PREDICTIVE SYSTEMS

COUNTER

HACK

Hack, Counter Hack

Purpose of the seminar and general trends

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Exploiting systems
- Step 4: Keeping access
- Step 5: Covering the tracks
- Putting it all together
- Conclusions

Purpose of the Seminar

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

—Sun Tzu, *The Art of War*

We're not here to teach you how to hack.…
However, to defend yourself, you must understand your adversaries' strategies and tactics.

General Trends

- The rise of the anti-disclosure movement
  - Full-disclosure has its problems—tell everyone everything
  - Anti-disclosure has a whole new set of problems
- Hacktivism
  - In times of war, you can make a political point
- Worms, worms, everywhere
  - 2001 was the year of the worm
  - We ain't seen nothin' yet
  - Distributed attacks on the rise
- Polymorphism
  - Make things look different every time they run
  - Much harder to track down
- Intrusion Detection System (IDS) evasion

Hack, Counter Hack

Purpose of the Seminar and general trends

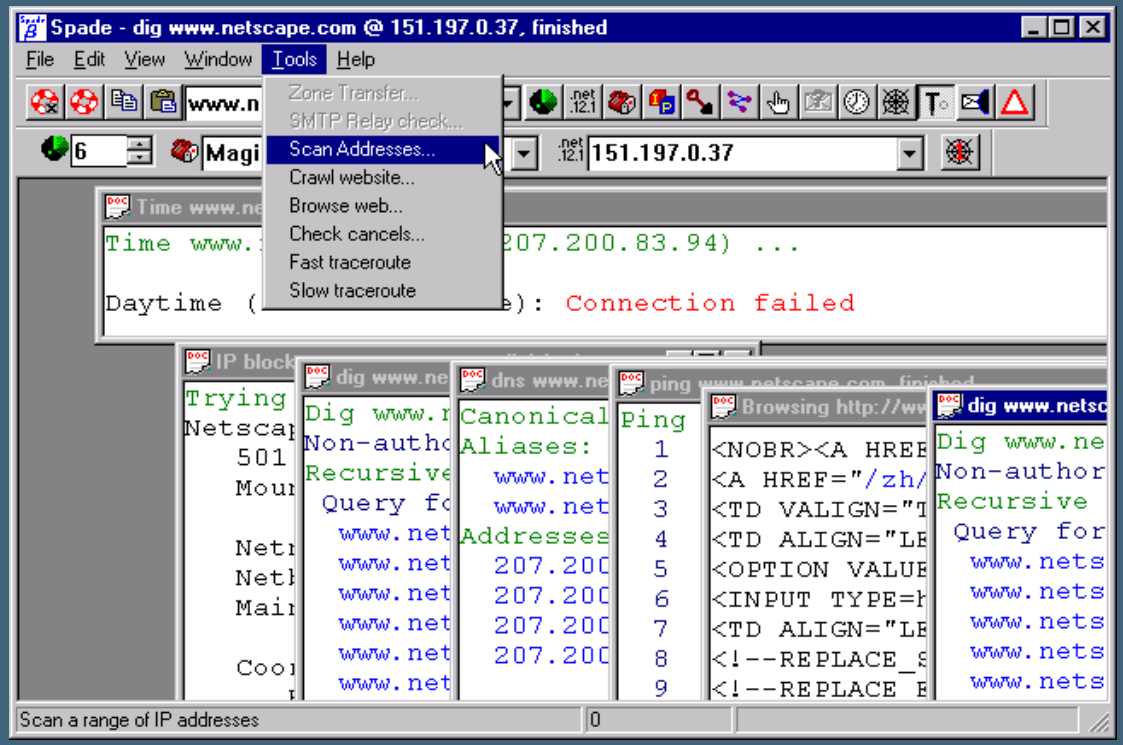
- **Step 1: Reconnaissance**
- Step 2: Scanning
- Step 3: Exploiting Systems
- Step 4: Keeping Access
- Step 5: Covering the Tracks
- Putting It All Together
- Conclusions

Step 1: Reconnaissance Overview

- This step means “casing the joint”
- A huge amount of information is freely and publicly available about potential targets
  - “Whois” databases show contact names, addresses, and DNS servers
    - The white pages of the Internet
    - My favorite is www.allwhois.com
  - DNS interrogation
  - Web searches
    - Use “link:www.samplewebsite.com” to find everyone who links to the target system

Sam Spade: A Useful Tool and Website

- Available at www.samspade.org, a Website by Steve Atkins
- General reconnaissance tool, for Windows 9x, NT, 2000, supporting:
  - Ping
  - DNS Lookup
  - Whois
  - IP Block
  - DNS
  - Traceroute
  - Finger
  - Check Time
  - And so on



PREDICTIVE SYSTEMS

Reconnaissance Defenses

- Look through your publicly available information and make sure you aren't sharing too much
- Check out your:
  - Whois entries
  - DNS names and records
  - Websites (your own and others)

Hack, Counter Hack

Purpose of the seminar and general trends

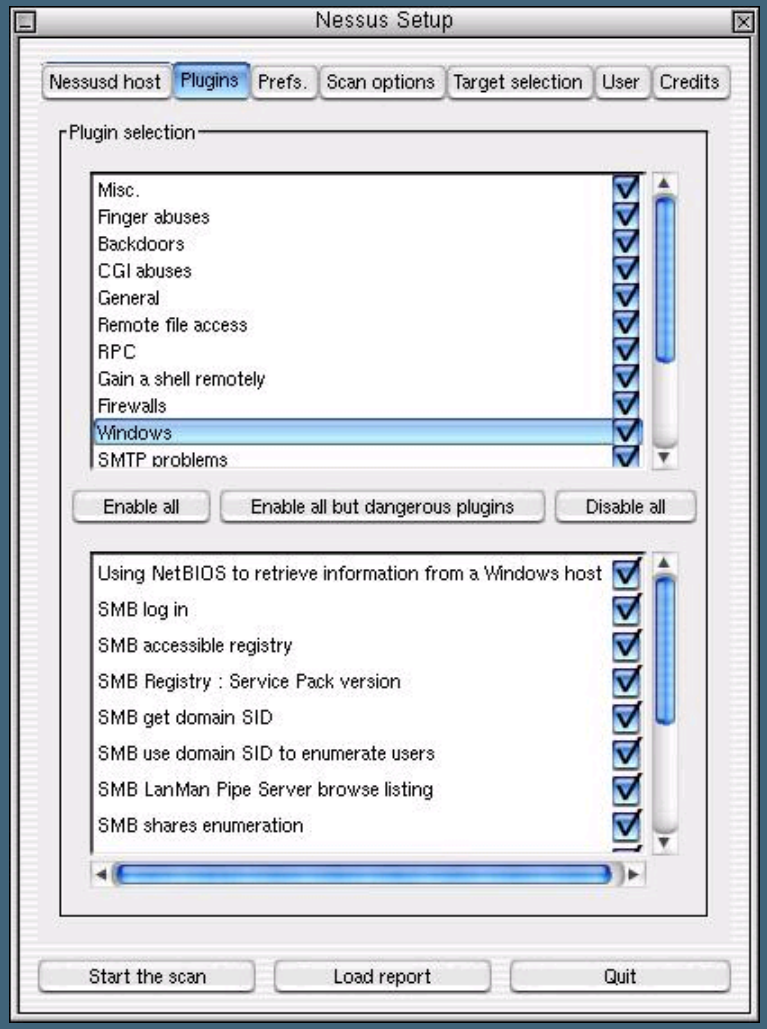
- Step 1: Reconnaissance
- **Step 2: Scanning**
- Step 3: Exploiting systems
- Step 4: Keeping access
- Step 5: Covering the tracks
- Putting it all together
- Conclusions

Step 2: Scanning Overview

- In this phase, the attacker looks for openings on the target system
- Many options for the attacker
  - War dial: Looking for rogue modems
  - Network scanning tools
    - Commercial
    - Free, open source
  - Wireless LAN attacks
    - “War driving”

Nessus: One of the Best Vulnerability Scanners

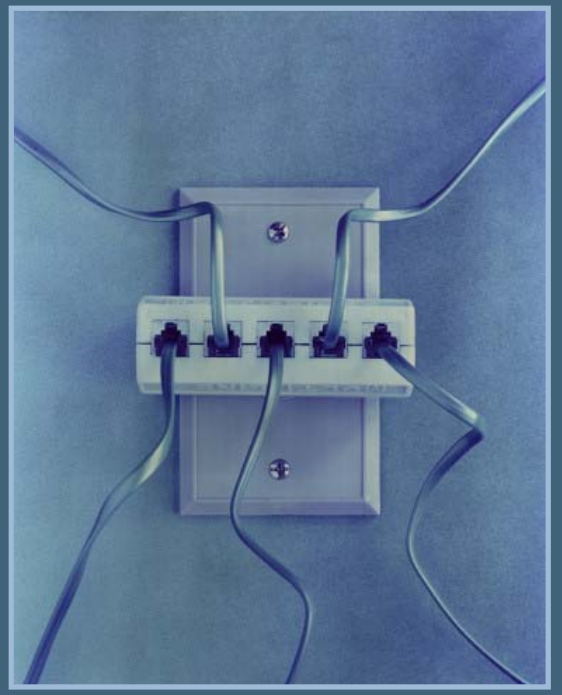
- Nessus is a free, open-source general vulnerability scanner
- As such, it is used by the white hat community and the black hats
- Project started by Renaud Deraison
- Available at www.nessus.org
- Consists of a client and server, with modular plug-ins for individual tests



PREDICTIVE SYSTEMS

Vulnerability Scanning Defenses

- Utilize intrusion detection systems
- Close unused ports
- Apply system patches



PREDICTIVE SYSTEMS

War Driving

- Wireless technology is getting much cheaper
- Base stations for less than $200, with wireless cards under $100
  - IEEE 802.11b standard is very popular
  - Employees setting up their own access points so they can roam around the halls
  - Very dangerous!
- With a laptop and wireless card, an attacker can drive down the street and join many wireless LANs!
- Tools to use:
  - NetStumbler: www.netstumbler.com
  - AirSnort: airsnort.sourceforge.net

War Driving Defenses

- Use Virtual Private Network (VPN)
- All data from end system to VPN gateway inside of wireless device encrypted and authenticated
- Use commercial VPN
- SLAN is a freeware VPN on Linux or Windows:
  - http://slan.sourceforge.net

Hack, Counter Hack

Purpose of the seminar and general trends

- Step 1: Reconnaissance
- Step 2: Scanning
- **Step 3: Exploiting systems**
- Step 4: Keeping access
- Step 5: Covering the tracks
- Putting it all together
- Conclusions

Step 3: Exploit Systems Overview

- Once attackers find a vulnerability, they want to take over the target system
- Many, many options in this realm:
  - Buffer overflows
  - Sniffing
  - Password cracking
  - Session hijacking
  - Custom application attacks

Exploit Systems: Here Come the Worms!

- Compromising systems one-by-one can be such a chore
- Worms are attack tools that spread across a network, moving from host to host exploiting weaknesses
- Worms automate the process:
  - Take over systems
  - Scan for new vulnerable systems
  - Self-replicate by moving across the network to another vulnerable system
  - Each instance of a worm is a “segment”
- 2001: Year of the Worm?
  - Ramen, L10n, Cheese, Sadmind/IIS, Code Red, Code Red II, Nimda
  - The list keeps growing…

Coming Soon: Super Worms

- To date, the worms haven't been nearly as nasty as they could be
- New generations of worms arrive every two to six months
- Be on the lookout for very nasty new worms, including:
  - Multi-functional
  - Multi-platform
  - Multi-exploit
  - Zero-day exploits
  - Polymorphic
- We've seen many of these pieces, but no one has rolled them all together… yet!

Worm Defenses

- You must have a very well-defined program for security alerts and applying patches, including:
  - Vulnerability notification… monitor vendor and public lists
  - Acquire fix
  - Test fix
  - Apply to production environment
- Incident response is also critically important!

