NWEN405: Security Engineering

Lecture 8

Secure Software Engineering : Introduction and Common Attacks

Engineering & Computer Science
Victoria University of Wellington
Dr Ian Welch (ian.welch@vuw.ac.nz)

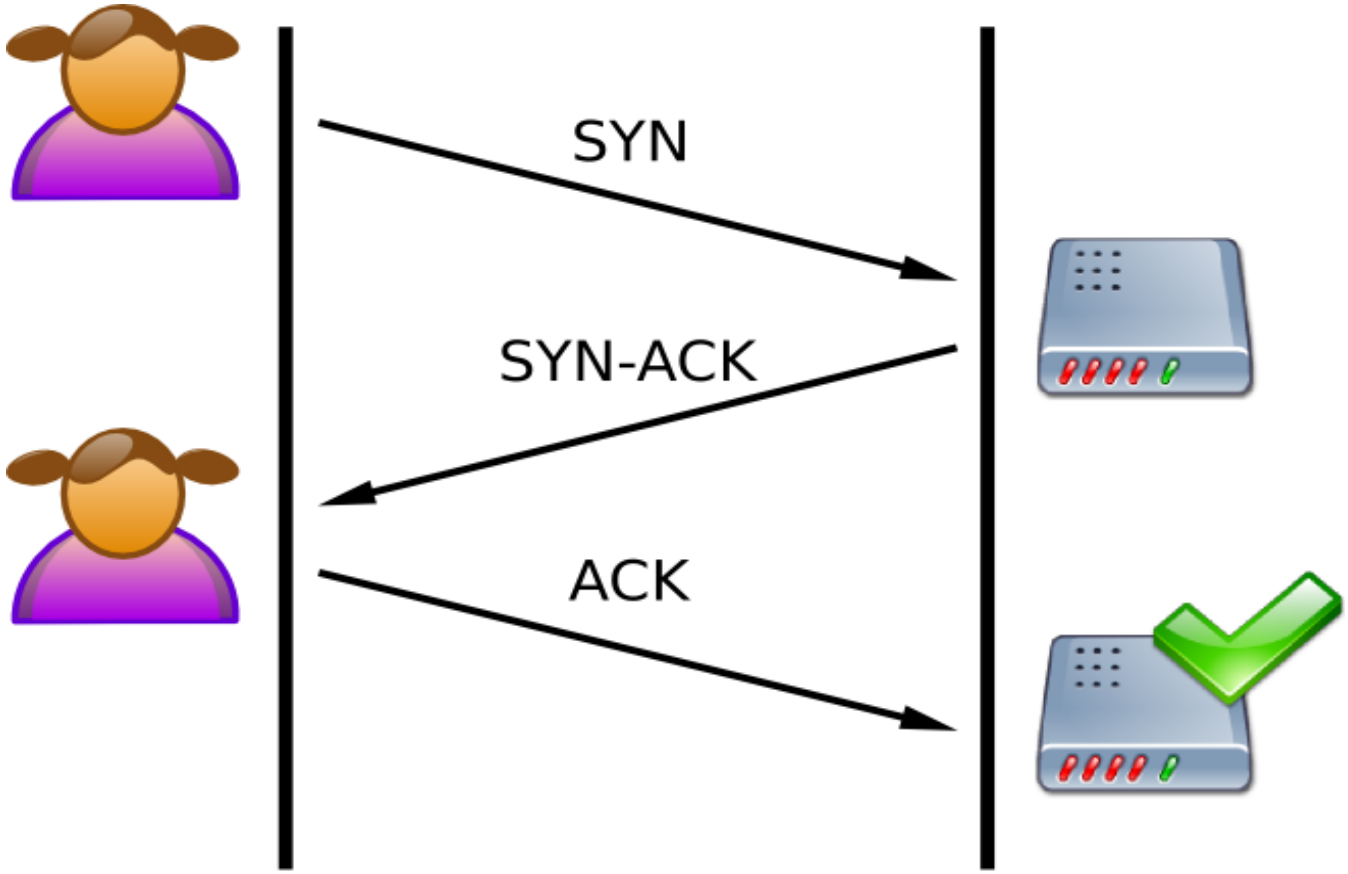
Panix, the NY area's oldest and largest Internet Service Provider, has been under attack from unknown sources since Friday, September 6 at about 5:30pm.

