



INFRAGARD of Middle Tennessee



Guarding the Nation's Infrastructure

A Demonstration in the Need for Layered Security

Presented by:

Bryant G. Tow

InfraGard National Members Alliance

Director / Vice President

Director of Security –GIS North America -

UNISYS

Imagine it • Done •

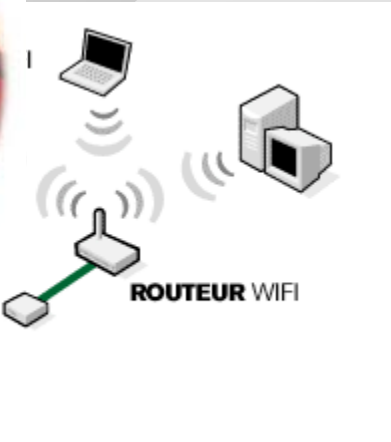
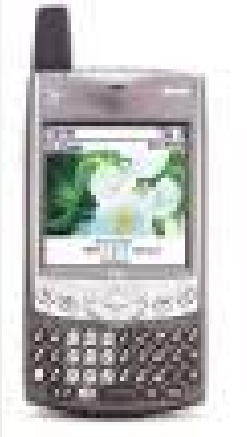
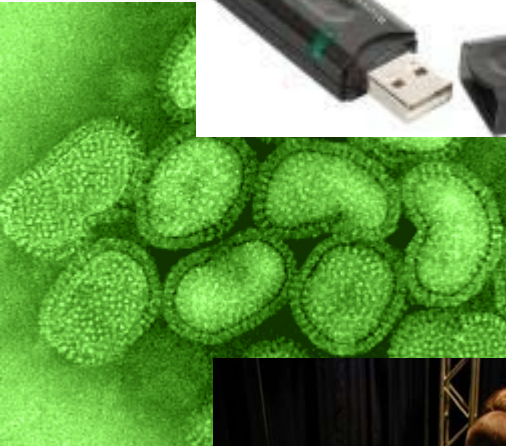
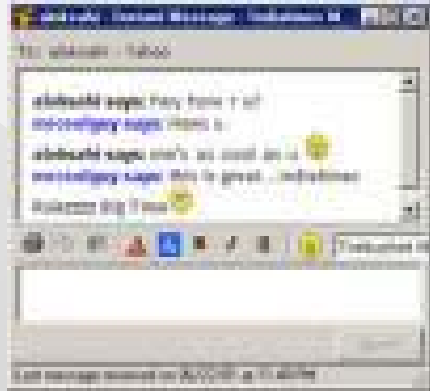
- > Systems Integration.
- > Outsourcing.
- > Infrastructure.
- > Server Technology.
- > Consulting.

Today's Agenda

- > New Network Entry Points
- > Penetration Demonstration & Root Kit Installation
- > Wireless Network Compromise
- > Phishing Demonstration
- > Security Strategy and Planning