Hack, Counter Hack

Purpose of the seminar and general trends

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Exploiting systems
- **Step 4: Keeping access**
- Step 5: Covering the tracks
- Putting it all together
- Conclusions

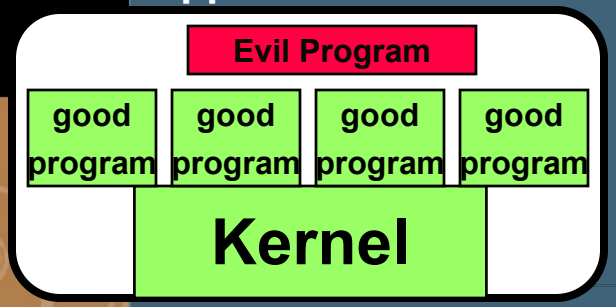
Step 4: Keeping Access Overview

- Once attackers gain access to a system, they want to *keep* that access
- They use a variety of techniques to accomplish this, including:
  - Backdoors
    - Bypass normal security controls
  - Trojan horses
    - Look nice, but really are evil
  - Trojan horse backdoors
    - A very damaging combination

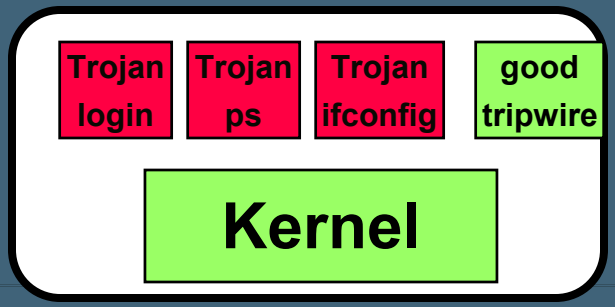
Trojan Horse Backdoors

Type of Trojan horse backdoor	Characteristics	Analogy	Example tools in this category
Application-Level Trojan Horse Backdoor	A separate application runs on the system	An attacker adds poison to your soup.	Sub7, BO2K, Tini, etc.
Traditional RootKits	Critical Operating System components are replaced.	An attacker replaces your potatoes with poison ones	Lrk6, T0rnkit, etc.
Kernel-Level RootKits	Kernel is patched.	An attacker replaces your tongue with a poison one.	Knark, adore, Kernel Intrusion System, rootkit.com, etc.

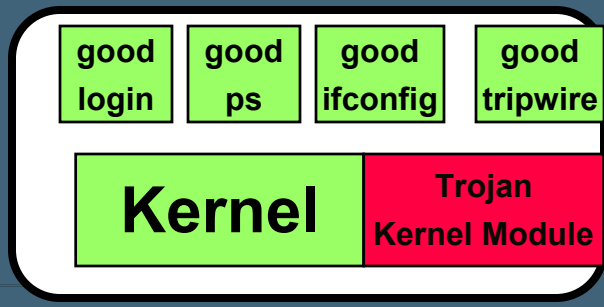
Application-level



Traditional RootKit



Kernel-level RootKit



Trojan Horse Backdoor Defenses

- Don’t let the attacker get root or admin privileges on the machine in the first place!
- Anti-virus tools
- File system integrity checking tools:
  - Tripwire, AIDE
- Kernel lockers and integrity checking tools

Hack, Counter Hack

Purpose of the seminar and general trends

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Exploiting systems
- Step 4: Keeping access
- **Step 5: Covering the tracks**
- Putting it all together
- Conclusions

PREDICTIVE SYSTEMS

Step 5: Covering the Tracks Overview

- The attacker doesn't want to get caught
- Most attacks are likely unobserved
- Attackers hide themselves using a variety of techniques, including:
  - Log editing
  - File and directory hiding
  - Process hiding
  - Network usage hiding—covert channels

Defenses from Covering the Tracks

- Guard the integrity of your system logs
- Use tools to search for hidden files
- All defenses from Trojan horse backdoors apply here as well!

Hack, Counter Hack

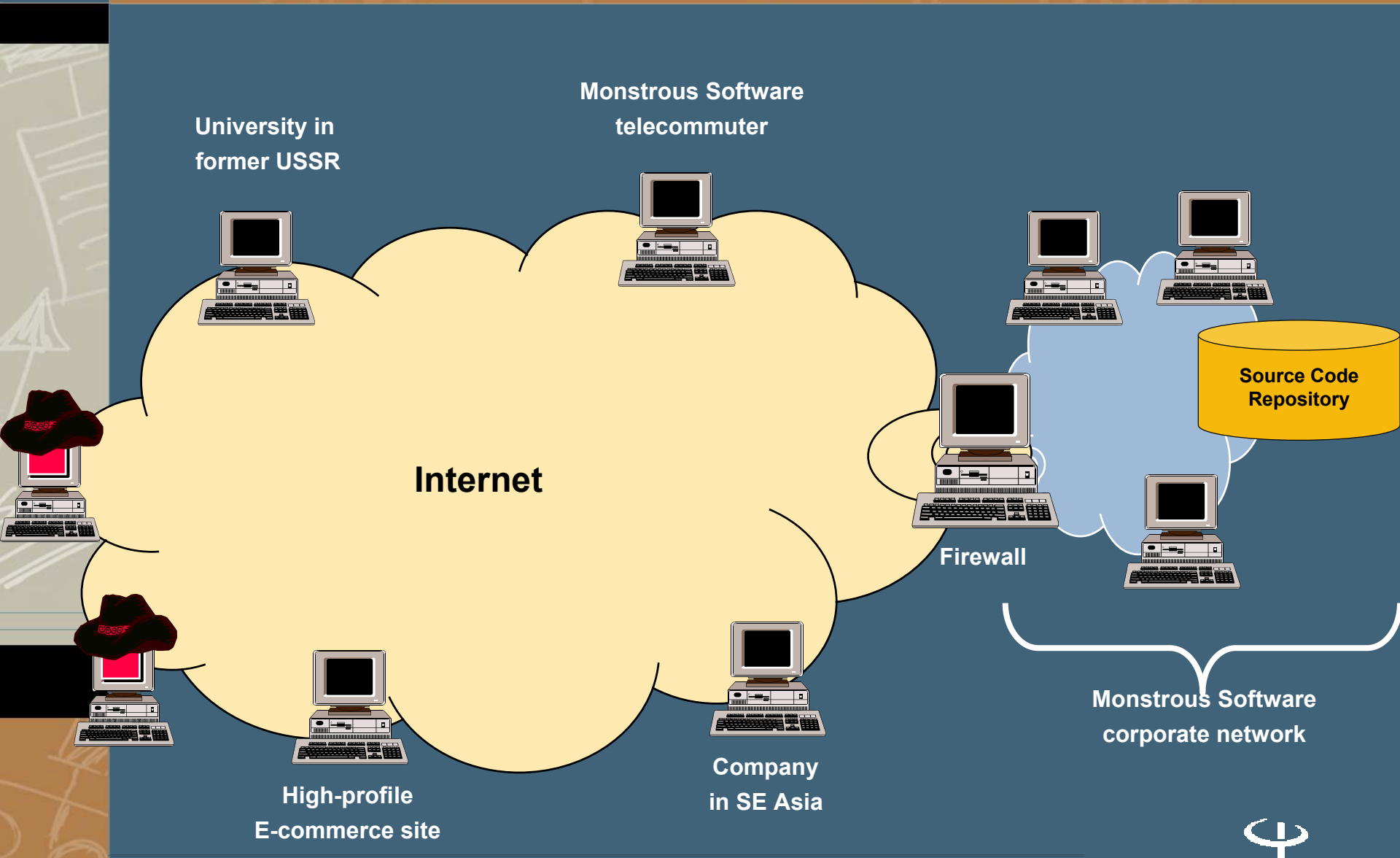
Purpose of the seminar and general trends

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Exploiting systems
- Step 4: Keeping access
- Step 5: Covering the tracks
- **Putting it all together**
- Conclusions

Scenario: Death of a Telecommuter

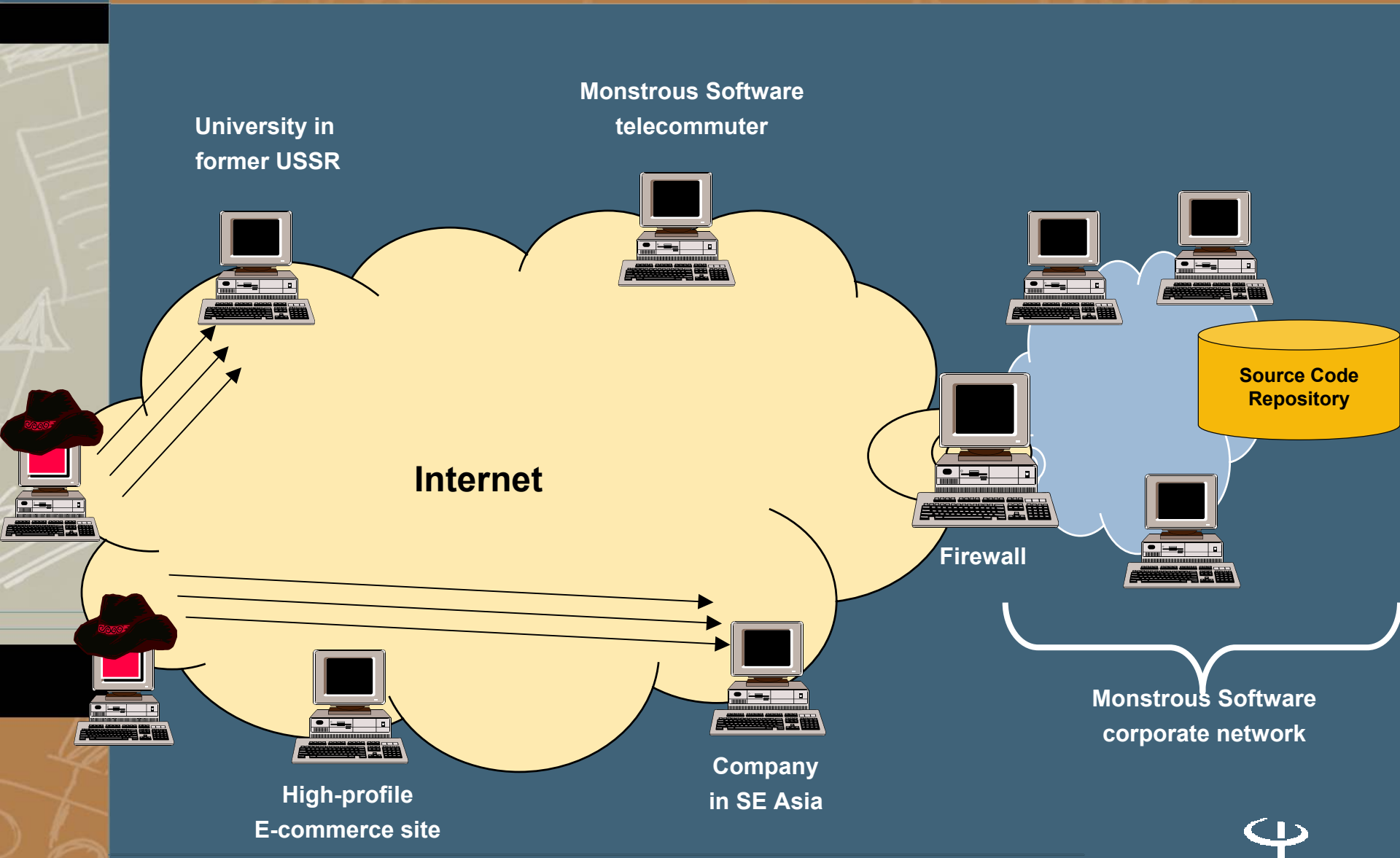
- The most skilled attackers are very pragmatic
- They construct elaborate attacks from the building blocks we've discussed
- Consider the following scenario:
  - Monstrous Software sells a software product called "foobar"
  - Bonnie and Clyde are funded to steal source code for foobar
  - They don't want to get caught, so indirection is key

Scenario: Steal the Source, Luke!



