SENG 360 - Security Engineering
Network Security (cont'd)

Jens Weber

Fall 2022

University of Victoria

Email security

End-to-End encryption (with PGP or CA-signed keys) has never caught on

Today most servers use **TLS** -> mitigates bulk eavesdropping

- **MTA Strict Transport Security (MTA-STS)** requires signed certificate

Domain Keys Identified Mail (DKIM) ties email to the sending domain (by digital signature)

Sender Policy Framework (SPF) ties email to sending IP (by sig.)

- No forwarding possible

Authentication Received Chain (ARC) re-signs email upon forward

Domain-based Message Authentication, Reporting and Conformance (DMARC)

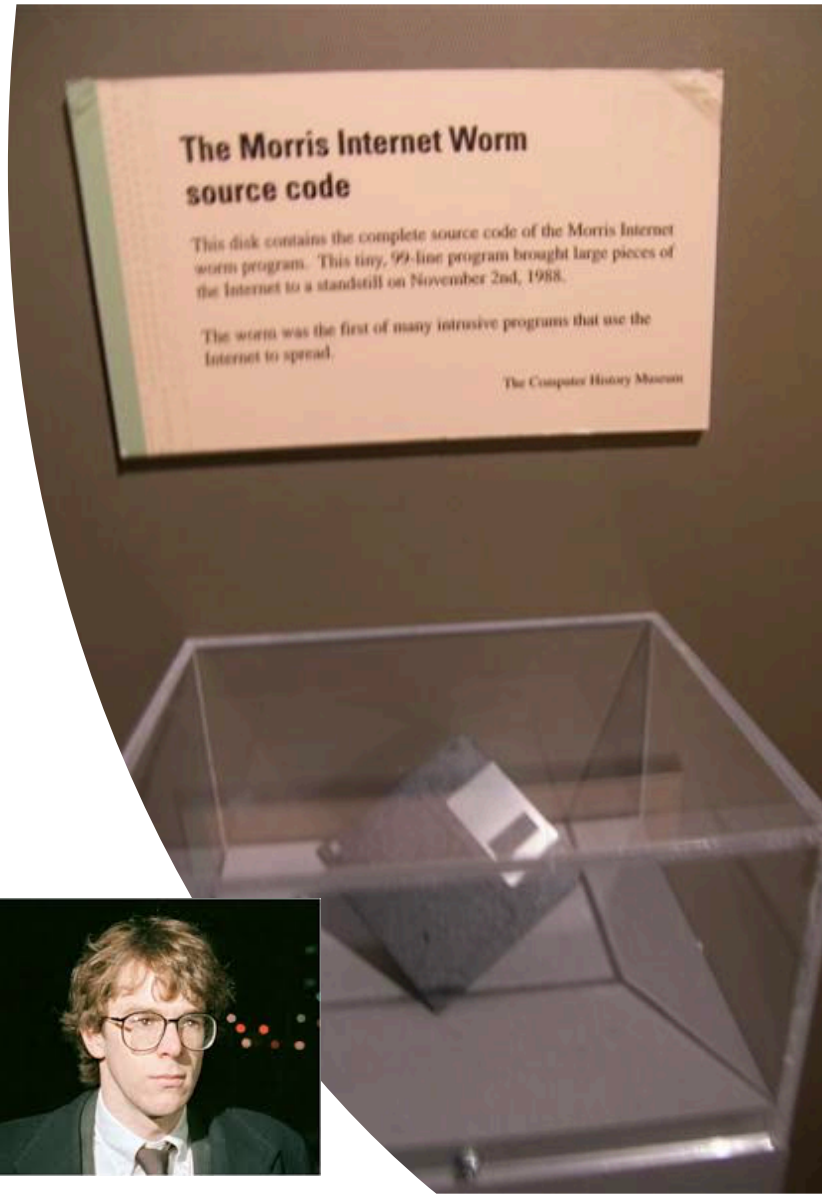
- A record attached to a DNS entry containing policies on emails received from there

Malware types (not mutually exclusive)

- A **Trojan** is a useful (or apparently useful) program containing a hidden (unwanted) function
- A **worm** is a malicious program that replicates itself on other systems
- A **virus** is code that hooks itself in code of other programs
- A **remote access Trojan (RAT)** is software that enables a remote party to access the device it runs on
- A **rootkit** is software that (stealthily) enables another party to control the device it runs on
- **Potentially unwanted software (PUS)** does something user doesn't want

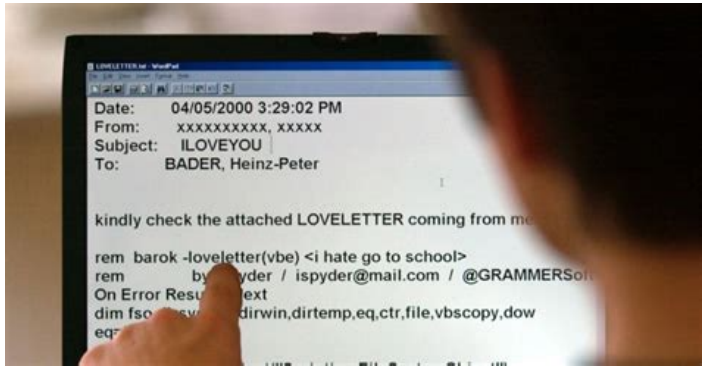
The first famous worm (1988): The Morris Worm

