

Operations Security (OPSEC)

Minimierung von Metadaten und Spuren

B9d3LMPmsn8lq F5FK907Rj62iA

HnsYy7EsHuITKZTIOT3

 <http://zqkctlwi4fecvo6ri.onion/>,  noone@example.net

Überall und immer
Universum.

Table of Contents I

Table of Contents II

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 (schwarze) Magie, Praxis seit Jahrhunderten
- 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?

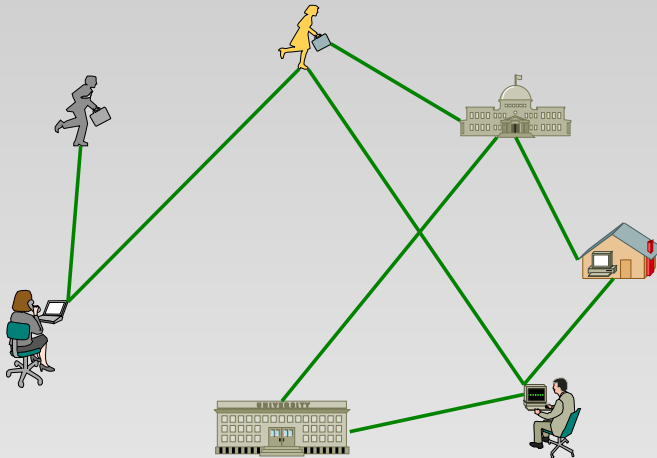
■ Metadatenverhalten

- das tückische „Drumherum“
- kein Tag vergeht ohne Datenspuren

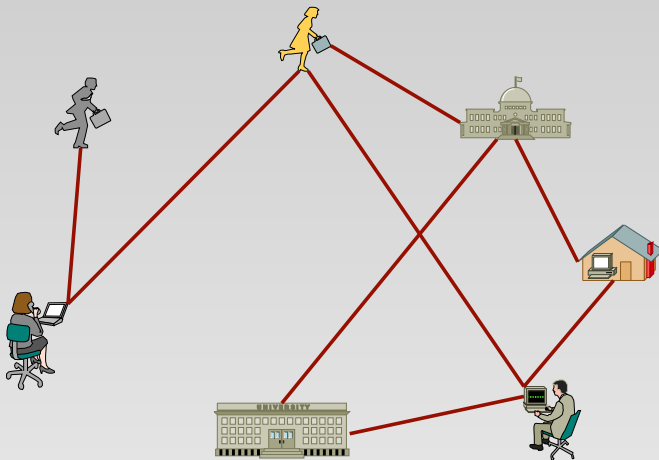
Crypto Folklore - Lustiger Algorithmenstadl

- Verschlüsselung / Crypto ist Heiliger Gral™
- Wirkung vorhanden, da *three letter agencies* verzweifeln
- Nebenwirkungen ebenso vorhanden
 - wohliges Gefühl, verringerte Aufmerksamkeit
 - Selbstüberschätzung
 - Panzertür an Holzhaus, Bartschlüssel in Brieftasche
- Applikationen, Expertinnen und Benutzer schlecht vorbereitet
- Metadaten werden völlig vergessen - siehe HUMINT

