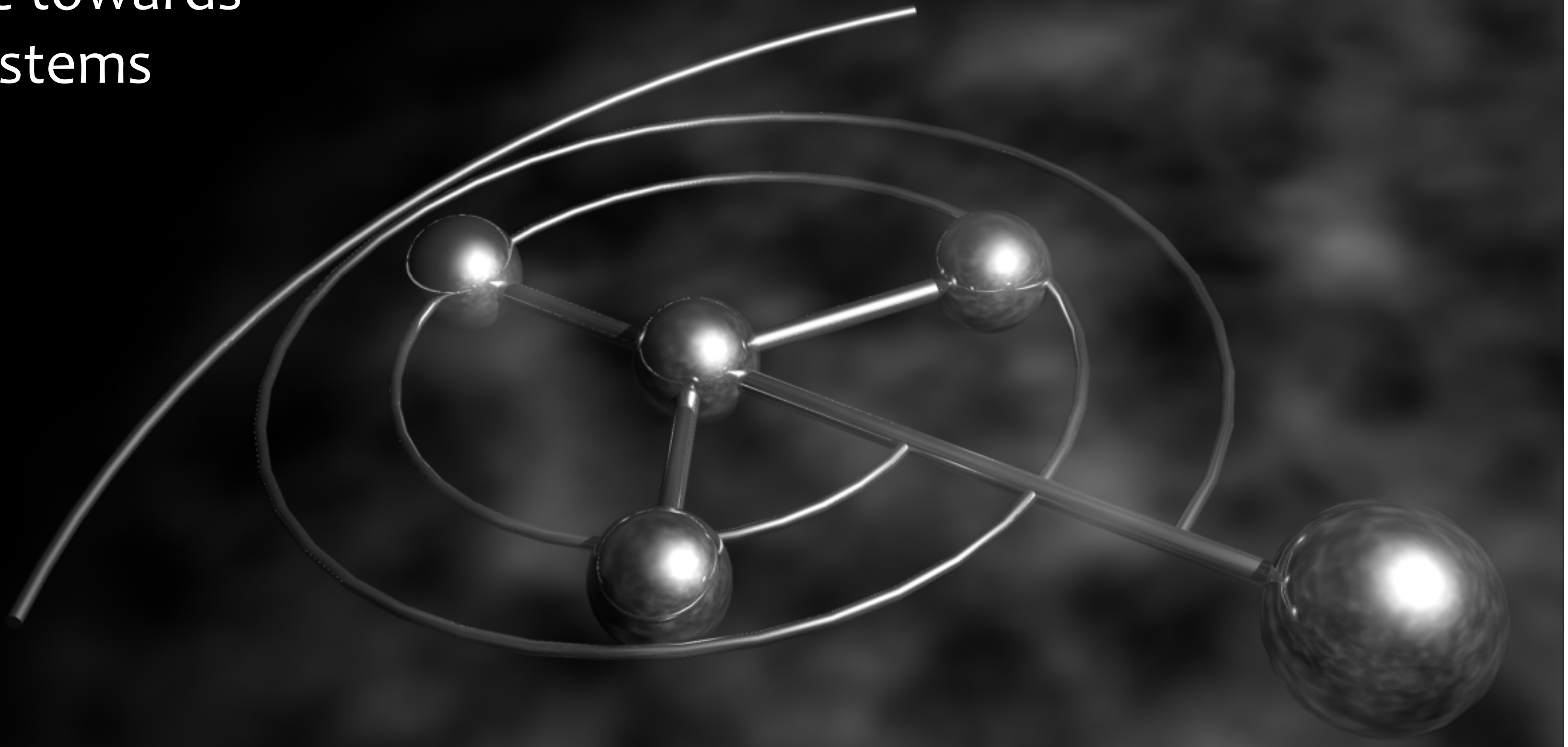
Your Other Network

The Ignorance towards
Embedded Systems



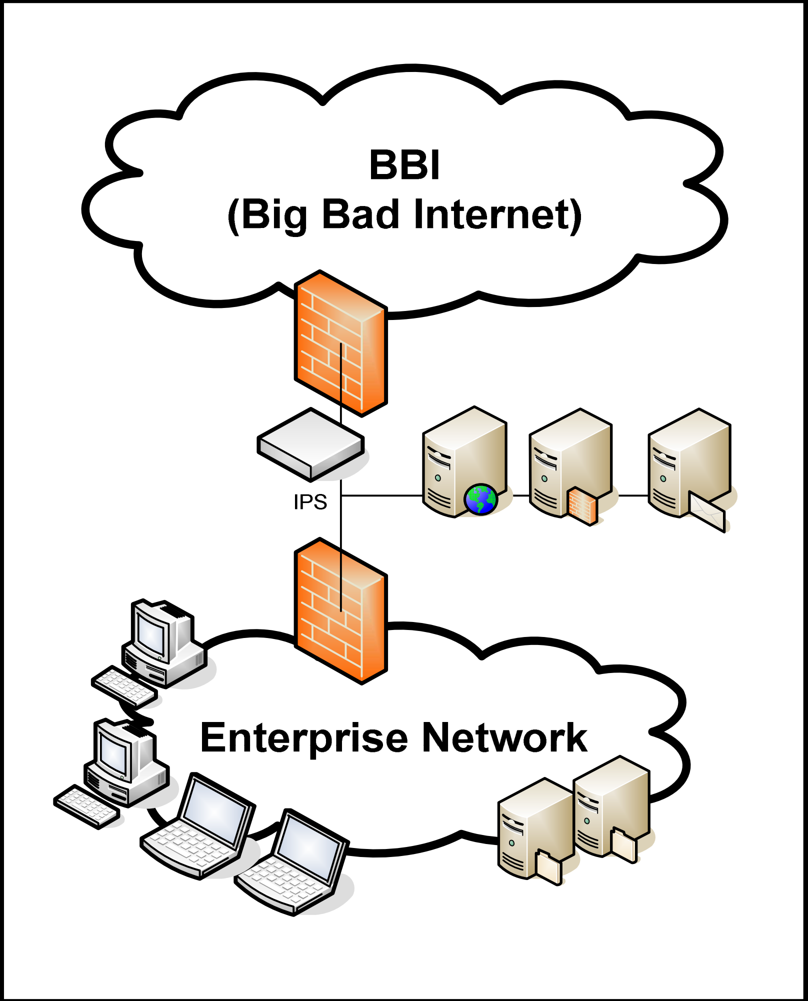
Felix ‘FX’ Lindner, Fabian ‘fabs’ Yamaguchi,
Recurity Labs GmbH
22nd FIRST Conference, Miami

Agenda

- Your Network
- Your Other Network
- Known Attacks
- How attacks are used
- Network level protections
- Policy level protections
- Patching Embedded Systems

Your Network

- Commonly designed following the Perimeter Security Paradigm
  - Internal network is trusted
  - Various DMZ networks
  - Outside network (Internet) is not trusted
- Routed and switched environment
  - Supposedly protects against traffic interception within the network
  - Occasionally with Port Security