- Uses the Unix “finger” program to discover remote users / machines
- Cracks passwords (dictionary / brute force)
- Exploits trapdoor ”debug option” in remote process that receives email
- Clogged up the Internet (Arpanet)



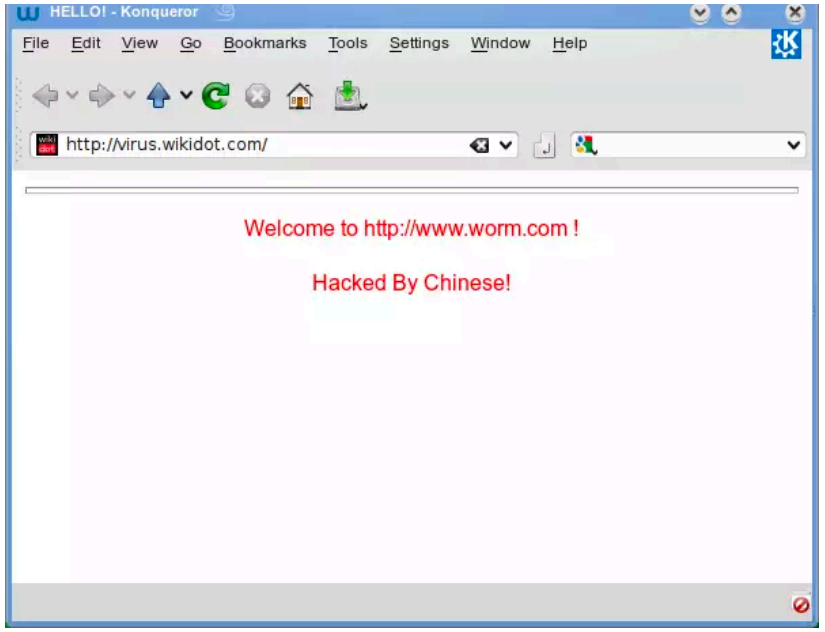
Macro-worms:
The Love Bug (2000)

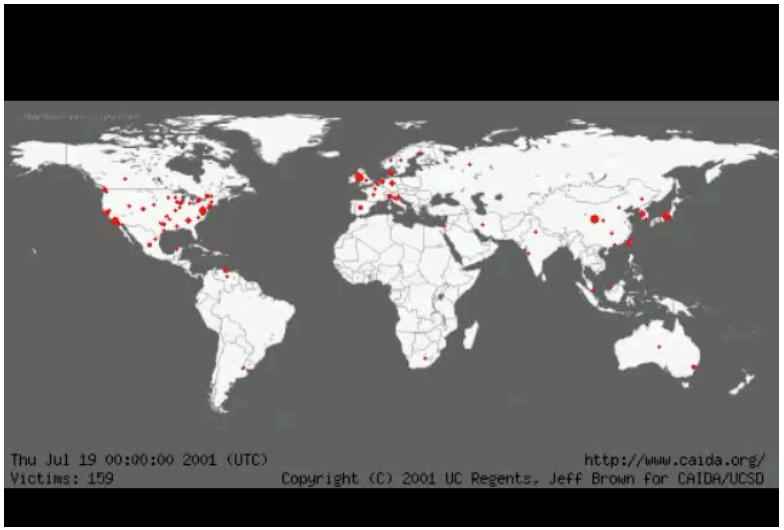
- Used “macro” languages of “office programs”
- Attached “LOVE-LETTER-FOR-YOU.txt.vbs” to emails
- Upon opening, sends emails to all in address book
- Infected 10 million computers
- US$ 5.5-8.7 billion damages



Flash worms: Code Red (2001)

- Exploits security hole in Internet Information Server (IIS)
- Targets random IP addresses
- Carries out DoS attack on government sites





Spyware and adware

Log in | Sign up | Forums

The Register®
Biting the hand that feeds IT

DATA CENTRE | SOFTWARE | SECURITY | DEVOPS | BUSINESS | PERSONAL TECH | SCIENCE

Security

German states defend use of 'Federal Trojan'

Skype-snooping Bundestrojaner legal, insists gov

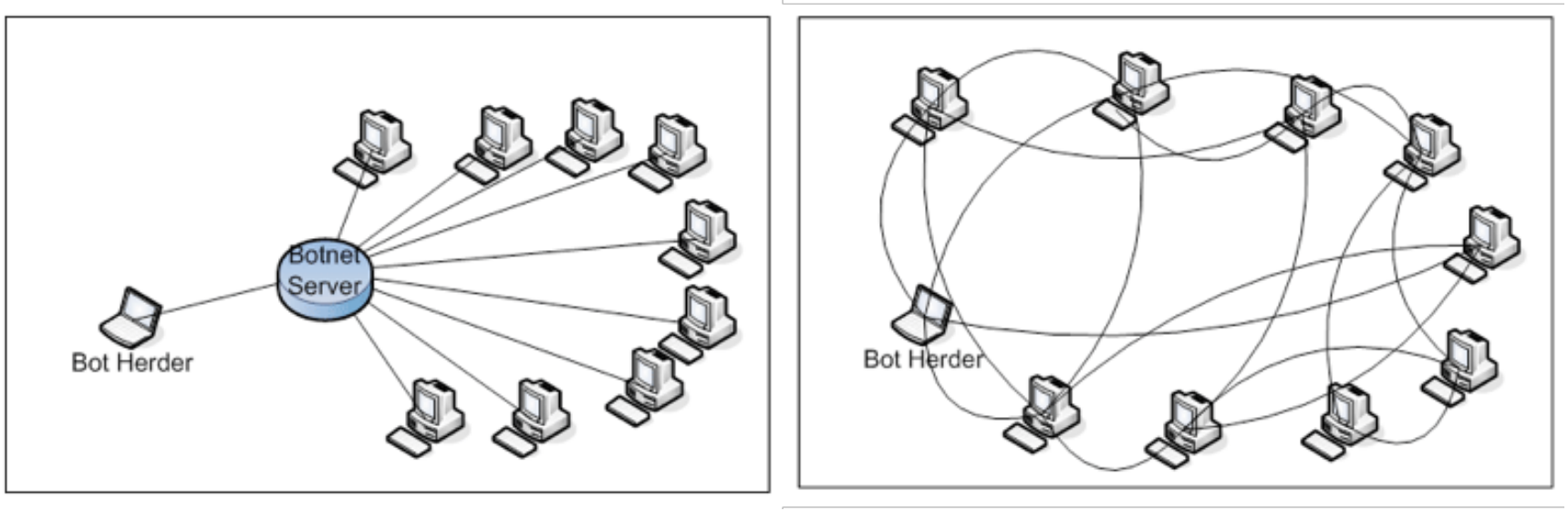
By John Leyden 12 Oct 2011 at 15:19 28 SHARE ▼

