Harvesting Voice Conference Bridges

Andrei Costin <andrei@andreicostin.com>

Affiliation - PhD student

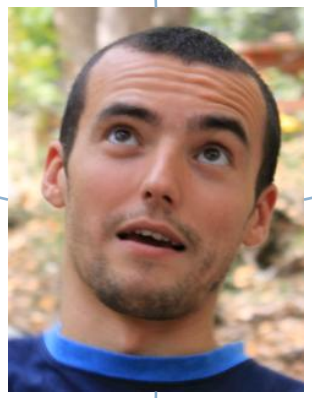
EURECOM
Sophia Antipolis

whoami: in-between SW/HW hacker

Hacking MFPs (for fun & profit)

Mifare Classic MFCUK

Holistic Security Interest



http://andreicostin.com/papers/

Agenda

1. What?
2. Why?
3. Where?
4. How?
5. So?

Short intro to voice conference bridges

- A conference bridge is an ATC (Audio Tele-Conference)
- Companies commonly use specialized service providers which
  - Maintain bridge (HW/SW)
  - Provide access phones and PINs
- This research started with my Outlook VBA “conference room codes & attachments” automation

Agenda

1. What?
2. Why?
3. Where?
4. How?
5. So?

Because it's an EASY task

- Voice bridge tapping not yet perceived as risk
  - Bridge details freely float around
- Not easy to detect
  - Attacker is not forced to respond to “bridge chair” call-out
  - Usually, there is no "visual control panel" of attendees
- Limited security features
  - PINs are usually 4-6 digits, linked to personality
  - Limited [0-9] alphabet used, low key-space
  - Usually “brute-force lock-out” is NOT implemented
- Can give wealth of information (see below)

Because it's a HARD task

- Need reliable actionable inteligence extraction
  - Conf detail data: phone number, access code, date/time
  - Transcripted data:
  - 0.00$: google mail
  - +INF$: alchemyapi, opencalais, zemanta, coveo
- Need reliable voice transcript extraction
  - 0.00$: google voice
  - +INF$: jott, nuance/dragon