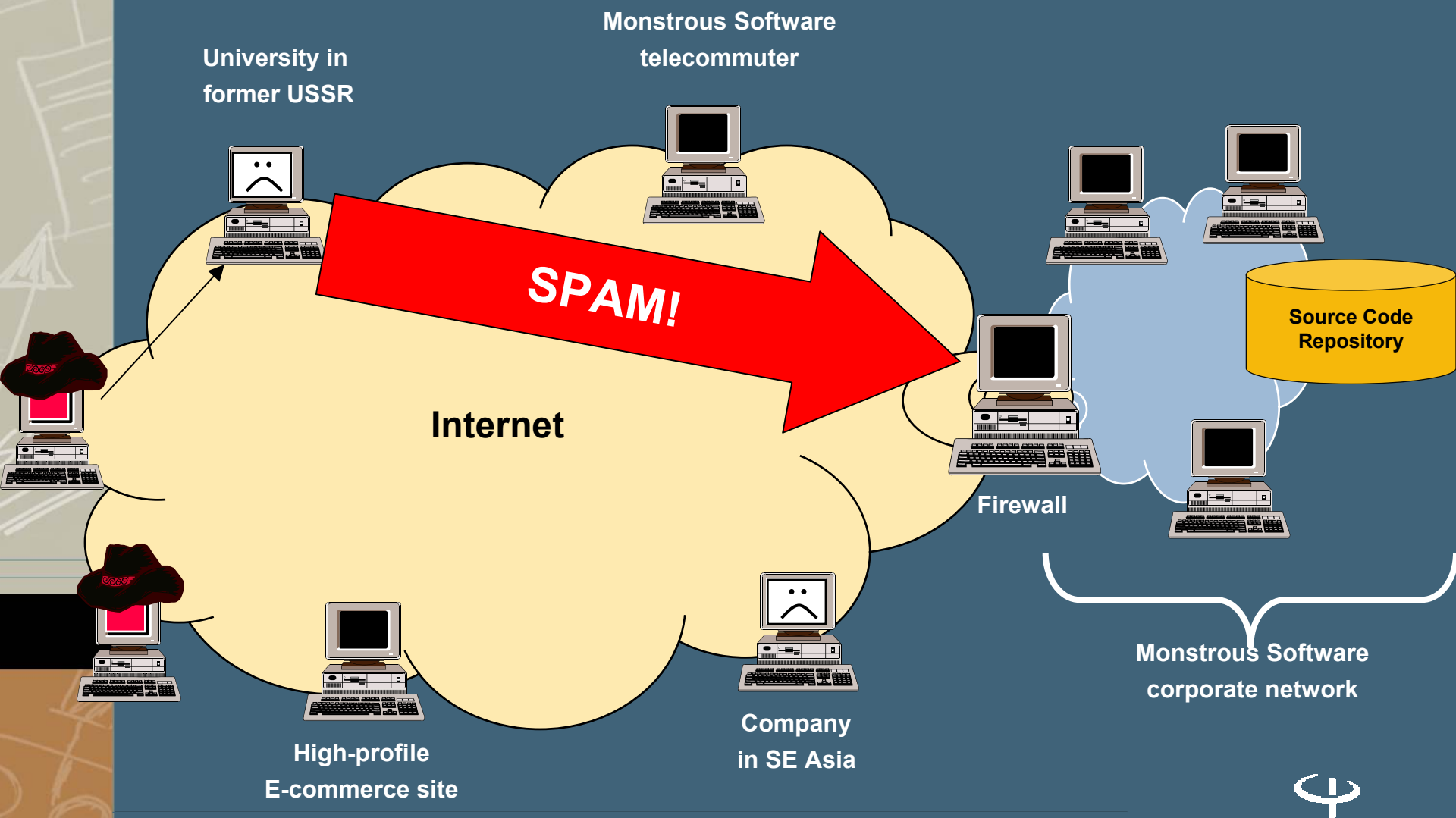
PREDICTIVE SYSTEMS

Attackers Scan for Intermediaries



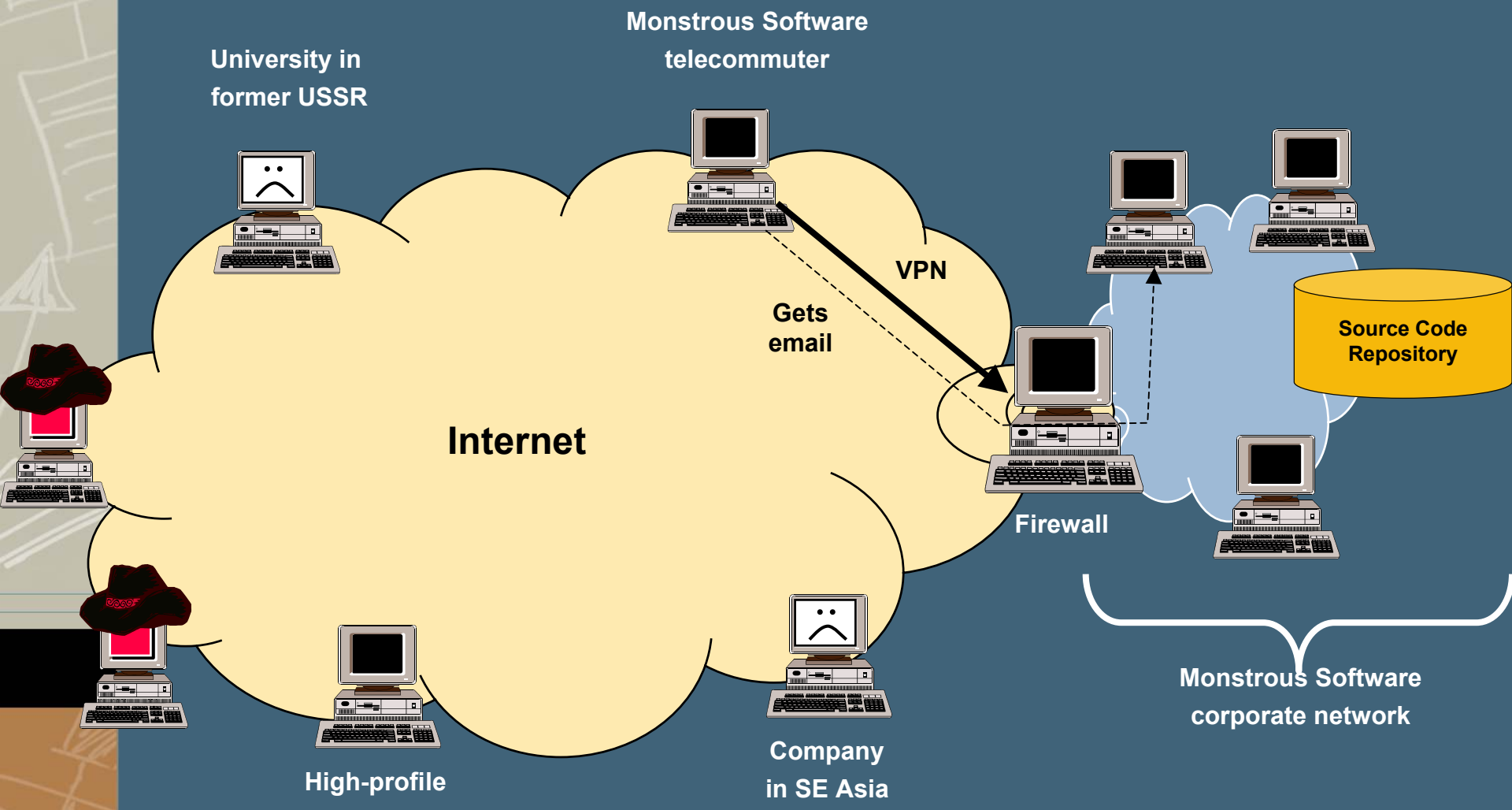
PREDICTIVE SYSTEMS

Send Email Spam re: Cool Game



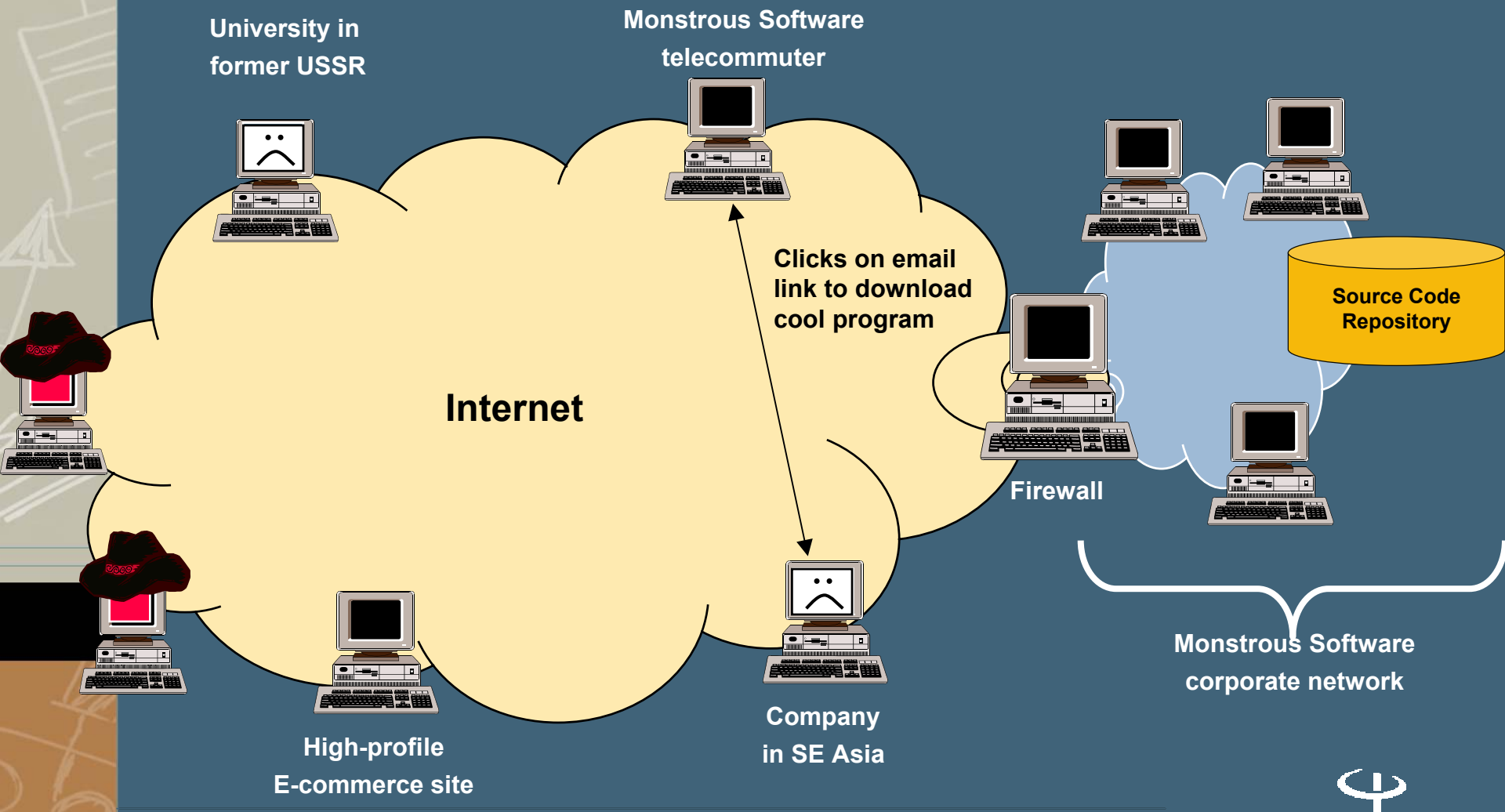
PREDICTIVE SYSTEMS

Telecommuter Gets Email through VPN



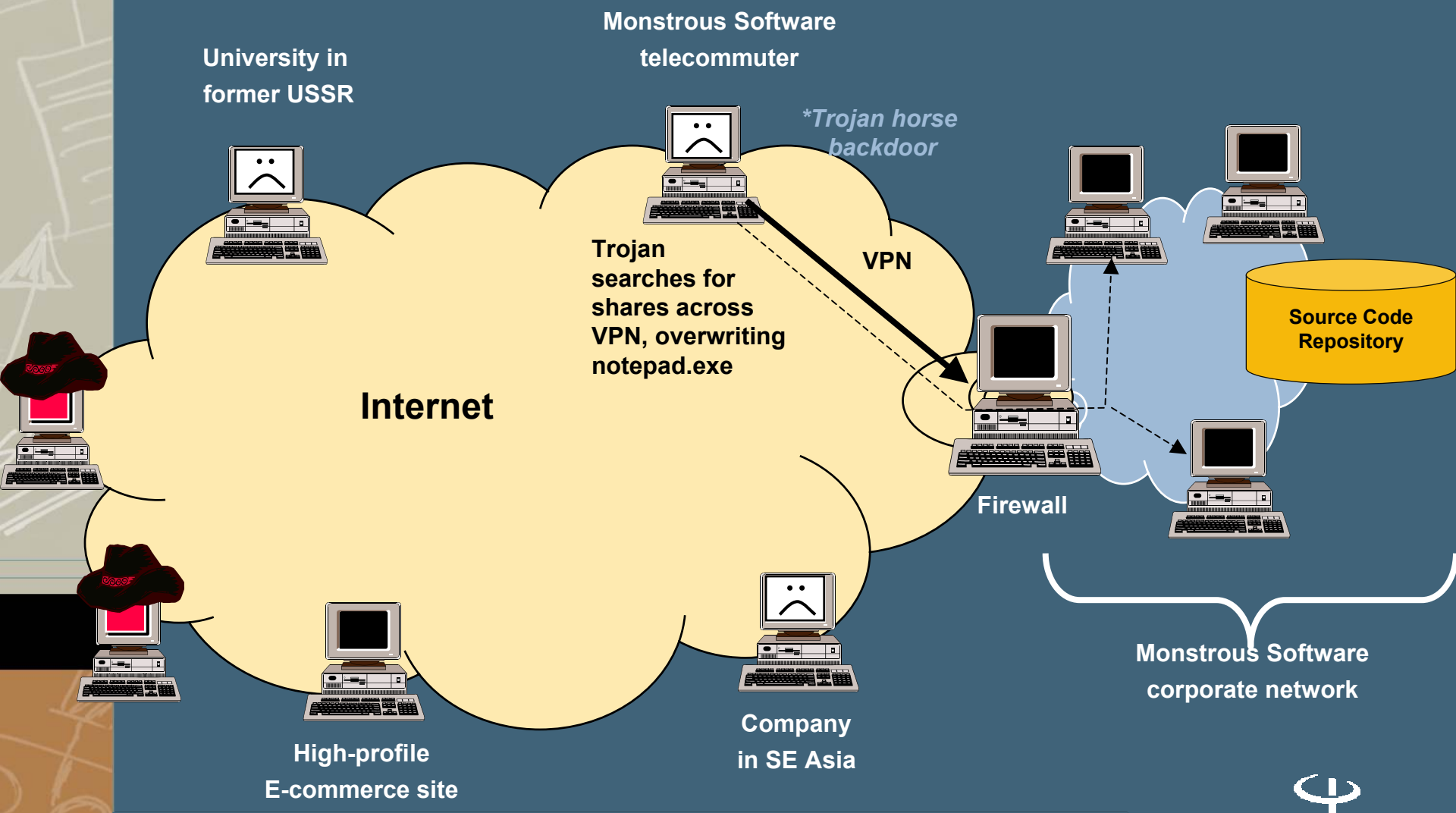
PREDICTIVE SYSTEMS

Download Game: Oops, It's a Trojan



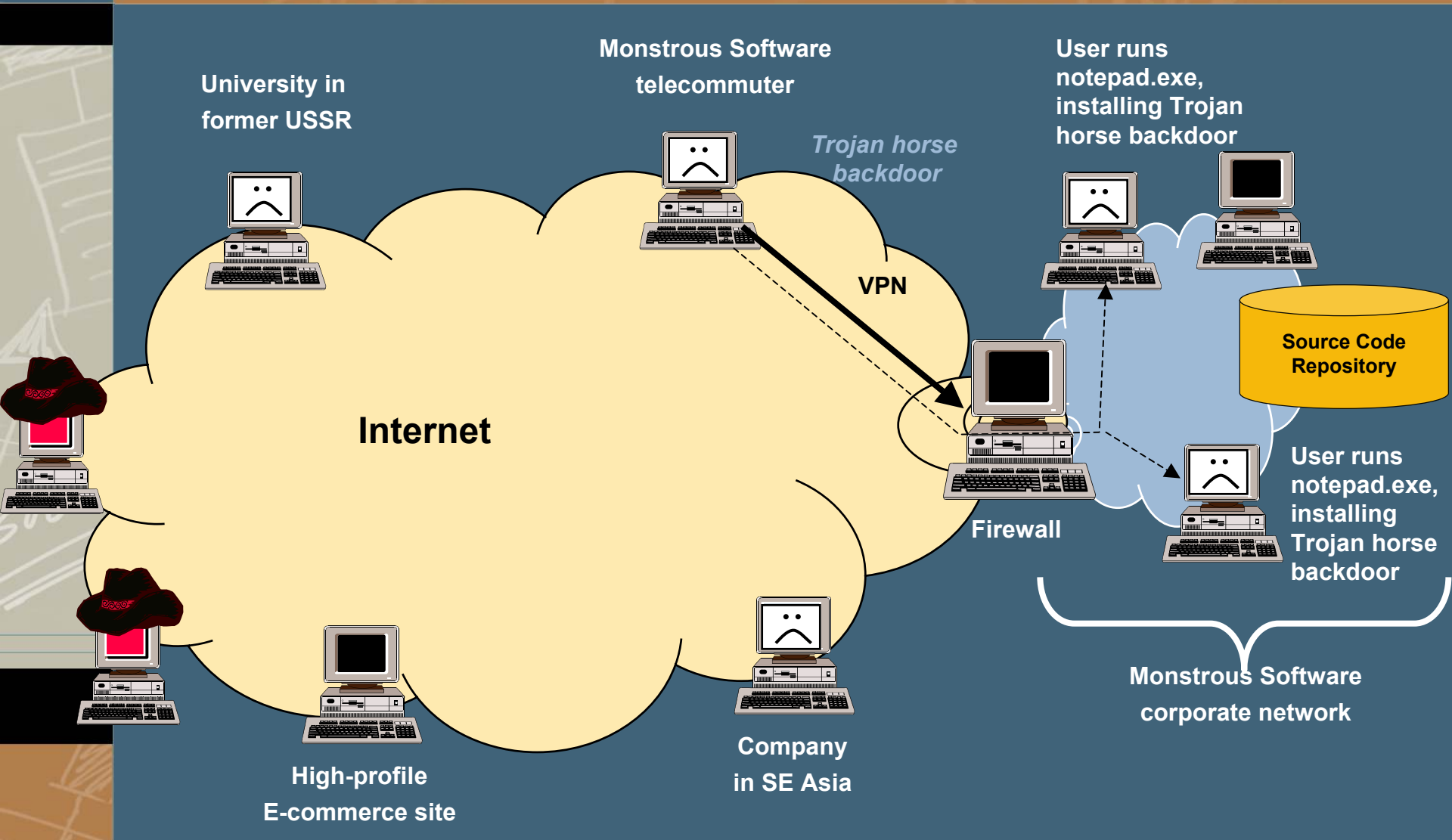
PREDICTIVE SYSTEMS

Trojan Copies Itself to Intranet through VPN



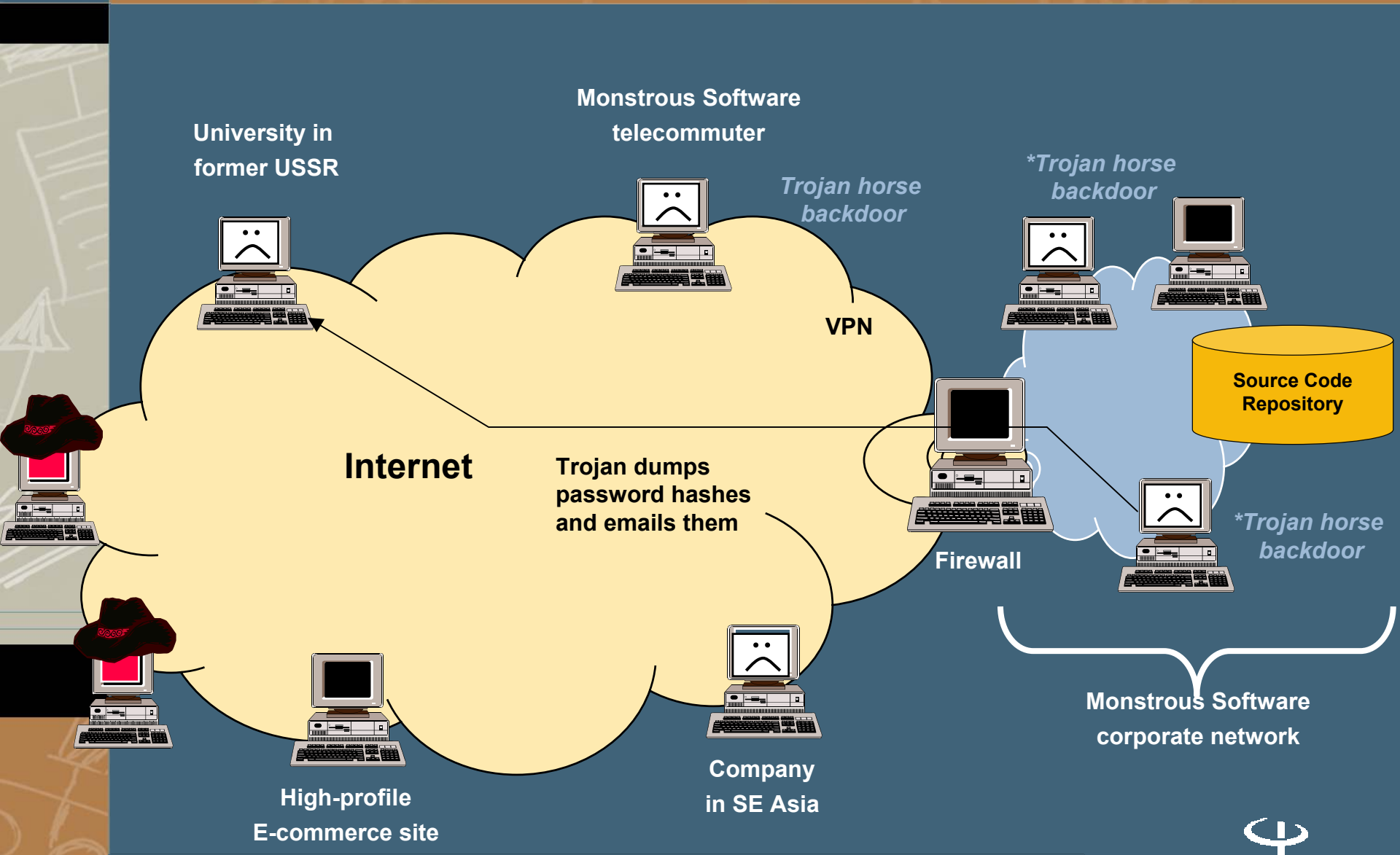
PREDICTIVE SYSTEMS

Trojan Installed on Internal Network



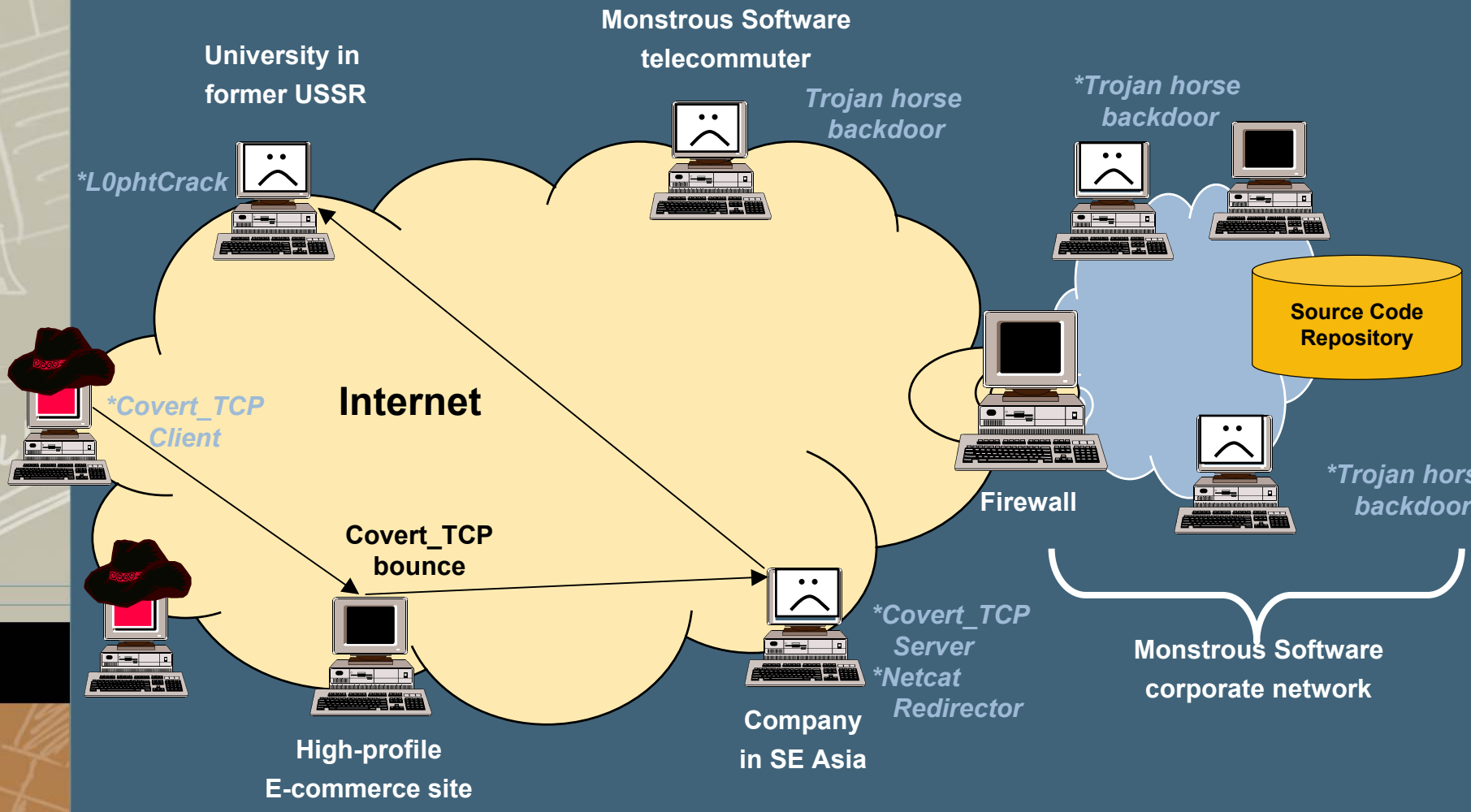
PREDICTIVE SYSTEMS

Trojan Steals Passwords



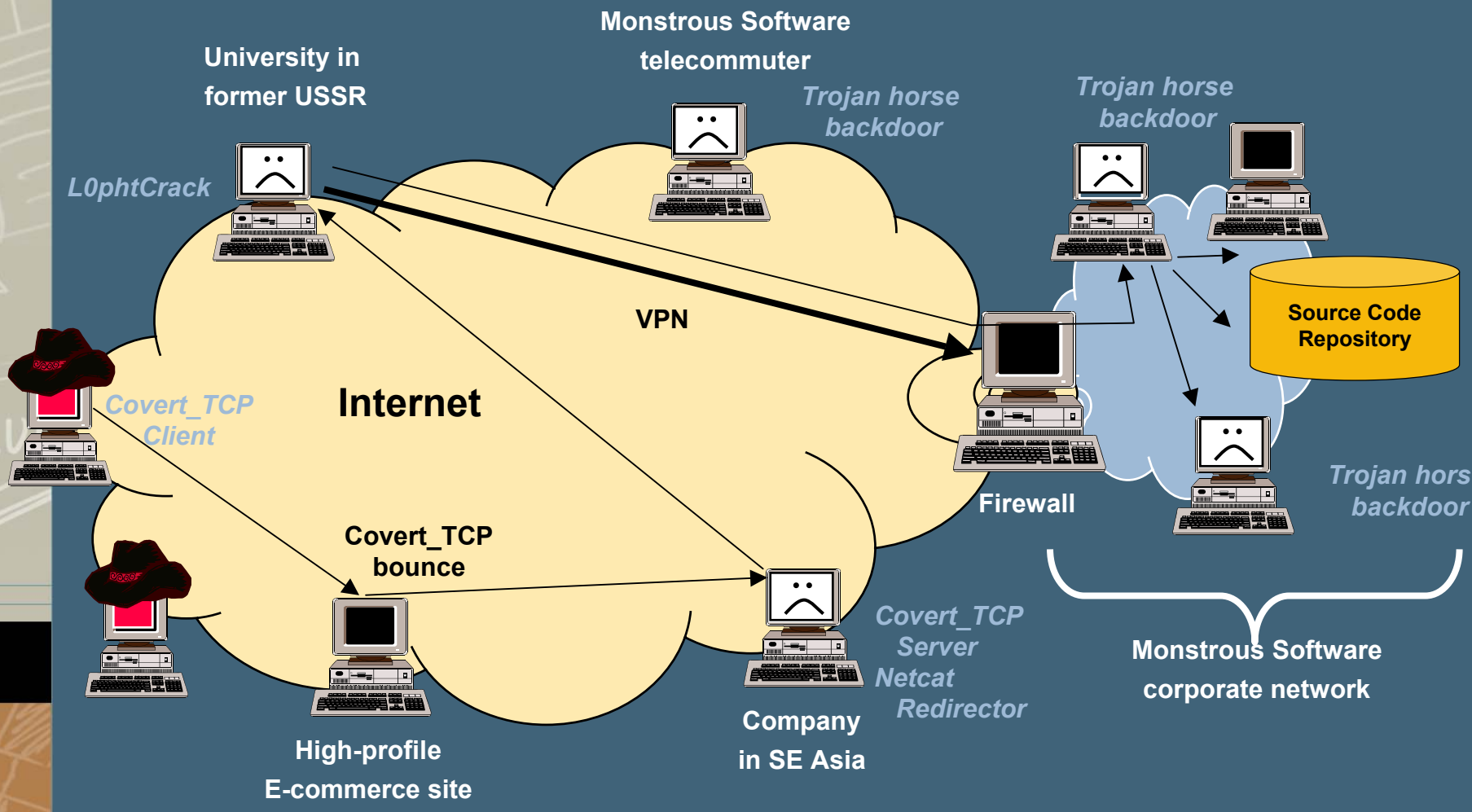
PREDICTIVE SYSTEMS

Attackers Retrieve Passwords



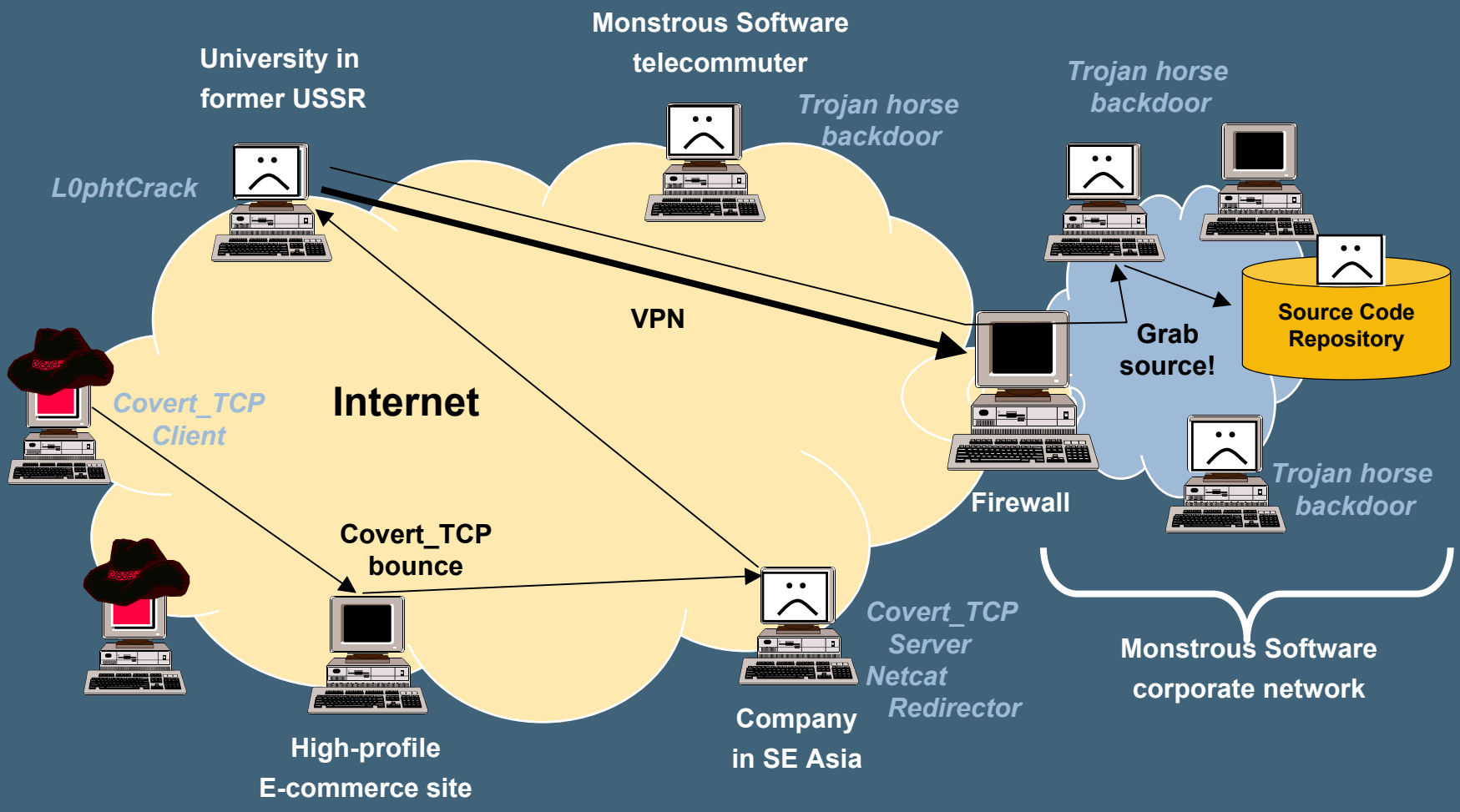