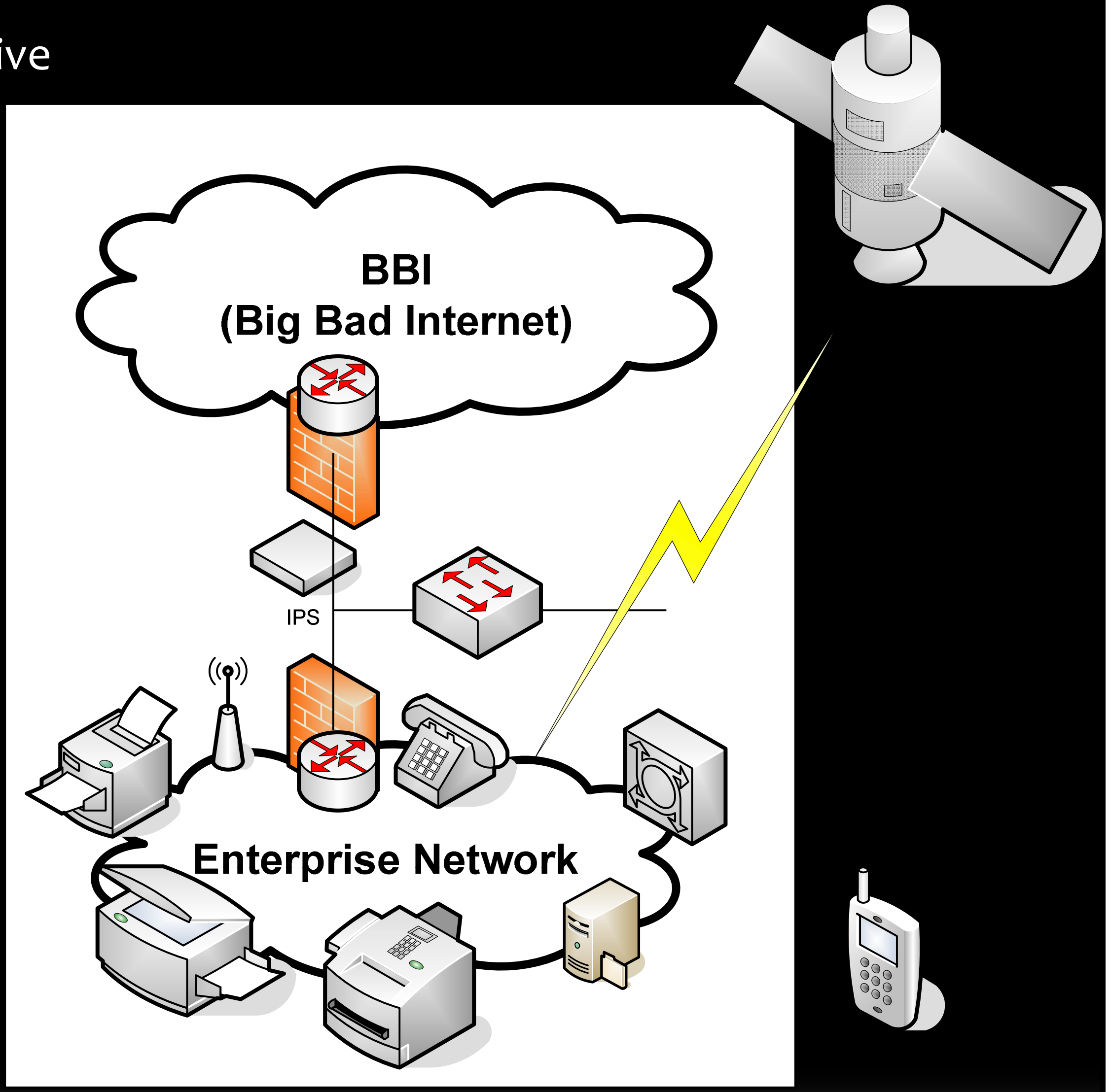


Reasons for Perimeter Security Designs

- Perimeter Security network architectures are still the norm
  - Historically, this paradigm is the oldest and best understood
  - Many (security) products implicitly only support perimeter security
    - Think of firewalls with “outside” interfaces
- Trusting the “internal” network simplifies deployment
  - When it is internal, we don’t have to harden the machines
  - When it is internal, we don’t need authentication
- Attacks and security policy violations are not detected
  - Nobody tackles a problem that doesn’t hurt business operations
  - Only very few businesses monitor their internal networks, simply because of the scale

Your Other Network

- Switches
- Routers
- IDS/IPS
- VPN Termination
- Satellite Links
- VoIP Phones
- PBX
- Embedded Storage
- Printer
- Copier
- FAX Machines
- Mobile Phones



How Switches get Attacked

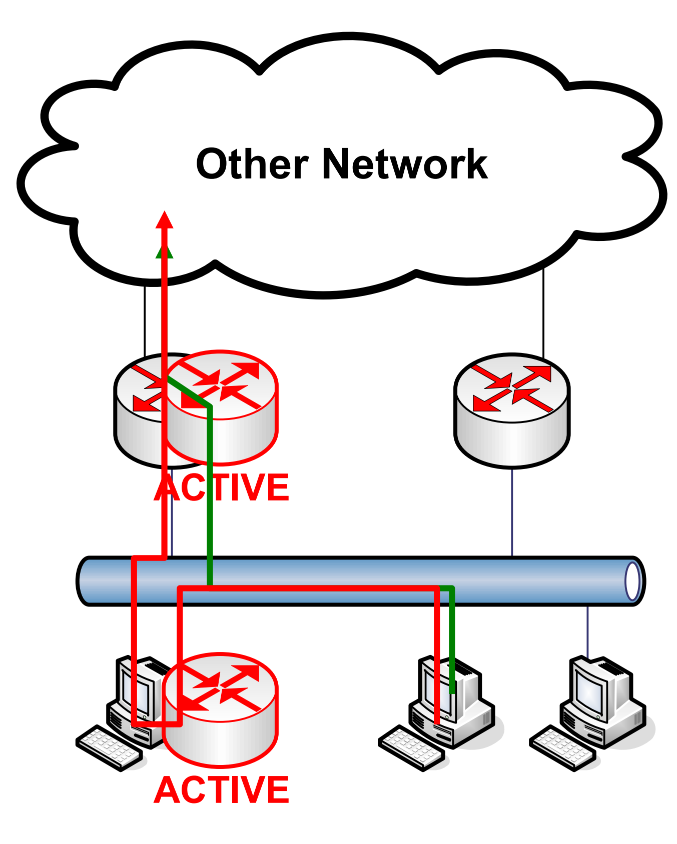
- Most switches announce themselves with great detail
  - Cisco CDP, HP CDP
  - They never get updated
- Switches are an excellent target for capturing data
  - Access to the switch allows to configure a monitor port, obtaining all data from other ports using the switches’ own functionality.
- Switches can change the network layout using dynamic VLAN protocols
  - DTP allows to become a trunking partner for a switch
  - VTP allows to reconfigure VLAN trunks without any need for interactive access to the configuration

How Routers get Attacked

- Attacks on routers are rarer than attacks on switches
  - More unknowns for the attacker
  - Higher visibility if anything goes wrong
  - Less benefits for the attacker
- Most commonly, routers are targeted to remove filters / ACLs
  - Functional vulnerabilities in the router software (e.g. IOS HTTP bug)
  - Protocol based vulnerabilities that already give the desired control (e.g. SNMPv3 vulnerability in many vendor’s router software)
  - Protocol functionality based attacks that don’t require an vulnerability in the router’s software (e.g. HSRP takeover)

Example: Hot Standby Router Protocol (HSRP)

1. The active router announces via multicast to everyone on the LAN
   - Includes a priority, 100 by default
   - May include a password in clear text, “cisco” by default
2. Whoever announces a higher priority is considered active and transparently becomes the default router



How Routers do not get Attacked

- Router software exposes vulnerabilities as any other software
  - Routers are rarely updated to hold network SLAs
- Successful exploitation of router software vulnerabilities is comparably hard
  - Considerable amount of work
  - Considerable experience and skill required
- Therefore, exploits against routers are expensive
  - Not “wasted” on enterprises
  - There may be exceptions

When IDS and IPS become the Risk

- IDS / IPS are touted as attack detection technology
  - IDS sensors are often only “listening” to the network traffic
    - But their other connection goes straight to the management network
  - IPS are placed “in path” of the network traffic, with full control
- Modern IDS/IPS support hundreds of protocols
  - Most of these have never been tested thoroughly
  - IDS/IPS testing by certification labs does not include attacks against the device
- Successful exploits have been developed as early as 2004
  - eEye: Server Message Block (SMB) Processing Overflow in all Proventia products
- Nobody would notice a compromised IPS, since nobody is looking at its log data anyway

