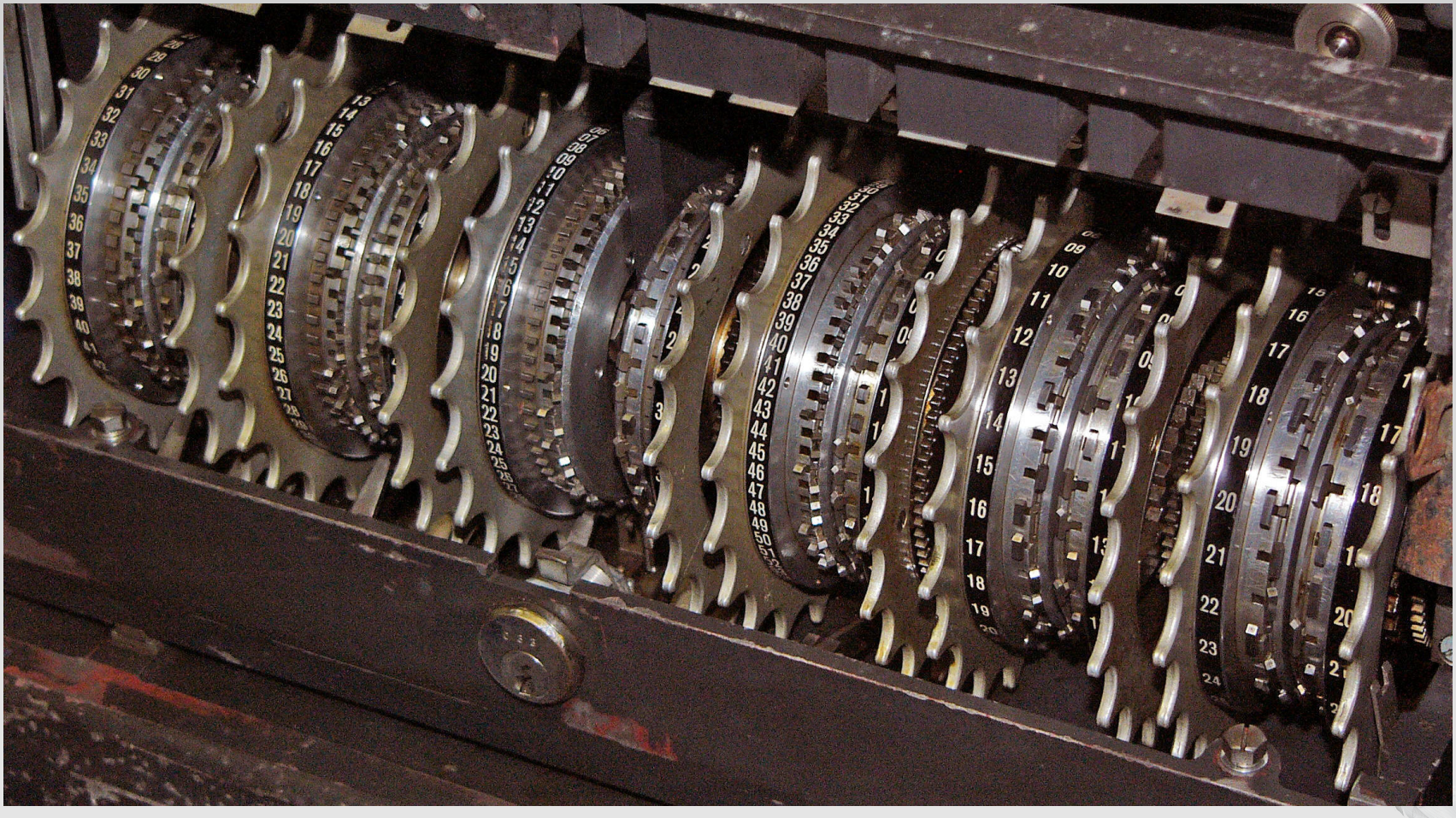
Werkzeuge (2)

- Automatisierung!
  Scripting ist tägliches Brot in Systemadministration
- Ablaufdaten
  Alles, was abläuft, wird periodisch erneuert
- Versionierungssysteme
  Subversion, Mercurial, git, Darcs, . . .
- (zentrales) Logging
  Fehler zeichnen sich ab, wenn sich Logs aufzeichnen

Table of Contents I

Table of Contents II

Kryptographie



Motivation – Warum?