Five German states have admitted using a controversial backdoor Trojan to spy on criminal suspects.

Samples of the so-called R2D2 (AKA "0zapftis") Trojan came into the possession of the Chaos Computer Club (CCC), which published an analysis of the code last weekend.

German federal law allows the use of malware to eavesdrop on Skype conversations. But the CCC analysis suggests that the specific Trojan it wrote about is capable of a far wider range of functions than this – including establishing a backdoor on compromised machines and keystroke logging. The backdoor creates a means for third parties to hijack compromised machines, while the lack of encryption creates a

Botnets (late 2000 until now)



Note: traditional botnet architectures are easy to “decapitate”

Microsoft Takes Down Dozens of Zeus, SpyEye Botnets

March 26, 2012 52 Comments

Microsoft today announced the execution of a carefully planned takedown of dozens of botnets powered by **ZeuS** and **SpyEye** — powerful banking Trojans that have helped thieves steal more than $100 million from small to mid-sized businesses in the United States and abroad.

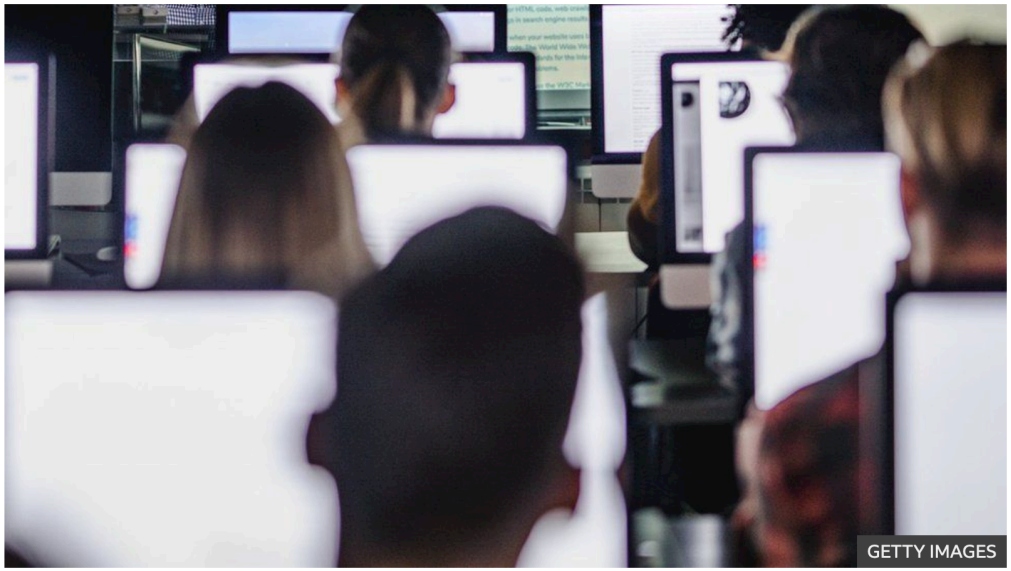
In a consolidated legal filing, Microsoft received court approval to seize several servers in Scranton, Penn. and Lombard, Ill. used to control dozens of ZeuS and SpyEye botnets. The company also was granted permission to take control of 800 domains that were used by the crime machines.The company published a video showing a portion of the seizures, conducted late last week with the help of U.S. Marshals.

Microsoft, U.S. Marshals pay a surprise visit to a Scranton, Pa. hosting facility.

This is the latest in a string of botnet takedowns executed by Microsoft's legal team, but it appears to be the first one in which the company invoked the Racketeer Influenced and Corrupt Organizations (RICO) Act.