Virtual Private Network Termination Points

- Virtual Private Network termination is often implemented on routers or firewalls
  - VPN makes heavy use of cryptographic protocols and authentication
  - The largest amount of code is executed before the actual authentication happens
- IPsec ISAKMP exploits are known to exist in underground circles
  - Yielding direct access to the VPN published network from the Internet
  - Vendors try to keep quite about the vulnerabilities, silently fixing them in new software releases
- Because the customers don’t know about the risk, VPN termination devices are rarely updated

Virtual Private Network Termination Points

- Virtual Private Network termination is often implemented on routers or firewall
  - VPN on
  - The cation hap
- IPsec I es
  - Yiel rnet
  - Ven em in new soft
- Becaus tion devices are rarely updated

Cisco IronPort Encryption Appliance devices contain **two vulnerabilities that allow remote, unauthenticated access to any file** on the device and **one vulnerability that allows remote, unauthenticated users to execute arbitrary code with elevated privileges.** There are workarounds available to mitigate these vulnerabilities.

http://www.cisco.com/warp/public/707/cisco-sa-20100210-ironport.shtml

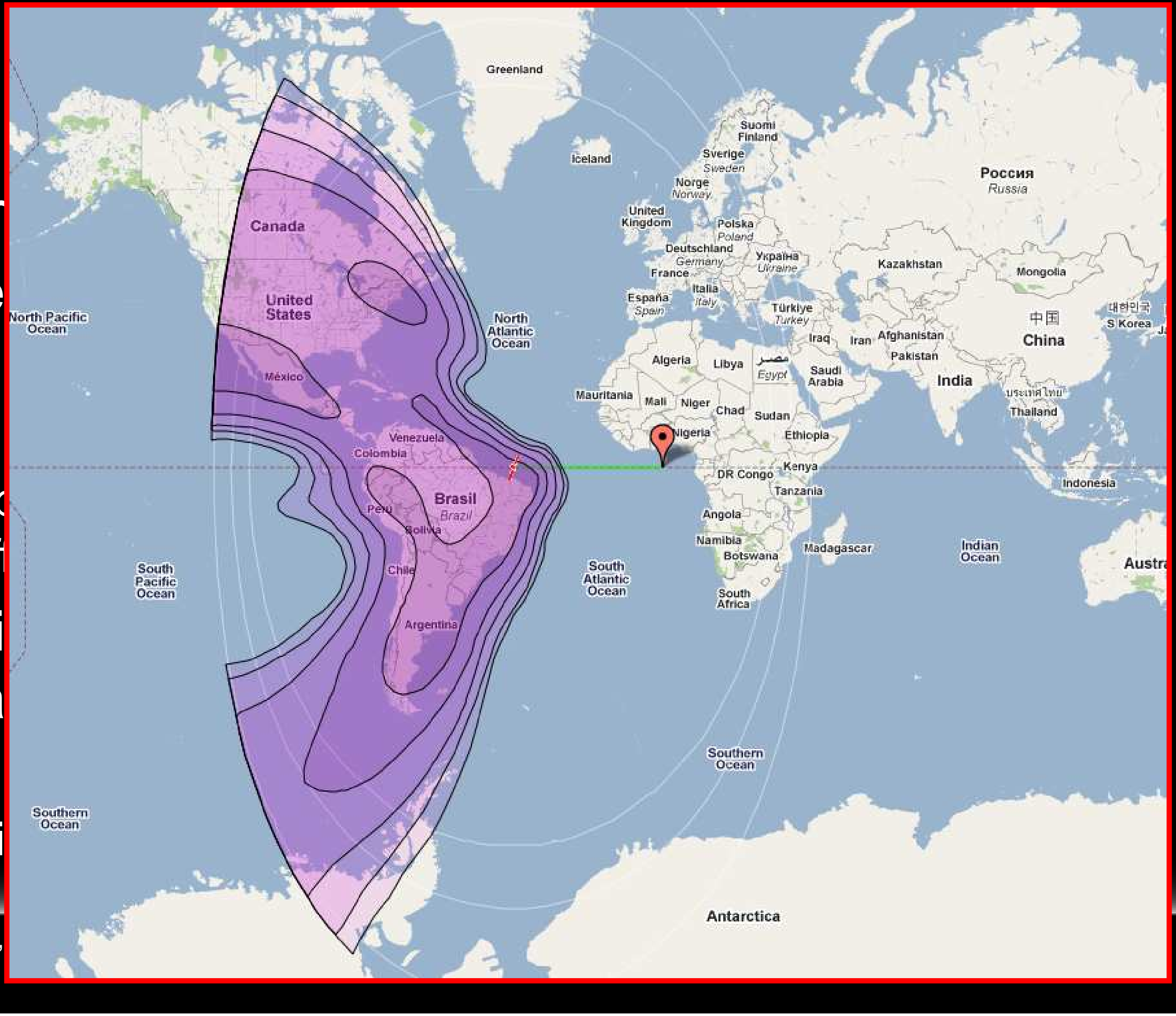
Satellite Links

- Satellite links are the easiest way into an enterprise network
- Research by Leonardo NVE Egea* shows about 30% of all data traffic from satellites is GRE encapsulated internal networks
  - GRE does not provide any security whatsoever when the attacker can monitor the traffic
- Simple application of asymmetric routing and GRE encapsulation allows the attacker to place himself inside the network
  - Requires satellite equipment for about $100 and a Linux machine

* „Playing in a Satellite environment 1.2”, CONFidence 2.0, Warsaw, 2009

Satellite Links

- Satellite links ar
- Research by Le data traffic from networks
  - GRE does not p monitor the traf
- Simple applicati encapsulation a network
  - Requires satelli



* „Playing in a Satellite environment 1.2"

Voice over IP Phones

- Enterprises are increasingly moving towards VoIP telephony
- Most VoIP deployments entirely rely on VLAN separation
  - See the points about switch security
- VoIP Phones often get their configuration and software images using unauthenticated clear text protocols
  - E.g. downloading configuration and software via TFTP (Cisco)
- Other vendors have been found to use static cryptographic secrets
- Cisco VoIP Phones can be customized (i.e. re-programmed) using XML services running on the phone
- Critical vulnerabilities are constantly discovered, but enterprise VoIP networks are rarely updated
  - Not even when there is a direct risk to the Active Directory*

* http://www.cisco.com/warp/public/707/cisco-sa-20090311-cucmpab.shtml

Private Branch Exchanges (PBX)

