GATES, GUARDS, AND GADGETS: AN INTRODUCTION TO THE PHYSICAL SECURITY OF IT

Kai Axford, MBA, CPP, CISSP, ACE
Manager, IT Security Services
Accretive Solutions
kaxford@accretivesolutions.com
THIS SESSION **WILL NOT**…

- Tell you to “lock your PC, when you leave”
- Be dull and dry
- Turn you into a physical security guru
THIS SESSION WILL...

• Serve as an intro to aspects of Physical Security you may not have previously considered. Remember *convergence*!
• Cover a lot of topics and controls
• Give you a chance to see (and feel) some of the controls
• Allow you to develop and discuss the topic intelligently with your physical security teams.
WHY DO YOU EVEN CARE?

• Because the physical breach is only a means to an end....

• If I can bypass your 17 Internet facing, application layer firewalls, it cuts down on the amount of “leet’ness” I need to possess.

• Physical access is KEY.
Spy Development™ - Products - Disguised transmitters

DU-75

USB cable UHF transmitter. When plugged to a USB port the cable works as usual and the transmitter inside the cable transmits conversations or any sound to a distant receiver. No batteries needed. The transmitter works as long as it remains plugged to a USB port. With our Automatic Gain Control system it is able to pick up a whisper up to 40 feet away from the transmitter microphone as clearly as loud speech near it. Exceptional audio performance.

Features

- USB cable works and looks as usual.
- Nothing unusual can be found.
- Powered by a USB port, no battery required for the transmitter.
- Only one end of the cable needs to be plugged to provide power.
- Extremely sensitive built-in microphone.
- Automatic microphone gain control.
- Crystal frequency control.

Price: $340.00 £165.00

Available connector types: A-B, A-miniB.
You may provide your requirement during checkout.

Available color: Black

Technical data

Length: 1.8 meter (6 feet)
Interface: USB 2.0, USB 1.1
Range: 500 meters (1700 feet) in open field
- 200 meters (700 feet) in a city
Power requirement: USB port
Output power: 20 mW
Frequency: 433 - 434 MHz (300 - 434 MHz on demand)
Modulation type: NFM
Operating temperature: -20 to +60 °C (-4 to 140 °F)

* each UHF transmitter works on a separate frequency channel so several of them can be used simultaneously.
Pwn Plug

SheevaPlug microserver loaded with pentesting goodness!

Just plug it in!

Automatically shovels a reverse persistent shell to your external pentest box over SSH!

:: Bypasses strict egress firewall filters!
:: Unpingable! No open ports! Virtually invisible!
:: Preloaded with Ubuntu, Metasploit, nmap, dsniff, nikto, scapy, ettercap, medusa, and more!
:: 4.3 x 2.7 x 1.9 inches! 2.3 watts when idle!
:: 1.2GHz ARM cpu with 512M SDRAM, 512M flash HDD!
:: Gbit NIC, USB, SD card ports! Optional wireless!

Price: $180 USD
<DEMO>

1337 PLUG PWNAGE
AGENDA

• You don’t know what you don’t know…
• No such thing as “de-perimeterization”…
• In it to win it….
• No place like 127.0.0.1…
AGENDA

• You don’t know what you don’t know…
• No such thing as “de-perimeterization”…
• In it to win it….
• No place like 127.0.0.1…
A QUICK REVIEW OF DEFENSE IN DEPTH

Physical Security

Policy, Procedure, and Awareness

Perimeter

Networks

Host

Application

Data
WHAT IS “PHYSICAL SECURITY”?