Microsoft takes down global zombie bot network

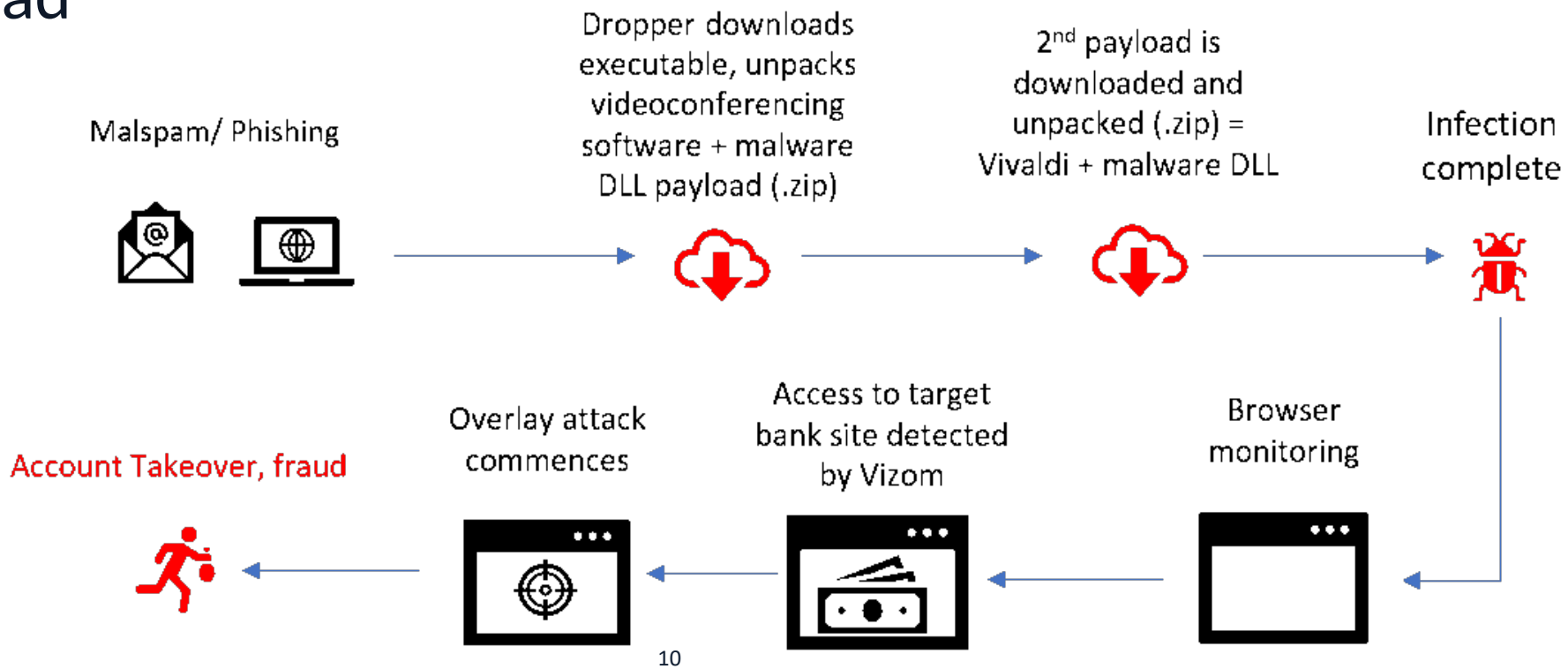
11 March 2020



Microsoft has said it was part of a team that dismantled an international network of zombie bots.

How malware works

Two components: Replication mechanism (dropper) and payload



Countermeasures

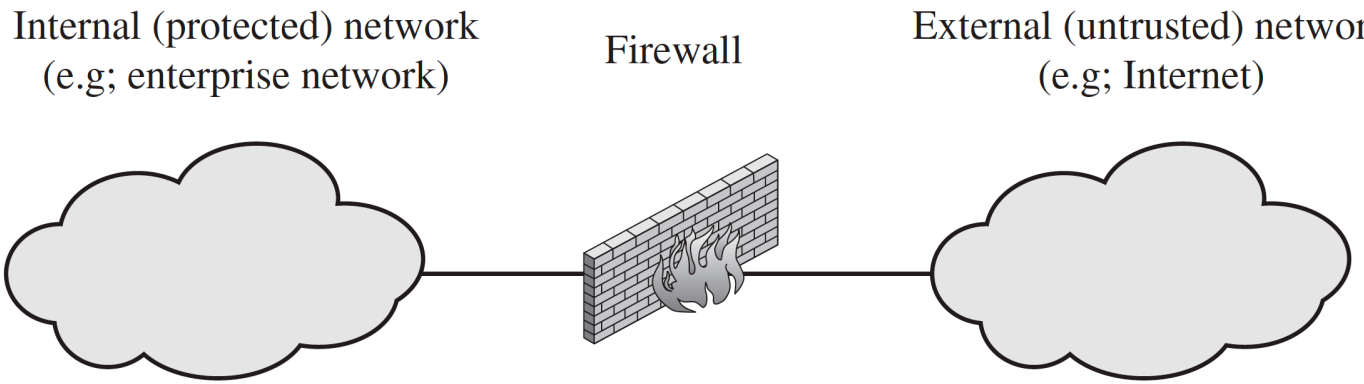
Antivirus software:

- Scanners
  - Search for indicators of compromise (IoC)
  - Stealth/polymorphic malware complicates this
- Check-summers
  - Whitelist executables with checksums

