Security Skills for Sysadmins (II)

Wieviel Kryptografie muß im root Hirn stecken?

René 'Lynx' Pfeiffer

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

Linuxwochen Wien
FH Technikum Wien, Wien, Österreich.

Table of Contents I

Table of Contents II

1 Systemadministration

2 Operations Security (OpSec)

3 Werkzeuge

4 Zusammenfassung

5 Fragen?

6 Über die Crowes Agency OG

Systemadministration

Geschichte (verkürzt)

- letztes Jahr gab es schon einen solchen Vortrag. . .
- . . .daher dieses Jahr Fokus auf wichtige Grundlagen.
- „Sysops kümmern sich um Computer“
- tatsächliches Berufsbild viel komplizierter
- Studienfach *Theoretische 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
- Kommunizieren (neuer Punkt)
- . . .

Verhältnis zur Sicherheit

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

Primärziel

INSIDE THE NSA'S SECRET EFFORTS TO HUNT AND HACK SYSTEM ADMINISTRATORS


Ryan Gallagher, Peter Maass

Mar. 21 2014, 12:07 a.m.

„Ich habe nichts zu verbergen.“ ist Kündigungsgrund für Sysadmins!

Table of Contents I

Table of Contents II

1 Systemadministration

2 Operations Security (OpSec)

3 Werkzeuge

4 Zusammenfassung

5 Fragen?

6 Über die Crowes Agency OG

Operations Security (OpSec)

Operations Security? (OpSec?)

- Ursprung (US) Militär
- Durchführung in mehreren Phasen
  1. Identifizieren eigener Aktionen, die Feind beobachten kann
  2. Identifizieren kritischer Informationen, die Feind nutzen kann
  3. Analyse der Bedrohungen
  4. Analyse der Schwachpunkte
  5. Einschätzung der Risiken
  6. Setzen von Maßnahmen zum Schutz Tätigkeiten oder Daten
- keine Hexerei
- gesunder Menschenverstand, Disziplin notwendig

Intelligence - SIGINT, HUMINT

- Signals Intelligence (SIGINT)
  - Communications Intelligence (COMINT) - zwischen Menschen
  - Electronic Intelligence (ELINT) - zwischen Maschinen
- Human Intelligence (HUMINT)
  NATO Definition: *a category of intelligence derived from information collected and provided by human sources*
- HUMINT > SIGINT

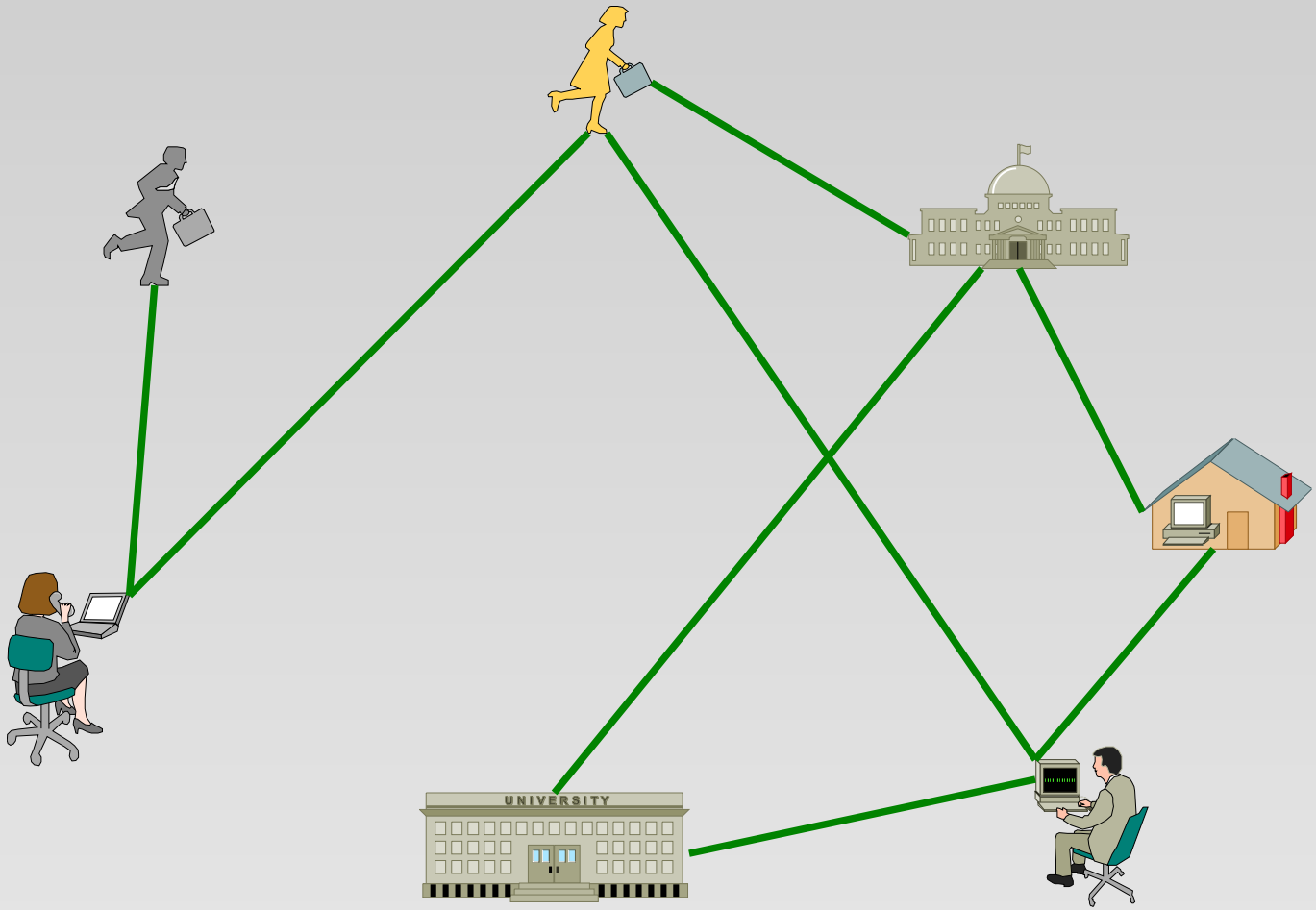
Bühne - Worum geht es?