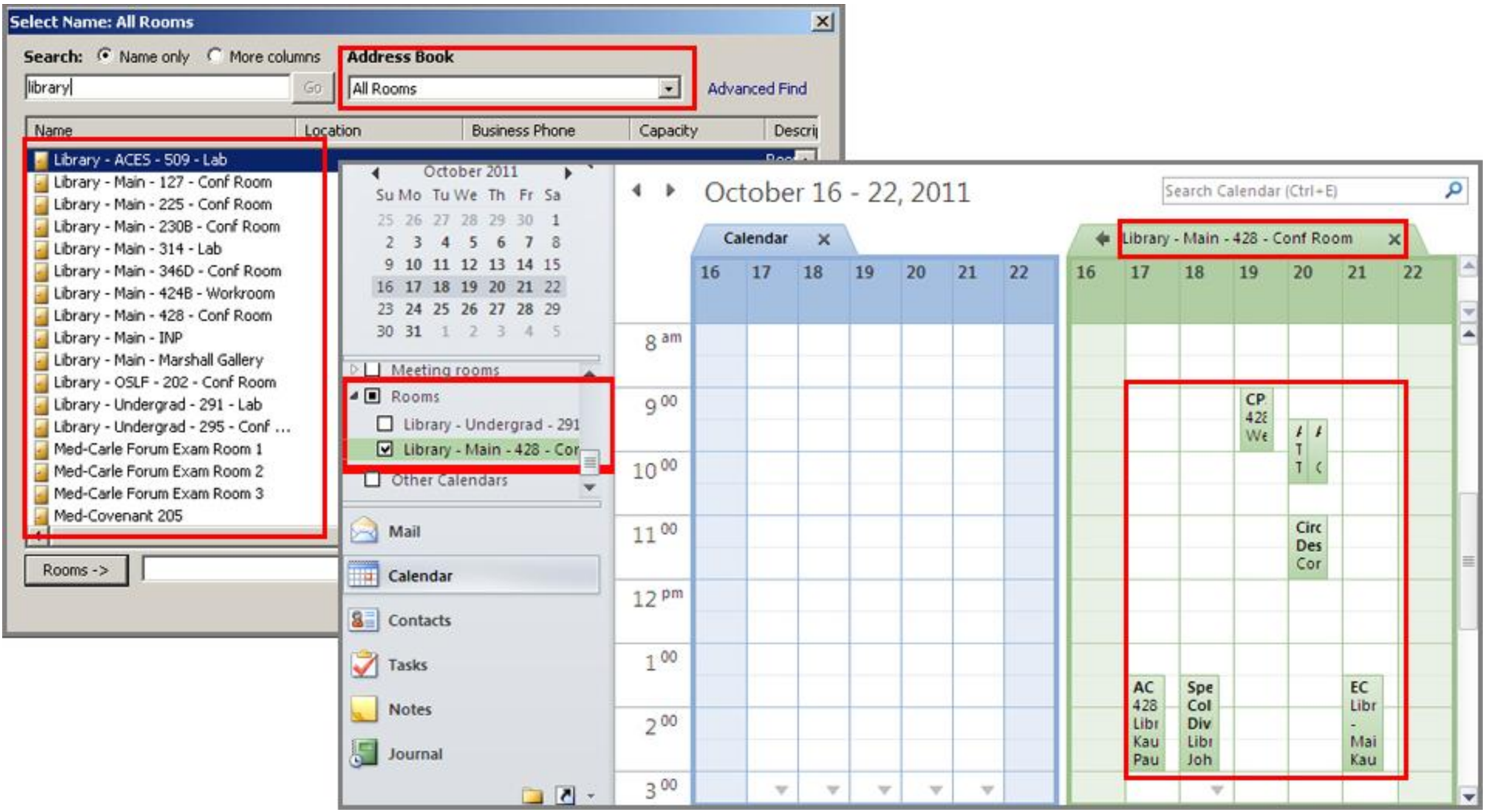
Agenda

1. What?
2. Why?
3. Where?
4. How?
5. So?

Outlook shared/public “Conference Room”

- The “necessary evil” in enterprises
  - Logistics
    - Physical conference rooms booking
    - Conference material sharing
  - Materials
    - Sensitive attachments (a future todo)
    - **Voice bridge details**
  - All shared/public
  - Included in TO/CC
  - An IT security nightmare
- Real life job example:
  - ~500 conference rooms worldwide
  - Every “room” user on avg 5 years of shared calendars
  - Automate!

Example – Outlook 2010 + “Pattern-able” names



Example – Outlook VBA automation source code

```
Sub SaveSharedCalendar()
    ' Outlook
    Dim outApp As Object, outNS As Outlook.Namespace
    Dim myAddressList As Outlook.AddressList
    Dim myAddressEntries As Outlook.AddressEntries
    Dim myAddressEntry As Outlook.AddressEntry
    Dim myListMember As Outlook.AddressEntry
    Dim myRecipient As Outlook.Recipient
    Dim CalendarFolder As Outlook.mapiFolder
    Dim myAddressEntryName As String

    ' CDO/MAPI
    Dim objCDOSession As MAPI.Session
    Dim objCDOAE As MAPI.AddressEntry
    Dim cdoField As MAPI.Field

    ' Misc
    Dim StringValue As Variant
    Dim i As Long, j As Long
    Dim crntDistList As Long, crntUser As Long
    crntDistList = 1
    crntUser = 1

    Set outApp = CreateObject("Outlook.Application")
    Set outNS = outApp.GetNamespace("MAPI")