Defenses combine tools, management and incentives

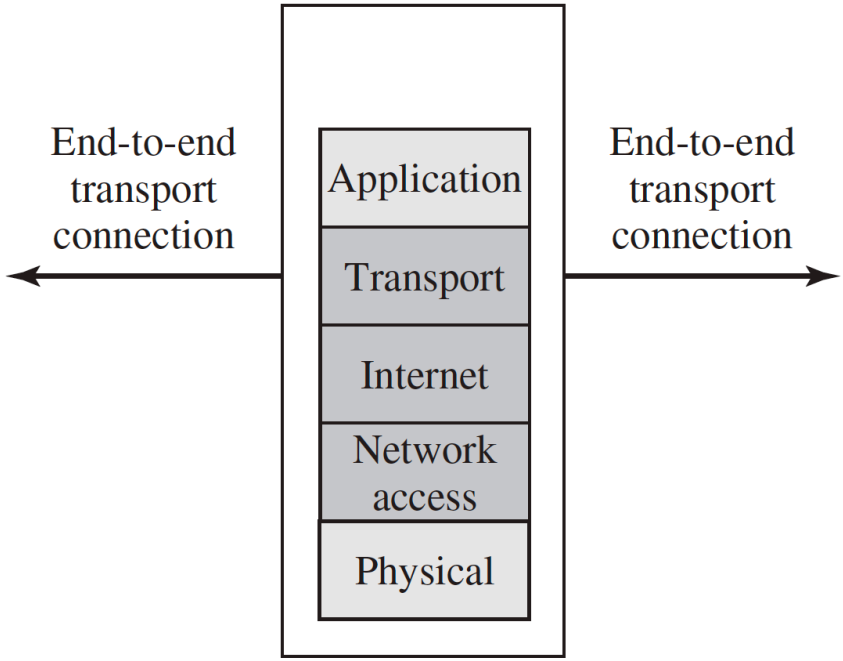
Filtering: firewalls

- All traffic from inside to outside, and vice versa, must pass through the firewall
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration



Packet filtering

Applies rules to each incoming and outgoing IP packet



Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

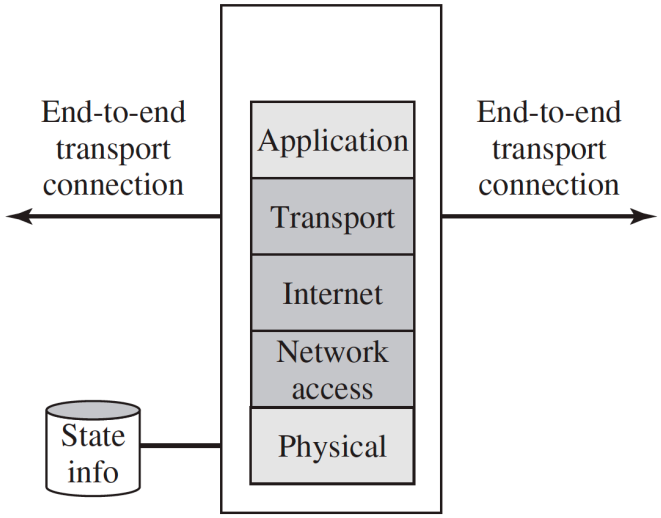
Limitations of Packet Filtering

- Cannot block application-specific vulnerabilities
- Limited logging functionality
- No/limited capability to detect network address spoofing
- Easy to “misconfigure” due to the limited configuration choices

University of Victoria

Circuit gateways

- Keep track of connection status
- Work at the session/TCP level
- Can also provide VPN functionality



University of Victoria

Application proxies

- Work at the application level
- Understand one or more application services (e.g., mail, web)
- Can become bottlenecks
- Important for zero-trust model (a proxy in front of any service)