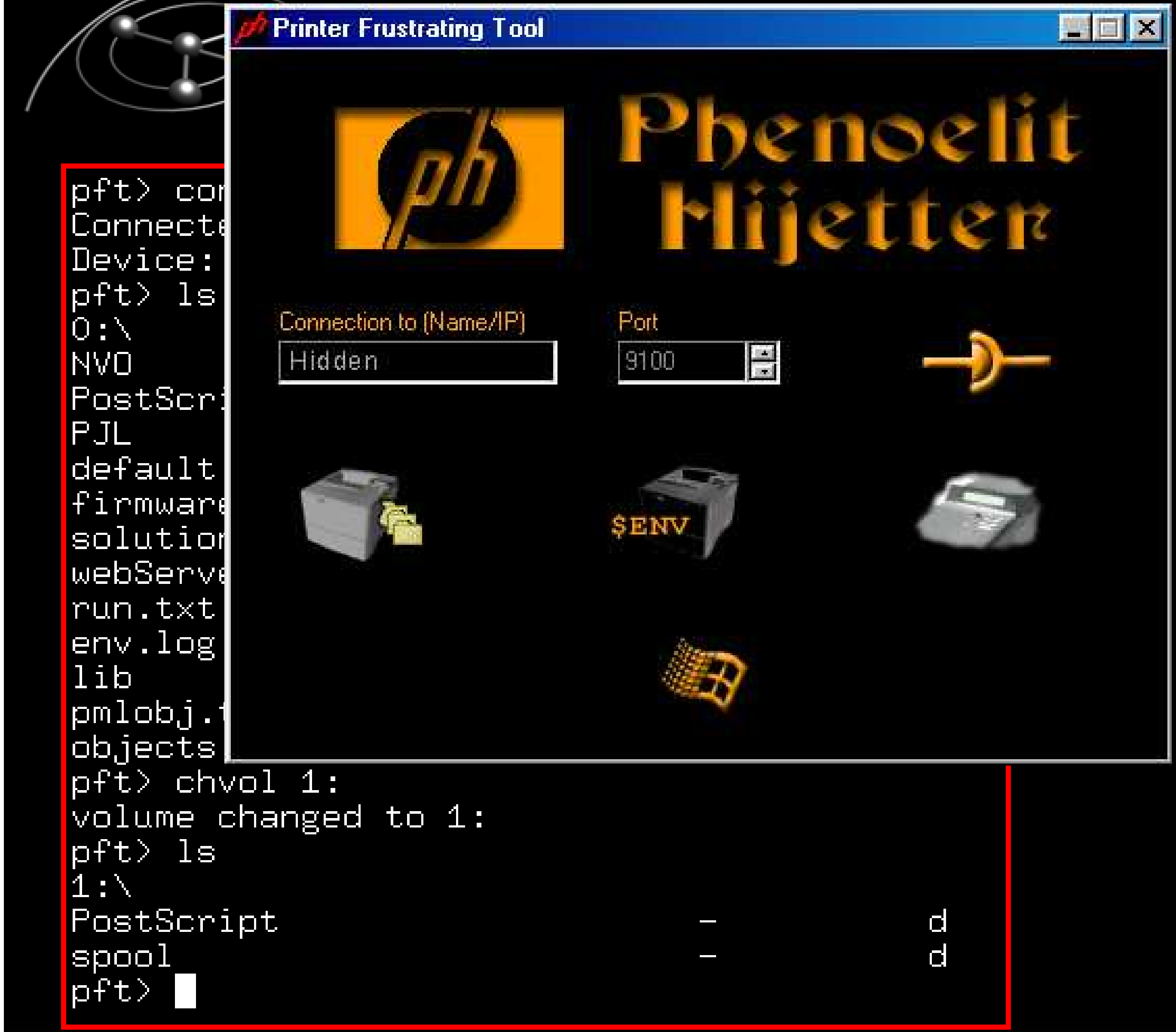
- PBX installations used to be isolated from the network
  - Large PBX installations (e.g. Siemens HiPath) changed that back in the 90's already, but only for management
- Modern PBX are software stacks on regular computers
  - Affected by vulnerabilities and known exploitation methods
  - Often not updated, as the software is only certified to run on a unmodified (i.e. not patched) version of the operating system
- PBXs receive less attention since VoIP was introduced
  - Penetration tests of PBX installations a decade ago often found them locked down
  - Penetration tests of PBX installations today often find them without any passwords
    - Allows to configure a dial-in port with PPP and hereby a new network access point
- Very few tests of PBX software for security issues

Embedded Storage

- Out of the box workgroup Network Attached Storage (NAS) solutions are commonly found in enterprise environments
  - People get around the quota limitations of IT managed servers
- The devices are made by storage vendors
  - Little to no security testing
  - Encryption provided is meaningless, since the key is stored on the same device in most cases
- Even if the devices were secure, the workgroup will share the entire storage on the network without authentication
  - Authentication would require a link to central IT

Printers

- Printers are guaranteed to be present in enterprise networks
  - They handle most critical information
  - They are network connected
- Attacks on printers, primarily Hewlett-Packard, published in 2002
  - Remote file system access and document retrieval
  - Software installation on printer web server
- In 2006, Brendan O'Connor presented extensive information on breaking into Xerox WorkCentre™ printers
  - Accessing authentication credentials from users printing
  - Document copy and retrieval
  - Printing a paper clip on every document



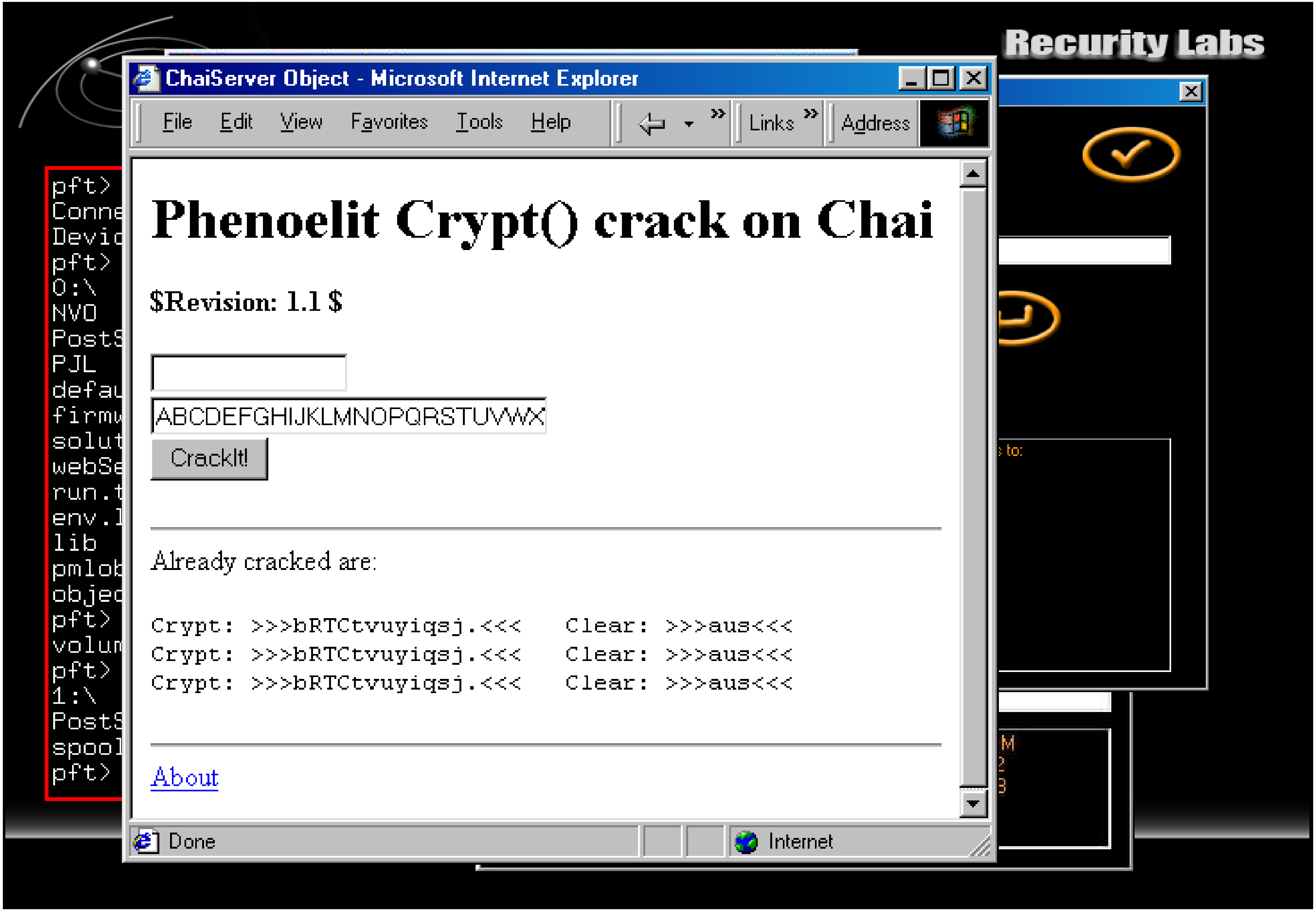
Printer Frustrating Tool

Phenoelit Hijetter

Connection to (Name/IP): Hidden

Port: 9100

```
pft> cor
Connecte
Device:
pft> ls
0:\
NVO
PostScri
PJL
default
firmware
solution
webServe
run.txt
env.log
lib
pmlobj.t
objects
pft> chvol 1:
volume changed to 1:
pft> ls
1:\
PostScript                          -          d
spool                               -          d
pft> 
```



