Computer Hacking and Intrusion Detection

Alan S H Lam
Networking Technology Exchange Center (NTEC),
Information Engineering Department,
CUHK

OUTLINES

- Computer Hacking
  - Two real cases
  - Man-in-the Middle Attack
- Intrusion Detection
  - System and Network Monitoring
  - Network Intrusion Detection System (NIDS)

Computer Hacking

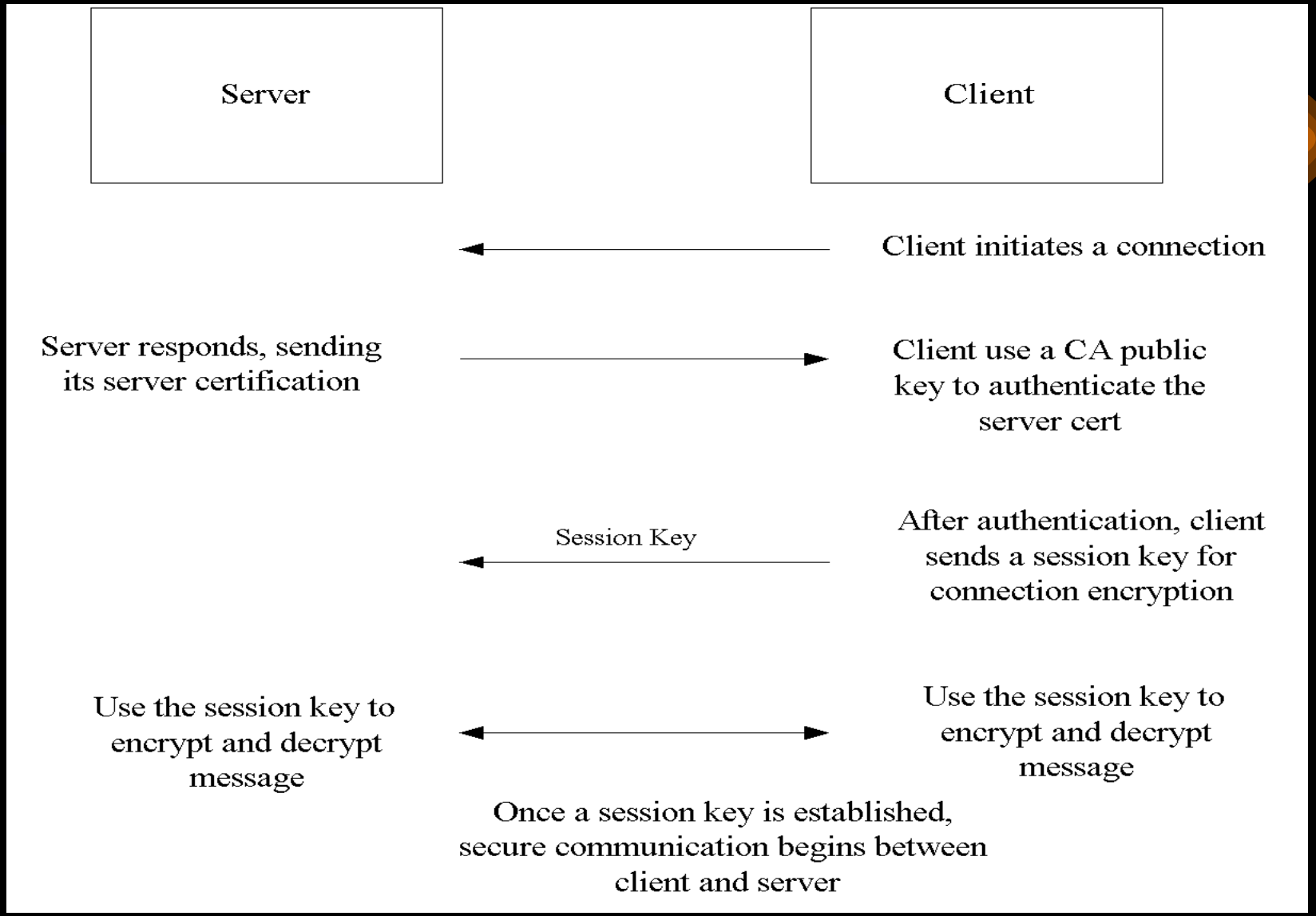
Two real cases

- AMD Hacking (Jan 2000)
- BIND 8.2 NXT bug hacking (Feb 2000)