    Set myAddressList = outNS.Session.AddressLists("Global Address List")
    Set myAddressEntries = myAddressList.AddressEntries

    Set objCDOSession = CreateObject("MAPI.Session")
    objCDOSession.Logon "", "", False, False, 0

    If objCDOSession Is Nothing Then
        MsgBox "No active session, you must log on"
        Exit Sub
    End If

    On Error GoTo ErrHandler

    myAddressEntryName = getNextOutlookRecipient()
    ' Check if it is a room user - then export it's appointments to .MSG files
    If checkRecipientIsPublicConferenceRoom(myAddressEntryName) = 0 Then
        Set myRecipient = outNS.CreateRecipient(myAddressEntryName)
        myRecipient.Resolve
        If myRecipient.Resolved Then
            Set CalendarFolder = outNS.GetSharedDefaultFolder(myRecipient, olFolderCalendar)
            ' user Replace("", "", "") to remove any path non-friendly chars
            MkDir (ActiveWorkbook.Path & "\\" & prefixStr)
            Dim AptItem As Outlook.AppointmentItem
            For Each AptItem In CalendarFolder.Items
                AptItem.SaveAs ActiveWorkbook.Path & "\\" & prefixStr & "\\" & Format(AptItem.Start, "yyyymmdd") & " - " & AptItem.Subject & ".msg", olMSG
                AptItem.SaveAs ActiveWorkbook.Path & "\\" & prefixStr & "\\" & Format(AptItem.Start, "yyyymmdd") & " - " & AptItem.Subject & ".txt", olTXT
                Next
        End If
    End If

    MsgBox "Completed"
```