Alexis Rosen, President and co-owner of Public Access Networks Corp., which runs Panix, said on Wednesday that attacks have been made against different computers on the provider's network, including mail, news and web servers, user "login" machines, and name servers--all key computers that provide customers with access to one or more major Internet services.

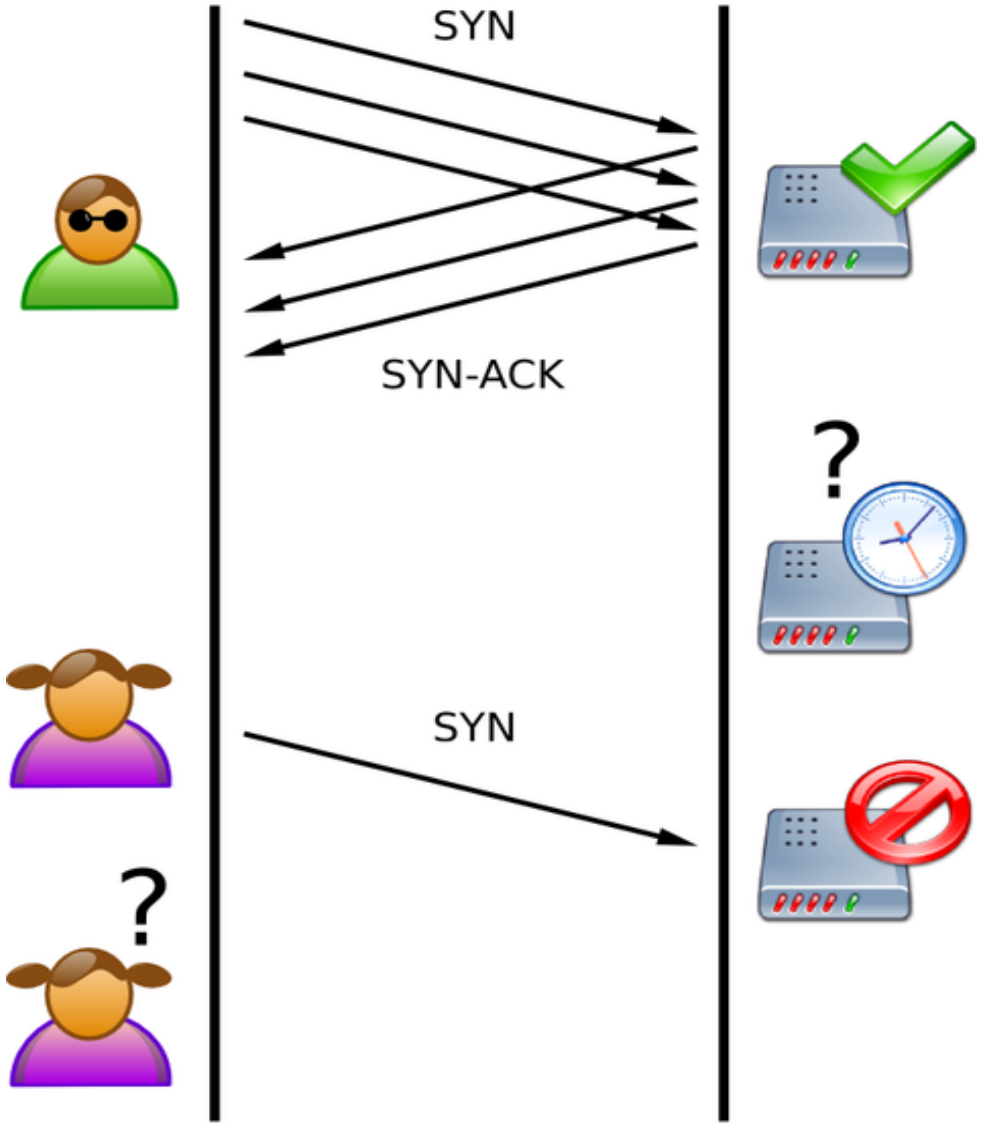
Attacks consist of flooding the machines with so much data that they cannot respond to legitimate requests, and faking the origin of the hostile data. This makes it impossible to trace its source without a major effort on the part of all Internet service providers between Panix and the attacking party. This is equivalent to needing the participation of multiple telephone companies in tracing the origin of an international call.

