

Mobile Telefonie phun with Phones – Teil 2

Michael Müller

Senior Consultant S3

23.06.09

SMS als Angriffsvektor

- Die Service SMS
 - WAP Push Service Indication
 - Zeigt z.B. an das neue Dienste verfügbar sind
 - WAP Push Service Load
 - Zwingt z.B. das Mobiltelefon Dienste zu laden
- Absender ist verschleierbar
- Anonyme Nachrichten via MMS-Notification
- MWI als Scherzartikel
- Ausführen von beliebigem Code
- Viele Hersteller / Betriebssysteme betroffen
 - (Blackberry, Windows Mobile, Motorola, Sony-Ericsson, etc.)

Das Labor



„Bad Guy“



Opfer 1:
Blackberry



Opfer 2:
Windows Mobile

Zeit für etwas Praxis...

- Experiment #1: „Unter falscher Flagge“ – WAP-Push SI
- Experiment #2: MMS Notification – Mein Handy als Provider
- Experiment #3: „Sie haben Post!“ – Nervende MWI
- Experiment #4: „You‘re Owned“ – Dein Handy ist mein Handy

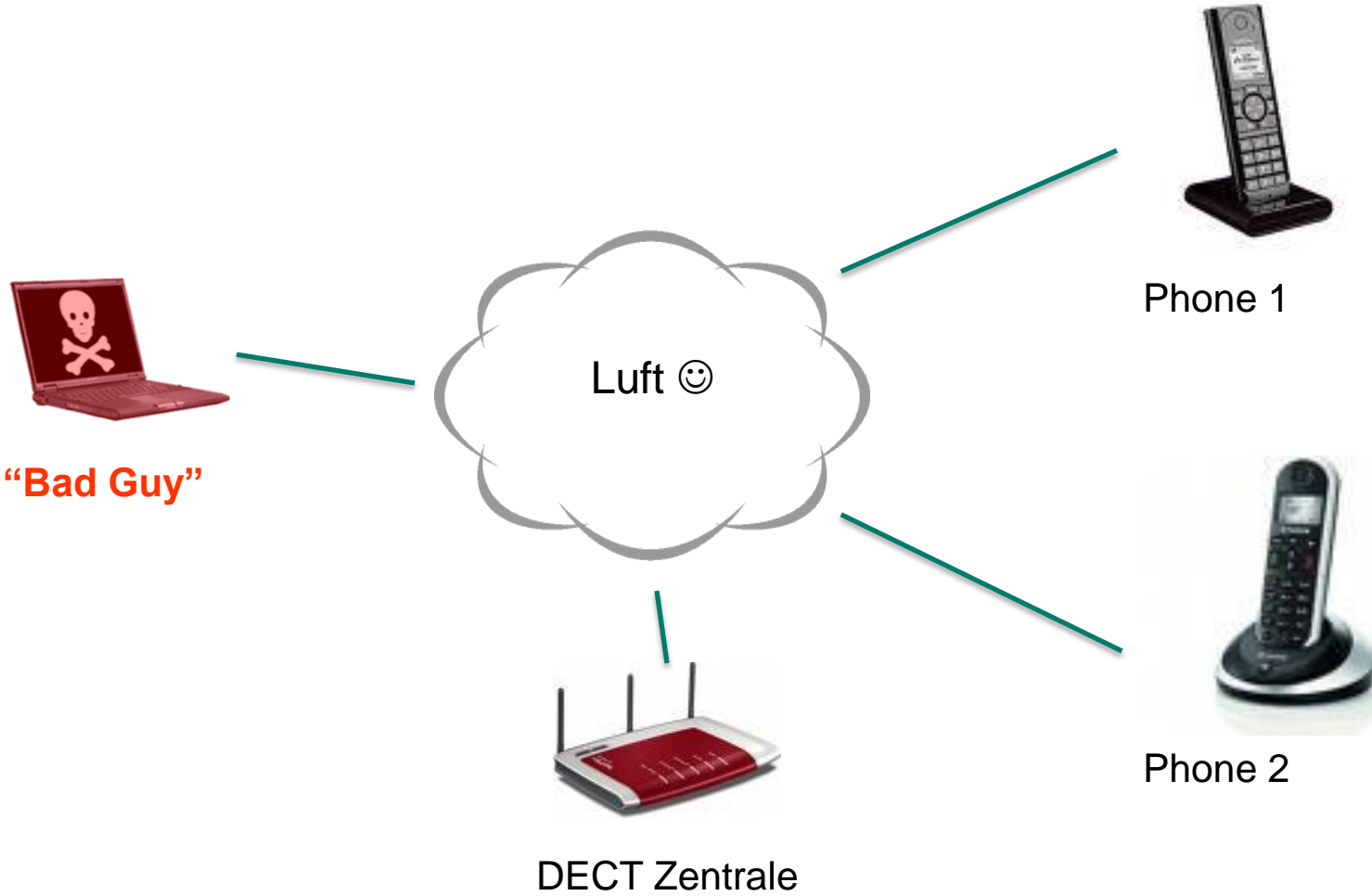
Abhilfe schaffen

- Empfang von Service Nachrichten deaktivieren
 - Windows Mobile: Registry Eintrag
 - Blackberry: Sicherheitseinstellungen
 - Andere: Erweiterte Einstellungen
- Nicht auf aktive Inhalte in SMS zugreifen
- GSM / SMS als unsicheres Medium bewusst wahrnehmen
- Smartphones / PDA / etc. im Unternehmensumfeld als Teil der IT Sicherheit bewusst wahrnehmen und in die Sicherheitsrichtlinien mit einbinden

