Firewalls

COMP620

“I wish my wish would not be granted!”

Douglas R. Hofstadter

Gödel, Escher, Bach: An Eternal Golden Braid

Mu Puzzle

Start with the string **MI** and convert to **MU**

Rule 1 – If the string ends in **I**, you can add **U** to the end

- **MI** can change to **MIU**

Rule 2 – A string **M***x* can be changed to **M***xx*

- **MIU** can change to **MIUIU**

More Mu

Rule 3 – If the string ends in **III**, you can replace the **III** with a **U**

- **MUIII** can change to **MUU**

Rule 4 – If **UU** occurs in a string, you can drop the **UU**

- **MUUII** can change to **MII**

To Be Discussed Wednesday

"There you have it. Now you may begin trying to make MU. Don't worry if you don't get it. Just try it out a bit – the main thing is for you to get the flavor of this MU-puzzle. Have fun."

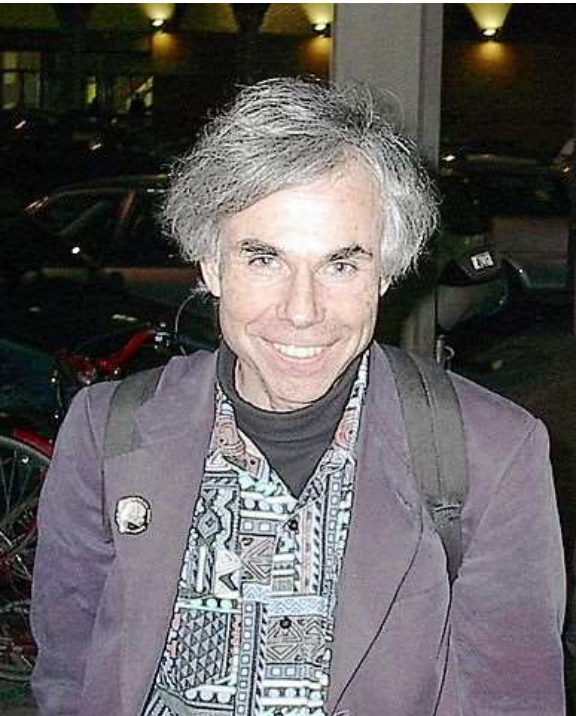


photo by Maurizio Codogno

Douglas Hofstadter

Gödel, Escher, Bach: an Eternal Golden Braid

Proof that you cannot get from MI to MU

- Consider the number of **`I`**'s in the string
- Only rule 2 and 3 change the number of **`I`**'s
  - rule 2 will double the number of **`I`**'s
  - rule 3 will reduce it by 3
- The number of **`I`**'s is never divisible by 3
  - The initial one **`I`** is not divisible by 3
  - If n is not divisible by 3, neither is 2n
  - if n is not divisible by 3, neither is n - 3
- Eliminating the **`I`** to get MU creates zero **`I`**'s, which is divisible by 3. Thus it cannot be done.

So What?

- What do we learn from the MU puzzle besides a %$#! problem with no solution?
- If there was a solution, you could demonstrate the solution by giving a list of rules that would transform MI to MU
- Following the four rules of the system, you cannot show that cannot transform MI to MU
- You have to “jump out of the system” and start to reason *about* the system

Gödel's Incompleteness Theorems

- Kurt Gödel wrote these in 1933
- Demonstrates the inherent limitations of every formal axiomatic system capable of modelling basic arithmetic
- The first incompleteness theorem states that no consistent system of axioms whose theorems can be listed by an effective procedure (i.e., an algorithm) is capable of proving all truths about the arithmetic of the natural numbers
- Formal systems have truths that cannot be proven