- Kommunikationsverhalten
  - direkte Interaktion (sprich Treffen und Sprechen)
  - Telefonie
  - (Instant) Messaging
- Datenverhalten
  - Was wird wo wie gespeichert?
  - Was wird (je) wie genau gelöscht?
  - Wer liest wo welche Daten?
- Metadatenverhalten
  - das tückische „Drumherum“
  - kein Tag vergeht ohne Datenspuren

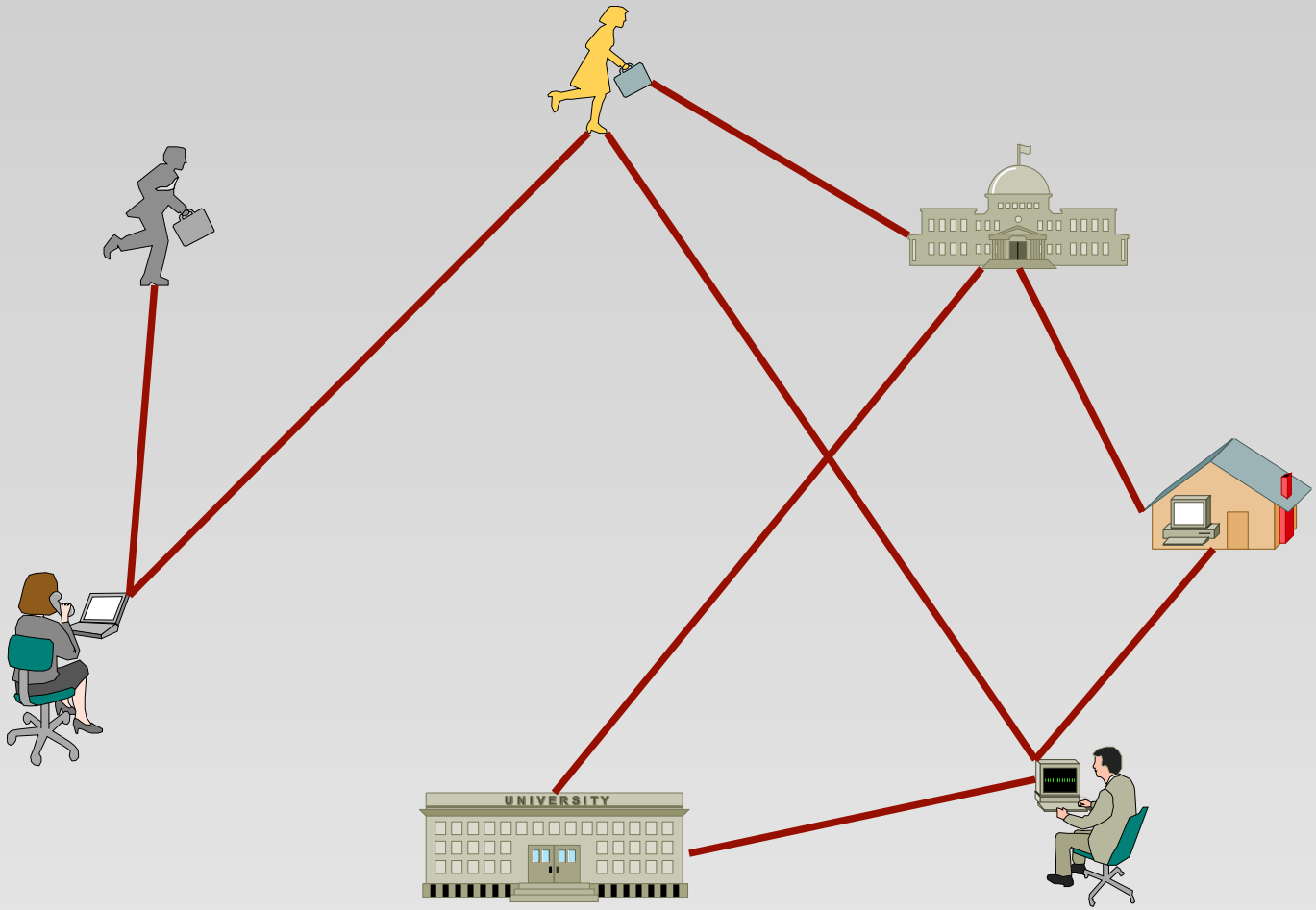
Crypto Folklore - Lustiger Algorithmenstadl