Recurity Labs
ChaiServer Object - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Address
Done
Internet

```
pft>
Conne
Devic
pft>
0:\
NVO
PostS
PJL
defau
firmw
solut
webSe
run.t
env.l
lib
pmlob
objec
pft>
volum
pft>
1:\
PostS
spool
pft>
```

Phenoelit Crypt() crack on Chai

$Revision: 1.1 $

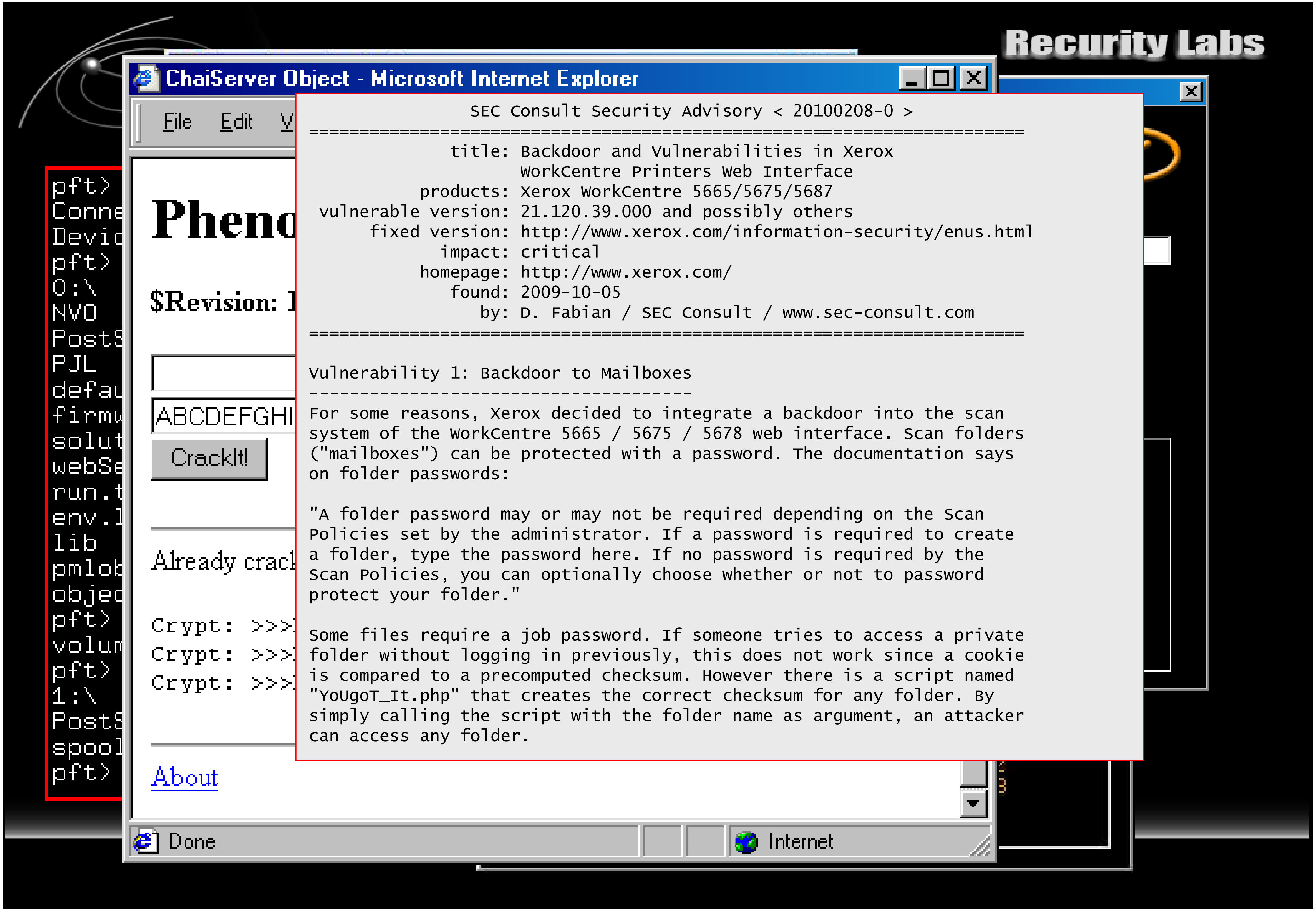
ABCDEFGHIJKLMNOPQRSTUVWX

CrackIt!

Already cracked are:

```
Crypt: >>>bRTCtvuyiqsj.<<<   Clear: >>>aus<<<
Crypt: >>>bRTCtvuyiqsj.<<<   Clear: >>>aus<<<
Crypt: >>>bRTCtvuyiqsj.<<<   Clear: >>>aus<<<
```

About



```
pft>
Conne
Devic
pft>
0:\
NVO
PostS
PJL
defau
firmw
solut
webSe
run.t
env.l
lib
pmlob
objec
pft>
volum
pft>
1:\
PostS
spool
pft>
```

```
Crypt: >>>
Crypt: >>>
Crypt: >>>
```

```
                 SEC Consult Security Advisory < 20100208-0 >
=======================================================================
                  title: Backdoor and Vulnerabilities in Xerox
                         WorkCentre Printers Web Interface
               products: Xerox WorkCentre 5665/5675/5687
     vulnerable version: 21.120.39.000 and possibly others
          fixed version: http://www.xerox.com/information-security/enus.html
                 impact: critical
               homepage: http://www.xerox.com/
                  found: 2009-10-05
                     by: D. Fabian / SEC Consult / www.sec-consult.com
=======================================================================

Vulnerability 1: Backdoor to Mailboxes
--------------------------------------
For some reasons, Xerox decided to integrate a backdoor into the scan
system of the WorkCentre 5665 / 5675 / 5678 web interface. Scan folders
("mailboxes") can be protected with a password. The documentation says
on folder passwords:

"A folder password may or may not be required depending on the Scan
Policies set by the administrator. If a password is required to create
a folder, type the password here. If no password is required by the
Scan Policies, you can optionally choose whether or not to password
protect your folder."

Some files require a job password. If someone tries to access a private
folder without logging in previously, this does not work since a cookie
is compared to a precomputed checksum. However there is a script named
"YoUgoT_It.php" that creates the correct checksum for any folder. By
simply calling the script with the folder name as argument, an attacker
can access any folder.
```