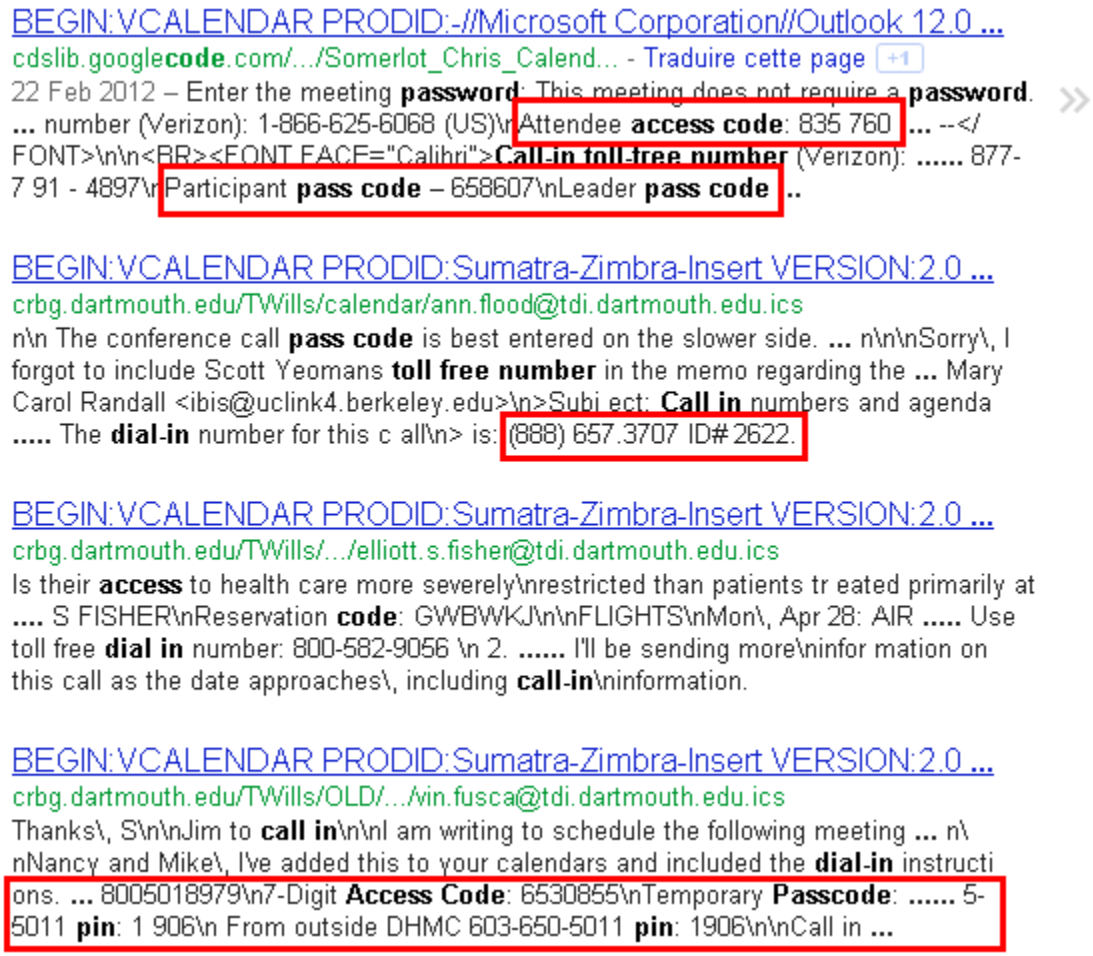
Example – Google Dorks

"Access Number"
"Call in number"
"Dial-in number"
"Toll-free number"
"Call-in number"
"Dial in"
"Dial-in"
"Dialing"
"Calling"
"conference number“
"Conference Entry Password“
"toll free number"
"audio access"
"participant dial in"

"Participant code"
"Participant passcode"
"Access code"
"Conference code"
"Access PIN"
"Participant pin"
"conference ID"
"pass code“
“passcode”
“pass-code”
"call passcode"
"audience passcode“
“BEGIN:VCALENDAR”
filetype:ics

Example - .ICS files

("dial-in" OR "dial in" OR "dialing" OR "call-in" OR "call in" OR "access number" OR "toll-free number") AND ("passcode" OR "pass-code" OR "pass code")(access or pass pin or code) filetype:ics



BEGIN:VCALENDAR PRODID:-//Microsoft Corporation//Outlook 12.0 ...
cdslib.google**code**.com/.../Somerlot_Chris_Calend... - Traduire cette page +1
22 Feb 2012 – Enter the meeting **password**: This meeting does not require a **password**. ... number (Verizon): 1-866-625-6068 (US)\rAttendee **access code**: 835 760 ... --</FONT>\n\n
<FONT FACE="Calibri">**Call-in toll-free number** (Verizon): ..... 877-7 91 - 4897\rParticipant **pass code** – 658607\nLeader **pass code** ..

BEGIN:VCALENDAR PRODID:Sumatra-Zimbra-Insert VERSION:2.0 ...
crbg.dartmouth.edu/TWills/calendar/ann.flood@tdi.dartmouth.edu.ics
n\n The conference call **pass code** is best entered on the slower side. ... n\n\nSorry\, I forgot to include Scott Yeomans **toll free number** in the memo regarding the ... Mary Carol Randall <ibis@uclink4.berkeley.edu>\n>Subj ect: **Call in** numbers and agenda ..... The **dial-in** number for this c all\n> is: (888) 657.3707 ID# 2622.

BEGIN:VCALENDAR PRODID:Sumatra-Zimbra-Insert VERSION:2.0 ...
crbg.dartmouth.edu/TWills/.../elliott.s.fisher@tdi.dartmouth.edu.ics
Is their **access** to health care more severely\nrestricted than patients tr eated primarily at .... S FISHER\nReservation **code**: GWBWKJ\n\nFLIGHTS\nMon\, Apr 28: AIR ..... Use toll free **dial in** number: 800-582-9056 \n 2. ..... I'll be sending more\ninfor mation on this call as the date approaches\, including **call-in**\ninformation.

BEGIN:VCALENDAR PRODID:Sumatra-Zimbra-Insert VERSION:2.0 ...
crbg.dartmouth.edu/TWills/OLD/.../vin.fusca@tdi.dartmouth.edu.ics
Thanks\, S\n\nJim to **call in**\n\nI am writing to schedule the following meeting ... n\nNancy and Mike\, I've added this to your calendars and included the **dial-in** instructi ons. ... 8005018979\n7-Digit **Access Code**: 6530855\nTemporary **Passcode**: ..... 5-5011 **pin**: 1 906\n From outside DHMC 603-650-5011 **pin**: 1906\n\nCall in ...