University of Victoria

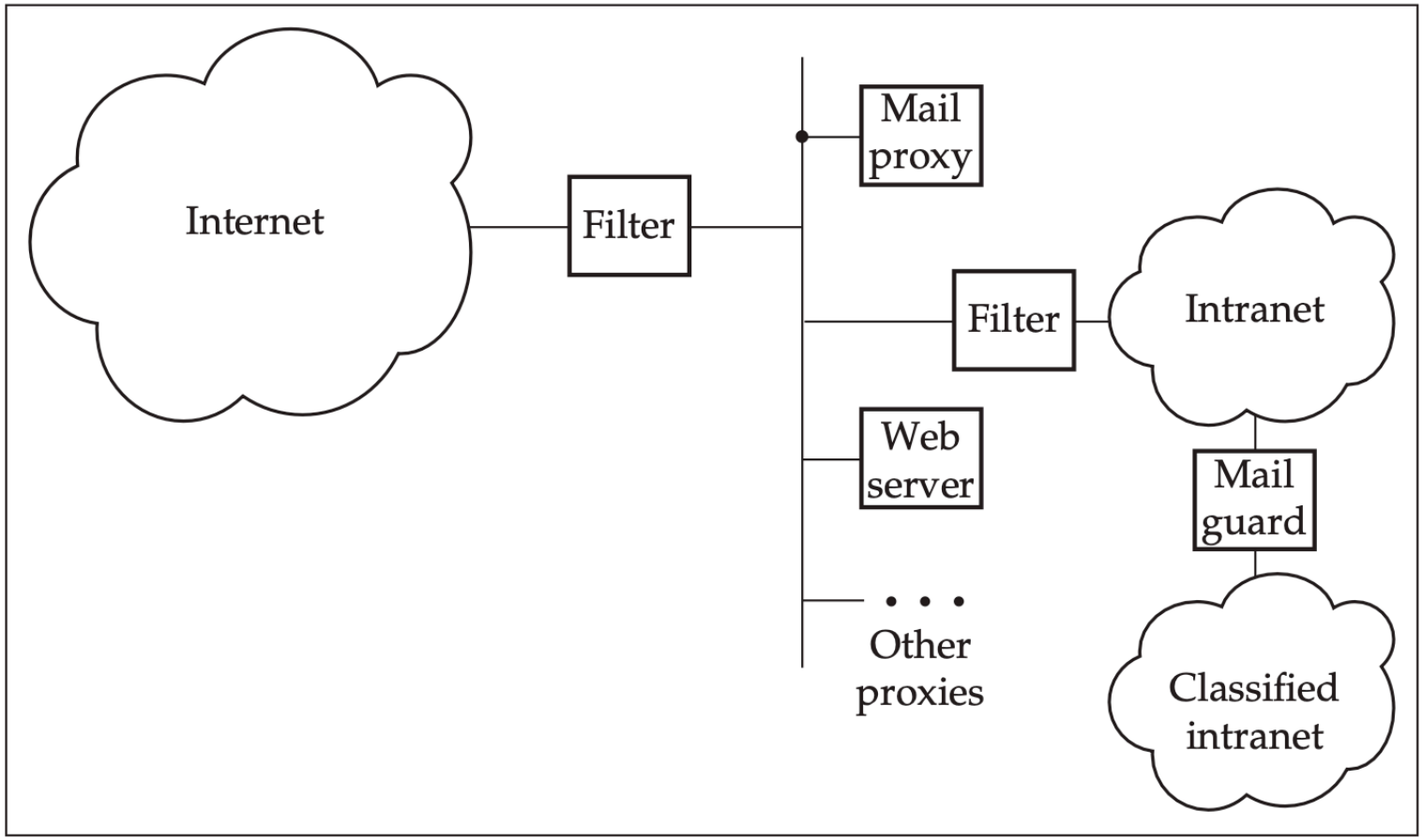
Ingress vs egress filtering

Most firewalls look outwards, but modern firewalls also filter traffic from within

- Source address validation (against IP address spoofing)
- Data leakage prevention (DLP)

University of Victoria

Architecture



University of Victoria

Intrusion Detection

Intrusion Detection System (IDS) are networking devices that detect, e.g.,

- a machine trying to contact a ‘known bad’ service
- packets with forged source addresses – such as packets that claim to be from outside a subnet
- spam coming from a machine in your network.

University of Victoria

Types of intrusion detection

Misuse detection detects suspicious behaviour

- e.g., user draws maximum daily amount for 3 days
- signature-based

Anomaly detection

- Learn “normal” behaviour and detect anamalies

Honeypots

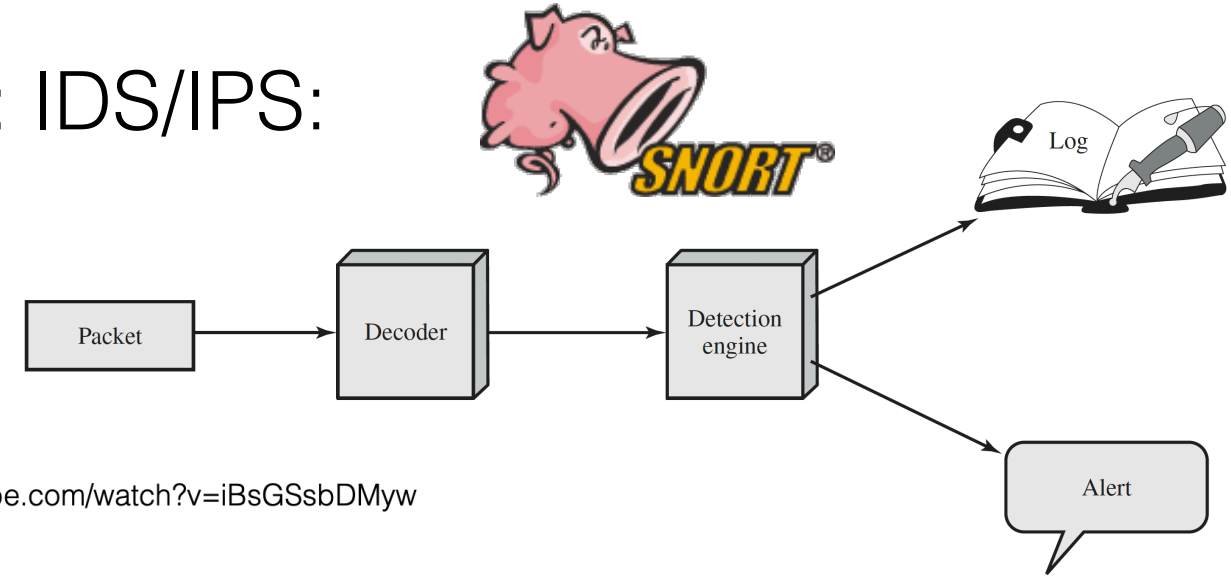
- Attractive target for attackers

University of Victoria

Intrusion Prevention Systems

IPS and are extension of IDS with capabilities to prevent or block detected malicious activity

Demo: IDS/IPS:



https://www.youtube.com/watch?v=iBsGSsbDMyw

University of Victoria

Limitations of intrusion detection

The problem of telling apart legit use from misuse is difficult, in general

Fine balancing act of over-blocking vs. under-blocking

As more traffic becomes encrypted, network-based IDS become less effective

- Need end-point IDS and networked IDS

University of Victoria

Honeypots

Honeypots are **decoy systems** that are designed to lure a potential attacker away from critical systems.

- **Divert** an attacker from accessing critical systems.
- **Collect** information about the attacker's activity.
- Encourage the attacker to stay on the system long enough for administrators to **respond**.