- Kryptographie ist wichtige Sicherheitskomponente
- Klartext ist so 2000 . . . aber **weit vor Christus!**
  (∃ altägyptische Kryptographie des Alten Reiches)
- Klartext ist fahrlässig (schon **sehr** lange!)
- Verschlüsselung macht neugierig (seit über 1200 Jahren)
- Muß `root` Algorithmen und Methoden verstehen?

Was man wissen muß – light version

- Kryptographie $\subset$ mathematische Forschung
- $\frac{n_{\text{Publikationen}}}{t} \gg \frac{n_{\text{lesbare Artikel}}}{t}$
- $\exists$ Standards für Implementationen in Praxis
  $\longrightarrow$ Abkürzung für Auswahl
  $\longrightarrow$ (leichte) Garantie für Kryptanalyse/Tests
- Fokus standardisierte Algorithmen und Auswahlprozesse

NSAs und RSAs Angriff auf TLS

- Dual EC PRNG + TLS = DualECTLS
- Dual EC PRNG vorhanden in
  - RSA BSAFE Share for C/C++
  - RSA BSAFE Share for Java
  - Microsoft® Secure Channel (SChannel; verwendet von IIS)
  - OpenSSL FIPS Object Module
- Studie fand Dual EC Attacken auf TLS Transmissionen möglich
- RSA BSAFE Library hat *TLS Extended Random Modus*
  - auf Bitte von NSA eingefügt (2008)
  - Modus beschleunigt Attacken um Faktor $\approx$ 65000
  - leise deaktiviert von RSA Monate nach Snowden Leaks
- *klare* Anzeichen für gezielte Attacke auf TLS

Standards und Alternativen

- Advanced Encryption Standard – NIST, USA
  Gewinner Rijndael-Algorithmus
- *(NIST muß mit der NSA zusammenarbeiten)*
- CRYPTREC (Cryptography Research and Evaluation Committees) – Japan
- NESSIE (New European Schemes for Signatures, Integrity and Encryption) – EU
- ECRYPT (European Network of Excellence in Cryptology) – EU
- Unbedingt beachten:
  - *Keine Algorithmen verwenden, die nicht untersucht wurden!*
  - *Keine Algorithmen selbst entwickeln!*
  - *Algorithmen testen!*
    $f_{decrypt}(cipher) = f'_{decrypt}(cipher)$

Zufall und Schlüssel

- Schlüssel müssen zufällig erzeugt werden
  - symmetrische Schlüssel ≥ 128 Bit
  - asymmetrische Schlüssel ≥ 2048 Bit (RSA)

  (Länge abhängig von Einsatzdauer)
- kryptographisch geeignete Zufallsquelle notwendig
  - Fortuna/Yarrow (FreeBSD)
  - `/dev/urandom` (Linux)
  - `CryptGenRandom()` (Win32 API)
- (proprietäre) Hardwarezufallsgeneratoren vermeiden
  - Broadcom BCM2835
  - Intel® RDRAND
  - VIA Padlock

Algorithmen

- Analyse von Algorithmen sehr schwer
- „verwendbar“
  - AES, ~~Blowfish~~, Twofish, Camellia, Serpent
  - SHA-2 Familie (SHA256, SHA384, SHA512, . . .), RIPEMD Familie, Tiger, Whirlpool
  - SHA-3 (Keccak)
- Nicht verwenden!
  - Digital Signature Algorithm (DSA) in jeder Form
  - RC4 (gute Attacke 2013 publiziert)
  - DES (!)
  - 3DES (mit Key Option 2 & 3, und generell)
  - Hashalgorithmen MD5, SHA1, ~~NIST Version von SHA-3~~

Betriebsarten von Blockchiffren

- Blockchiffren lassen sich in Stromchiffren umwandeln
  - Cipher Block Chaining Mode (CBC Mode) sehr verbreitet
  - CBC in TLS v1.0 angreifbar (BEAST Attacke)
    behoben in TLS v1.1 und höher
- gute Alternativen sind
  - Counter Mode (CTR) – leicht(er) verfügbar
  - Galois/Counter Mode (GCM) – mit Vorbehalt
- *Randnotiz:* Attacken erforden (oft) hohe Bandbreite