Wikipedia

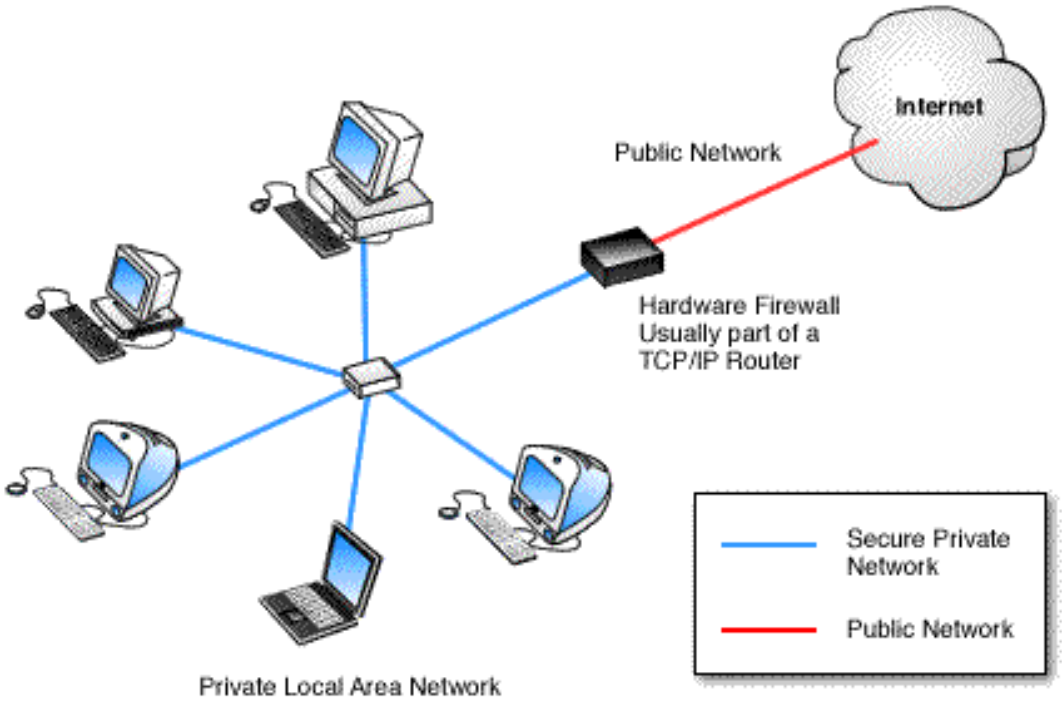
Ken Thompson on Trusting Trust

Ken Thompson & Dennis Richie

- A story in three parts
  - You can write a program that duplicates itself
  - A compiler can be trained to map source to output not shown in the source
  - A compiler can be corrupted to insert a Trojan Horse in the generated machine language
- By applying these steps, you can create a compiler with a Trojan Horse that does not appear in the compiler source code

Firewall Purpose

- A **firewall** is designed to block unauthorized access while permitting authorized communications



Hardware or Software

- Computers may have firewall software which filters network traffic to and from that computer
- Firewalls can be built into network routers. These are often placed between the local network and the Internet
- Separate firewall boxes are available to filter the traffic

Types of Firewall Techniques

- Packet filter – Network layer
- Circuit-level gateway – Transport layer
- Application gateway – Application layer
- NAT or Proxy server

Packet Filtering

- A simple firewall is a packet filter. It only allows packets to pass through the firewall if they meet a specified criteria.
- Firewalls need to be configured to define what network traffic is desired and what should be prohibited

Filter Criteria

Firewalls can filter traffic at the network level based on several criteria

- **Source address** – The IP address of the computer sending the packet. *This can be forged.*
- **Destination address** – The IP address of the computer to receive the packet
- **Port number** – The UDP or TCP port of the destination
- **Protocol** – The network protocol used

Application Filtering

- Applies security mechanisms to specific applications, such as FTP and Telnet
- Can be very effective, but can impose a performance degradation
- Modern application firewalls may also offload encryption from servers

Circuit-Level Firewalls

- Applies security mechanisms when a TCP connection is established
- Once the connection has been made, packets can flow between the hosts without further checking
- More efficient since checks are only made during connections
- Not applicable to UDP

Configuration

- Typically a firewall needs to be configured to define what you want to prevent or allow
- A new application may require access to the Internet in a manner that was previously denied
- There is a wide range of firewall configuration interfaces

