

PKI and SSL: E-Business Enabler or a House of Cards?

P2P, Web Services, Wireless, and Beyond:
O'Reilly Emerging Technology Conference

May 13-16, 2002
Santa Clara, CA

Disclaimers & Warnings

The views contained in this presentation are those of the author - and might not be shared by other people, companies, or even his employer.

No animals were harmed in the making of this presentation.

I am not a PowerPoint guru.

Trust in Cyberspace

Easy to do in real world

End-Users are far too trusting; assume too much

Both a Threat and A Vulnerability

...but a slick marketing tool, especially today!

What got me thinking...

CERT® Advisory CA-2001-04 Unauthentic "Microsoft Corporation" Certificates

Original release date: March 22, 2001
Last revised: March 30, 2001
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Systems whose users run code signed by Microsoft Corporation.

Overview

On January 29 and 30, 2001, VeriSign, Inc. issued two certificates to an individual fraudulently claiming to be an employee of Microsoft Corporation. Any code signed by these certificates will appear to be legitimately signed by Microsoft when, in fact, it is not. Although users who try to run code signed with these certificates will generally be presented with a warning dialog, there will not be any obvious reason to believe that the certificate is not authentic.

I. Description

Microsoft released a security bulletin on March 22, 2001, describing two certificates issued by VeriSign to an individual fraudulently claiming to be an employee of Microsoft.

Microsoft warns of hijacked certificates

By [Robert Lemos](#)
Staff Writer, CNET News.com
March 22, 2001, 2:20 PM PT

update Two digital certificates have been mistakenly issued in Microsoft's name that could be used by virus writers to fool people into running harmful programs, the software giant warned Thursday.

According to Microsoft, someone posing as a Microsoft employee tricked VeriSign, which hands out so-called digital signatures, into issuing the two certificates in the software giant's name on Jan. 30 and Jan. 31.

Such certificates are critical for businesses and consumers who download patches, updates and other pieces of software from the Internet, because they verify that the software is being supplied from a particular company, such as Microsoft.

In this case, a person using the VeriSign-issued certificates could post a virus on the Web that would appear to be from Microsoft but could actually be used to wipe out a person's hard drive, for example.

"Our main interest right now is to get the word out and let people know what they can do," said Steve Lipner, manager of Microsoft's Security Response Center. Microsoft first heard of the incident last week when VeriSign notified the Redmond, Wash.-based company. Lipner added that the FBI has been asked to investigate.

A Microsoft [security bulletin](#) issued Thursday states that the vulnerability could affect "all customers using Microsoft products."