Agenda

1. What?
2. Why?
3. Where?
4. How?
5. So?

The harvesting flow in a nutshell

Find conf details	**Extract bridge and code detail**	**Automate call-in and call-auth**	**Speech-to-text automation**
Outlook VBA	*gmail.com & APIs*	*SkypeKit SDK*	Automated
Google Dorks	*alchemyapi.com*	*Skype4py*	*Google Voice*
Plain-text SMTP/POP3	*opencalais.com*	*python-skype*	*Jott*
	zemanta.com	*pySkype*	*Nuance/Dragon*
	coveo.com		Manual/human
			MechanicalTurk
			CastingWords
			PurpleShark
			Kedrowski

Other ideas - Voice

- Build automated speaker recognition
  - On joining, usually a “greeting” is recorded like “John Smith”
  - ATC plays “John Smith has joined the conference”
    - “John Smith” – recording, i.e. person label
    - “has joined the conference” – system generated
  - Gather “greetings” to train speaker identification database
  - Use the bridge recording to
    - Enhance the training data-set
    - Assign “transcribed knowledge” to “identified person”
- Tools/frameworks
  - ALIZE
  - MARF
  - CMU Sphinx4

Other ideas - PINs

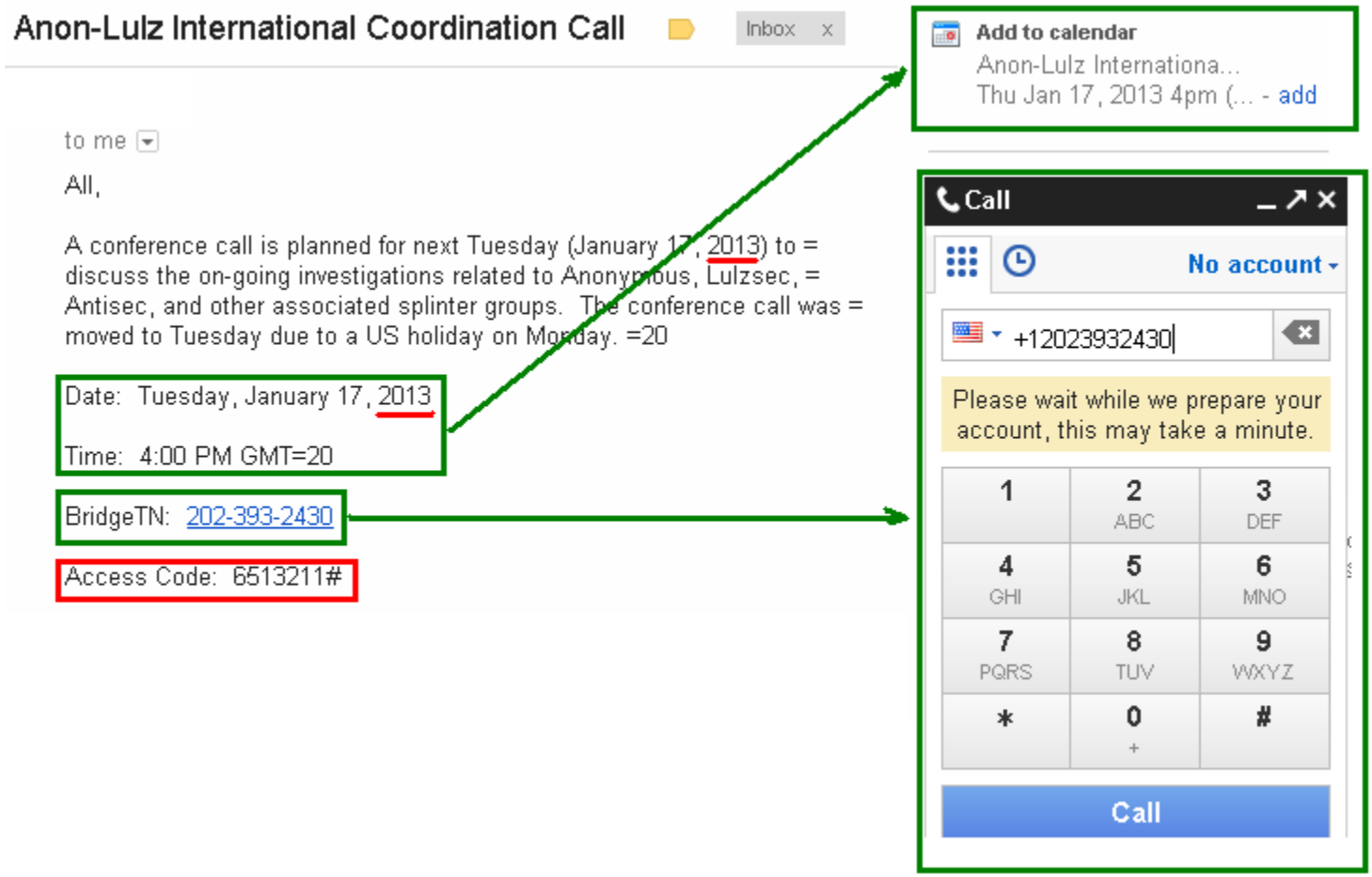
- User-settable bridge PIN codes can be a reuse of
  - A bank card PIN
  - A personal date reuse (birthday, anniversary, kids)
  - Digipass PIN
  - Area access control PIN