New Network Entry Points



Penetration Demonstration

(Disclaimer !)*

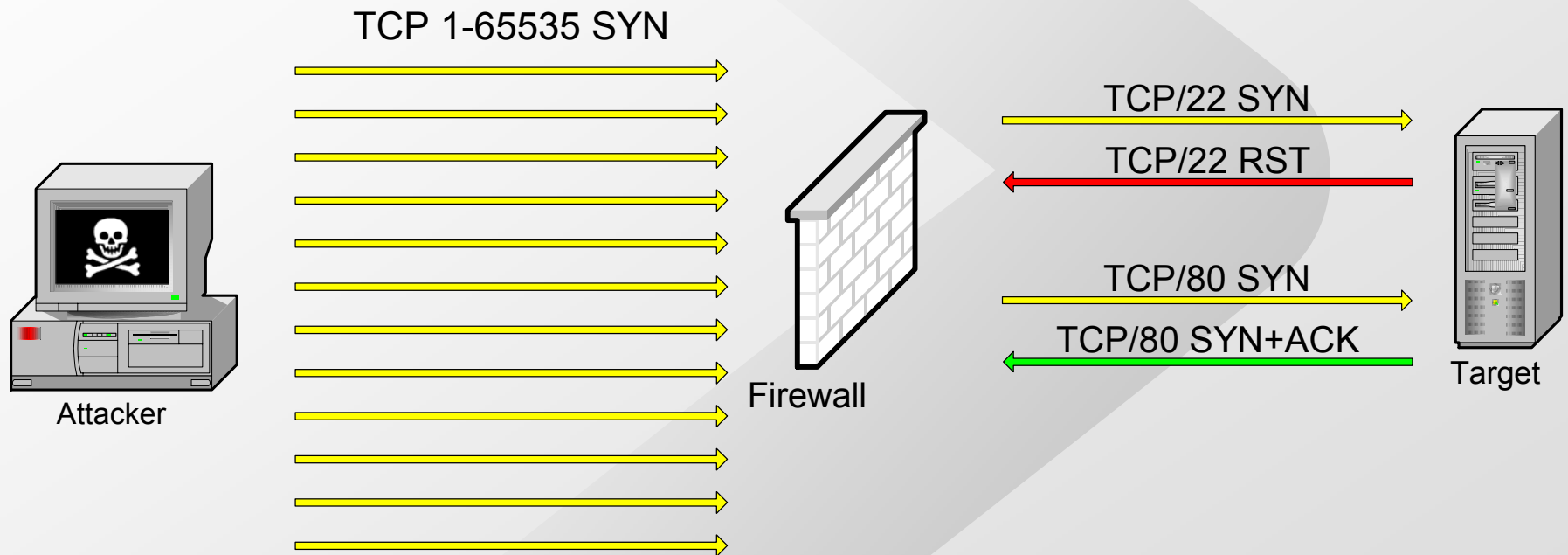


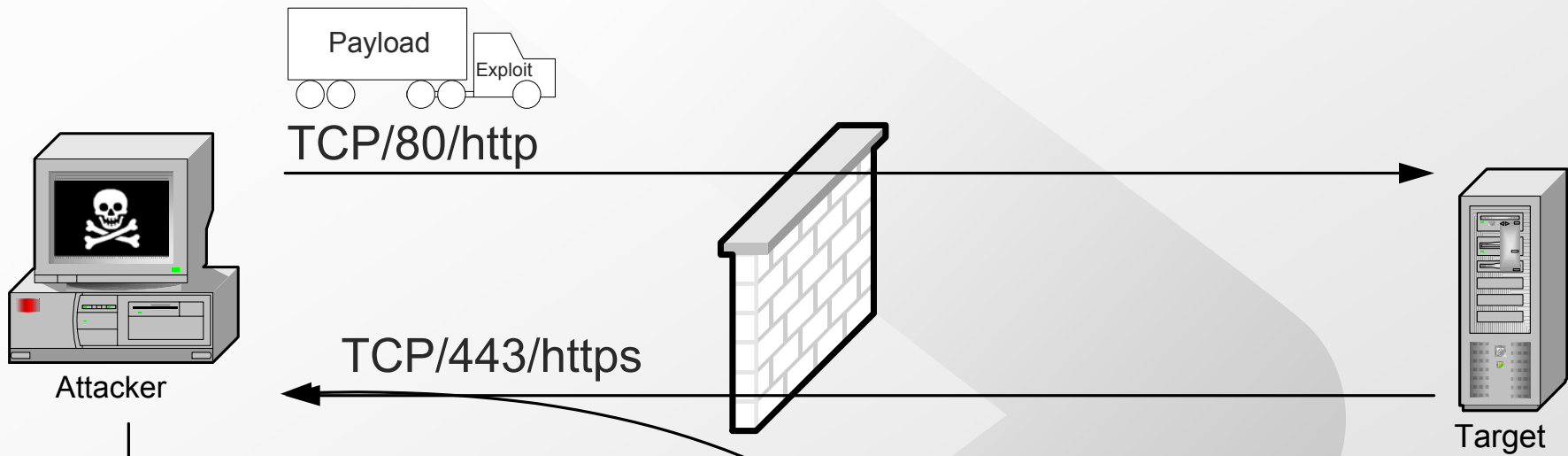
Exploiting a Vulnerable Server

- 1. Profile a target set**
- 2. Identify available services**
- 3. Find one or more canned exploits for any observed platform/service combinations**
- 4. Try them all, see what sticks**
- 5. Penetrate and Radiate**



Profiling the Target





```
C:\WINNT\system32\cmd.exe
C:\Documents and Settings\Administrator>_
```

```
C:\WINNT\system32\cmd.exe
C:\Documents and Settings\Administrator>_
```



Mitigation: Penetration & Root Kit

Underlying Causes

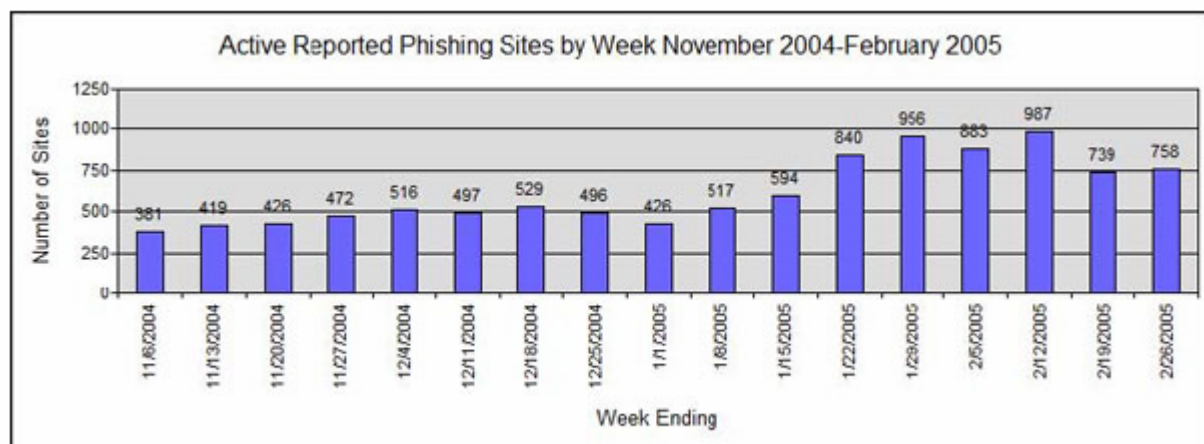
- Technical
 - The system was missing a patch
 - No visibility as to the state of system patches
- Operational
 - The systems management team did not detect a machine was missing a patch
 - No internal assessment processes to detect a vulnerable host
- Strategy
 - Any existing efforts to manage patches or detect vulnerable systems did not take into account this one particular host – strategies should apply controls effectively across all resources