FAQ: Microsoft's security breach and how it affects you
▶ story

A MATTER OF TRUSTING TRUST

Why Current Public-Key Infrastructures are a House of Cards

<http://www.infowarrior.org/articles/2001-01.html>

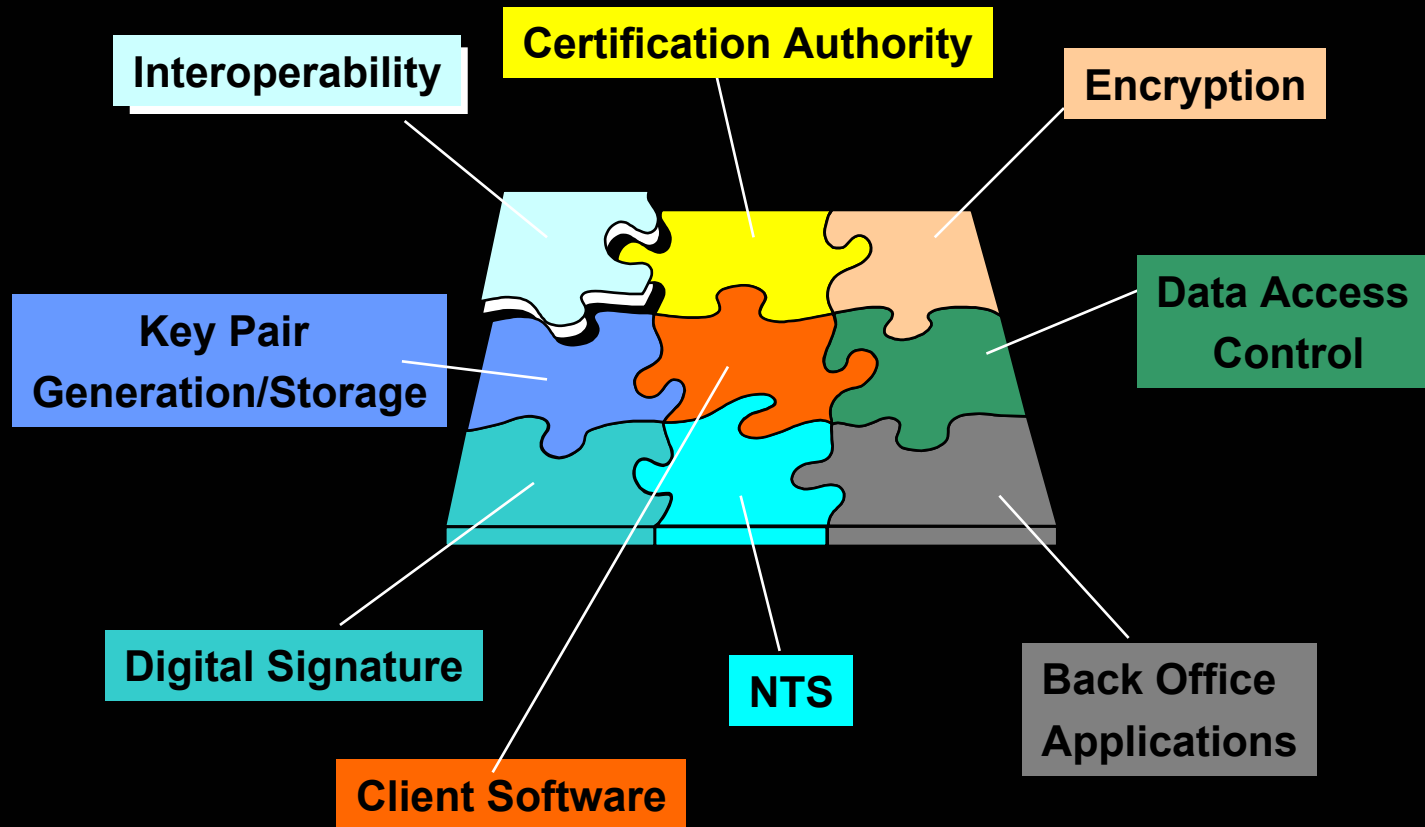
PKI: A Question of Trust and Value

Inside Risks 132, CACM 44, 6, June 2001

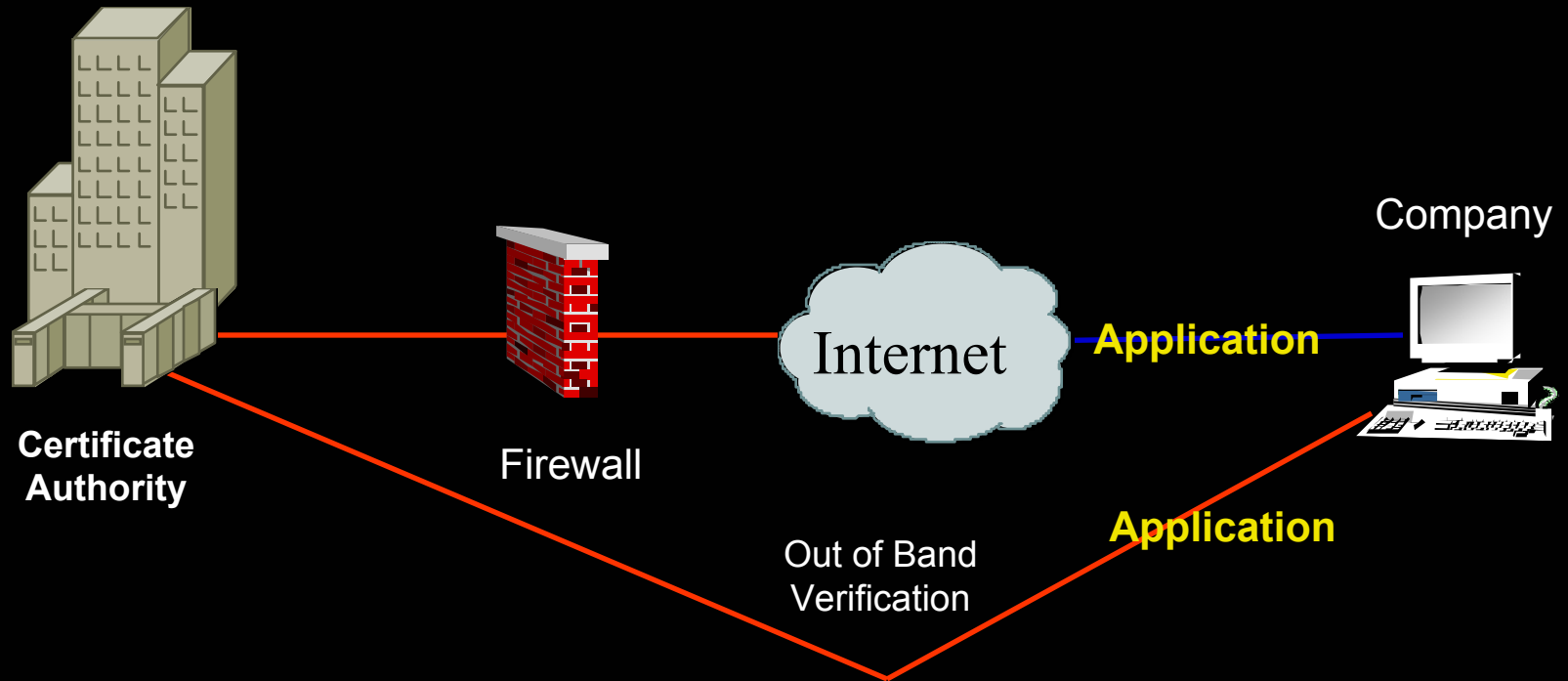
<http://www.csl.sri.com/users/neumann/insiderisks.html#132>