- Verschlüsselung / Crypto ist Heiliger Gral™
- Wirkung vorhanden, da FBI verzweifelt
- Nebenwirkungen ebenso vorhanden
  - wohliges Gefühl, verringerte Aufmerksamkeit
  - Selbstüberschätzung
  - Panzertür an Holzhaus, Bartschlüssel in Brieftasche
- Applikationen und Sysadmins schlecht vorbereitet
- Metadaten werden völlig vergessen - siehe HUMINT

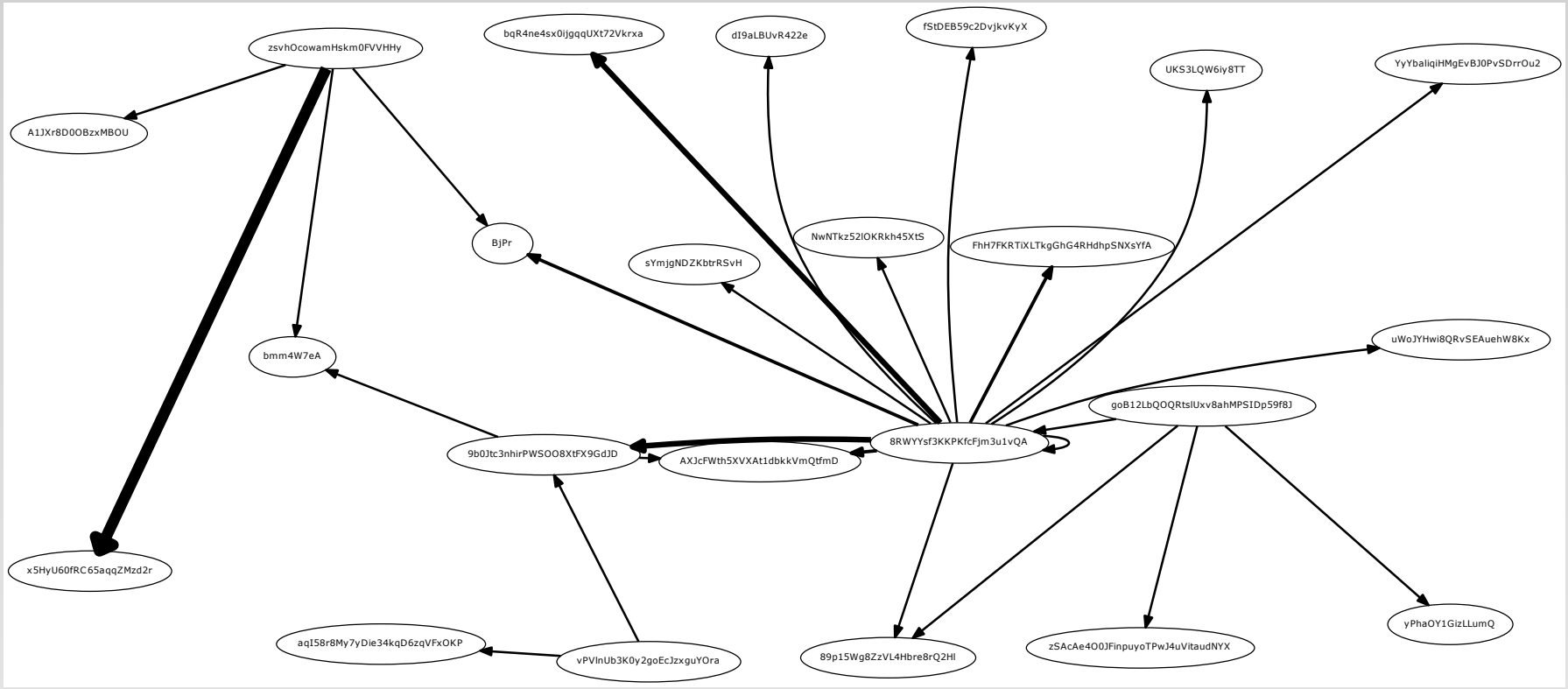
Plaintext Apocalypse Now



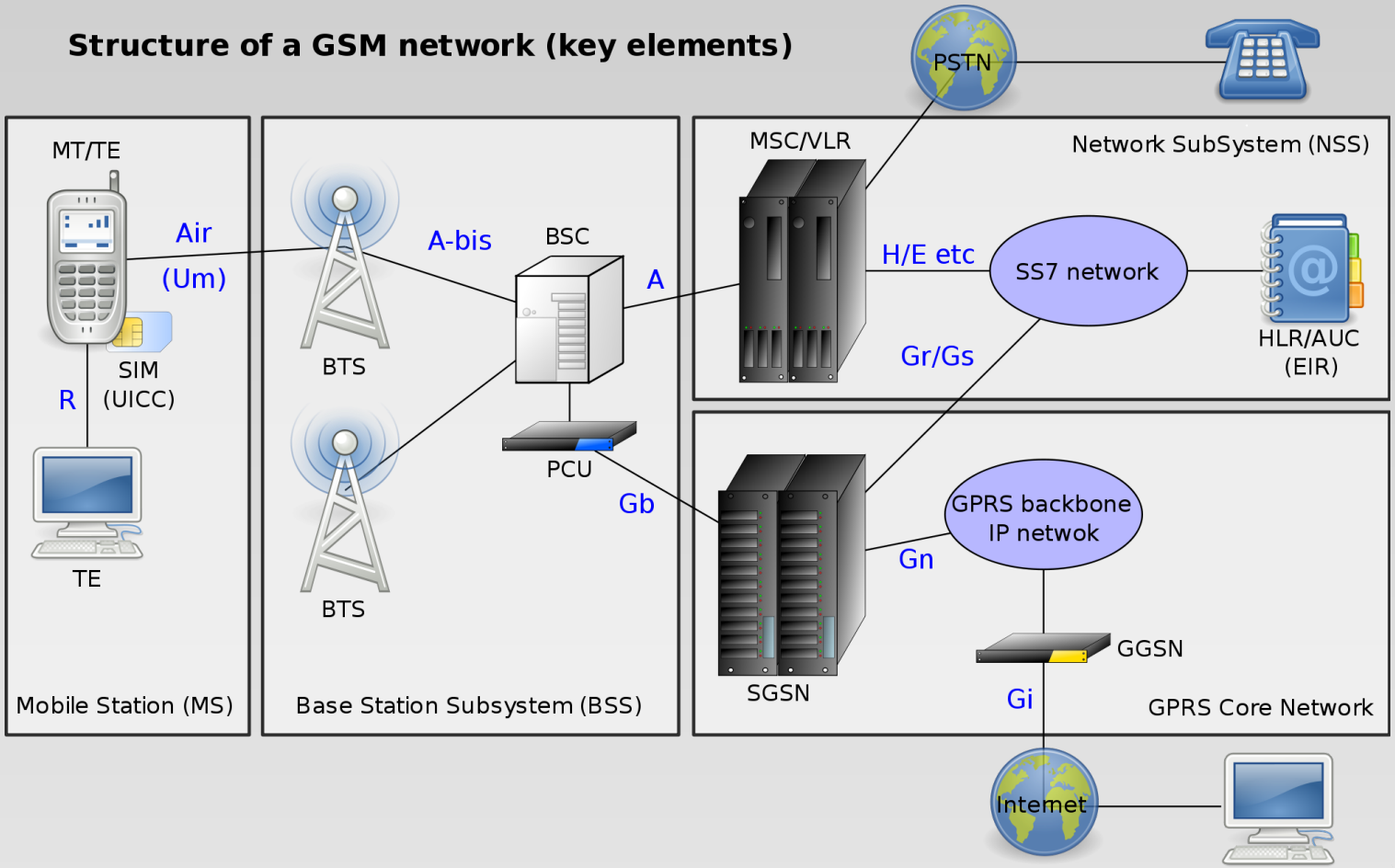
Metadata Apocalypse Now