Phishing



Phishing Statistics



Graphic courtesy Tumbleweed Communications

Recent Phishing Attacks:

Phish Alerts Courtesy Tumbleweed Communications' Message Protection Lab

- ◆ 20-04-05 - Barclays - 'Barclays Verification Service'
- ◆ 19-04-05 - Bank Of America - 'Online Banking Alert (Change of Email Address)'
- ◆ 18-04-05 - eBay - 'eBay Verify Accounts'
- ◆ 14-04-05 - Associated Bank - 'Online Alert: online account is blocked'
- ◆ 11-04-05 - Union Planters bank - 'Customer Alerting Service - Account is on hold'
- ◆ 07-04-05 - Comcast - 'Comcast account reactivation'
- ◆ 01-04-05 - Paypal - 'Yout PayPal account will be suspended'

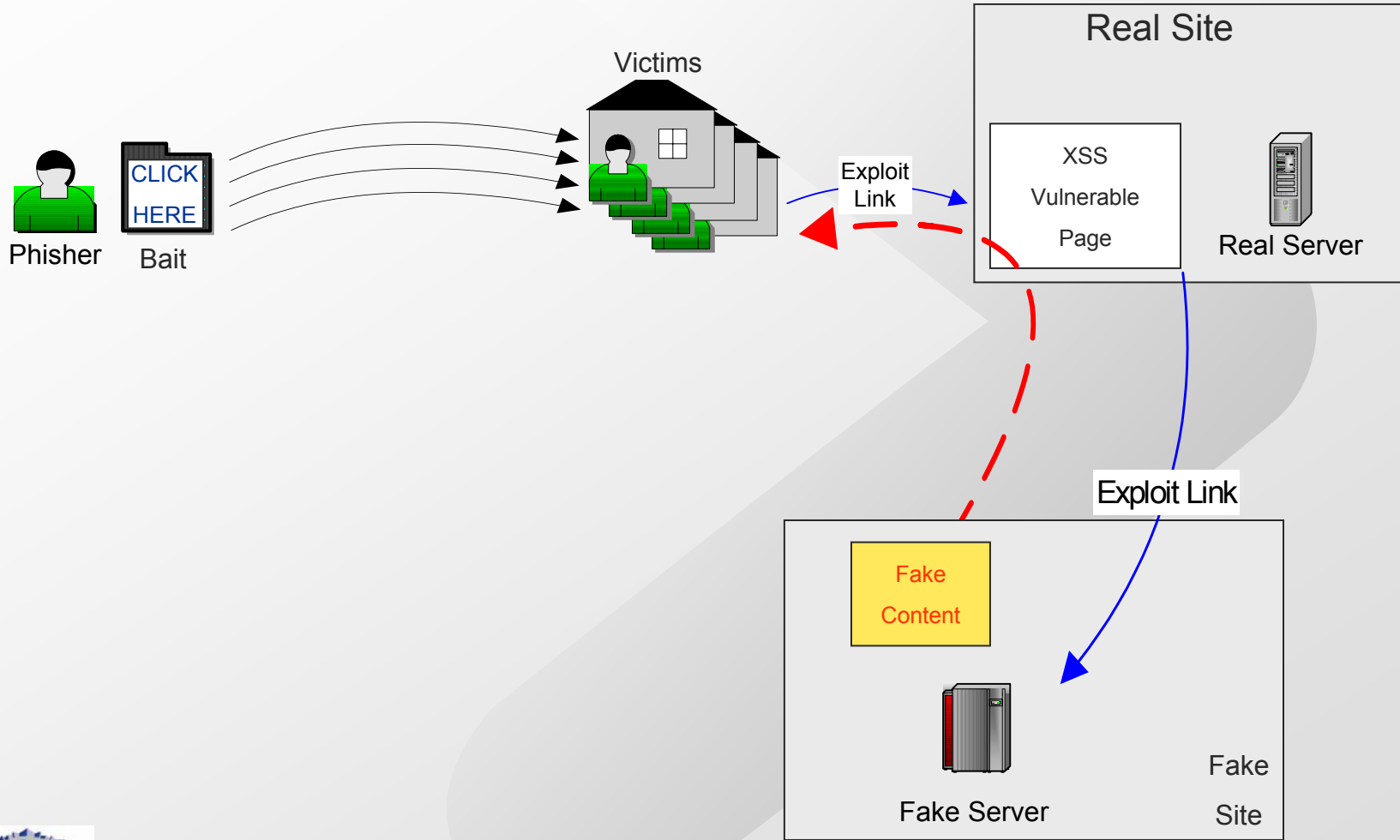


Phishing by Cross-Site Scripting (XSS)