PREDICTIVE SYSTEMS

Attackers Gain Access through VPN



PREDICTIVE SYSTEMS

Attackers Grab Source Code!




```
Foobar
source
code
main()
...
```

PREDICTIVE SYSTEMS

Hack, Counter Hack

Purpose of the seminar and general trends

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Exploiting systems
- Step 4: Keeping access
- Step 5: Covering the tracks
- Putting it all together
- **Conclusions**

Conclusions

- Attacks are becoming more sophisticated, yet easier to launch
- Attacks are seldom isolated, one-type events. Various hacks are combined
- All the defensive strategies we've discussed come down to:
  - Do a thorough, professional job of securing your systems
- This does not guarantee that you will not be attacked
  - But it does help to ensure you will have an effective means of handling attacks
- By remaining diligent, you can defend your systems and maintain a sound, secure environment!

PREDICTIVE SYSTEMS

Security Incidents and Information

Case Studies and Solutions

Types of Incidents

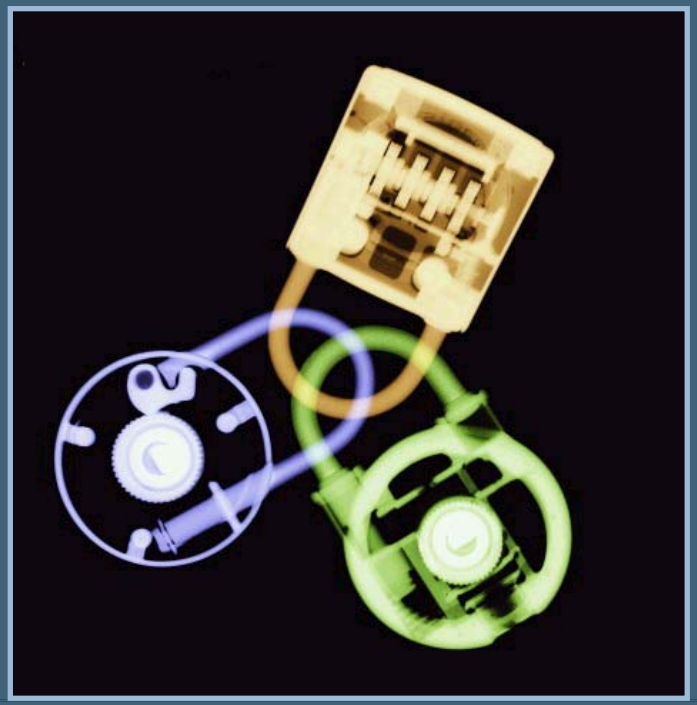
- Denial of service
- System compromise:
  - Local/remote
  - Root/admin/user
  - Vulnerability
  - Configuration
  - Accounts
  - Virus/worm

Other:

- Email
- Errors
- Deception
- Social engineering
- Misuse

Typical Investigation Goals

- Compromised? How? When? Depth?
- Post-compromise activity?
- Source?
- Recommendations? Immediate and future?



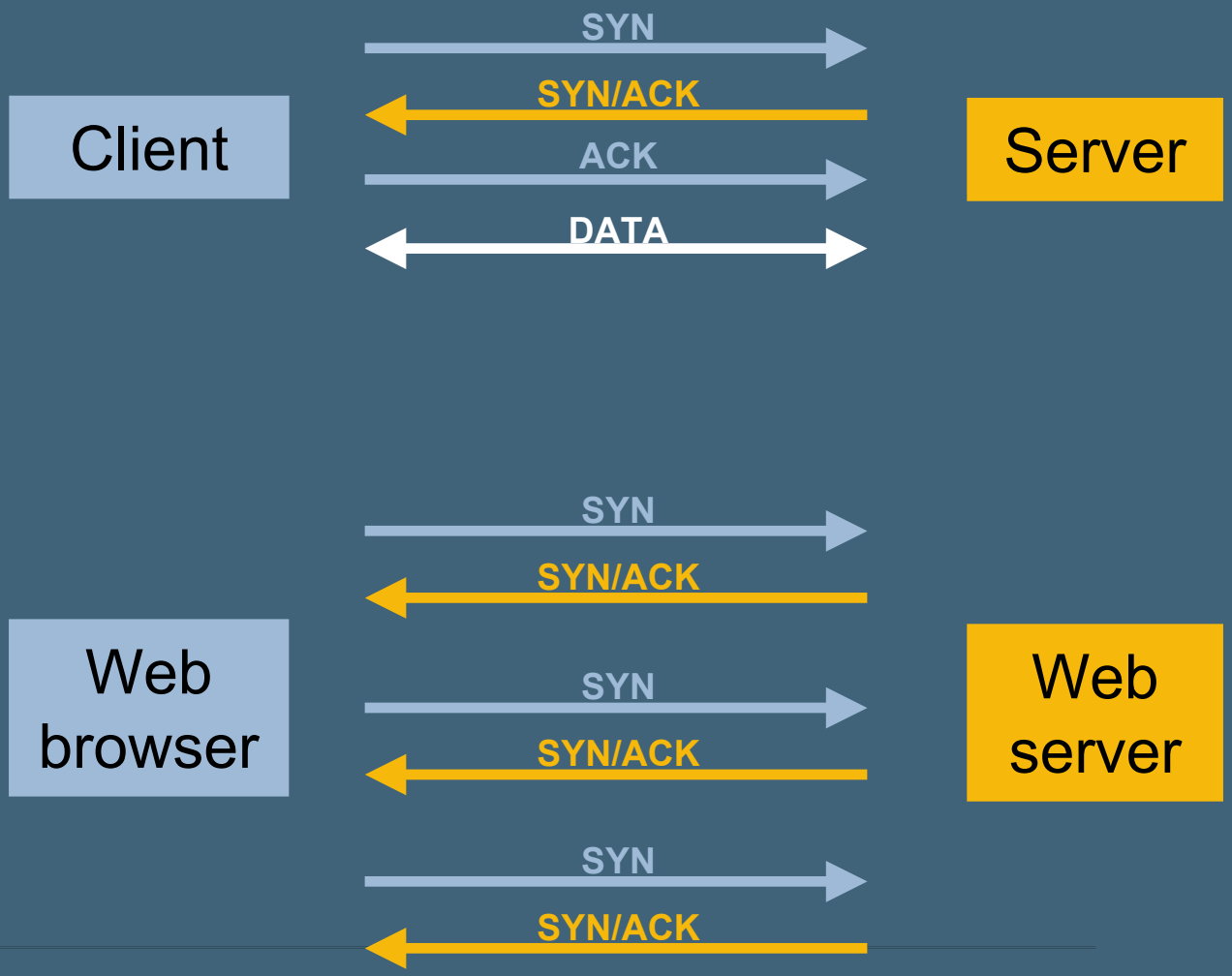
PREDICTIVE SYSTEMS

Types of Analysis

- UNIX
- NT
- Network
- Email
- Various logs (firewall, Web server, etc.)
- Process, architecture
- Profiling
- Interviews

