

Security Breakout (1)

- Scenario: Industry espionage by traffic analysis
 - Anonymity as countermeasure
 - Attacker models:
 - Public network: Anonymity-Overlay: ToR lacks performance and anonymity (not many relays)!
 - On server: Browser fingerprint blurring
 - On client: Anti-Malware... but: APT :-(
- Observations:
 - Attacker tries to be cost efficient
 - APT are expensive and should not be used exhaustively by an attacker
 - Better endpoints through secure programming languages? Also for OS, Driver, etc.

Security Breakout (2)

- Defense against Inside Attackers
 - Does anonymity make it worse?
 - Golden Key vs. Access Control
 - Hidden vs. open distrust
 - Some organizations are able to defend (e.g. gmail), is this generalizable? Are processes adaptable?
- Insider attacks through social engineering on the rise
 - Spear phishing, CEO fraud

Security Breakout (3)

- GDPR reveals difficulties of organizations to define and document classes of data and their processing
- Why not defining security policies based on these classes?
- Meaningless generality versus complex exceptions?
- Risk Management to the rescue?