1. Find a reputable site with an XSS vulnerability on any of its pages
 2. Harvest a large number of live email addresses
 3. Draft an email
 4. Insert an XSS exploit hyperlink into the email for the user to click on
 5. Send it to all of the live email addresses
 6. Wait
- * The XSS attack will make some javascript execute inside the victim's session with the real server – this could be used to steal cookies, passwords, etc.
- * This could also be used with vulnerable SSL pages



XSS Phishing Mechanism





Sign In

[Help](#)

New to eBay?

or

Already an eBay user?

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

[Register >](#)

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

[Forgot](#) your User ID?

Password

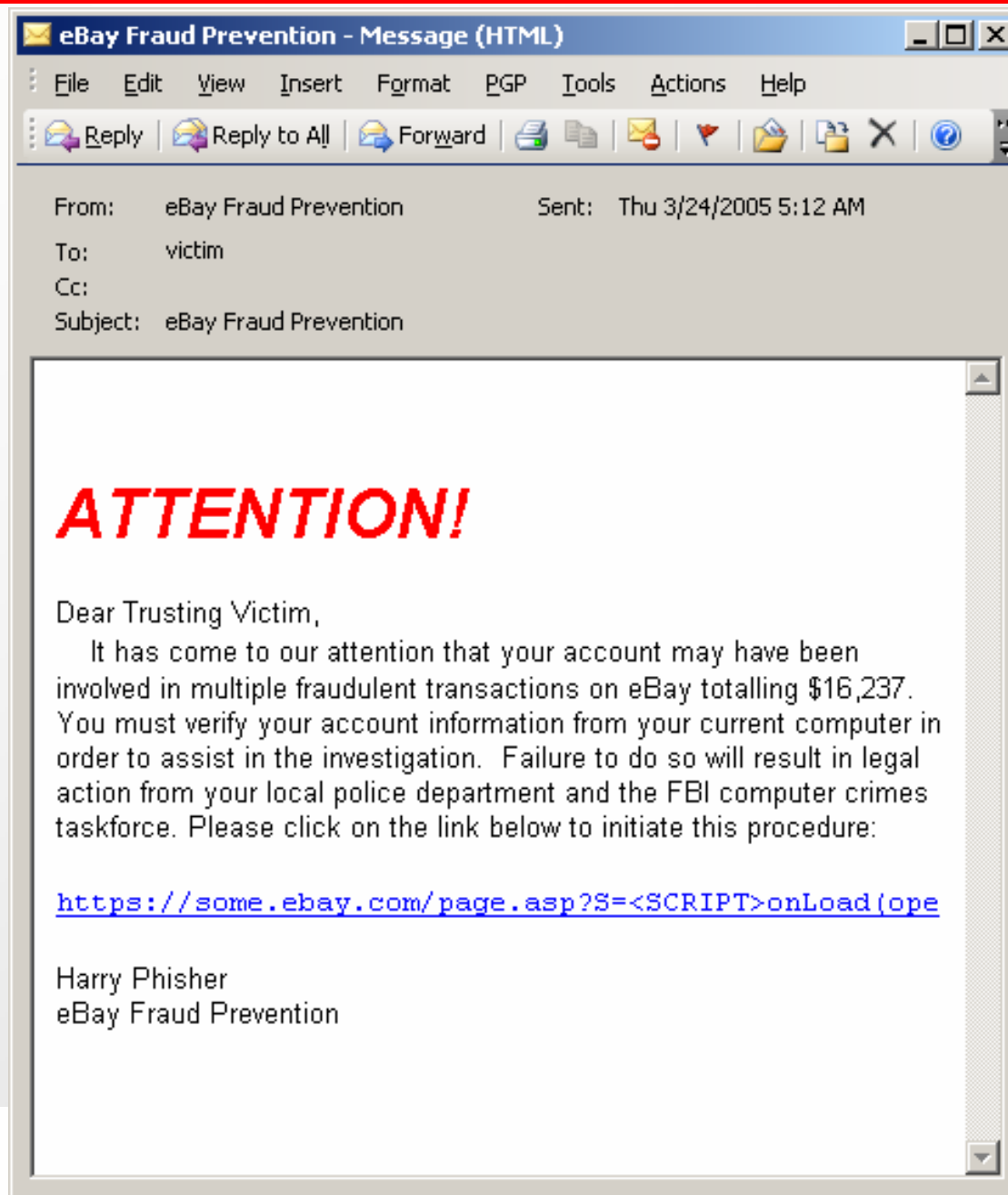
[Forgot](#) your password?

[Sign In Securely >](#)

[Keep me signed in](#) on this computer unless I sign out.

[Account protection tips](#)

Be sure the Web site address you see above starts with <https://signin.ebay.com/>



UNISYS

Imagine it • Done •



Sign In

[Help](#)

or

New to eBay?