- The part of security concerned with the measures/concepts to safeguard personnel; to prevent unauthorized access to equipment, installations, materiel, and documents; and to safeguard them against espionage, sabotage, damage, and theft.¹

PHYSICAL SECURITY CONCEPTS: 4D

- Detect
- Delay
- Deter
- Deny
YOUR PHYSICAL IT SECURITY FUNCTION SHOULD WORK WITH

- Corporate Security
- IT Security
- Network Security
- Law Enforcement
- Private Security Consultants or Staff
PHYSICAL SECURITY STARTS WITH A PLAN

- Security Assessment
- Overview and Mission Statement
- Organizational Responsibilities
- Duty Officers
- Contact Lists
- Security Procedures for
  - Datacenter
  - Department Servers
  - Laptops
- …and many more!
AGENDA

• You don’t know what you don’t know…

• No such thing as “de-perimeterization” = THE PERIMETER
  • Site Selection
  • Barrier Planning
    • Structural Barriers
    • Fences and Wire
    • …and Gadgets!!

• In it to win it….

• No place like 127.0.0.1…
THE PERIMETER

SITE SELECTION

• Build New or Use Existing
• Think CPTED!
• Three Rule of Real Estate = Location….Location….Location
  • City? Inner city? Wooded area? Open Space area?
THE PERIMETER
BARRIER PLANNING

• What most people think of when we say “physical security”.
• Defined as “a natural or manufactured obstacle to the movement of persons, animals, vehicles or materials”.
• Designed to stop 3 types of penetration:
  • By Accident – “Oops! Wrong place.”
  • By Force – “Here I come! Try and stop me!”
  • By Stealth – “Shhhh……I’m a ninja.”
• Do your threat assessment! There is no such thing as a “foolproof barrier”.
  • It’s not “if”….it’s “when”.


THE PERIMETER

BARRIER PLANNING – STRUCTURAL BARRIERS

• What most people think of when we say “physical security”.
• Includes things like concrete barriers (aka “cement planters”) or bollards.
• But do they work? Do they delay or deter?
  • Concrete barrier?
  • Bollards?
THE PERIMETER
BARRIER PLANNING – FENCES AND WIRES

• Chain Link
  • No less than 7 feet
  • 9 Gauge or heavier
  • No more than 2” between mesh openings
  • Weld your hardware!
  • Include a “top guard”.

• Barbed Wire is **not** Barbed Tape! Think Razor Ribbon!

• Wrought Iron looks much better
  • …but does it work?
THE PERIMETER
BARRIER PLANNING – GADGETS

• Under vehicle inspection systems
• License plate readers
BAD GUY BREAK
WHAT ARE THE BAD GUYS USING?

- Blueprints
  - This was made public.
- Satellite imagery
  - Nice photos of your facility.
  - Does anyone know what this place is?
AGENDA

• You don’t know what you don’t know…
• No such thing as “de-perimeterization”…
• In it to win it = THE MIDDLE LAYER
  • Think “INSIDE the box!”
  • Doors
  • Windows
  • What did you not think about?
• No place like 127.0.0.1…
THE MIDDLE LAYER

• Think "INSIDE the box!"
• Doors
• Windows
• What did you not think about?
MIDDLE LAYER

THINK “INSIDE THE BOX”

• Everything is better in 3-D!
  • You must consider top and bottom...not just the four walls.
  • It’s not a tough “mission”, nor is it an “impossible” task.
  • It’s not fantasy. This stuff really happens.
MIDDLE LAYER

DOORS

• Doors are obvious threat vectors and need to be reinforced
• Consider electrical and mechanical means
• Man traps, turnstiles, etc. are also very effective

http://www.turnstiles.us/
MIDDLE LAYER

WINDOWS (AKA “GLAZING”)

• Tempered Glass v. Laminated Glass
• Plastic v. Acrylic v. Glass
• Also consider bars, heavy steel mesh, etc.
• Any window less than 18’ from the ground is at risk
• A bad “Apple” makes the point…
MIDDLE LAYER
WHAT DID YOU NOT THINK ABOUT?