University of Victoria

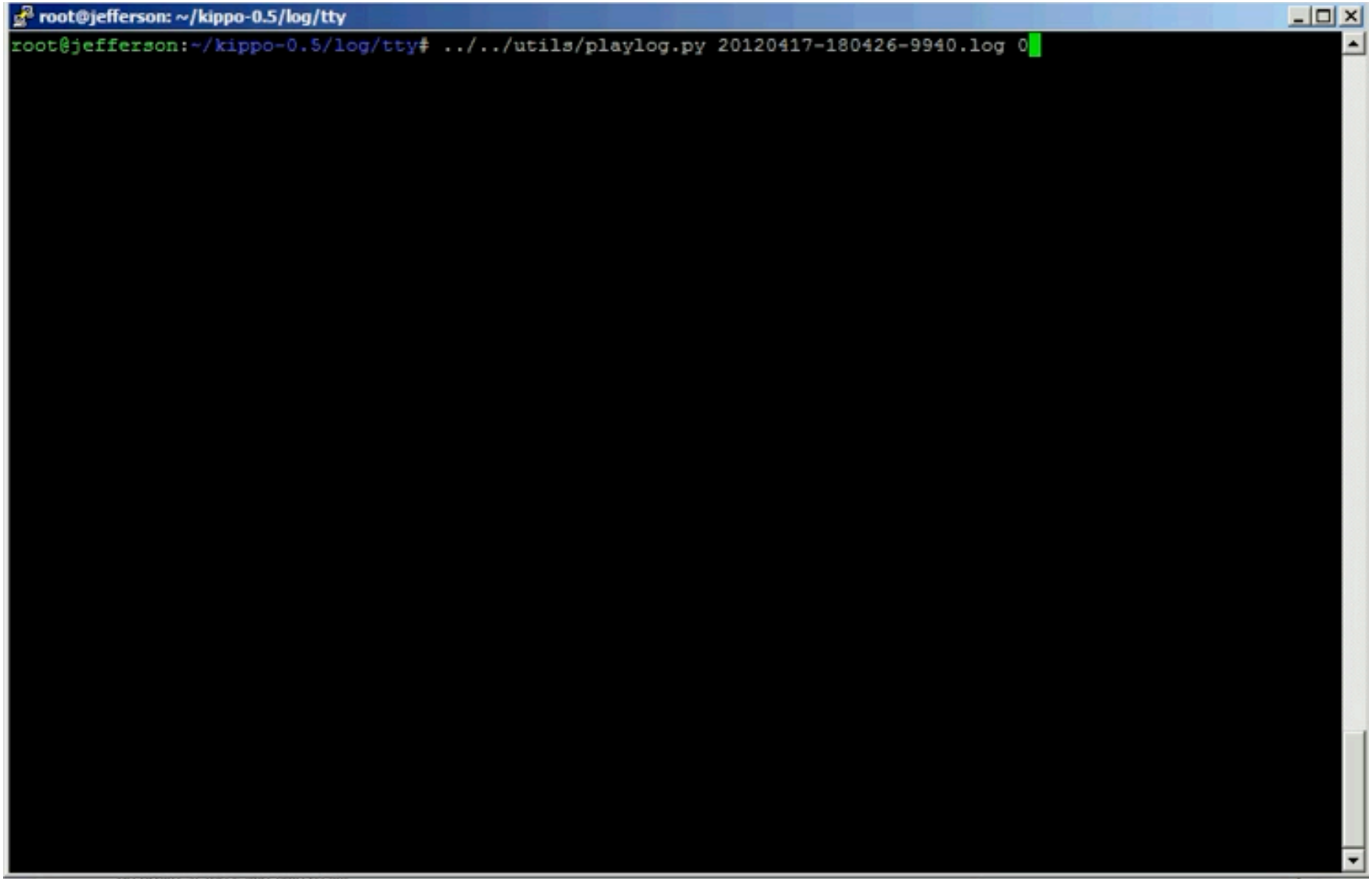
Types of Honeypots

- ***Low interaction Honeypots***: emulates particular IT service or system initially well enough – but does not execute full version
- ***High interaction Honeypots***: Real system with full interactions – but heavily instrumented with IDS

Example Honeypot: *Kippo (and SSH medium interaction HP)*

University of Victoria

https://youtu.be/QatJIMGF6Xo



Cryptography and Networking

Adding crypto to networking sometimes solves one problem and creates another

- See DoH and DNSSEC discussed earlier

SSH (Secure Shell) allows remote login without communicating password in the clear.

Most devices (incl. cars, printers, etc.) are SSH enabled. Passwords can be guessed, keys can be stolen

University of Victoria

Wireless networking - Wifi

- *WEP* (wired equivalent protocol) easily broken (weak encryption, design flaw, no IV)
- *WPA2* (using AES) used today
- *Universal Plug and Play (UPnP)* lets any device punch a hole in the router's firewall
- Many routers never get patched
- Others do get patched (by the ISP) and reset to the default password…

University of Victoria

Wireless networking - Bluetooth

- *Personal area network*
- Problem with “linking” devices that have no keyboards (MITM attacks)
- Many devices never patched

University of Victoria

Medtronic

Sign

Diabetes | Products | Support | Community | Contact | Diabetes.shop

Alert: Product and Recall Notices

URGENT MEDICAL DEVICE CORRECTION

MiniMed™ 600 Series Pump System Communication Issue

Insulin Pump	Model Number
MiniMed™ 630G	MMT-1715, MMT-1755, MMT-1754
MiniMed™ 670G	MMT-1780, MMT-1781, MMT-1782, MMT-1760, MMT-1761, MMT-1762, MMT-1740, MMT-1741, MMT-1742

MiniMed™ 600 Series Pump System Communication Issue - Notification

Download >

September 2022

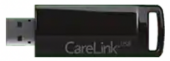
For your safety, we want to inform you of a potential issue associated with the communication protocol used by your pump system. Unauthorized access to your pump's communication protocol could compromise your pump's delivery of insulin. This letter provides actions and mitigations you should take so please carefully review the information below.