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

[Register >](#)

Already an eBay user?

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

[Forgot](#) your User ID?

Password

[Forgot](#) your password?

[Sign In Securely >](#)

[Keep me signed in](#) on this computer unless I sign out.

[Account protection tips](#)

Be sure the Web site address you see above starts with <https://signin.ebay.com/>



Sign In [Help](#)

New to eBay?

or

Already an eBay user?

If you want to sign in, you'll need to register first.
Registration is fast and **free**.

[Register >](#)

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

trustingvictim

[Forgot](#) your User ID?

Password

XXXXXXXXXXXX

[Forgot](#) your password?

[Sign In Securely >](#)

[Keep me signed in](#) on this computer unless I sign out.

[Account protection tips](#)

Be sure the Web site address you see above starts with <https://signin.ebay.com/>

Mitigation: Phishing with XSS

Underlying Causes

- Technical
 - Failure to filter inputs for javascript-related characters
- Operational
 - Development process does not have a security testing phase
- Policy
 - Security policy does not mandate a customer-oriented security awareness campaign
 - Security review not part of initial project planning
- Strategy
 - Failure to adopt an appropriate threat model for application development



What to do...

- Be suspicious of any email with urgent requests for personal financial information
- Don't use the links in an email to get to any web page
- Avoid filling out forms in email messages that ask for personal financial information
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
- Consider installing a Web browser tool bar to help protect you from known phishing fraud websites
<http://www.earthlink.net/earthlinktoolbar>
- Regularly log into your online accounts
- Ensure that your browser is up to date and security patches applied



How to Report Phishing

- forward the email to reportphishing@antiphishing.com
- forward the email to the Federal Trade Commission at spam@uce.gov
- forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
- when forwarding spoofed messages, always include the entire original email with its original header information intact
- notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/



Wireless



Threats

- **Wired Network Compromise**
- **Wireless Network Compromise**
- **Wired Network Abuse (Third Party)**
- **Theft of Service (WISP)**
- **Interception of Traffic (Wireless Sniffing)**
- **Hotspot Hijinks**



Countermeasures

- > WEP
- > Closed Network Access Control (“Disabling Broadcast SSID”)
- > MAC Address Filtering
- > LEAP (Cisco)
- > WPA
- > 802.11i