Case Study #1

Situation: E-commerce site under SYN flood attack



PREDICTIVE SYSTEMS

Case Study #1

- Situation: E-commerce site under SYN flood attack
- Investigation:
  - Source IPs spoofed
  - Identified attack tool, number of sources
  - Traceback
  - Monitor

TIME	SOURCE IP ADDRESS	IP-1	IP-2	IP-3	IP-4	SRC PORT	DST IP	DST PORT
99483436.27	64.135.72.199	64	135	72	199	61287	192.168.0.4	80
99483436.60	151.178.183.9	151	178	183	9	63564	192.168.0.4	80
99483436.93	238.221.39.74	238	221	39	74	306	192.168.0.4	80
99483437.26	70.9.150.139	70	9	150	139	2583	192.168.0.4	80
99483437.59	157.52.6.204	157	52	6	204	4860	192.168.0.4	80
99483437.92	244.95.117.14	244	95	117	14	7137	192.168.0.4	80
99483438.25	76.138.228.79	76	138	228	79	9414	192.168.0.4	80
99483438.58	163.181.84.144	163	181	84	144	11691	192.168.0.4	80
99483438.91	250.224.195.209	250	224	195	209	13968	192.168.0.4	80
99483439.24	82.12.51.19	82	12	51	19	16245	192.168.0.4	80

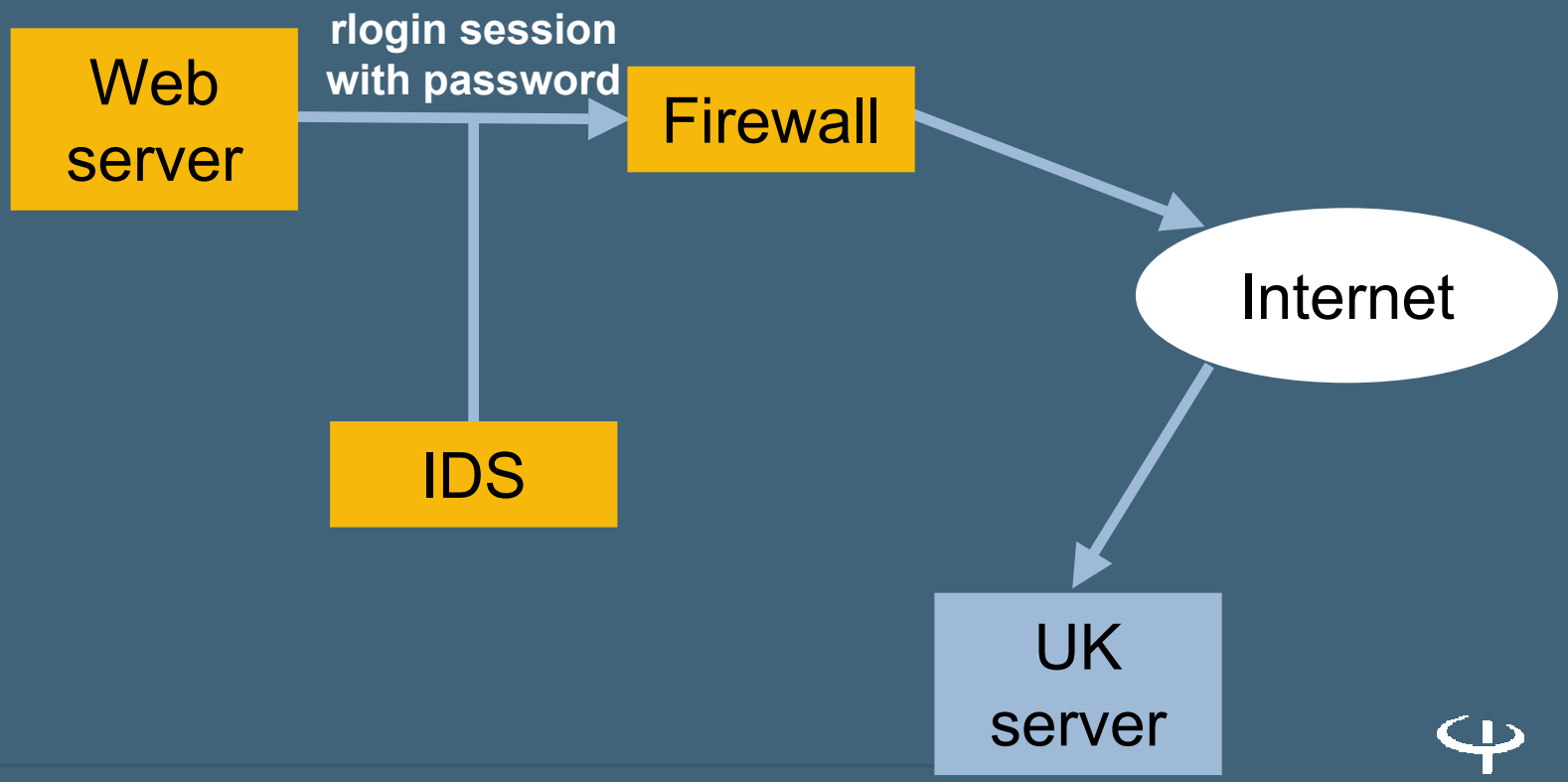
Case Study #1

- Situation: E-commerce site under SYN flood attack
- Investigation:
  - Source IPs spoofed
  - Identified attack tool, number of sources
  - Traceback
  - Monitor
- Results: Attacks ceased

PREDICTIVE SYSTEMS

Case Study #2

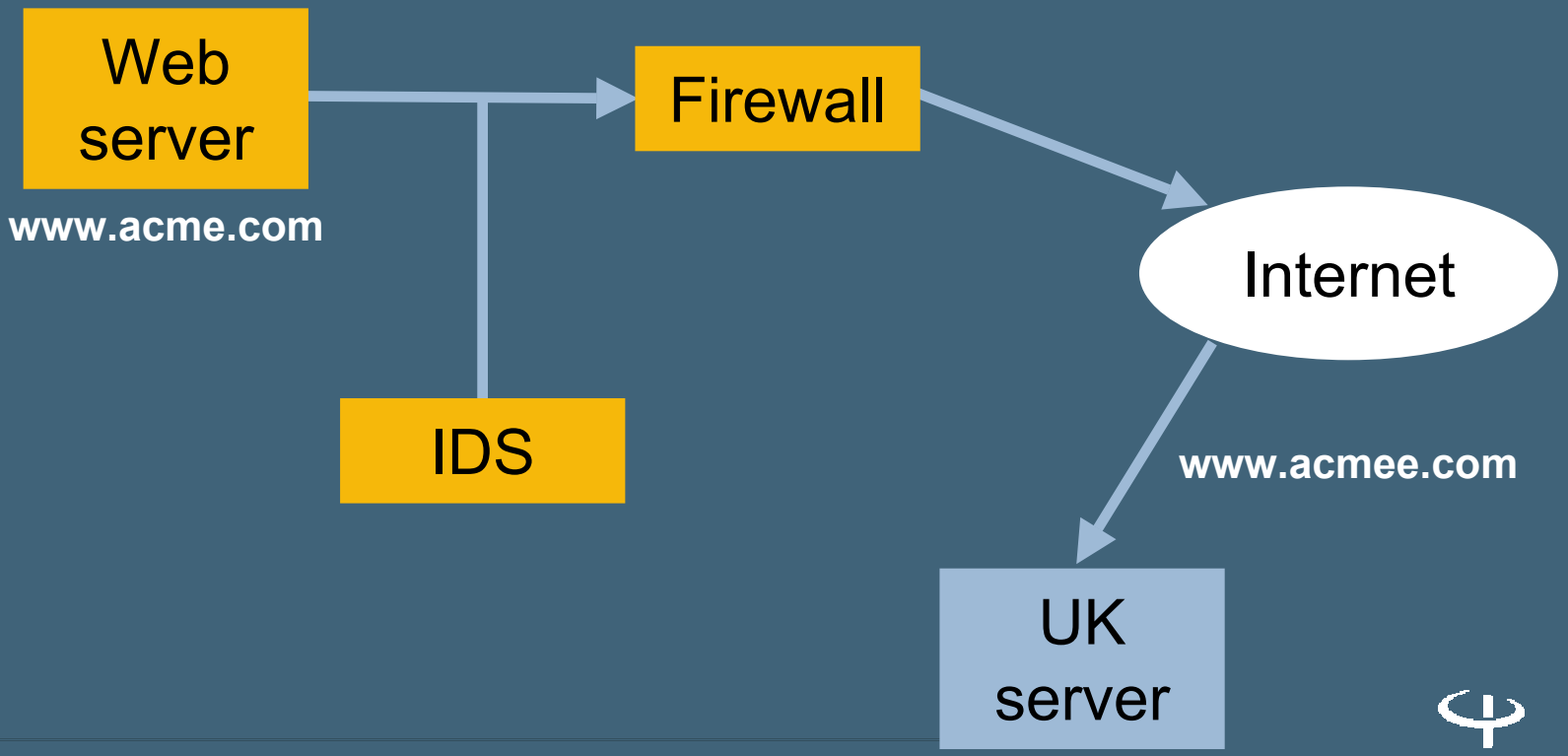
Situation: Passwords sent to remote site



PREDICTIVE SYSTEMS

Case Study #2

- Situation: Passwords sent to remote site
- Investigation:
  - Remote site adopting similar domain names
  - Administrator mistyped domain name



Case Study #2

- Situation: Passwords sent to remote site
- Investigation:
  - Remote site adopting similar domain names
  - Administrator mistyped domain name
- Results: Accidental, some malicious aspects

Case Study #3

Situation: 14 of 16 site firewalls crashed, unbootable

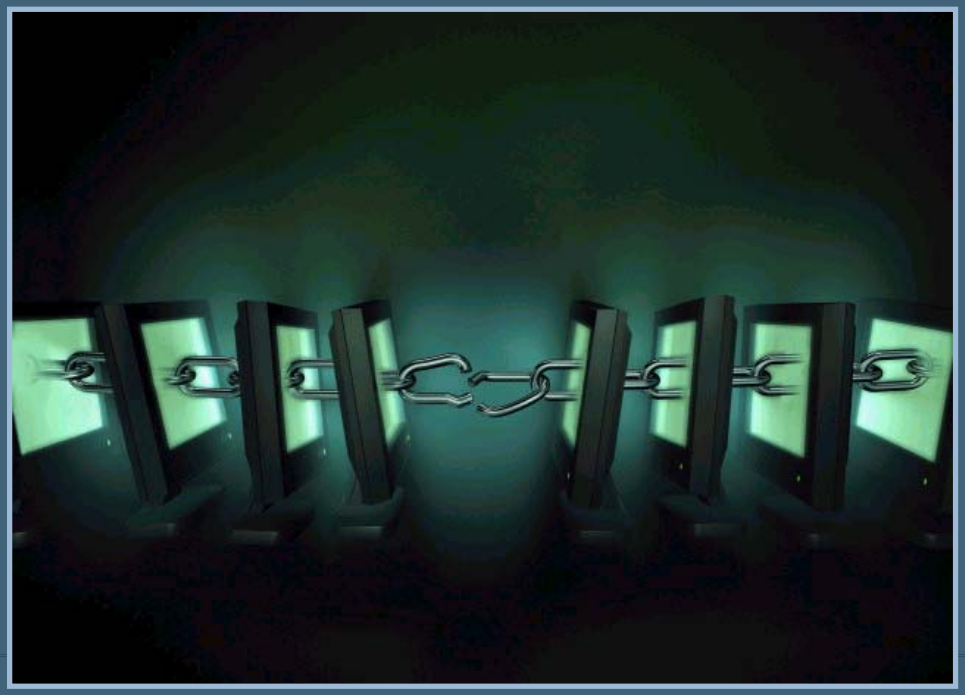
Case Study #3

- Situation: 14 of 16 site firewalls crashed, unbootable
- Investigation:
  - Reviewed build process
  - Dangerous scripts

```
!#/bin/sh
cd /var/log/fw
gzip *.log
cp *.gz
/home/log/storage/
rm -r *
```

Case Study #3

- Situation: 14 of 16 site firewalls crashed, unbootable
- Investigation:
  - Reviewed build process
  - Dangerous scripts
- Results: Accidental, process problem



PREDICTIVE SYSTEMS

Case Study #4

- Situation: Site received extortion demand regarding sensitive proprietary data

PREDICTIVE SYSTEMS

Case Study #4

- Situation: Site received extortion demand regarding sensitive proprietary data
- Investigation:
  - Rootkit material discovered on internal server
  - Default configuration allowed external access

