

Voice-over-IP phun with Phones – Teil 1

Michael Müller

Senior Consultant S3

23.06.09

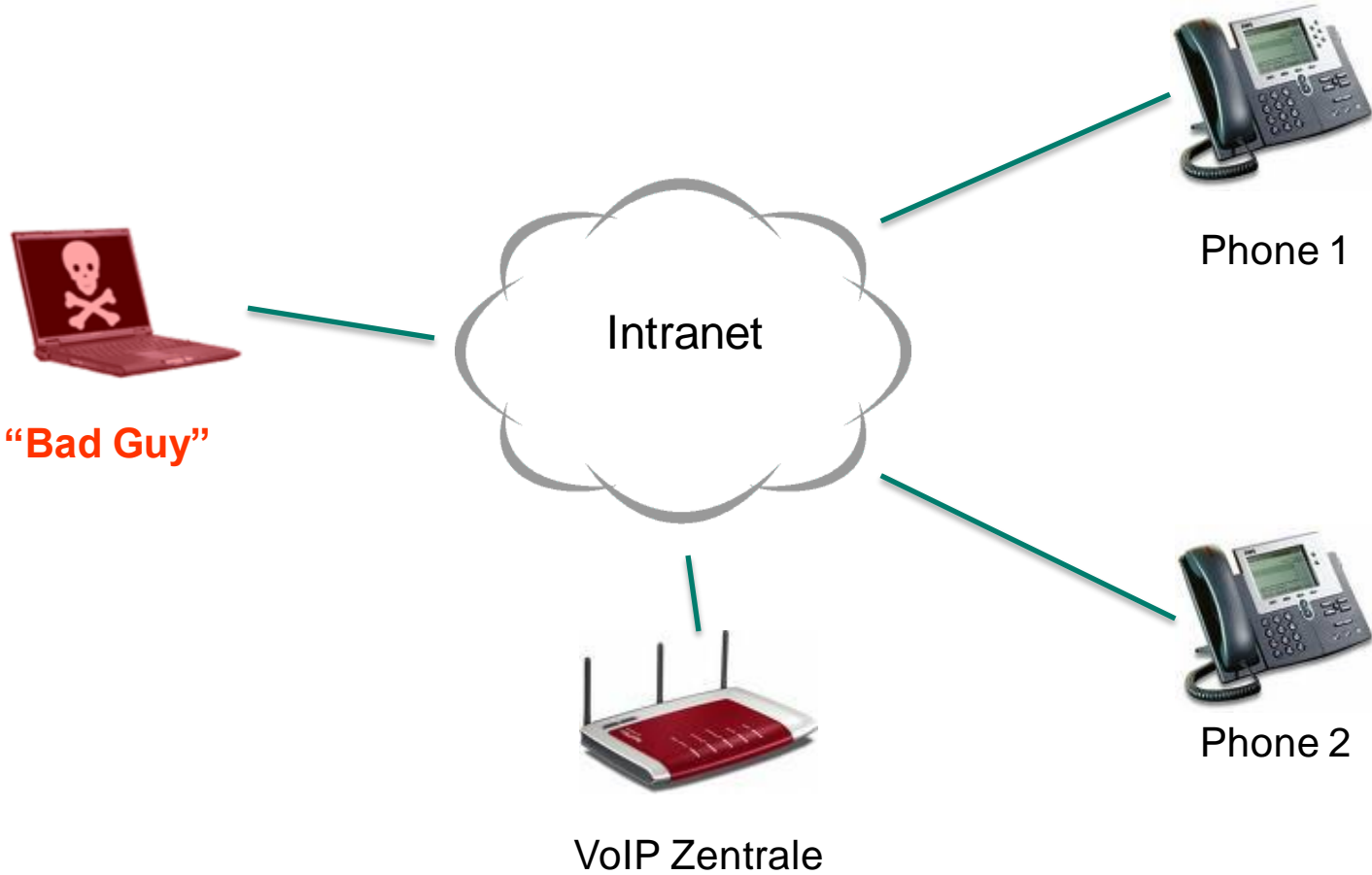
VoIP ist anders...

- Gleiche Gefahren wie bei klassischer Telefonie, aber...
 - Angriffe sind leichter durchzuführen
 - Keine spezielle Hardware erforderlich
 - “Jeder” im Netzwerk hat u.U. Zugriff
- Kompromittierung von VoIP-Endgeräten kann zur Gefahr für das ganze Netzwerk werden
 - Siehe z.B. Buffer Overflows mit Code Execution bei Cisco (SIP Bsp: CVE-2008-0530, CVE-2008-0528, CVE-2008-0529, CVE-2008-0531)