The nature of the Internet, which is designed to let machines communicate with a minimum exchange of identifying information, makes *every* site on the Internet vulnerable to this sort of attack. No matter how much money, time, and engineering expertise is expended on the problem, the only solution involves strong cooperation on the part of all Internet service providers.

September 6, 1996



Normal TCP Handshake



SYN Flood

CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks

Original issue date: September 19, 1996
Last revised: November 29, 2000
Updated vendor information for the Linux kernel.

A complete revision history is at the end of this file. **This advisory supersedes the IP spoofing portion of CA-95.01.**

Two "underground magazines" have recently published code to conduct denial-of-service attacks by creating TCP "half-open" connections. This code is actively being used to attack sites connected to the Internet. There is, as yet, no complete solution for this problem, but there are steps that can be taken to lessen its impact. Although discovering the origin of the attack is difficult, it is possible to do; we have received reports of attack origins being identified.

Any system connected to the Internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is potentially subject to this attack. Note that in addition to attacks launched at specific hosts, these attacks could also be launched against your routers or other network server systems if these hosts enable (or turn on) other TCP services (e.g., echo). The consequences of the attack may vary depending on the system; however, the attack itself is fundamental to the TCP protocol used by all systems.

If you are an Internet service provider, please pay particular attention to Section III and Appendix A, which describes step we urge you to take to lessen the effects of these attacks. If you are the customer of an Internet service provider, please encourage your provider to take these steps.

September 19, 1996

To: syncookies@koobera.math.uic.edu
cc: djb@koobera.math.uic.edu
Subject: A new thought on TCP SYN attacks
Date: Wed, 25 Sep 1996 18:09:37 -0400
From: "Eric Schenk" <schenk@cs.toronto.edu>
Message-Id: <96Sep25.180941edt.15394@dvp.cs.toronto.edu>

The following is a revised version of a message I originally sent
out to the linux netdev mailing list. Dan Bernstein asked me
to forward the idea to this list. I've updated the text of
my original message to address some concerns that have been
raised since my original posting.

I've been thinking a bit about D.J. Bernstein's proposed method
of dealing with TCP SYN flooding, and I think I've come up with
a new twist that might make it usable, at least in some reasonable
subset of cases.

September 25, 1996

November 8, 1996 4:15 PM PST

New York Times site hacked

November 8, 1996

By Rose Aguilar and Janet Kornblum
Staff Writers, CNET News

Related Stories

Chess Club waits for next move
September 18, 1996

ISPs search for a cure
September 17, 1996

Hacker bombardment keeps site in check
September 16, 1996

Jury still out on hacking
August 18, 1996

The Net's most wanted

The *New York Times* Web site, among the most popular online news outlets, this week became the latest victim of an attack from cyberspace that led to a slowdown in service.

The so-called denial-of-service attacks are becoming more commonplace, where someone perpetrates a simple but nasty ruse that keeps thousands of people from being able to log on to a targeted Web site.