Printers & Copiers

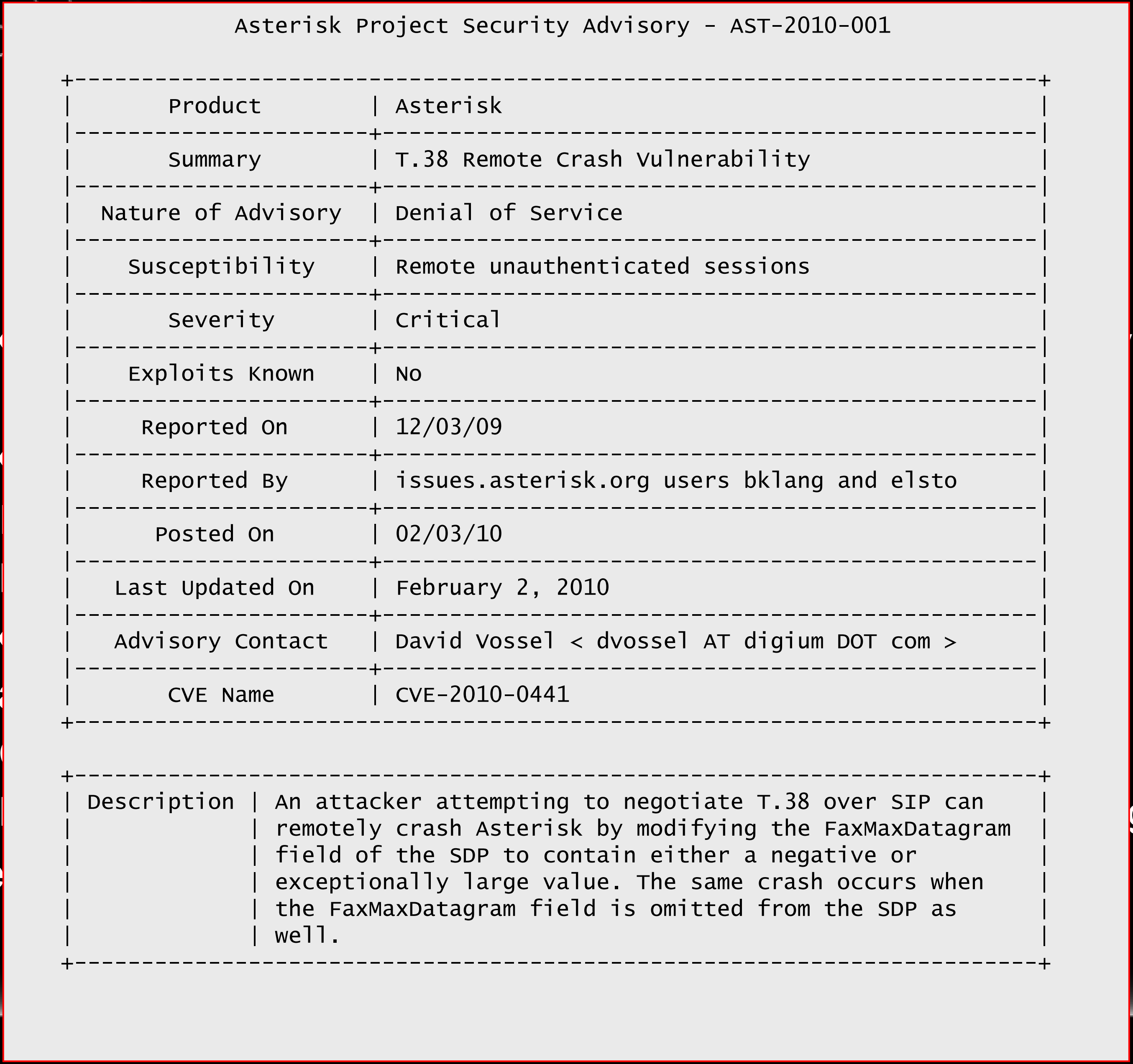
- Development cost of embedded firmware drives most vendors to embedded Linux environments
  - This turns the “embedded system” into a Linux server
- Software on printers and similar devices is rarely or never security tested before roll-out
  - It is also rarely or never updated
- The printers we work with today are security-wise the same as unmanaged Linux (or similar) servers on the network

FAX Machines and Servers

- FAX is in many legislations still the fastest transport of legally binding documents
- FAX machines used to be very solid devices
  - Invalid input wasn’t an exception but the rule
  - FAX codecs were developed with that in mind
- FAX servers implement the same functionality, but with a PC attitude towards malformed data
  - Crafted input exposes vulnerabilities in the codecs
  - Email integration simplifies the process to attack FAX servers significantly
- There is very little research on the topic published

FAX

- FAX … binding doc…
- FAX
  - …
  - …
- FAX … attitude towa…
  - …
  - …gnificantly
- The…



```
              Asterisk Project Security Advisory - AST-2010-001

+------------------------------------------------------------------------+
|       Product        | Asterisk                                        |
|----------------------+-------------------------------------------------|
|       Summary        | T.38 Remote Crash Vulnerability                 |
|----------------------+-------------------------------------------------|
|  Nature of Advisory  | Denial of Service                               |
|----------------------+-------------------------------------------------|
|    Susceptibility    | Remote unauthenticated sessions                 |
|----------------------+-------------------------------------------------|
|       Severity       | Critical                                        |
|----------------------+-------------------------------------------------|
|    Exploits Known    | No                                              |
|----------------------+-------------------------------------------------|
|     Reported On      | 12/03/09                                        |
|----------------------+-------------------------------------------------|
|     Reported By      | issues.asterisk.org users bklang and elsto      |
|----------------------+-------------------------------------------------|
|      Posted On       | 02/03/10                                        |
|----------------------+-------------------------------------------------|
|   Last Updated On    | February 2, 2010                                |
|----------------------+-------------------------------------------------|
|   Advisory Contact   | David Vossel < dvossel AT digium DOT com >      |
|----------------------+-------------------------------------------------|
|       CVE Name       | CVE-2010-0441                                   |
+------------------------------------------------------------------------+

+------------------------------------------------------------------------+
| Description | An attacker attempting to negotiate T.38 over SIP can    |
|             | remotely crash Asterisk by modifying the FaxMaxDatagram  |
|             | field of the SDP to contain either a negative or         |
|             | exceptionally large value. The same crash occurs when    |
|             | the FaxMaxDatagram field is omitted from the SDP as      |
|             | well.                                                    |
+------------------------------------------------------------------------+
```

Mobile Phones and Enterprise Integration

- Smart Phones are a business requirement today
  - They must have access to messaging, contacts and calendar
  - They shall have the capabilities to view and edit common office documents
- The major players in this market follow different approaches
  - RIM BlackBerry uses a centralized Blackberry Enterprise Server
  - Microsoft Windows Mobile integrates the smart phone in the Windows network
  - Apple just makes every manager wanting an iPhone

Blackberry: secure devices, infrastructure at risk

- The RIM device and transport security model is pretty solid
- The Achilles’ heel is the attachment conversion service on the BES
    - Slow but steady stream of newly discovered vulnerabilities
- Most installations do not separate the service from the BES
    - Access to all key material
    - Impersonating the attacked enterprise towards RIM
    - Rolling out of “trusted” applications to all handhelds
    - Administrator access to connected Exchange servers

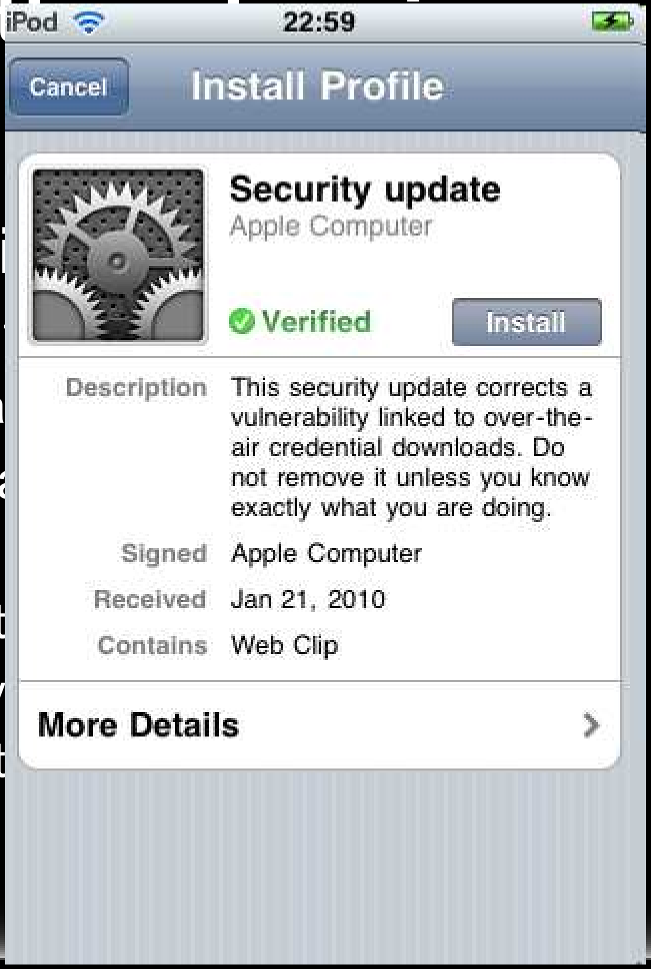
Apple iPhone: just not made for the enterprise

