Cloud Surveillance

Die ersten Überwacher Sozialer Netze waren deren Betreiber. Dann kamen „rogue attacks“ durch Kriminelle und Geheimdienste. Nun werden deren Methoden - „Man in the Middle Attacks“ - für Strafverfolger standardisiert.

erich@moechel.com Joanneum Research , Graz 2013 01 28

USP: Totale Überwachung

- Soziale Netze als erste WWW-basierte Dienste mit integrierter Totalüberwachung als USP
- Aus Rohdaten extrahierte, angereicherte und verknüpfte Daten => Profil
- Facebook & Co haben weit mehr und ganz andere Daten über die User, als diese glauben
- Angriffe: Erst Kriminelle, dann Staaten
- Deep Packet Inspection, Firewalls und Trojaner im Arabischen Frühling. Twitter et al. =>HTTPS

Angriff auf Verschlüsselung

- 2009 11, erste Diskussionen in ETSI 3GPP SA3 LI über Vorschläge von ZTE [China]
- 2010 10 Das GCHQ über die "britische Perspektive" beim Angriff auf Verschlüsselung
- GCHQ: "To retrospectively decrypt communications the Man-in-the-Middle-Attack must have been performed on all subscribers."
- UK setzt auf temporäres "key escrow" = Hinterlegung von Schlüsselderivat

Wenn sich Methoden schlagen

- ETSI präferiert Methode MIKEY-IBAKE aus rechtlichen Gründen. Gemeinsamkeiten:
- Manipulation von Timestamps, Randomness
- Fälschung der Derivate von Zertifikaten durch Netzbetreiber, der mitspielen muss
- Beides sind Man-in-the-Middle-Attacks. Die verwendeten Methoden sind inkompatibel
- MIKEY SAKKE und IBAKE als IETF Standards

Und nun zu etwas Interessanterem als Folien

- Weiter gehts nämlich mit den neuesten technischen Dokumenten und den im ETSI beteiligten Personen

Die bösen Schlüsse

- Systematische, staatliche Angriffe auf HTTPs, SSL etc. wenigstens in USA , UK Routine
- "Man in the Middle" = Telekoms
- Integrität digitaler Zertifikate, HTTPs, SSL etc. sine qua non für E-Commerce und Informationsgesellschaft
- Ein Login via Smartphone kann die Sicherheit eines Firmennetzes kompromittieren

erich.moechel.com
/munications

F

Freundlichen Dank für Ihre Aufmerksamkeit
respektive Geduld
PGP Key 0xEA7DC174
http://moechel.com/kontakt.html

http://fm4.ORF.at/erichmoechel

erich@moechel.com Joanneum Research, Graz 2013 01 28