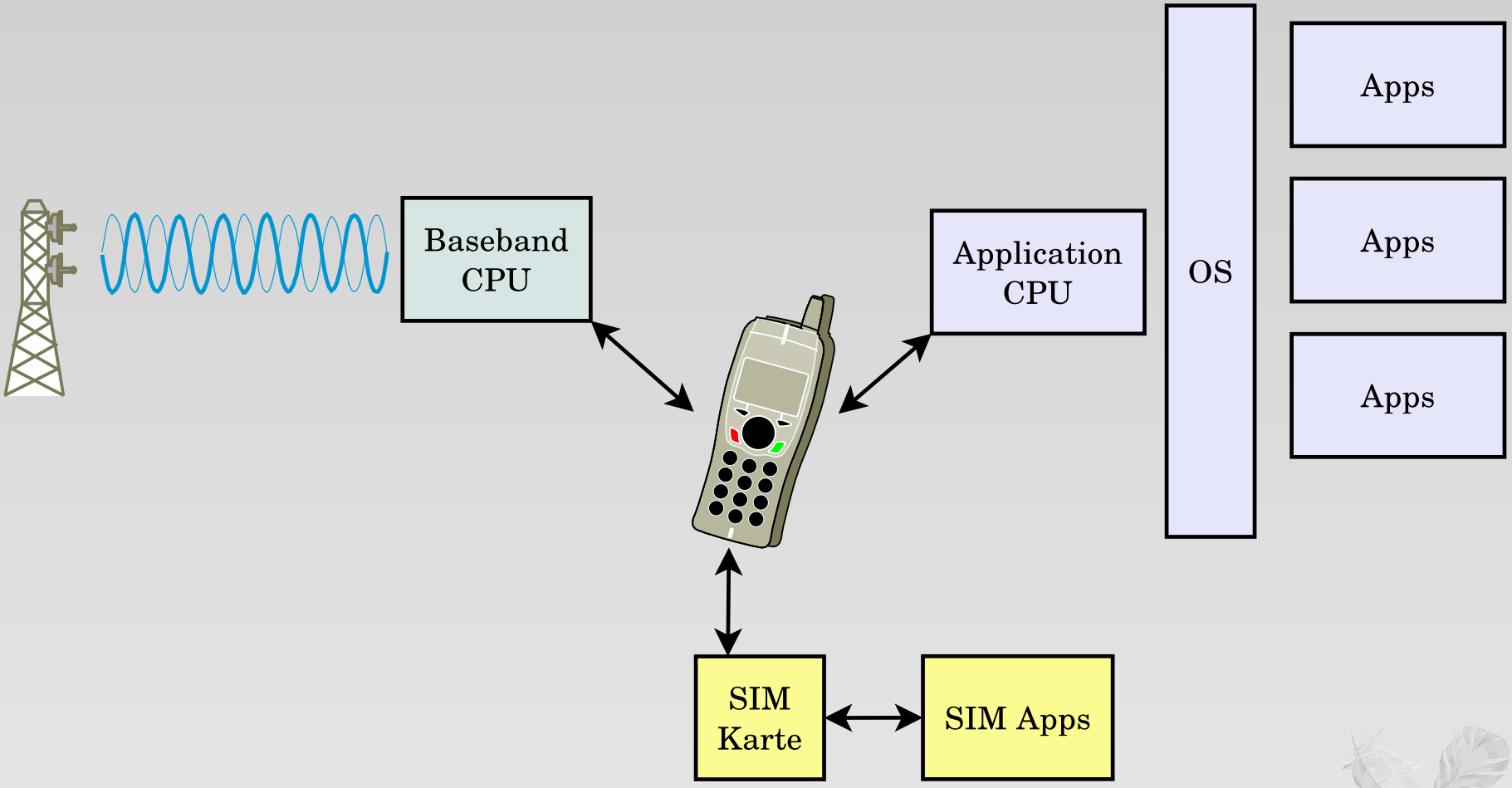
Kommunikationsverhalten



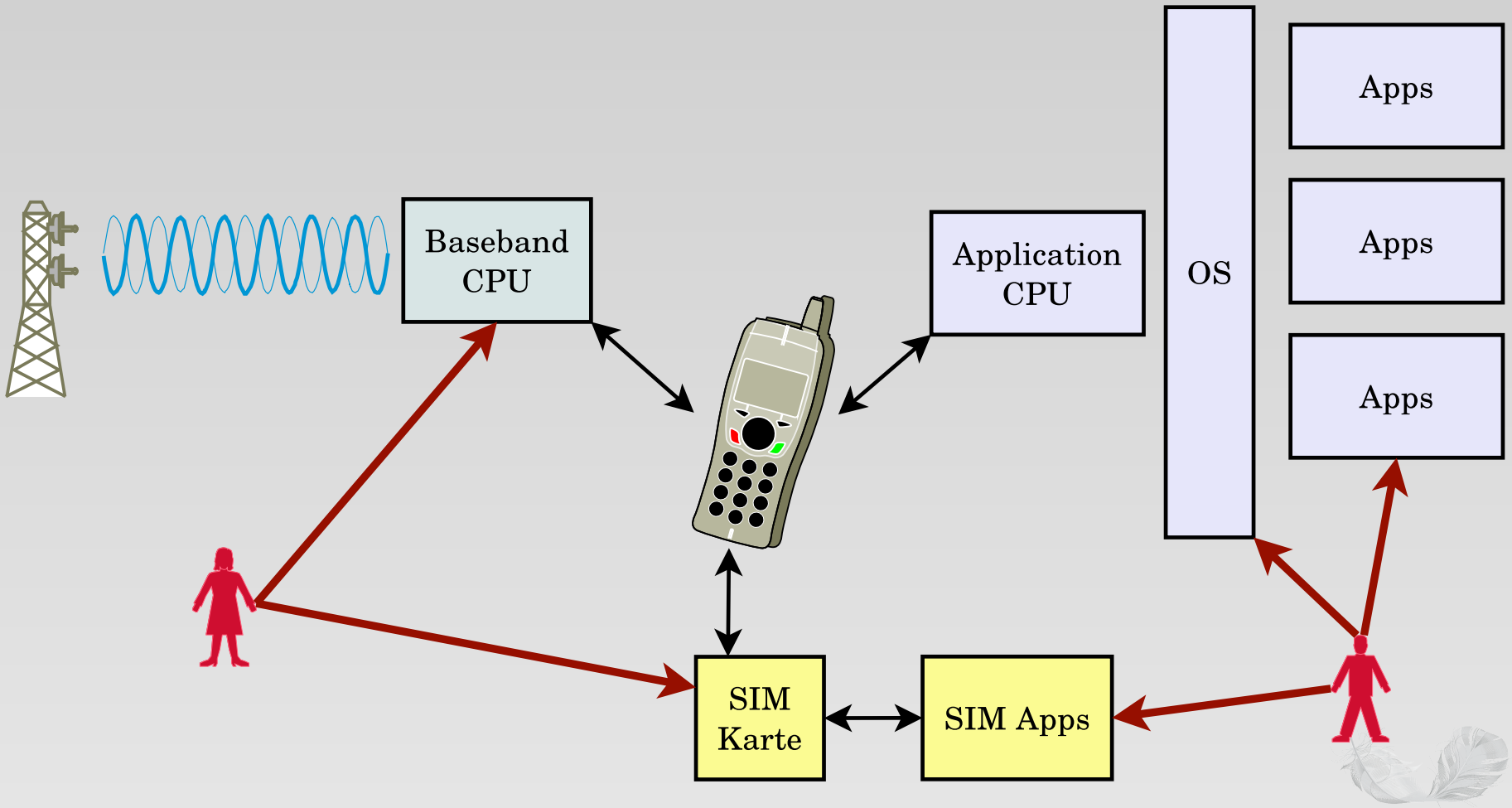
Mobilfunkgesellschaft



Smartphonegesellschaft (1)



Smartphonegesellschaft (2)



Vertrauensverhältnisse

- Identität wird nicht hinterfragt
- Kontaktdaten sind zu überprüfen
  - `george.w.bush@mailinator.com`
  - `rpfeiffer@gmy.net`
  - `+43.1.123456789-0`
  - `4WFYBWCJ`
  - `7A1C 9988 909E E1DD B673 B799 28CA C51F 8C41 3583`
- *„Kenne ich vom Sehen.“* gilt nicht!
- Social Media gilt auch nicht!