Case Study #4

- Situation: Site received extortion demand regarding sensitive proprietary data
- Investigation:
  - Rootkit material discovered on internal server
  - Default configuration allowed external access
- Results: Suspect arrested, data not released

Case Study #5

Situation: Unauthorized site mirror discovered

PREDICTIVE SYSTEMS

Case Study #5

- Situation: Unauthorized site mirror discovered
- Investigation:
  - Attacker site had links to attacker data
  - Used to perpetrate financial fraud

Case Study #5

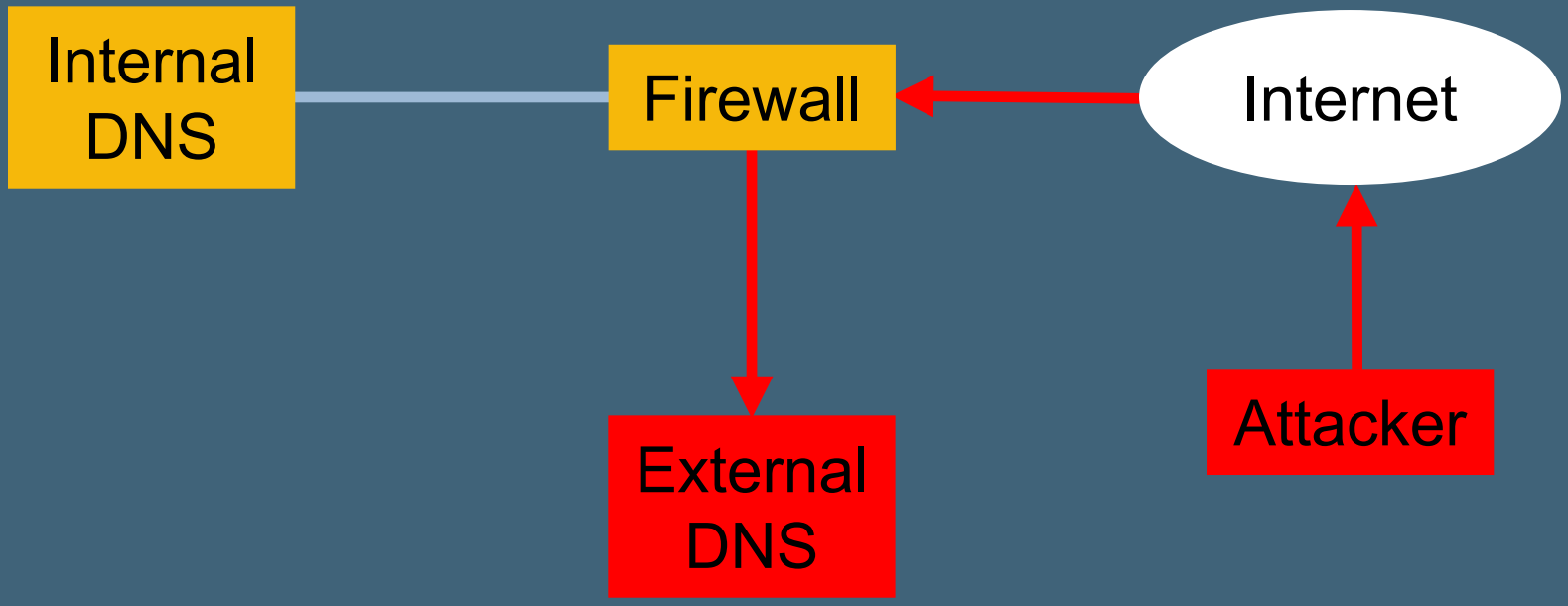
- Situation: Unauthorized site mirror discovered
- Investigation:
  - Attacker site had links to attacker data
  - Used to perpetrate financial fraud
- Results: Site removed,
  trace data collected

Case Study #6

Situation: Unexplained directory on DNS server

Case Study #6

- Situation: Unexplained directory on DNS server
- Investigation:
  - Attacker exploited well-known vulnerability
  - Site admins erased critical evidence
  - Attacker was not aware of internal access

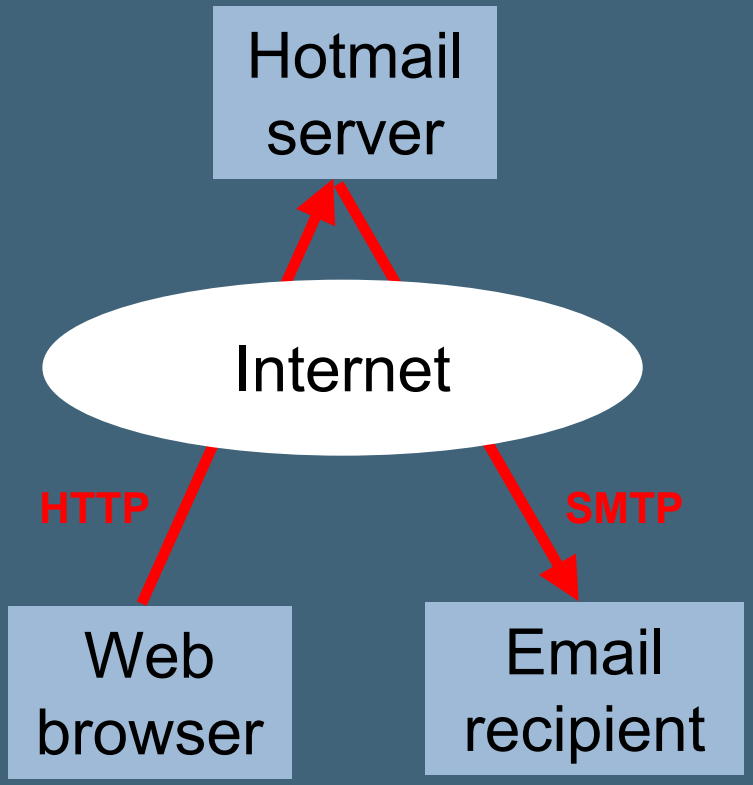


Case Study #6

- Situation: Unexplained directory on DNS server
- Investigation:
  - Attacker exploited well-known vulnerability
  - Site admins erased critical evidence
  - Attacker was not aware of internal access
- Results: No further compromise

Case Study #7

Situation: Malicious email via Hotmail



Case Study #7

- Situation: Malicious email via Hotmail
- Investigation:
  - Source address from school network
  - Email sent 10:00 p.m. Friday evening
  - Physical access logs

```
[email header]
Received by: …
…
X-IP-Source: 192.168.0.6
…

[email body]
Dear Smith,
<insert threat here>
...
```

Case Study #7

- Situation: Malicious email via Hotmail
- Investigation:
  - Source address from school network
  - Email sent 10:00 p.m. Friday evening
  - Physical access logs
- Results: Sender not identified

PREDICTIVE SYSTEMS

Why Is There a Problem?

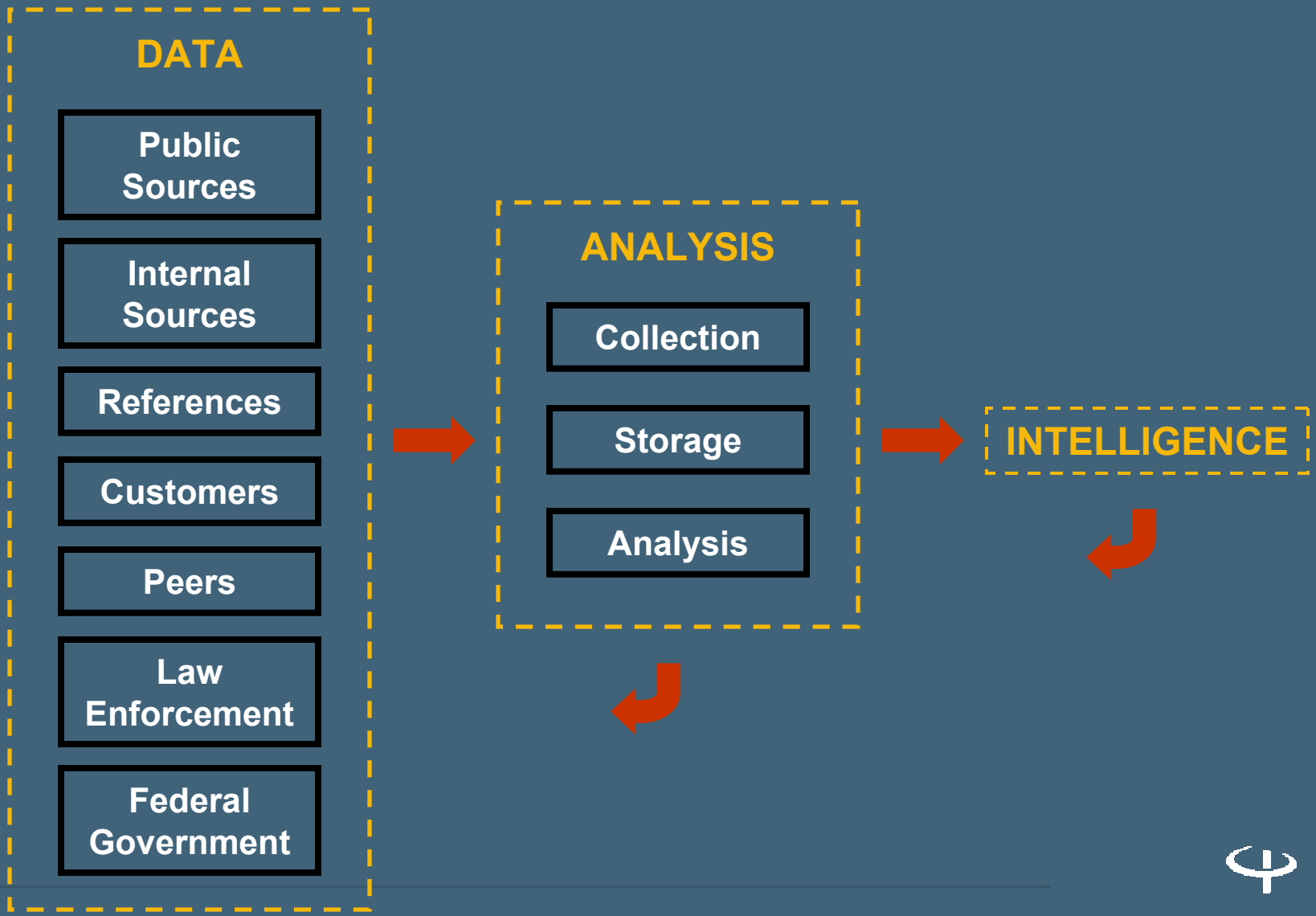
- Companies assume vendors are doing the right thing
- Web speed = not enough time to think about security:
  - Corporations and vendors
- Complexity of systems:
  - Millions of lines of code
  - Product interaction
- Automated tools lower level of required expertise
- Web security is inconsistent (weakest link)
- Many targets (commercial, personal, public)
- Policy enforcement
- Lack of useful information

Solutions

- Patch process,
- System maintenance,
- Regular testing,
- Defensive capabilities,
- Response plan and capability, and so on….