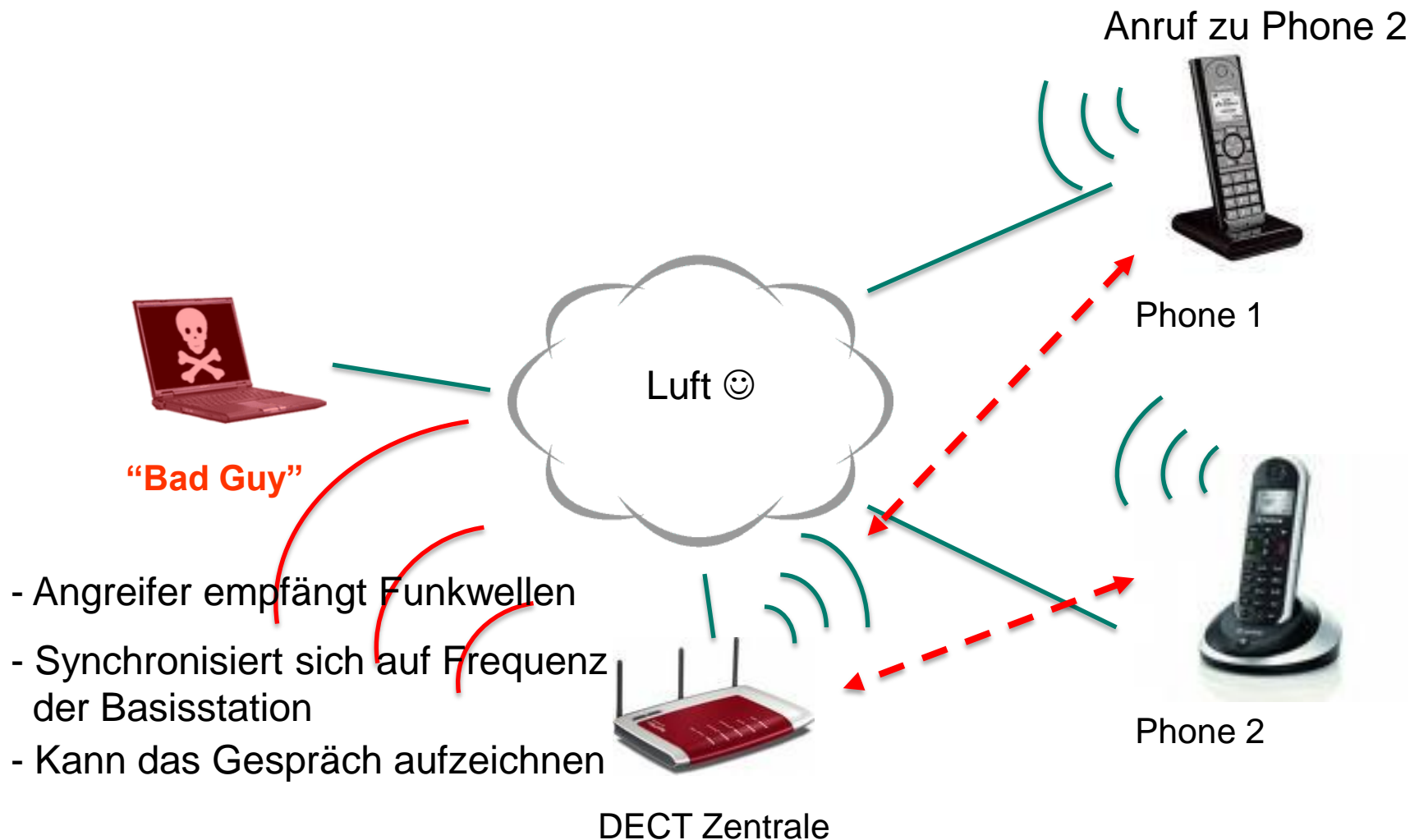
DECT – Abhören mal einfach gemacht

- Einsatz in den Bereichen
 - Telefonie
 - Zahlungsverkehr
 - Datenübertragung / Verkehrssteuerung / etc.
- Standard bietet Verschlüsselung und Authentisierung als Option, aber...
 - ...Basisstationen und Endgeräte verschlüsseln oft nicht
 - ...Authentisierung erfolgt meist, wenn überhaupt, nur von der Basisstation zum Mobilteil
- Angriffe sind leicht nachzuvollziehen
 - Keine „teure“ Hardware erforderlich
 - Infos und Tools gibt es auf dedected.org

Das Labor



Zeit für etwas Praxis



Zeit für etwas Praxis

DEMO

Abhilfe schaffen

- DECT im Privathaushalt
 - Prüfen ob Verschlüsselung möglich und aktiv
 - Ggf. durch neuere Geräte ersetzen
- DECT im Unternehmensumfeld
 - Lassen Sie Ihre TK-Anlage auditieren (DECT, Wardialing, etc.)
 - Führen Sie im Zweifelsfall keine vertraulichen Gespräche über DECT Telefone
 - Wenden Sie sich an den Hersteller

Fragen und Antworten



Integralis S3-Services
s3@integralis.de

Integralis[®] S3
System Security Services