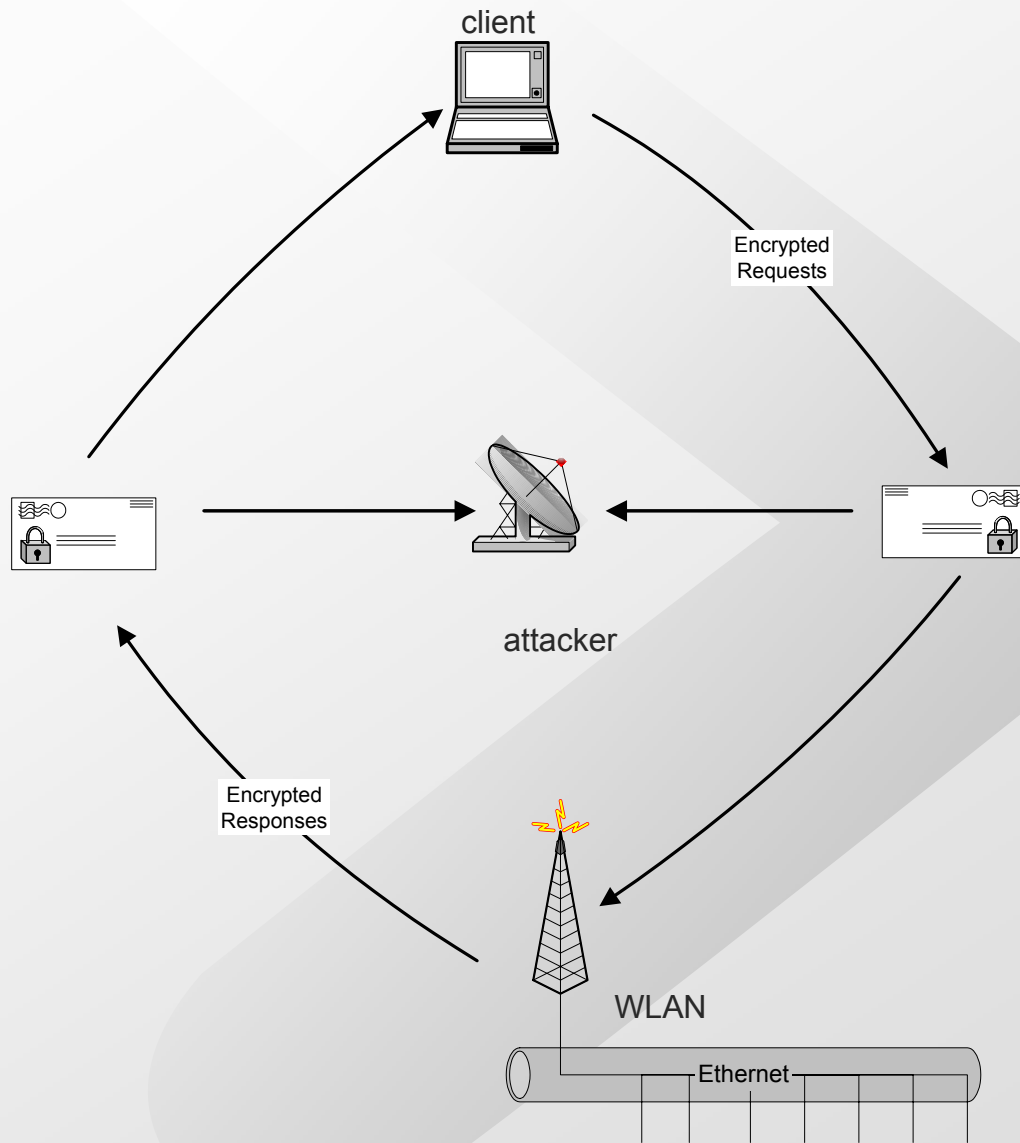


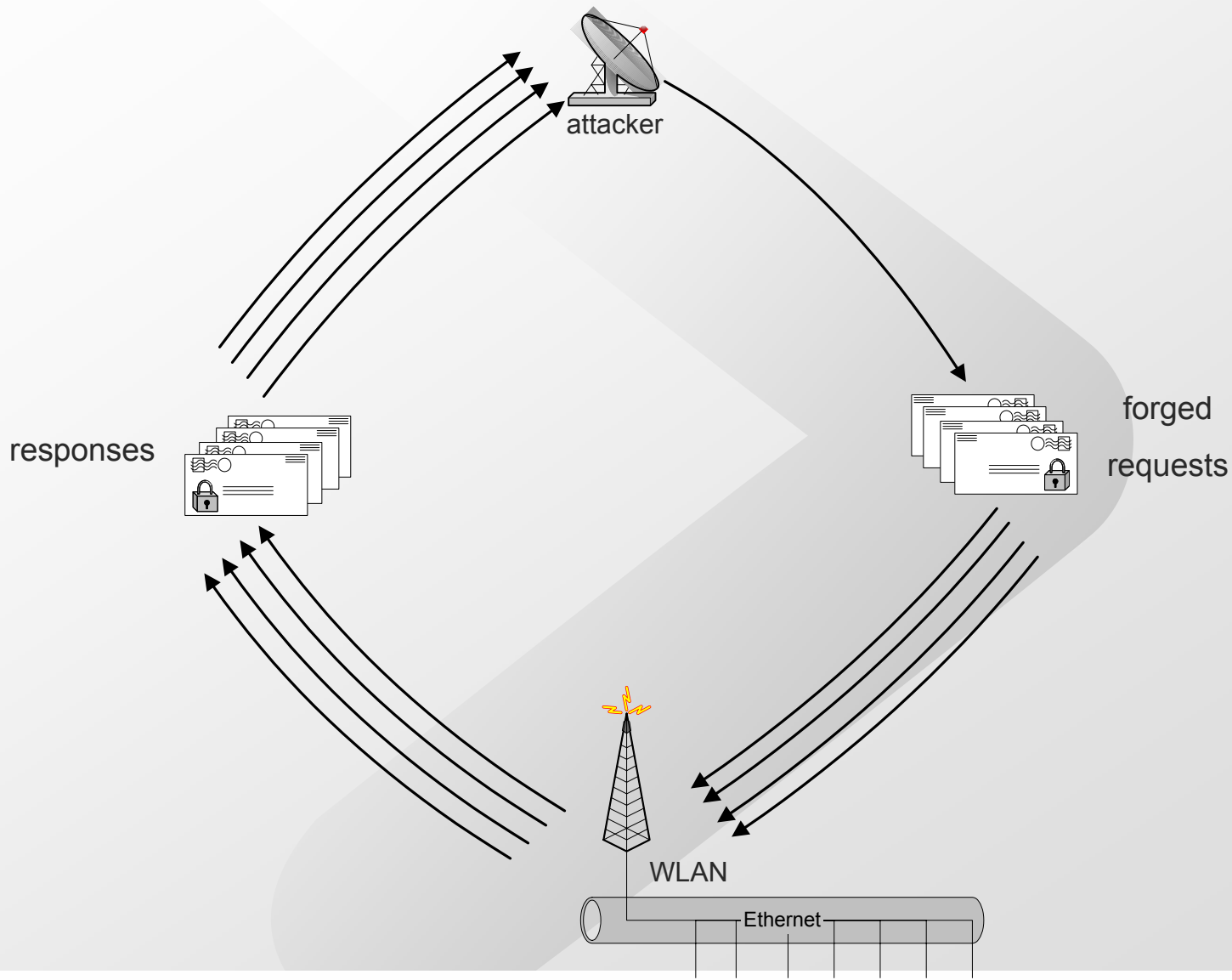
WEP Cracking

> More efficient methods available now

- Collect a few encrypted packets
- Use a tool to “replay” some of those encrypted packets on the WLAN to try and generate responses from other WLAN peers
- Collect many encrypted packets very quickly from response traffic
- Use statistical attacks on the weak IVs to recover the WEP key