- All control is in Apple’s hand
- Integration features constantly show critical vulnerabilities
  - Devices ignored security policies for VPNs to not store the password
    - Apple did not provide a fix, suggested upgrade to new device type
  - “mobileconfig” deployment settings accept arbitrary certificates*
    - Certificate chain validates to any certificate in the certificate store
    - Signature by any of the 224 trusted root certificates accepted
    - Reconfiguration of the iPhone’s HTTP proxy settings to arbitrary values
    - Reconfiguration of the iPhone’s certificate store

* http://cryptopath.wordpress.com/2010/01/29/iphone-certificate-flaws/

Apple iPhone: just not made for t

- All control is in Apple’s hand
- Integration features constantly show cri
  - Devices ignored security policies for VPNs
    - Apple did not provide a fix, suggested upgra
  - “mobileconfig” deployment settings accept a
    - Certificate chain validates to any certificate i
    - Signature by any of the 224 trusted root cert
    - Reconfiguration of the iPhone’s HTTP proxy
    - Reconfiguration of the iPhone’s certificate st



Security update
Apple Computer
✓ Verified
Install

Description: This security update corrects a vulnerability linked to over-the-air credential downloads. Do not remove it unless you know exactly what you are doing.
Signed: Apple Computer
Received: Jan 21, 2010
Contains: Web Clip

More Details

* http://cryptopath.wordpress.com/2010/01/29/iphone-certificate-flaws/

How These Attacks Are Used

Corporate Espionage for Small Coin

Condition:

- Some minor part of the network uses a satellite link and GRE
- People use printers

➔Cheap infiltration via satellite connection

  - Attacker installs document copy program on printers
    - Gains access to all documents that get printed
  - Attacker installs password capture program on larger printers
    - Gains access to Active Directory accounts used for print accounting

Getting Your Boss's Password

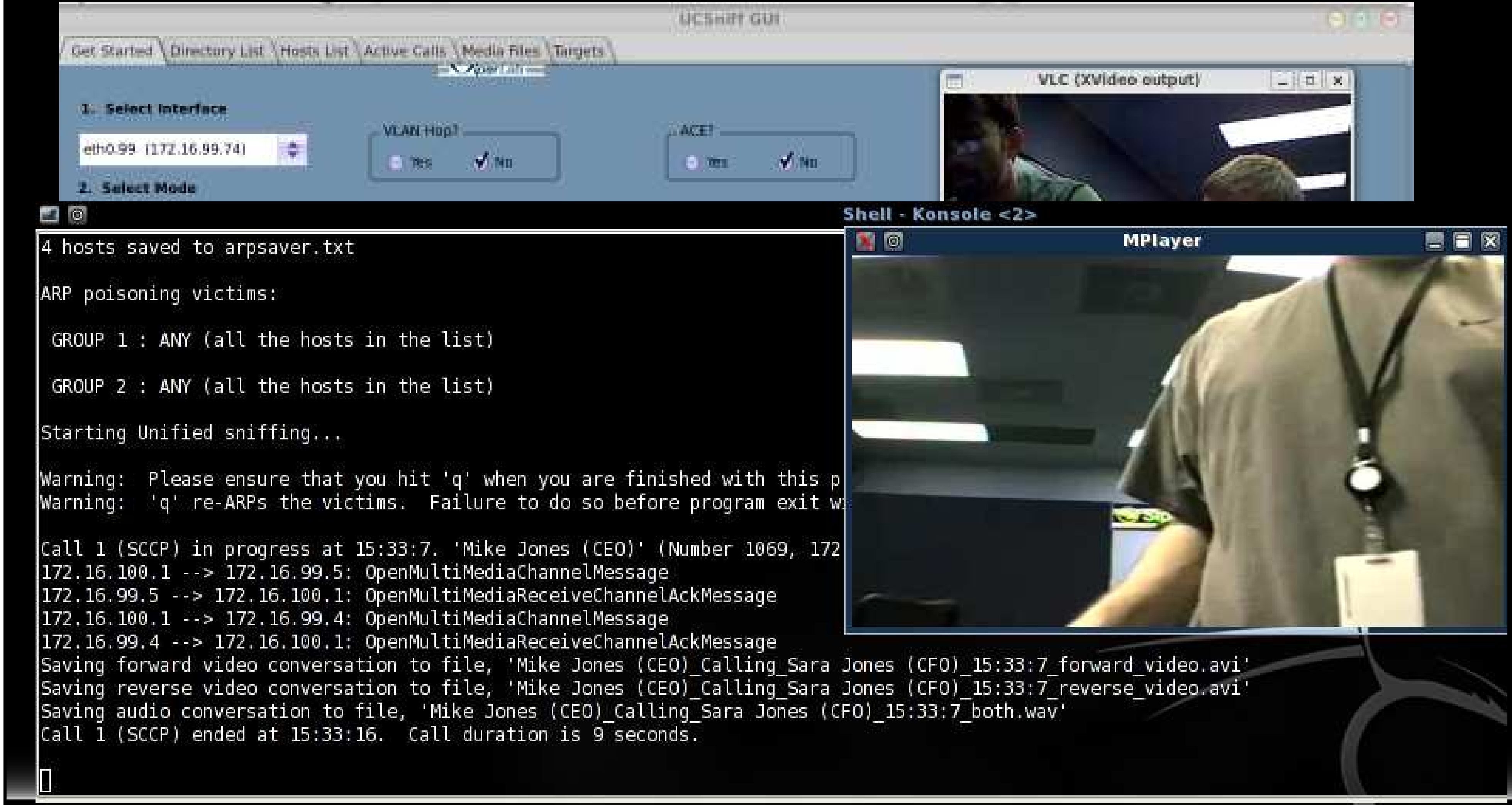
Condition:

- The person to be targeted sits in the same network
- Routers with HSRP

➔Stealing the virtual router IP address in the morning

- Sniffing all the traffic from clients to servers (unidirectional)
  - Getting all passwords that are transmitted in clear text
- Finding new systems that only your boss uses

How These Attacks Are Used



1. Select Interface

eth0.99 (172.16.99.74)

VLAN Hop? ○ Yes ✓ No

ACE? ○ Yes ✓ No

2. Select Mode

```
4 hosts saved to arpsaver.txt

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)

Starting Unified sniffing...

Warning:  Please ensure that you hit 'q' when you are finished with this p
Warning:  'q' re-ARPs the victims.  Failure to do so before program exit wi

Call 1 (SCCP) in progress at 15:33:7. 'Mike Jones (CEO)' (Number 1069, 172
172.16.100.1 --> 172.16.99.5: OpenMultiMediaChannelMessage
172.16.99.5 --> 172.16.100.1: OpenMultiMediaReceiveChannelAckMessage
172.16.100.1 --> 172.16.99.4: OpenMultiMediaChannelMessage
172.16.99.4 --> 172.16.100.1: OpenMultiMediaReceiveChannelAckMessage
Saving forward video conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_forward_video.avi'
Saving reverse video conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_reverse_video.avi'
Saving audio conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_both.wav'
Call 1 (SCCP) ended at 15:33:16.  Call duration is 9 seconds.
```