- Can be statistically analyzed versus leaked/analyzed PIN DBs
  - Bank PIN codes paper
  - Smartphone PIN codes articles

Real-life example – Antisec vs FBI – Conf details

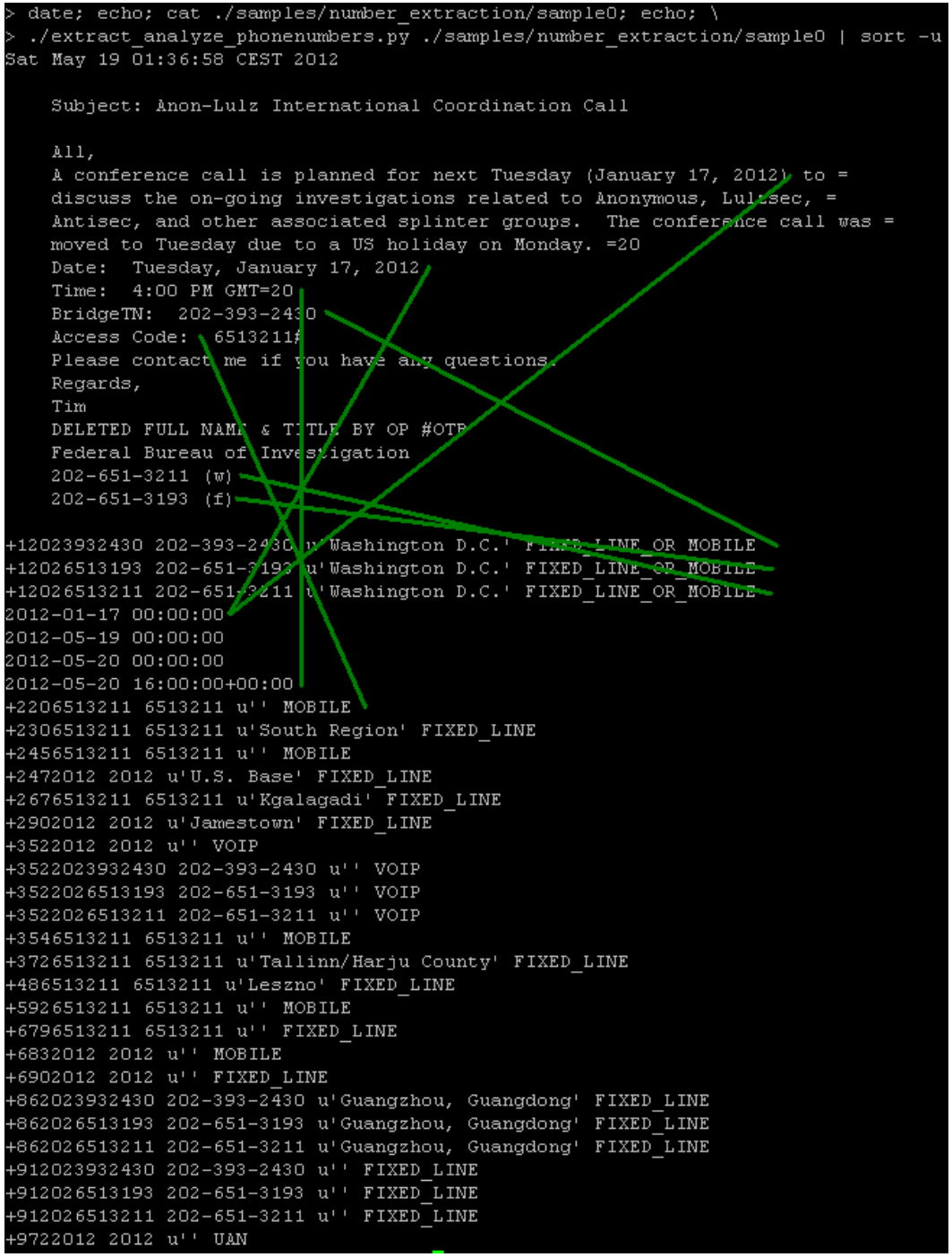
```
55.
56.
57.
58. All,
59.
60. A conference call is planned for next Tuesday (January 17, 2012) to =
61. discuss the on-going investigations related to Anonymous, Lulzsec, =
62. Antisec, and other associated splinter groups.  The conference call was =
63. moved to Tuesday due to a US holiday on Monday. =20
64.
65. Date:  Tuesday, January 17, 2012
66.
67. Time:  4:00 PM GMT=20
68.
69. BridgeTN:  202-393-2430
70.
71. Access Code:  6513211#
72.
```