ISSUE DESCRIPTION

MiniMed™ 600 series insulin pump*

Guardian™ Link 3 transmitter

Contour® Next Link 2.4 Blood Glucose Meter



CareLink™ USB

University of Victoria

HomePlug

- Networking over power cables
- Used for WiFi extenders
- Two modes:
  - secure mode (where keys need to be manually entered)
  - Simple mode (where keys are generated and exchanged in the clear)
- Most vendors only support “simple mode”

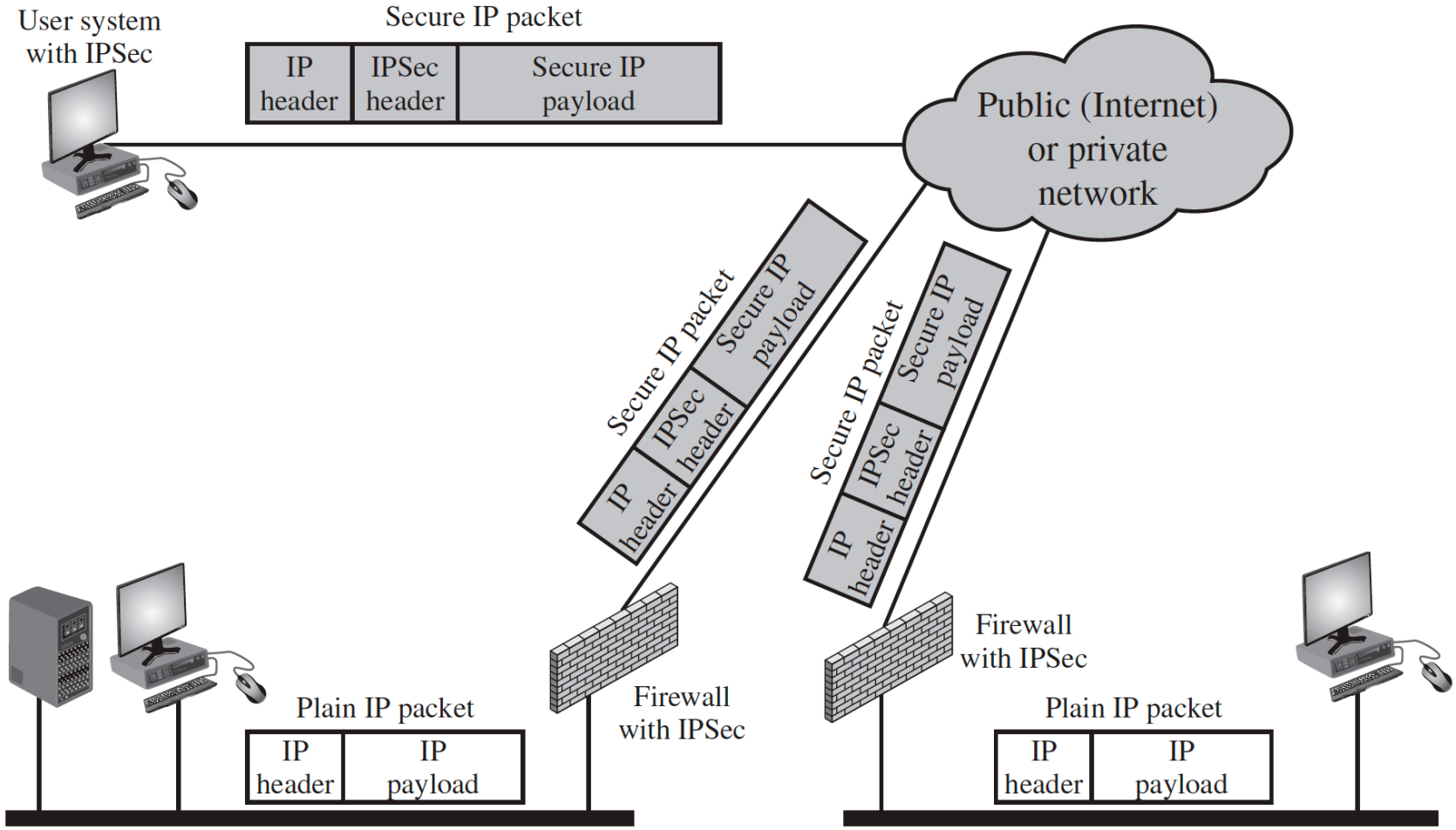
University of Victoria

VPNs

- Typically use encryption/authentication at IP layer, using a protocol called ***IPsec***
- Keys are exchanged using the **Internet Key Exchange (IKE)** protocol
- Configuration key to security (standard config insecure according to Snowden)

University of Victoria

VPN implementation inside Firewall



CAs and PKI

Many problems with CAs and PKI in practice

- Embedded in browsers and OS (hard or not to delete, may come back on update)
- Public CA may be hacked -> private CA?
- Companies use invalid certs., users learned to ignore warnings

University of Victoria