* http://ucsniff.sourceforge.net/

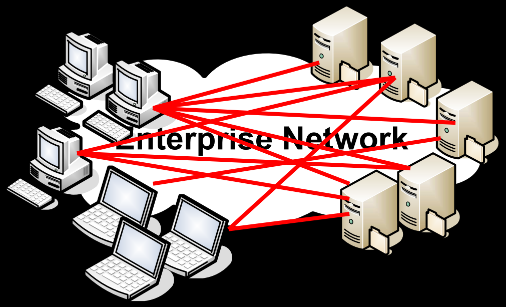
Protection Measures

Security from the Ground Up

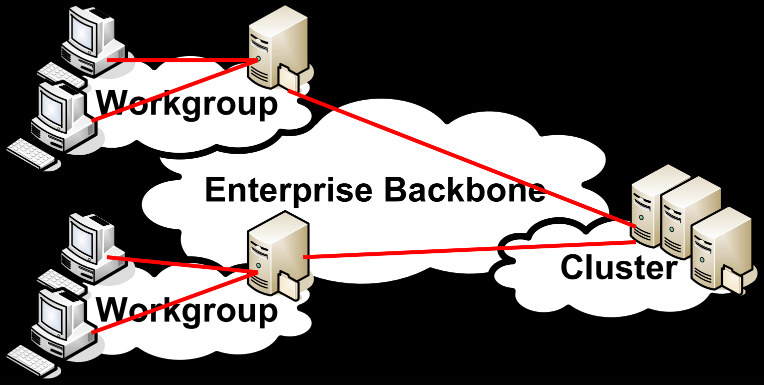
- Secure switch configurations
  - Disabling advertisement services (e.g. CDP)
  - Port configuration, distinguishing switch links from user ports
  - Centrally managed Port Security
  - Centrally managed, non-dynamic VLAN configuration
- Secure router configurations
  - Only use protected dynamic routing and high availability protocols
    - E.g. VRRP with MD5 instead of HSRP
  - Minimize services run on routers
  - Do not turn routers into VoIP servers

Structured Networks

- Flat networks are harder to control
  - Any-to-any communication cannot be controlled or monitored efficiently



- Structured networks allow control over the communication relations
  - Internal tracking becomes possible
  - Dramatically simplifies troubleshooting



Review Your WAN Links

- Only networks physically located on your premises are secure
- Wide Area Network links can always be controlled and monitored by someone else
  - MPLS network
  - Leased lines
  - Satellite links
- Consider encrypting WAN links
  - Most modern routing equipment can deal with the load
- Review the security SLAs with your WAN link provider

Think Security when Purchasing Equipment

- Embedded System Vendor Checklist:
  - Does the vendor have any track record in securing their product?
  - Is a security contact for researches available?
  - Are firmware updates available fixing security flaws?
  - Are advisories published for flaws identified?
  - Is the software update mechanism manageable?
- Add software update to service contracts and SLAs
  - When service technician is at your site, require software update
  - When a software update is released, require notification

Stop Buying Appliances

- Product is available as software solution or appliance? Opt for the software version!
  - Appliances are easily forgotten
  - The vendor will not manage the entire software stack
  - Staff will feel zero responsibility for the appliance
- Virtual appliances are not any better
  - Unless the have an integrated update mechanism for the entire software stack

Prevent Shadow-IT Creep

- Ensure that business requirements are met
    - Do not impose arbitrary restrictions where hardware is cheap
    - Proactively monitor resource utilization on central IT
    - Plan services with plenty of head room for the future
- Ensure that every system has an owner
    - Shadow-IT must have the same responsibilities as central IT
    - Measure everyone by the same standards
        - If Shadow-IT works, let them have it
- Ensure that network architecture considers Shadow-IT

The Patching Problem

- Most embedded systems cannot be patched
  - Complete firmware replacements are the norm
- Complete software updates often cause functionality failures
  - Cisco IOS is notorious for this problem
  - Other network equipment vendors have similar problems
- Software updates often cause configuration loss
  - Remote devices no longer manageable
  - Functional differences for the users before and after update
- Security fixes cause other products to no longer work
  - Third party products relied on a security issue to function properly

Patch / Update Strategies

- Ensure product lifecycle guarantees software updates
  - At least until “End of Life”
- Responsibility for all embedded systems of one type should be with the same group
  - Encourages keeping all devices on the same software version
    - Simplifies update testing
  - Ensures that responsibilities and fulfillment are controllable
- Open support cases with the vendor when updates fail
  - That’s what the support contract is for
  - It’s not a minor issue, it’s a failure of a critical function

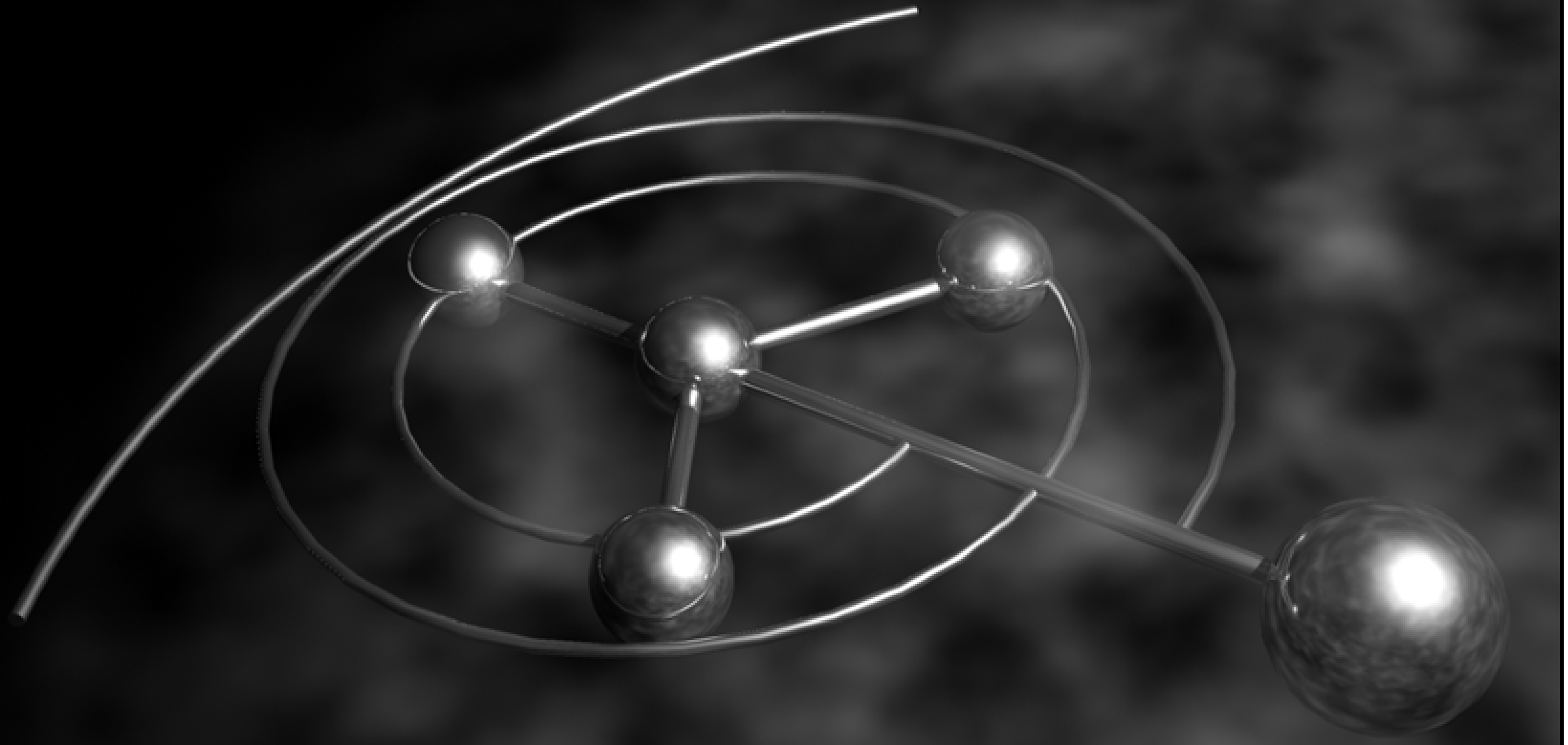
Summary

Summary

- There is more to the enterprise network than servers and PCs
- There is a heterogenic embedded system landscape
    - It is challenging to manage
    - It is easy to misuse
- Customers must exercise their power over embedded systems vendors
    - Require software quality and security standards
    - Require solid update paths for embedded system software
- Realize that all those little devices are computers in your network
    - They need to be managed and maintained

Thank you!

Questions?



Felix ‘FX’ Lindner, Fabian ‘fabs’ Yamaguchi,
Recurity Labs GmbH