Perimeter Protection

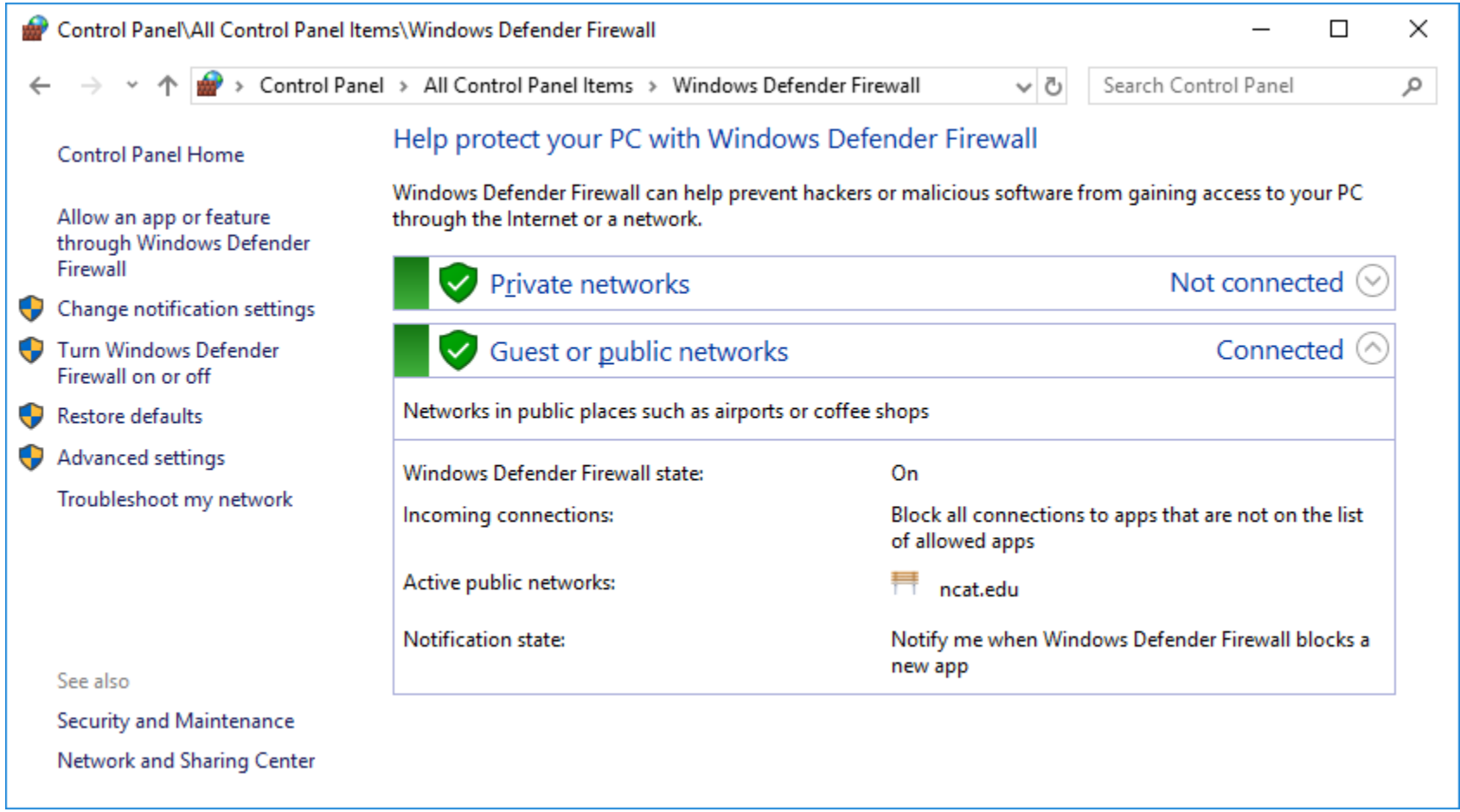
- Firewalls typically block traffic as it enters or leaves the network
- Attacks from within the local network are not filtered by a router firewall

DMZ

- An intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a “perimeter network” or demilitarized zone (DMZ)
- A public web server might be located in the DMZ. You have to allow public access although you may want to restrict the type of access