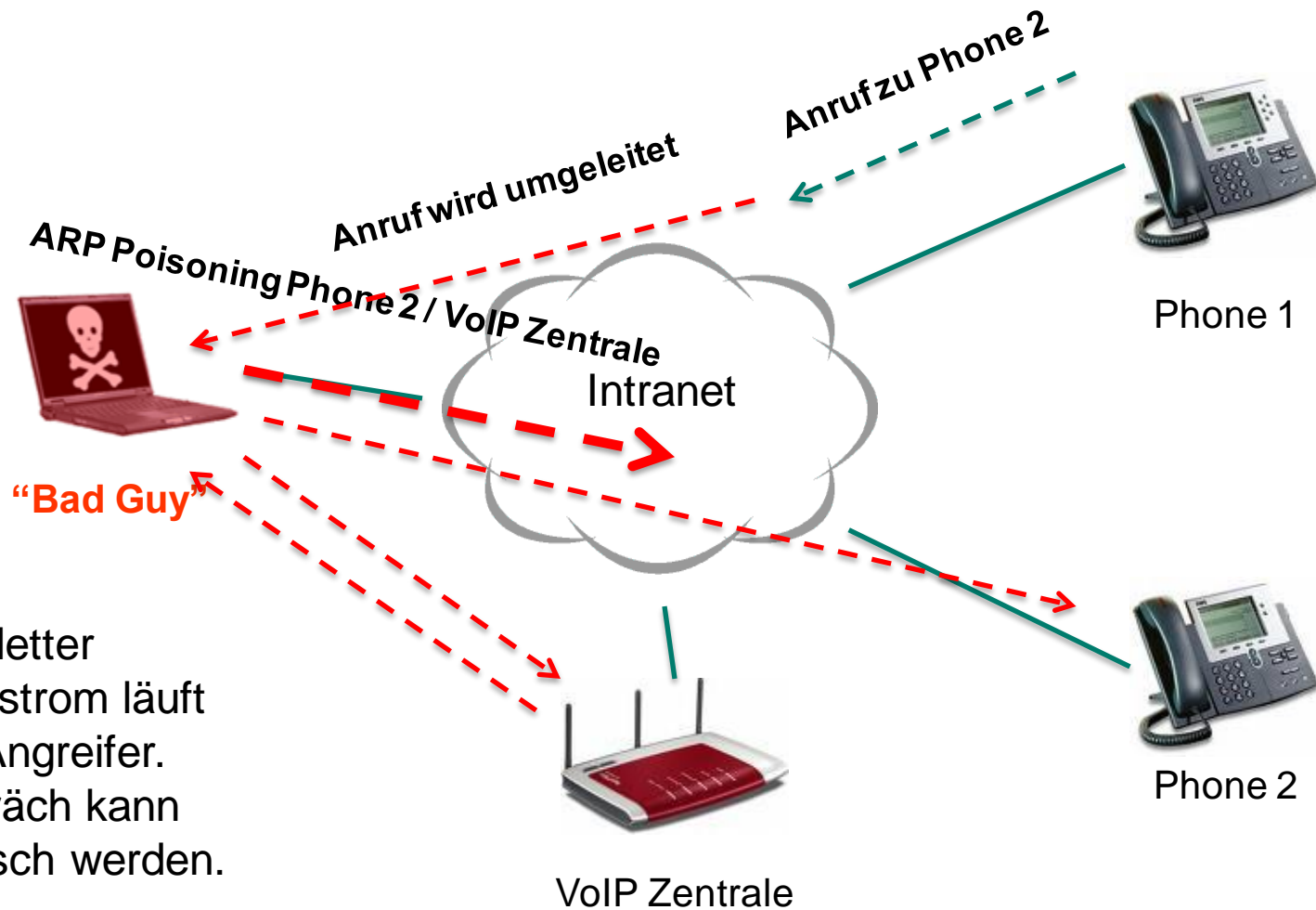
VoIP schwächtelt...

- Verschlüsselung möglich, aber...
 - ...selten genutzt; oft wegen technischer Probleme (WLAN Roaming, etc.)
 - ...ist teilweise nicht möglich, da Gespräche aufgezeichnet werden müssen (Handel, Callcenter, etc.)
- No more CIA
 - (C) Abhören möglich -> Verlust der Vertraulichkeit
 - (I) Manipulation der Gespräche möglich (wenn auch unwahrscheinlich) -> Verlust der Integrität
 - (A) Denial of Service sehr einfach -> Verlust der Verfügbarkeit

Das Labor



Experiment #1: Abhören eines Telefonates



Kompletter
Datenstrom läuft
über Angreifer.
Gespräch kann
belauscht werden.

Zeit für etwas Praxis

DEMO

Experiment #2: „Unter falscher Flagge“

Angreifer startet Softphone mit Auth-Daten und kann als Phone1 telefonieren



ARP Poisoning Phone 2 / VoIP Zentrale



“Bad Guy”

Authentisierungsdaten werden mitgelesen.