- All require information:
  - Timely
  - Integrated
  - Reliable
  - Solution-oriented
- Multi-source data collection, analysis, and dissemination

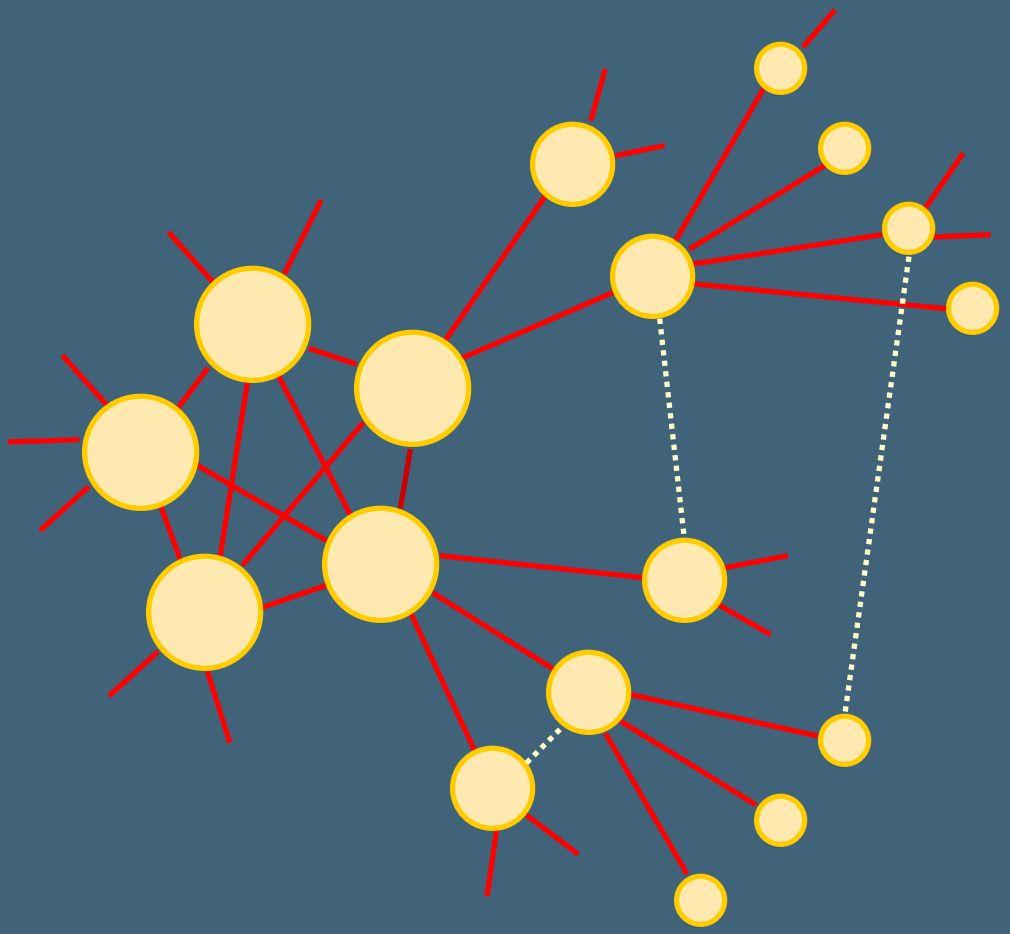
Data + Analysis = Intelligence



PREDICTIVE SYSTEMS

Information Sharing Framework

- Structure
- Data flow
- Data processing
- Analysis
- Intelligence flow
- Beneficiaries
- Iterative and flexible process



PREDICTIVE SYSTEMS

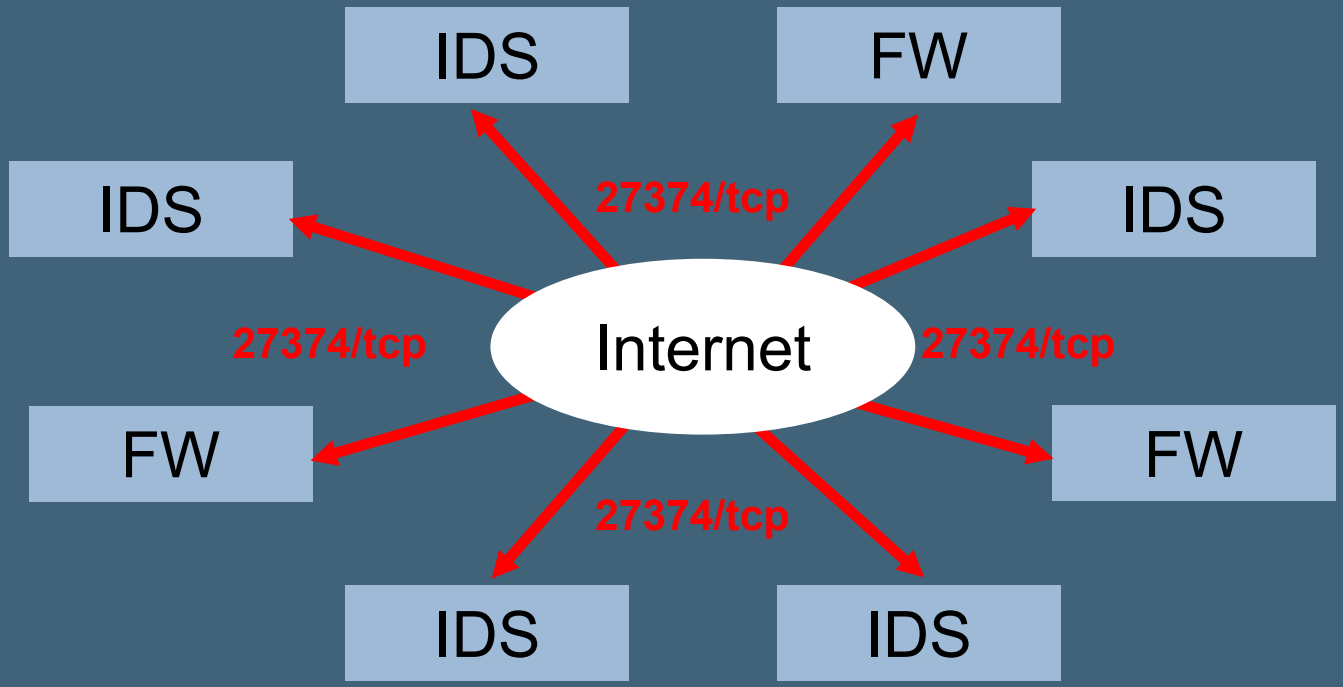
Benefits

- Early warning
- Accurate and complete threat assessment
- Comprehensive analysis (specific expertise)
- Empirical data and actionable recommendations
- Model supports a dynamic threat environment

PREDICTIVE SYSTEMS

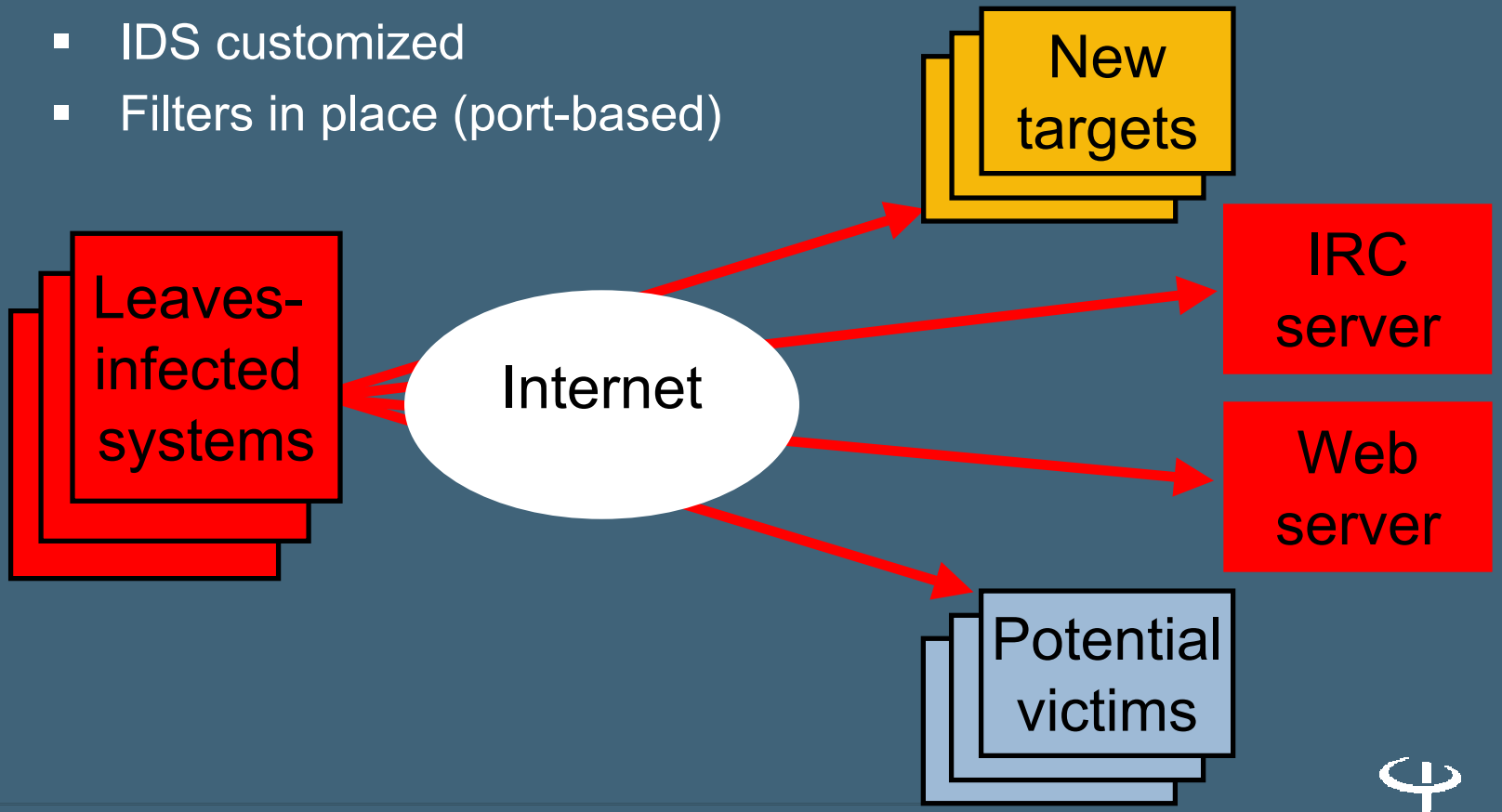
Case Study #8

Situation: Leaves



Case Study #8

- Situation: Leaves
- Investigation:
  - Emerging threat
  - IDS customized
  - Filters in place (port-based)



PREDICTIVE SYSTEMS

Case Study #8

- Situation: Leaves
- Investigation:
  - Emerging threat
  - IDS customized
  - Filters in place (port-based)
- Results:
  - Restricted spread
  - No attack
  - Arrest

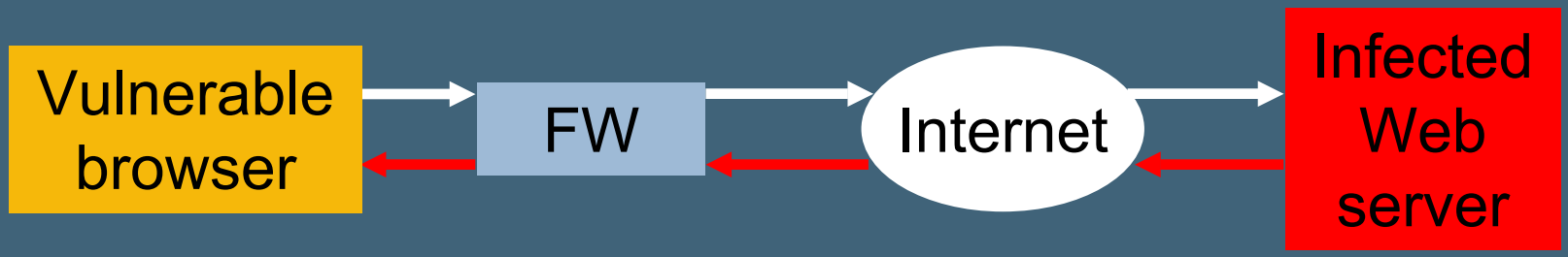
Case Study #9

Situation: Nimda

PREDICTIVE SYSTEMS

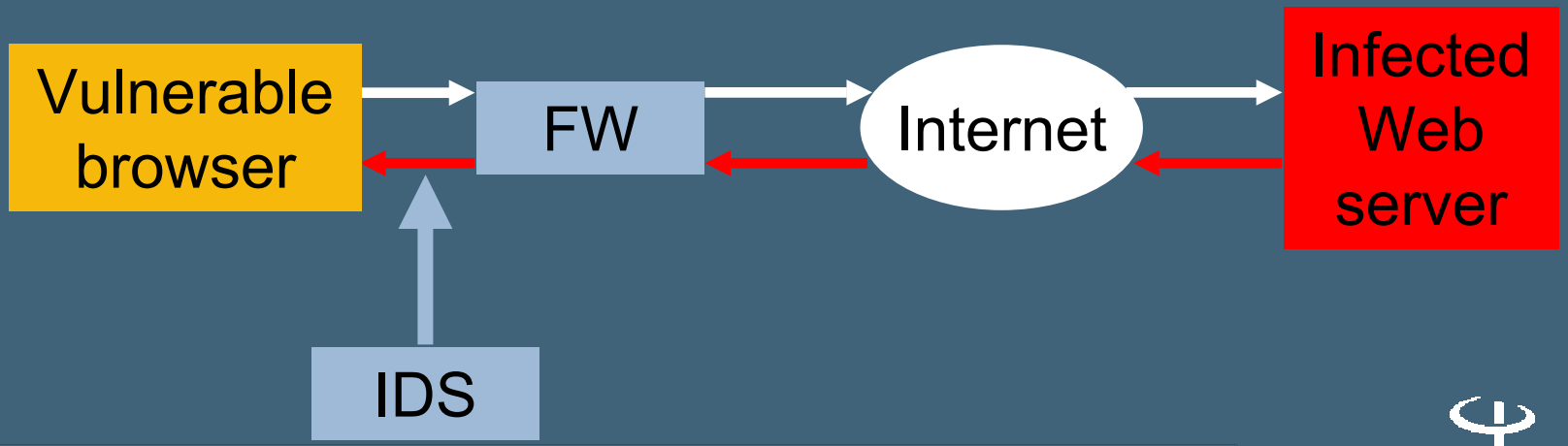
Case Study #9

- Situation: Nimda
- Investigation:
  - Emerging threat
  - IDS customized
  - Filters in place (email and script)



Case Study #9

- Situation: Nimda
- Investigation:
  - Emerging threat
  - IDS customized
  - Filters in place (email and script)
- Results:
  - Compromised system
  - No infection



Questions & Answers

PREDICTIVE SYSTEMS