Mitigation: Wireless

Underlying Causes:

- Technical
 - WEP is fundamentally broken
- Operational
 - No support for more robust authentication (WPA, EAP-TLS)
 - No monitoring wireless networks for sudden traffic spikes
- Policy
 - Treating wireless different from any other network service where shared authentication would be disallowed (e.g. VPN)
- Strategy
 - Failure to address evolving standard as such – implementation only took into account technology available with 1st generation deployment



Security Strategy & Planning

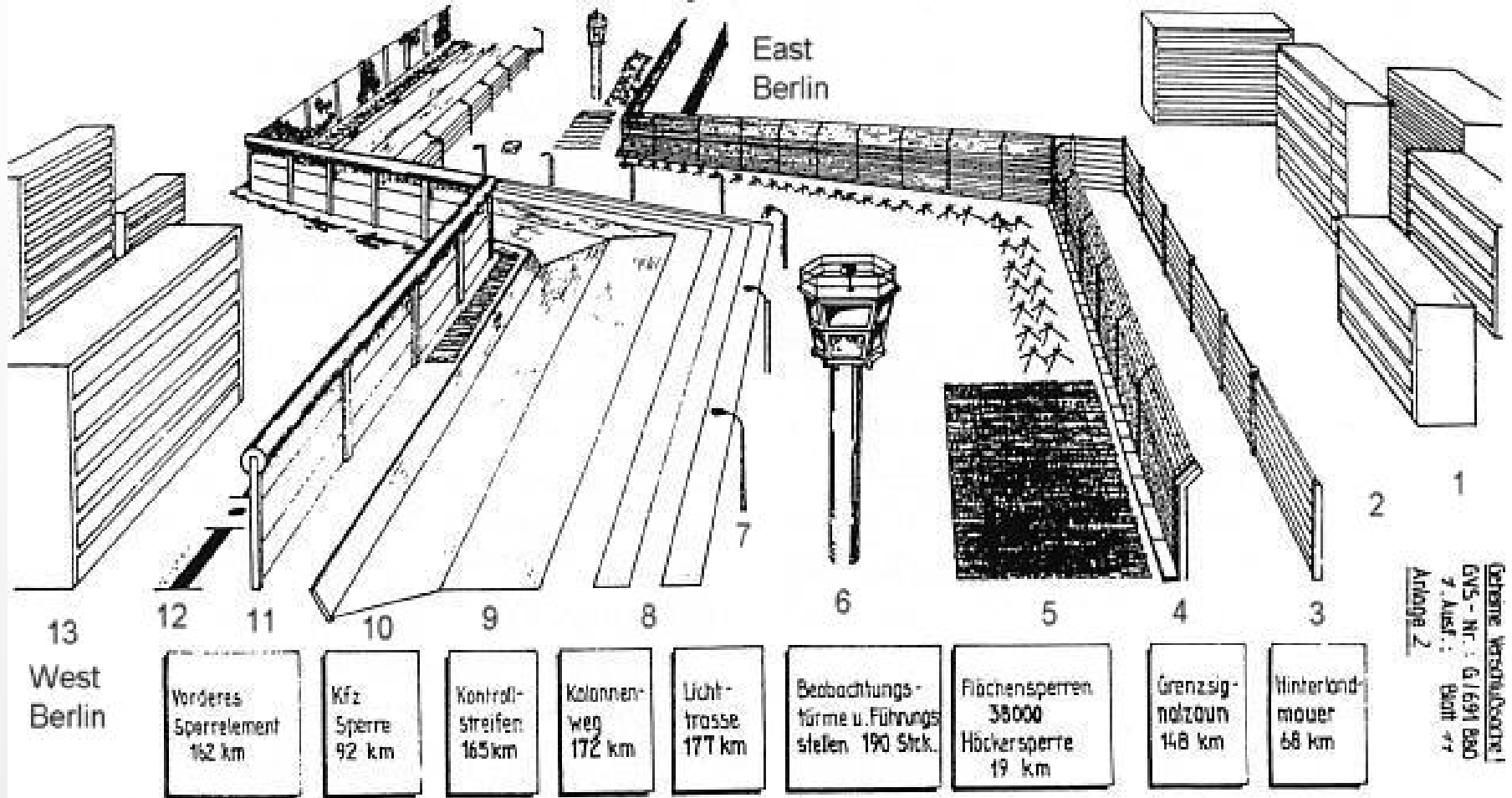




UNISYS

Imagine it • Done •

Pionier- und signaltechnischer Ausbau der Staatsgrenze zu BERLIN-West (gegenwärtig)



Gesamte Verschärfungsanlage
 GVS - Nr. : 61691 880
 7. Ausf. : Prot. 47
 Anlage 2