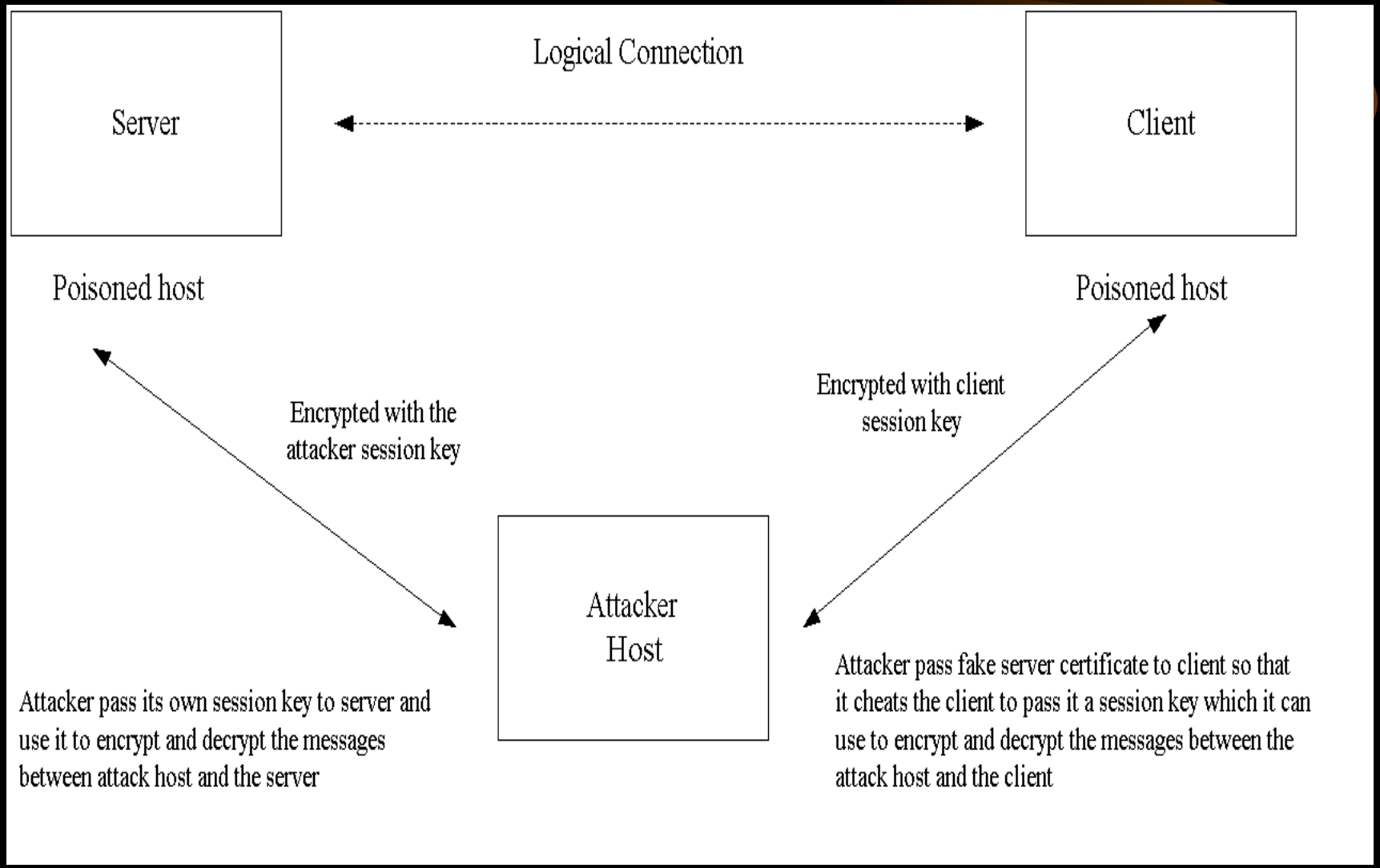
Man-in-the Middle Attack

- ARP Poisoning
- Sniffing SSH and HTTPS sessions

Connections are protected by session keys



Man-in-the-Middle Attack



Intrusion Detection

System and Network Monitoring

- Traffic Monitoring and Analysis
- Real Case: DDoS attack (Nov 2000)

Intrusion Detection System (IDS)

- Host base and Network base
- Real Case: Code Red and Nimda worm attack (Aug/Sept 2001)