Perfect Forward Secrecy (PFS/FS)

- Langzeitschlüssel $\longrightarrow$ Session Key für Transmission
- Idee: Session Key nicht kompromittiert, wenn Langzeitschlüssel kompromittiert
- Generierung Session Key erfordert **gute** Zufallszahlen!
- Perfect Forward Secrecy wird unterstützt von
  - IPsec (optional)
  - OpenSSL & GnuTLS
  - OpenVPN™ (nur mit SSL/TLS Authentication!)
  - OTR
  - SSH
- Enigma kannte Session Keys, moderne ISPs und Start-Ups anscheinend nicht!

PFS mit OpenSSL konfigurieren

Für nginx:

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_ciphers „EECDH+AESGCM EECDH+aRSA+AESGCM EECDH+SHA384 EECDH+SHA256
EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA RC4
!aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS“ ;
```

Für Apache (siehe auch Security/Server Side TLS):

```
SSLProtocol all -SSLv2 -SSLv3
SSLHonorCipherOrder on
SSLCipherSuite „EECDH+AESGCM EECDH+aRSA+AESGCM EECDH+SHA384
EECDH+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH
EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS“
```

Für mehr siehe Applied Crypto Hardening Projekt.

Wo und wie verschlüsseln?

- Data at Rest (DaR)
  - gespeicherte Daten
  - archivierte Daten
  - ausgedruckte Daten
- Data in Motion (DiM)
  - Daten auf dem Weg von A nach B
  - Netzwerktransmissionen
  - bewegte Datenträger
- Data in Use (DiU)
  - Daten am Endpunkt (Start oder Ziel)
  - Arbeitsstation, Endgerät, Server

DaR Beispiel: Diskverschlüsselung

- GNU/Linux
  - Linux Unified Key Setup (LUKS)
  - TrueCrypt / CipherShed
- Apple
  - ~~FileVault~~ / FileVault 2
  - VeraCrypt
- Microsoft® Windows
  - BitLocker
  - TrueCrypt / CipherShed
  - proprietäre Lösungen

DiM Beispiele

- HTTPS mit `curl`, `wget`
- `ncat` (aus `nmap`)
- OpenSSH mitsamt Tunneln (TCP, SOCKS5) & SFTP
- VPN Technologien
  - IPsec
  - OpenVPN™
  - L2TP
- Stunnel
- GnuPG & 7z für Verpackungen

Table of Contents I

Table of Contents II

Zusammenfassung

- Systemadministratoren müssen die „Innereien“ von Appplikationen kennen
- Periodische Updates auch für Krypto-Wissen notwendig
  $\longrightarrow$ Hausaufgabe: Vergleich elliptische Kurven mit RSA Algorithmen
- Kryptographie ist ein Teil des Ganzen
  - kein Schutz vor Einbrüchen
  - kein Allheilmittel
  - Schlüssel kann man stehlen/kopieren
- Kryptographie ist Standard!
- Klartext ist fahrlässiger denn je!

Table of Contents I

Table of Contents II

Über die Crowes Agency OG

Die Crowes Agency OG ist eine Gruppe von Experten aus verschiedenen Feldern. Wir bieten unsere Erfahrungen im Rahmen von großen und kleinen Projekten an. Der Fokus liegt auf den Gebieten Grafikdesign, Software-Entwicklung, öffentlichen Erscheinungen (wie beispielsweise Webseiten und Kommunikation mit der „Außenwelt“), Systemadministration, IT Sicherheit und Unternehmensberatung. Die Crowes Agency stellt aus ihrem Pool von Mitarbeitern Teams für die Lösung von Kundenproblemen zusammen.

Kontakt Crowes Agency OG

- http://www.crowes.eu/
- Kontaktinformation des Autors
  - rene@crowes.eu
  - PGP/GPG 0x28CAC51F8C413583
  - +43.676.5626390 (RedPhone & TextSecure verfügbar)
  - +43.680.2477579 (unverschlüsselte Sprache & TextSecure verfügbar)
  - Threema ID 76WHDZTR
- E-Mail allgemeine Anfragen enquiry@crowes.eu