Real-life example – Google is “poor-man’s intelligence/semantic extractor”



For python-loving ninjas

- Libs
  - python-libphonenumbers
  - python-dateutil
- Integrate skype/voip scripting
  - Cron/scheduler
  - Audio dumper
- Filter out false-positives
  - Static tel# analysis
  - Dynamic calling



Challenges – date or short-code PBX number?

```
> date; echo; cat ./samples/number_extraction/sample0_pbx; echo; \
> ./extract_analyze_phonenumbers.py ./samples/number_extraction/sa
Sat May 19 01:42:22 CEST 2012

    Subject: Anon-Lulz International Coordination Call

    All,
    A conference call is planned for next Tuesday (January 17, 201
    discuss the on-going investigations related to Anonymous, Lulz
    Antisec, and other associated splinter groups.  The conference
    moved to Tuesday due to a US holiday on Monday. =20
    Date:  Tuesday, January 17, 2012
    Time:  4:00 PM GMT=20
    BridgeTN:  202-393-2430 / 2012 (internal PBX)
    Access Code:  6513211#
    Please contact me if you have any questions.
    Regards,
    Tim
    DELETED FULL NAME & TITLE BY OP #OTB
    Federal Bureau of Investigation
    202-651-3211 (w)
    202-651-3193 (f)

+12023932430 202-393-2430 u'Washington D.C.' FIXED_LINE_OR_MOBILE
+12026513193 202-651-3193 u'Washington D.C.' FIXED_LINE_OR_MOBILE
+12026513211 202-651-3211 u'Washington D.C.' FIXED_LINE_OR_MOBILE
2012-01-17 00:00:00
2012-05-19 00:00:00
2012-05-20 00:00:00
2012-05-20 16:00:00+00:00
+2206513211 6513211 u'' MOBILE
+2306513211 6513211 u'South Region' FIXED_LINE
+2456513211 6513211 u'' MOBILE
+2472012 2012 u'U.S. Base' FIXED_LINE
+2676513211 6513211 u'Kalagadi' FIXED_LINE
+2902012 2012 u'Jamestown' FIXED_LINE
+3522012 2012 u'' VOIP
+3522023932430 202-393-2430 u'' VOIP
```

- Easy-not problem
- Need additional knowledge

2012

2012

202-393-2430

Agenda

1. What?
2. Why?
3. Where?
4. How?
5. So?

Take aways

- Periodically audit and validate (automation + manual) the shared calendar events details & attachments
- Have a scheduled WMI/WSH/VB script to securely archive and then purge the expired meeting events
- Ask MS (or your enterprise "outlook" vendor) to add finer granularity security settings

Take aways

- Choose ATC providers with strong PIN policies and secure ATC control panels
- Avoid sharing conf details on Outlook public “conference rooms” accounts or in public mails/pages
- Avoid having public/shared “conference room” user in your Outlook deployment

Questions?

Andrei Costin andrei@andreicostin.com
http://andreicostin.com/papers