User: 620

Pass: letmein

Anruf zu Phone 2



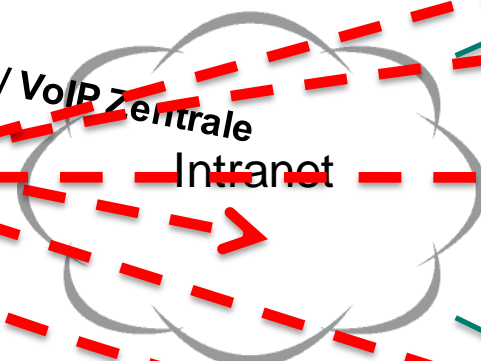
Phone 1



VoIP Zentrale



Phone 2

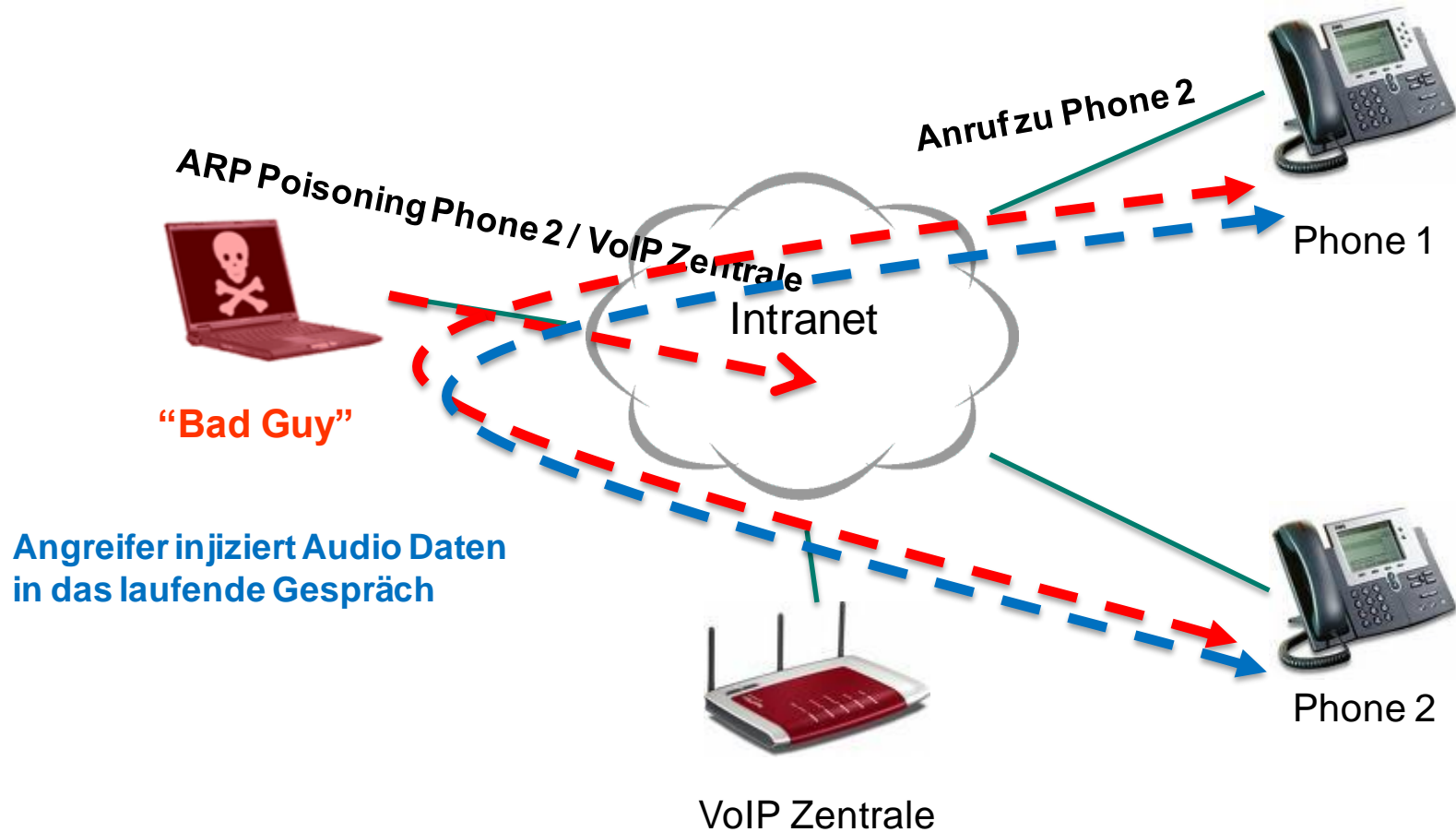


Zeit für etwas Praxis

DEMO

Experiment #3: Abteilung „phun“

Einspielen von Audio in aktives Telefonat



Zeit für etwas Praxis

DEMO

Schutzmaßnahmen

- PoE (Power over Ethernet)
- Netzwerkports am Telefon deaktivieren
- Admin Dienste auf Endgeräten deaktivieren (Telnet, SSH, HTTP)
- Verschlüsselung nutzen
- Netzwerkseitige Schutzmaßnahmen:
 - Eigenes VLAN für VoIP
 - Abschottung vom Rest des Netzwerkes
 - NAC / IPS
 - Config Server (TFTP) besonders sichern
- Regelmäßige Audits der Umgebung

Fragen und Antworten



Integralis S3-Services
s3@integralis.de

Integralis[®] S3
System Security Services