SÉCURITÉ.ORG

IEEE VoIP MaSe

Top three challenges in VoIP security and management

Nicolas FISCHBACH
Senior Manager, Network Engineering Security, COLT Telecom
nico@securite.org - http://www.securite.org/nico/

COLT

COLT and VoIP

- COLT Telecom
  - Voice, Data and Managed Services, Tier 1 ISP in EU
  - 14 countries, 60 cities, 50k business customers
  - 20 000 km of fiber across Europe + DSL
- VoIP “experience”
  - 3 major vendors
    - One “we're coming from the TDM world”
    - One “we're coming from the IP world”
    - One “we're a VoIP company”
  - Internet and MPLS VPN-based VoIP services
  - Own network (fiber + DSL) and wDSL
  - Going PacketCore + NGN + IMS

Top 3 security challenges

- VoIP protocols
  - No, VoIP isn't just SIP
  - H.323 and MGCP rock the carrier world
- Security issues
  - VoIP dialects
  - FWs / SBCs: do they solve issues or introduce complexity ?
  - Are we creating backdoors into customer networks ?
  - CPS and QoS

Top 3 security challenges

- Online services
  - Call Management (operator console)
  - IN routing
  - Reporting / CDRs
- Security issues
  - Multi-tenant capabilities
  - Have the vendors ever heard of web application security ?
  - Who needs security or lawful intercept if a kid can route your traffic via SQL injection

Top 3 security challenges

- TDM / VoIP : two worlds, two realms, becoming one ?
  - Security by “obscurity” / complexity vs the IP world
  - Fraud detection
- Security issues
  - New attack surface for legacy TDM/PSTN networks
  - No security features in old Class5 equipment
  - No forensics capabilities, no mapping to physical line
  - Spoofing and forging
  - People: Voice Engineers vs Data Engineers vs Security engineers. Engineering vs Operations. Marketing vs Engineering.