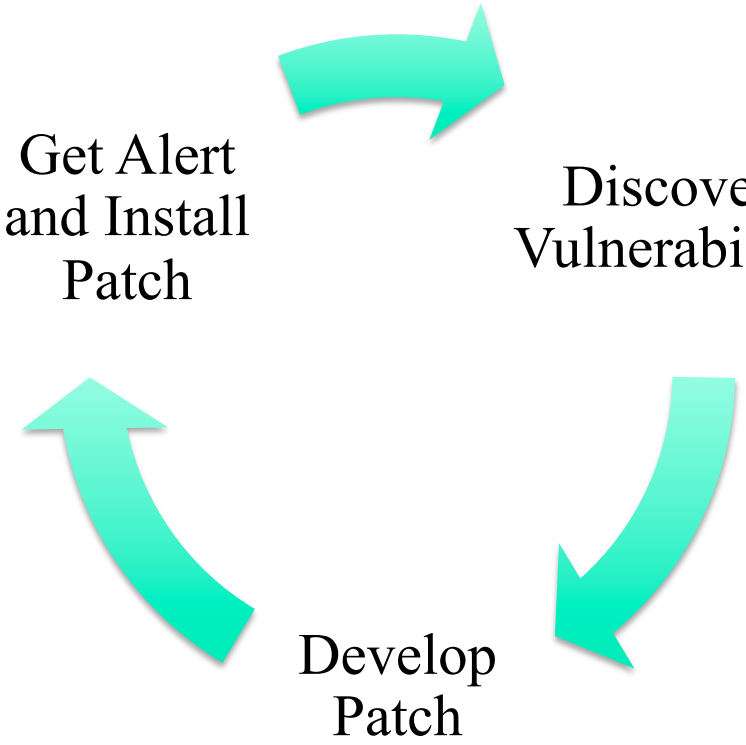
But catching the online saboteur isn't easy. In fact, it may not even be possible, although the *Times* is working with experts in the field to find a solution as well as increasing its server capacity.

The *Times'* Web site was hit by intruders on election night. The site received ten times the regular number of hits, overloading the system and causing slowdowns. Part of the extra traffic came from users who were eager to learn about the election results, but the rest came from online vandals who bombarded the site with bogus requests.

Recently, a new SYN cookie technique developed for release in FreeBSD 7.0 leverages the bits of the Timestamp option in addition to the sequence number bits for encoding state. Since the Timestamp value is echoed back in the Timestamp Echo field of the ACK packet, any state stored in the Timestamp option can be restored similarly to the way that it is from the sequence number / acknowledgement in a basic SYN cookie. Using the Timestamp bits, it is possible to explicitly store state bits for things like send and receive window scales, SACK-allowed, and TCP-MD5-enabled, for which there is no room in a typical SYN cookie. This use of Timestamps to improve the compromises inherent in SYN cookies is unique to the FreeBSD

RFC 4987,
August 2007

Standard Security Engineering



Is this sustainable?

Internet

100 key applications

100 vulnerabilities

= how many holes for hackers?

Is this sustainable?

Expert coder (1 bug/1,000 lines)

Size of Windows/Linux codebase about 100 million lines.