• Did you forget….
  • HVAC access
  • Sidewalk elevators
  • Utility tunnels
  • Storm sewers
  • Storm doors
  • Piers, docks, and wharves
• Because these guys probably did not…
AGENDA

• You don’t know what you don’t know…
• No such thing as “de-perimeterization”…
• In it to win it….
• No place like 127.0.0.1 = THE INNER LAYER
  • IP Surveillance
  • Alarms and Sensors
  • Locks
  • Safes & Vaults
THE PERIMETER
IP SURVEILLANCE

• It’s called **IP** surveillance…so what’s the impact on your network?
  • Is the physical security function really going to run their own cable and hubs?
  • Or will they just “piggyback” on yours?
• Video analytics are the true rockstars.
<DEMO>

IP VIDEO SURVEILLANCE
THE PERIMETER
IP SURVEILLANCE CONSIDERATIONS

- **Hardware**
  - Field of View
  - Power Source (PoE)
  - Resolution (VGA, Megapixel)
  - Day/Night
  - Scalability
  - Camera placement

- **Network**
  - Bandwidth
  - Frames per Second (FPS)
  - Storage requirements

- **Software**
  - Video analytics
INNER LAYER
ALARMS AND SENSORS

• Electro-Mechanical
  • Metallic Foil
  • Magnetic Switches
  • Pressure Mats

• Volumetric
  • Capacitance
  • Vibration
  • Microwave
  • Ultrasonic
  • Passive IR
  • Photo Electric
INNER LAYER
LOCKS

- They are only delaying mechanisms
- No lock is perfect
- Various types
  - Wafer locks
  - Pin Tumbler locks
  - Cipher locks
  - Code and card operated locks
  - Padlocks
INNER LAYER

LOCKS: WHY DO YOU CARE?

• It’s not guys like this who will breach your perimeter….

• …more likely it’s a guy like Jesse.

• A key control program is critical!

• Change locks and padlocks every 12 months or less.
INNER LAYER
SAFES AND VAULTS

- Categories
  - Fire Resistant
  - Burglary/Robbery Sensitive
- UL provides safe ratings for both

<table>
<thead>
<tr>
<th>Classification</th>
<th>Temperature</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>350-4</td>
<td>2000°F</td>
<td>4 hr</td>
</tr>
<tr>
<td>350-2</td>
<td>1850°F</td>
<td>2 hr</td>
</tr>
<tr>
<td>350-1</td>
<td>1700°F</td>
<td>1 hr</td>
</tr>
<tr>
<td>150-4</td>
<td>2000°F</td>
<td>4 hr</td>
</tr>
<tr>
<td>150-2</td>
<td>1850°F</td>
<td>2 hr</td>
</tr>
<tr>
<td>150-1</td>
<td>1700°F</td>
<td>1 hr</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification</th>
<th>Resistance</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>TL-15</td>
<td>Tool</td>
<td>15 min</td>
</tr>
<tr>
<td>TL-30</td>
<td>Tool</td>
<td>30 min</td>
</tr>
<tr>
<td>TRTL-30</td>
<td>Tool/Torch</td>
<td>30 min</td>
</tr>
<tr>
<td>TRTL-30x6</td>
<td>Tool/Torch</td>
<td>30 min</td>
</tr>
<tr>
<td>TXTL-60</td>
<td>Tool/Torch/Explosive</td>
<td>60 min</td>
</tr>
</tbody>
</table>
SUMMARY

- Detect, Delay, Deny, Deter
- Perimeter, Middle, Inner Layers
- Work together. You have a common goal.
- Stay alert!
  - (especially if you see some guy buying 125 pounds of ANFO and 62 pounds of steel nuts!)
TRACK RESOURCES

- PwnPlug – Grep8000 - Rocket Bear Labs
  - [http://grep8000.blogspot.com](http://grep8000.blogspot.com)
- Deviant Ollam – Lockpick Sage
  - [http://deviating.net/lockpicking](http://deviating.net/lockpicking)
- The Open Organization of Lockpickers (TOOOL)
  - [http://toool.us](http://toool.us)

- Thanks to these vendors for their support!
  - RazorRibbon - [http://www.razorribbon.com](http://www.razorribbon.com)
  - ShatterGARD - [http://www.shattergard.com](http://www.shattergard.com)
QUESTIONS?

Kai Axford, MBA, CPP, CISSP, ACE
Manager, IT Security Services
Accretive Solutions
kaxford@accretivesolutions.com