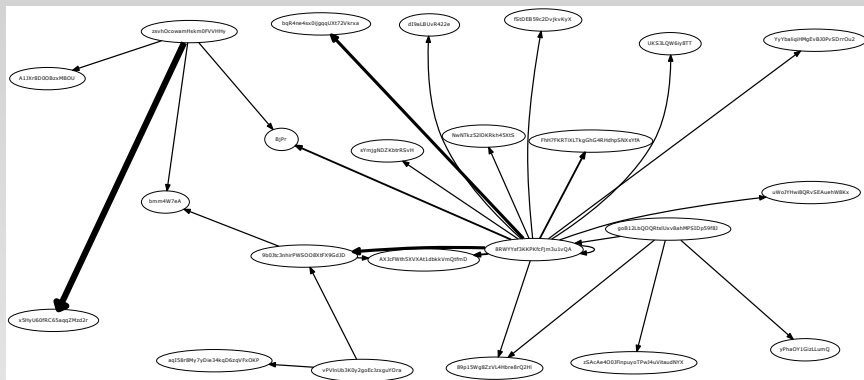
Plaintext Apocalypse Now



Metadata Apocalypse Now

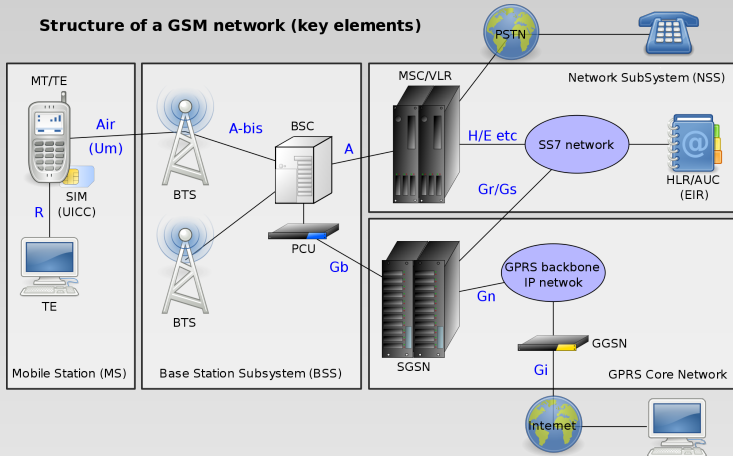


Kommunikationsverhalten

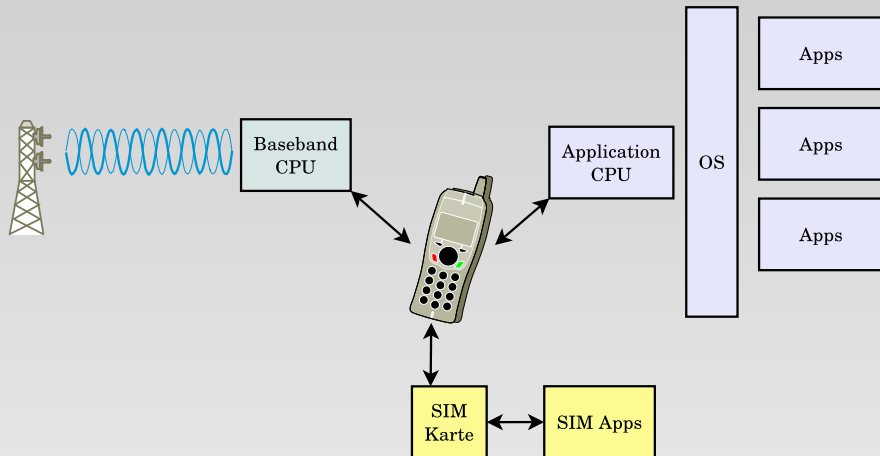


Mobilfunkgesellschaft

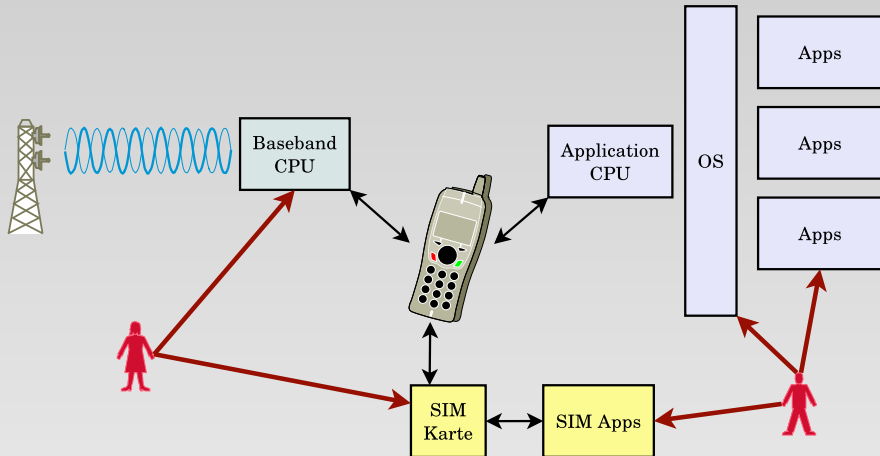
Structure of a GSM network (key elements)



Smartphonegesellschaft (1)



Smartphonegesellschaft (2)



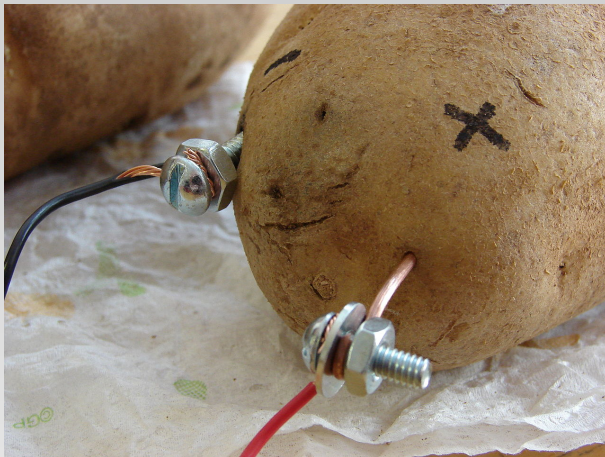
Vertrauensverhältnisse

- Identität wird nicht hinterfragt
- Kontaktdaten sind zu überprüfen
 - `george.w.bush@mailinator.com`
 - `ddrumpf@gmy.net`
 - `+43.1.123456789-0`
 - `5PATSDGM`
 - `02B9 1BA0 D4E6 4C27 E509 D220 BA4E C820`
`5238 E480`
- „*Kenne ich vom Sehen.*“ gilt nicht!
- Social Media gilt auch nicht!

Table of Contents I

Table of Contents II

Werkzeuge



Geheimnisse / Schützenswertes

Rule #4: The best way to keep a secret? Keep it to yourself. Second best? Tell one other person - if you must. There is no third best.

– A L. J. G

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, VeraCrypt)
 - Archive (7z, lrzip, ...)

Werkzeuge - Datentransport

- IPsec (in IPv6 enthalten, weil vorgeschrieben)
- 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

Zusammenfassung

- Jede(r) muß seine 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 letztlich 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

Fragen?

[illegible]