Table of Contents I

Table of Contents II

1 Systemadministration

2 Operations Security (OpSec)

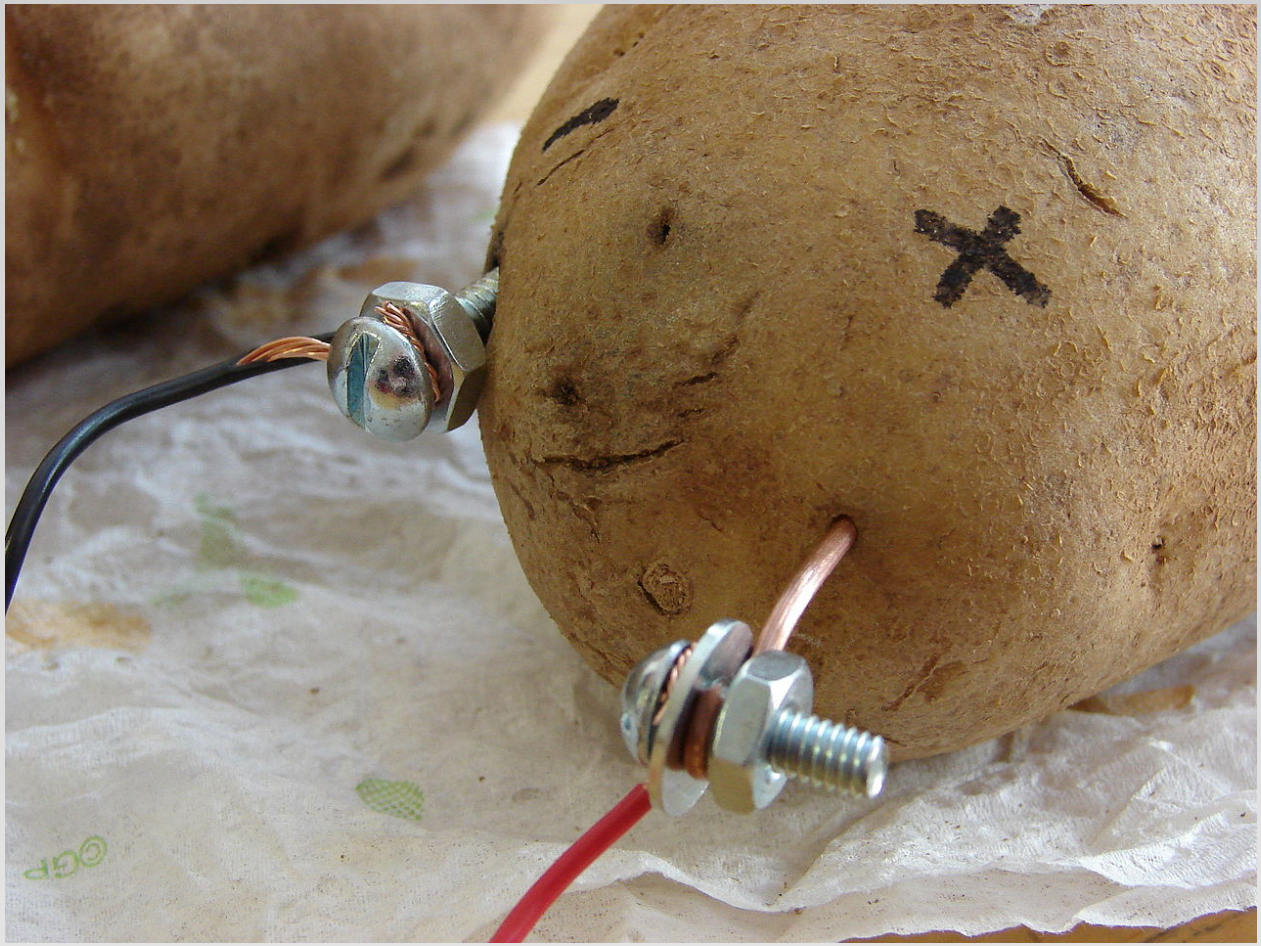
3 Werkzeuge

4 Zusammenfassung

5 Fragen?

6 Über die Crowes Agency OG

Werkzeuge



Wichtigstes Werkzeug überhaupt

Warum?

- *The quieter you become, the more you are able to hear.*
- beste HUMINT Gegenmaßnahme
- Funkdisziplin! - im Falle von SIGINT
- erster Schritt zur Metadatenreduktion
- *kein* Fallback auf unsichere Methoden!
- gilt *speziell* für gewohnte Umgebungen
  - LAN
  - Kaffeehaus
  - öffentlicher Verkehr
  - Straßen und Plätze
  - . . .

Digitale Kontamination

- Daten hinterlassen lesbare Spuren
  - beschriebene Datenträger
  - „Reste“ im Arbeitsspeicher
- Daten kontaminieren Umgebung
  - ☣ & ☢ sind gute Analogien
  - Datenträger *immer* reinigen oder vernichten
- Daten werden transportiert
  - ☣ Ansteckung, Epidemie
  - ☢ „Fallout“, Leck im Kühlsystem
  - Umgebung wird verunreinigt

BTW: Kontamination gilt auch für Vertrauensverhältnisse

Cryptofolklore in Wissen umwandeln

- Kenntnis Konfiguration *aller* verwendeten Applikationen in Bezug
  - zu Verschlüsselung und
  - zu Authentisierung und
  - zu Integrität
- Crypto 101
  - Algorithmen, Betriebsarten
  - Schlüsselverwaltung
  - X.509 - Zertifikate, Schlüssel, CSR, Annullierung
  - Public Key Infrastructure (PKI)
- Funktionsweise Kommunikationsprotokolle

Werkzeuge - Kommunikation

- Signal für Nachrichten und Telefonie
- GnuPG für Nachrichten (und Dateien)
- S/MIME-fähige Software für Nachrichten
- Instant Messenger mit Off-the-Record Messaging (OTR) Support
  - Adium (OS X)
  - ChatSecure & Orbot
  - Pidgin
  - SilentPhone/SilentText
  - Tor Messenger (noch β)
- Tor - minimiert Metadaten auf TCP/IP Basis
- Tor Hidden Services

Werkzeuge - Arbeitsumgebungen

- Virtualisierte Systeme - trennen, trennen, trennen, . . .
- gehärtete Systeme/Distributionen/Applikationen
- GNU/Linux Qubes OS
- SELinux
- Linux Grsecurity Patch
- Speichermedienverschlüsselung
  - `cryptsetup` (dm-crypt, loop-AES, TrueCrypt/VeryCrypt)
  - Archive (`7z`, `lrzip`, . . .)