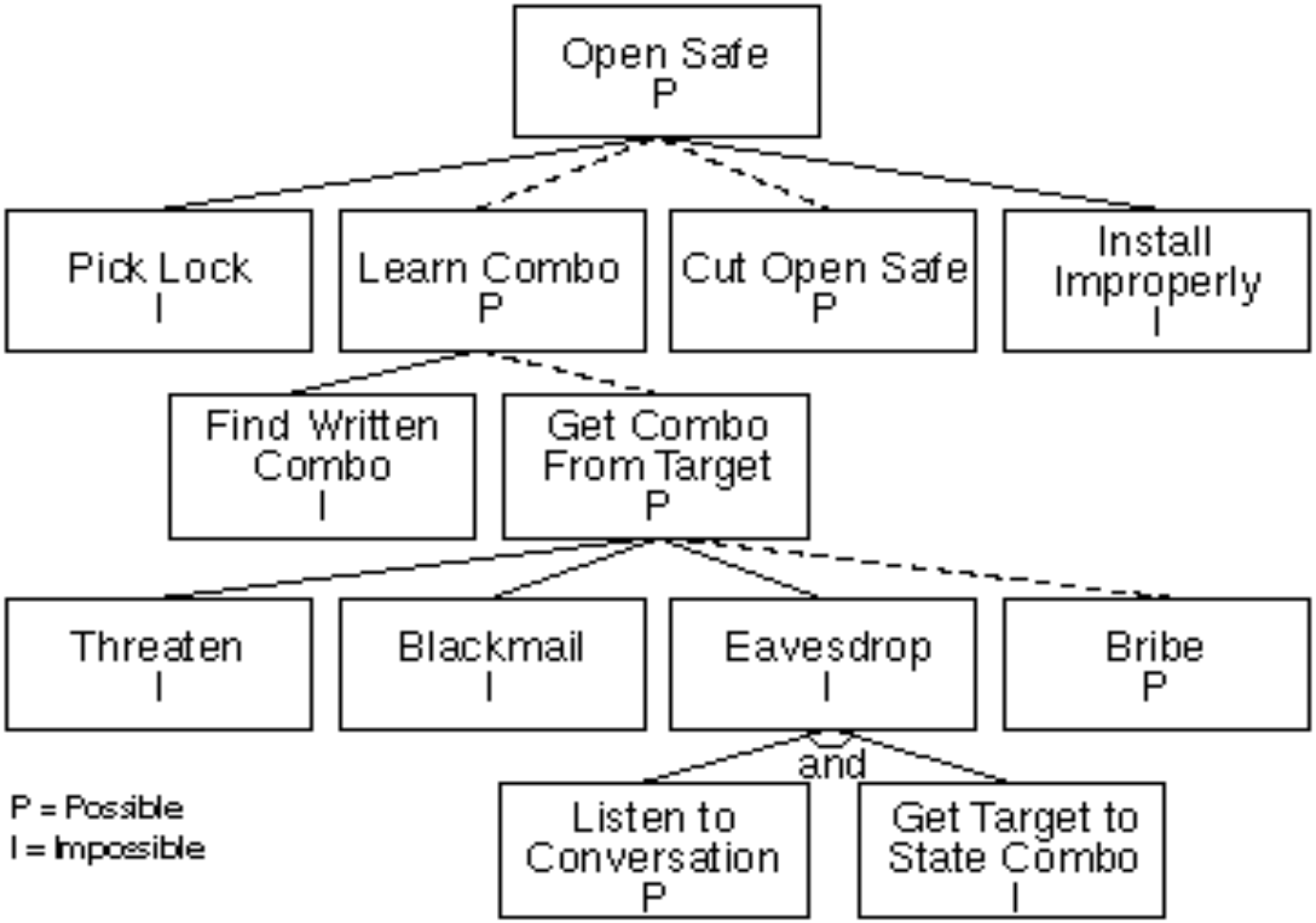
CERT posts advisories for 5,000 per year (2003).

How long to discover/fix all of these?

Better security engineering.

1. Adopt a security architecture.
2. Adopt good design and implementation practices.
3. Evaluate the security of the system before deployment.

What is an attack?



What is vulnerability?