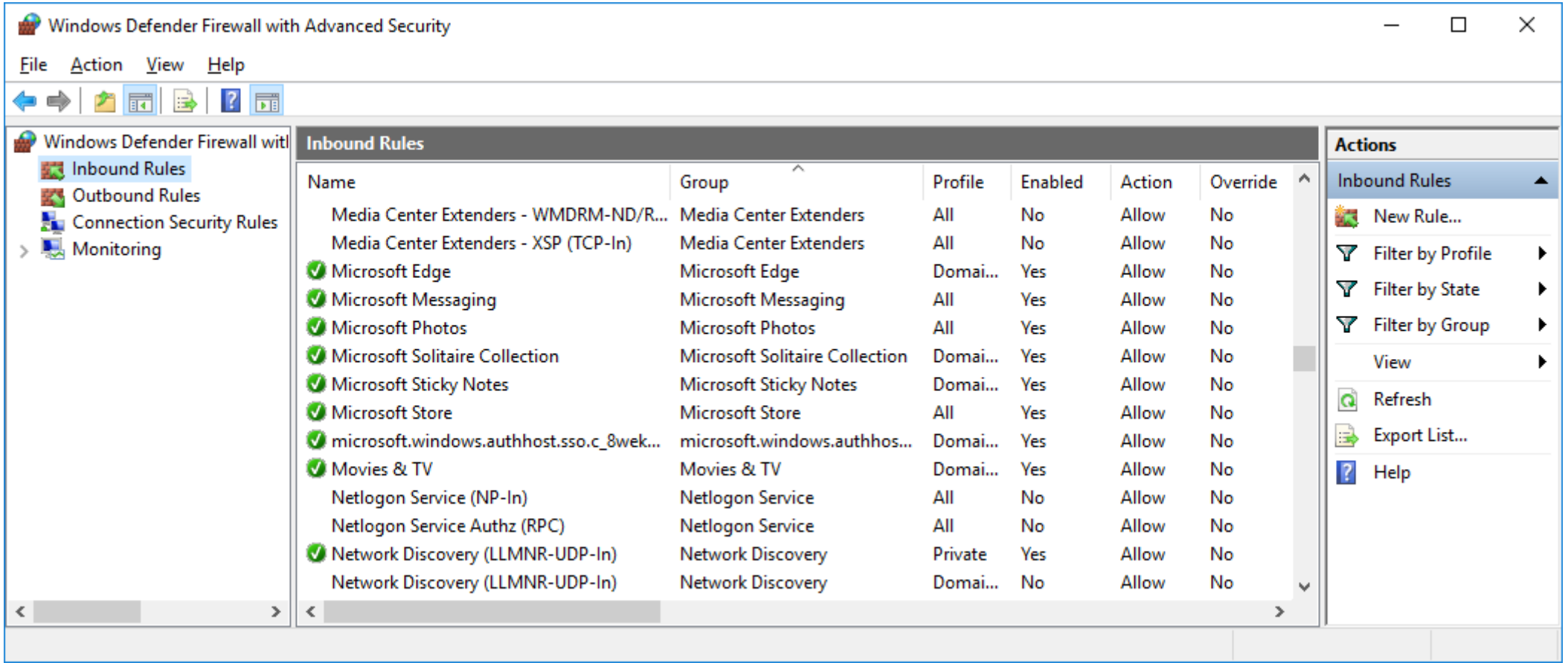
Microsoft Windows Firewall

- The firewall can be accessed from the control panel
- You can allow or prohibit specific network traffic



Windows Firewall Exceptions

- The general rule is to not allow anything
- You can add or remove programs or disable rules



How do you know a bad packet when you see one?

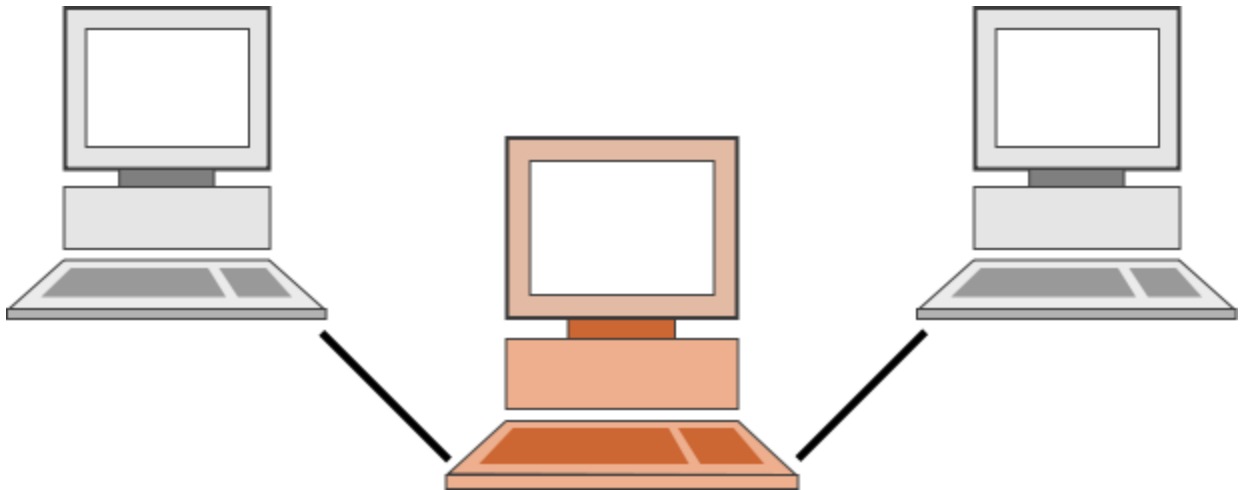
- It is often difficult to characterize an evil packet
- Many firewall systems block everything unless there is a known need for a specific traffic type
- Denial of service flooding attacks typically send a large number of “valid” packets

Email Filtering

- Email filters attempt to remove malicious email and spam
- More than 97% of all emails sent over the net are unwanted
- As of August 2010, the number of spam messages sent per day was estimated to be around 200 billion

Proxy Servers

- A proxy server acts as an intermediate between a client and a server
- All traffic between the client and server goes through the proxy



Proxy Server Services

- Filter malicious packets
- Cache frequently accessed information
- Block undesirable sites
- Bypass restrictions
- Provide tunneling using other protocols

Anonymous Proxy Servers

- Anonymous proxy servers can be used to allow users to send email or view a website without revealing their identity
- A user can send email to an anonymous email proxy which forwards it to the desired receiver after stripping all sender identification