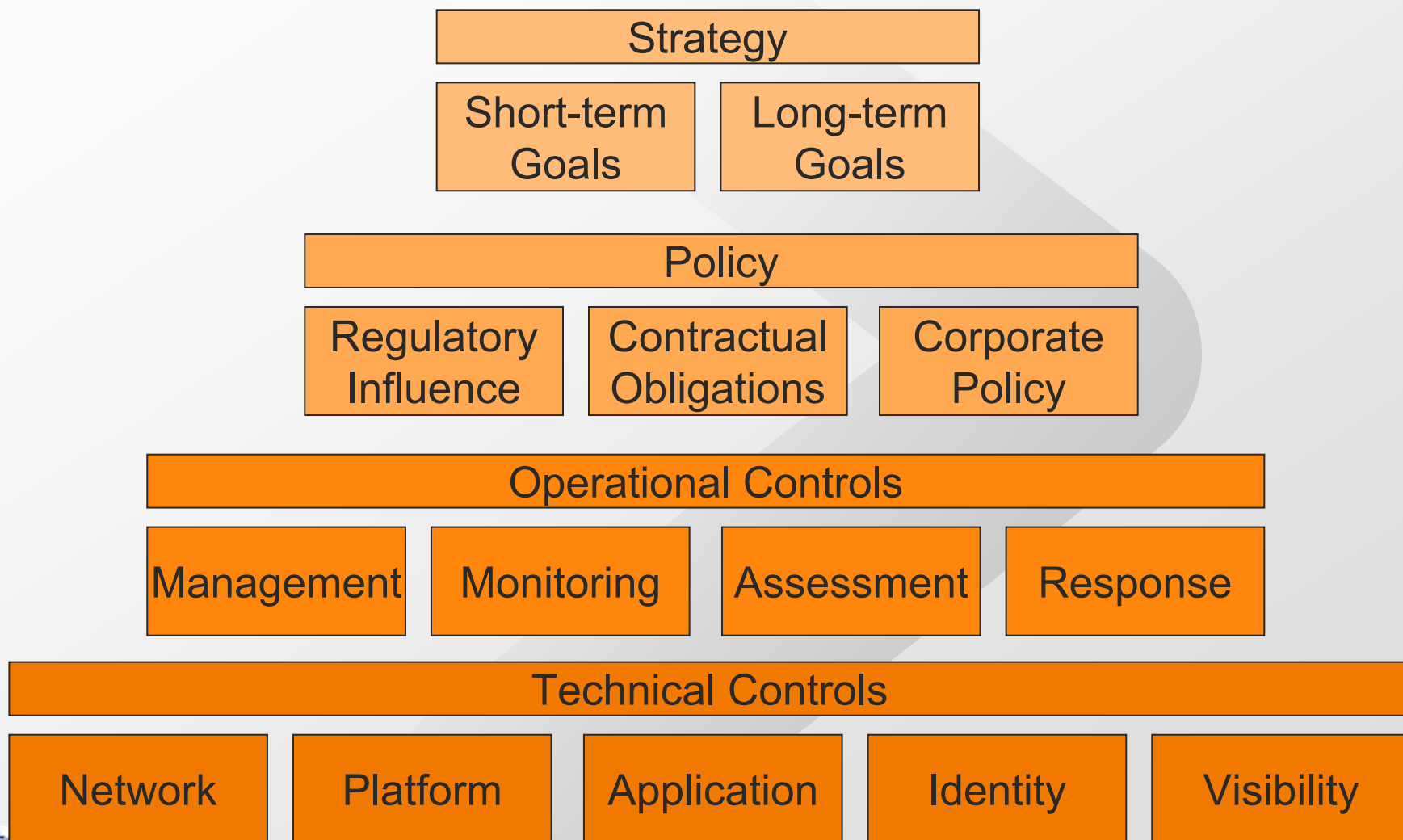


Reactive Security as an Ongoing Strategy

- Expensive
- Short-term results
- Steep learning curve
- Little time for validation
- Unpredictable resourcing
- Reduced operational efficiency
- Increased environmental complexity
- Distraction from long-term goals & objectives



Layered Defense as an Alternative

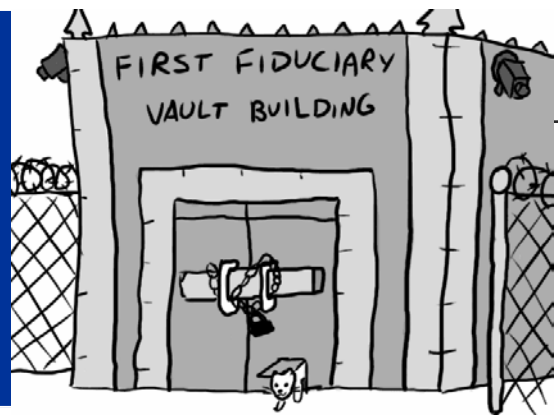




INFRAGARD of Middle Tennessee

Guarding the Nation's Infrastructure

Questions?



Bryant G. Tow

Bryant.Tow@Unisys.com

615.595.2960

InfraGard Middle TN, President &
InfraGard Southeast Regional Lead
Director of Security –GIS North America



- > Systems Integration.
- > Outsourcing.
- > Infrastructure.
- > Server Technology.
- > Consulting.

Imagine it • Done •