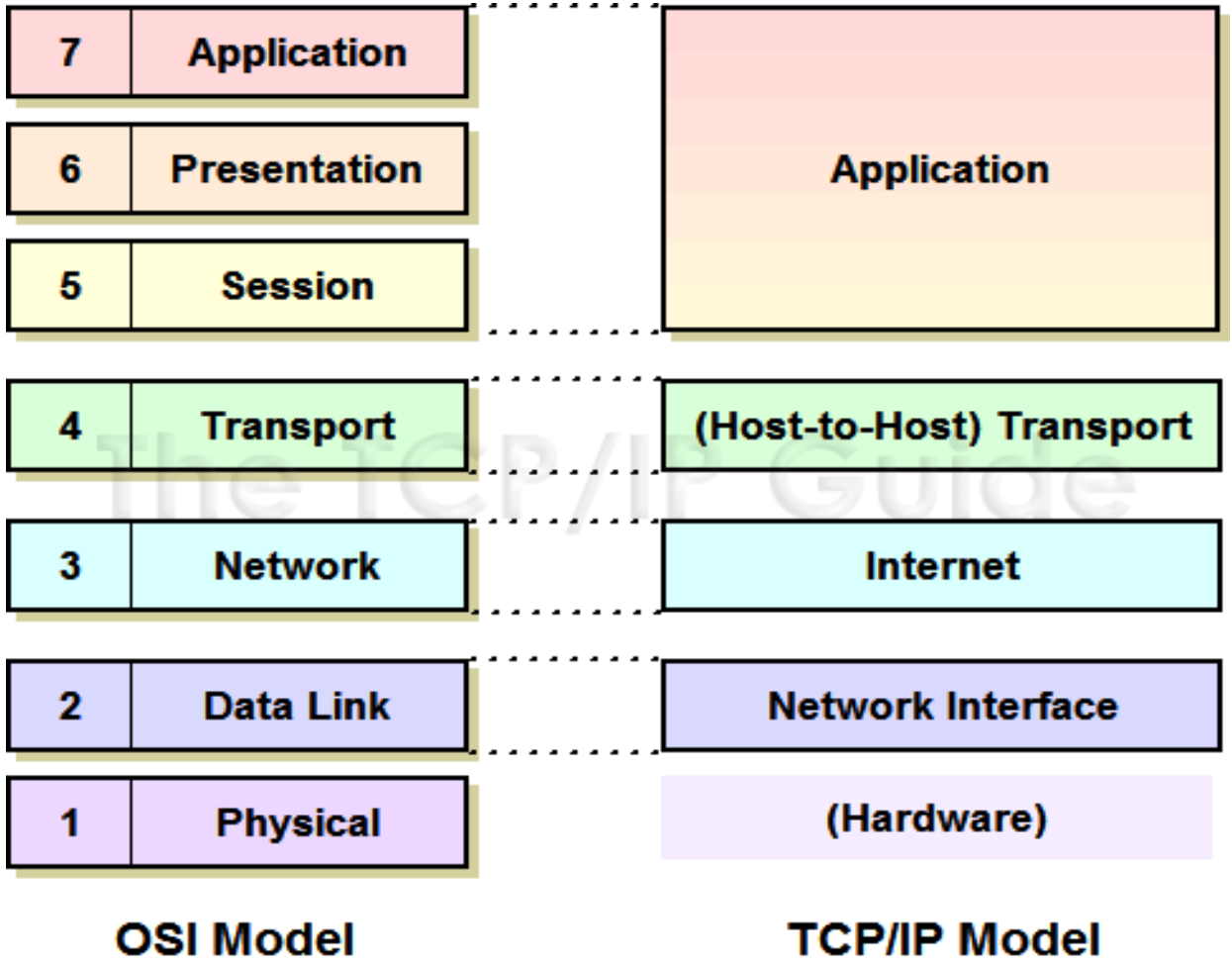
mistakes/bugs

design, implementation, usage

assumptions no longer holding

closed to open environment

Assumptions no longer holding



What are some common attacks?

- Architecture/design level
- Implementation level
- Operational level

Architectural/Design level:

- Man-in-the-middle
- Race condition attack
- Replay attack

Application and network level attacks.

Architectural/Design level:

- Sniffer attack
- Session hijacking attack
- Session killing attack

Network level that affect applications.

Implementation-level:

- Buffer overflow attacks
- Back door attack
- Parsing error attack

Operations-level:

- Denial-of-service attack
- Default accounts attack
- Password cracking.