Werkzeuge - Datentransport

- IPSec (in IPv6 enthalten)
- OpenSSH
  - Tunnel für TCP
  - Schlüsseltausch problematisch
- OpenVPN
  - Transport via TCP, UDP, HTTP(S)
  - möglichst X.509 verwenden (Perfect Forward Secrecy)
- Webserver mit TLS Unterstützung
  - TLS Konfiguration gut verstehen!
  - siehe Applied Crypto Hardening

Table of Contents I

Table of Contents II

1 Systemadministration

2 Operations Security (OpSec)

3 Werkzeuge

4 Zusammenfassung

5 Fragen?

6 Über die Crowes Agency OG

Zusammenfassung

- Systemadministratoren müssen ihre Gewohnheiten überdenken
- Periodische Updates für eigenes Wissen notwendig
- Kryptographie ist ein Teil des Ganzen
  - kein Schutz vor Einbrüchen
  - kein Allheilmittel
  - Schlüssel kann man stehlen/kopieren
- eigenes Verhalten bestimmt die Sicherheit
- Lieber 2 Tools verstehen als 10 Tools falsch anwenden!
- Mobile und „smarte“ Devices gleich wieder vergessen.

Table of Contents I

Table of Contents II

1 Systemadministration

2 Operations Security (OpSec)

3 Werkzeuge

4 Zusammenfassung

5 Fragen?

6 Über die Crowes Agency OG

Fragen?


egid:0/0, parent /usr/
rnel: [466.100239] PAX: execution
rnel: [466.100243] PAX: terminating task: /usr/
rnel: [466.100245] PAX: bytes at PC: c3 00 00 00 00 00 00 00 0000000000400c90 0000000000400c58
rnel: [466.100256] PAX: bytes at SP-8: 0000000000400c90 0000000100000000
038a81700870 000003da23831c38 000003da23831c38
ernel: [466.100265] grsec: bruteforce prevention initiated for the next 30 minutes or until service
he crash report for /usr/lib/paxtest/execheap[execheap:4190] uid/euid:0/0 gid/egid:0/0, parent /usr/lib/paxtest
kernel: [466.100276] grsec: more alerts, logging disabled for 10 seconds
kernel: [466.100914] PAX: execution attempt in: <stack>, 39f1b2b8000-39f1b2da000 3fffffdd000
kernel: [466.100916] PAX: terminating task: /usr/lib/paxtest/execstack(execstack):4193, uid/euid: 0/0, PC: 00
kernel: [466.100918] PAX: bytes at PC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
kernel: [466.100927] PAX: bytes at SP-8: 0000000000000000 0000000000400b79 0000000000000000
0000000000000 0000000000000000 0000000000000000
kernel: [466.101767] PAX: execution attempt in: /usr/lib/paxtest/shlibtest2.so, 3810d9a5000-3810d9a7000
kernel: [466.101770] PAX: terminating task: /usr/lib/paxtest/shlibbss(shlibbss):4196, uid/euid: 0/0, PC:
kernel: [466.101771] PAX: bytes at PC: c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
kernel: [466.101780] PAX: bytes at SP-8: 000003810ddc7538 0000000000400eef 0000000000400c9a
0000000000400c67 000003ca56a0e5e0 000003810cf62700 0000000000000000
ey kernel: [466.102654] PAX: execution attempt in: /usr/lib/paxtest/shlibtest2.so, 31f4606e000-31f46070000
ey kernel: [466.102658] PAX: terminating task: /usr/lib/paxtest/shlibdata(shlibdata):4199, uid/euid: 0/0, PC:
rey kernel: [466.102660] PAX: bytes at PC: c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
rey kernel: [466.102669] PAX: bytes at SP-8: 0000031f46490538 0000000000400eef 0000000000400c9a
0000000000400c67 000003844224a720 0000031f455f5700 0000000000000000
rey kernel: [466.103783] PAX: execution attempt in: <anonymous mapping>, 3a7da6f0000-3a7da6f1000
rey kernel: [466.103787] PAX: terminating task: /usr/lib/paxtest/mprotanon(mprotanon):4202, uid/euid: 0/0,
466.103790] PAX: bytes at PC: c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PAX: bytes at SP-8: 0000000000400a6a 0000000000400c70 0000000000000000
0000000100000000
/usr/lib/paxtest/mprotbss, 00601000-00602000
/mprotbss(mprotbss):4205, uid/euid: 0/0,

Table of Contents I

Table of Contents II

1 Systemadministration

2 Operations Security (OpSec)

3 Werkzeuge

4 Zusammenfassung

5 Fragen?

6 Über die Crowes Agency OG

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

- ℹ`http://www.crowes.eu/`
- Kontaktinformation des Autors
  - ✉`rene@crowes.eu`
  - PGP/GPG `0x28CAC51F8C413583`
  - +43.676.5626390 (RedPhone & TextSecure verfügbar)
  - +43.677.61356623 (unverschlüsselte Sprache & TextSecure verfügbar)
  - Threema ID `4WFYBWCJ`
- E-Mail allgemeine Anfragen ✉`enquiry@crowes.eu`