PKI Overview

PKI Infrastructure Components



Generating Trust



Government Documents

Credit Cards

Websites (Ecommerce)

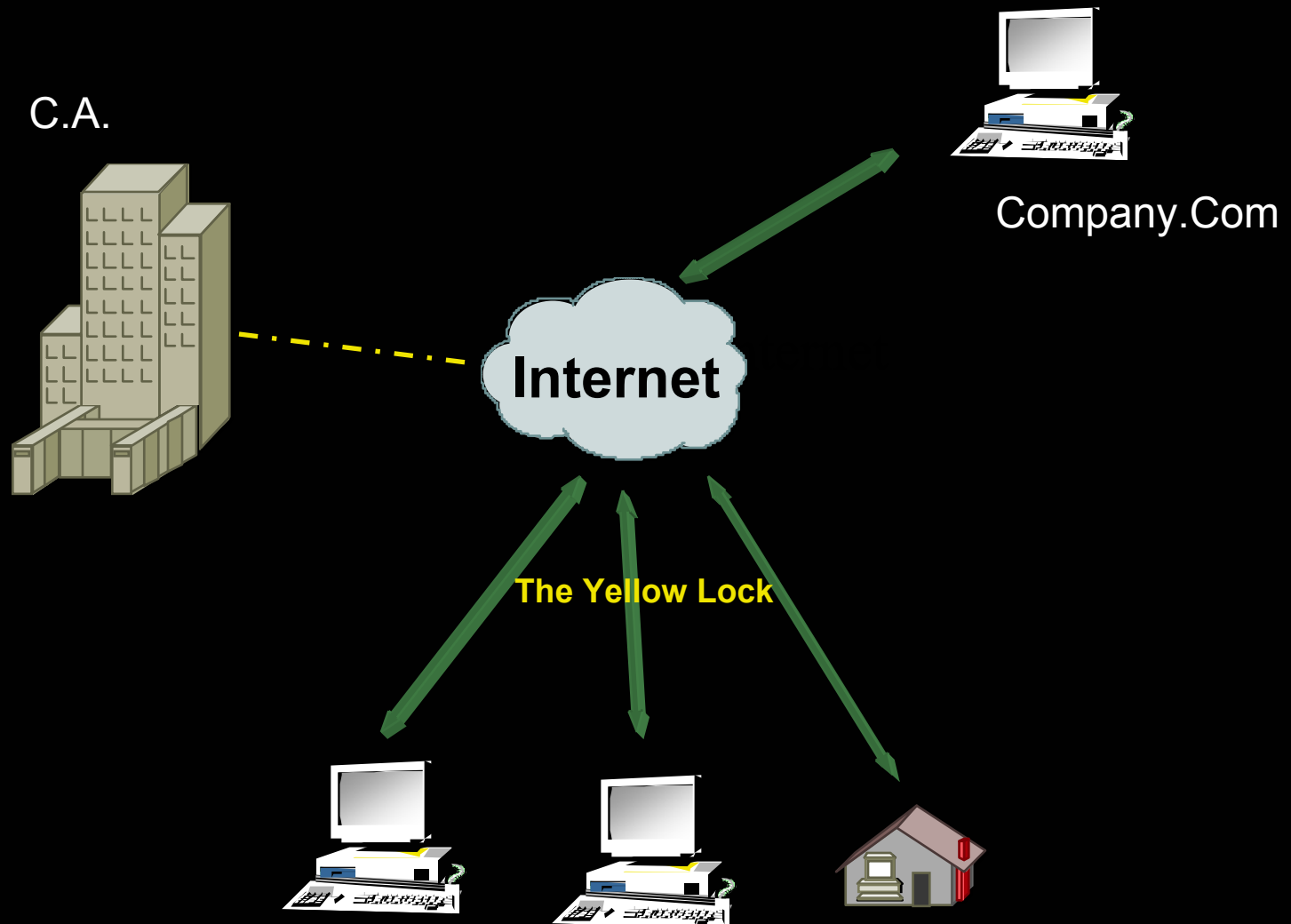
E-Mail

Selected Vulnerabilities

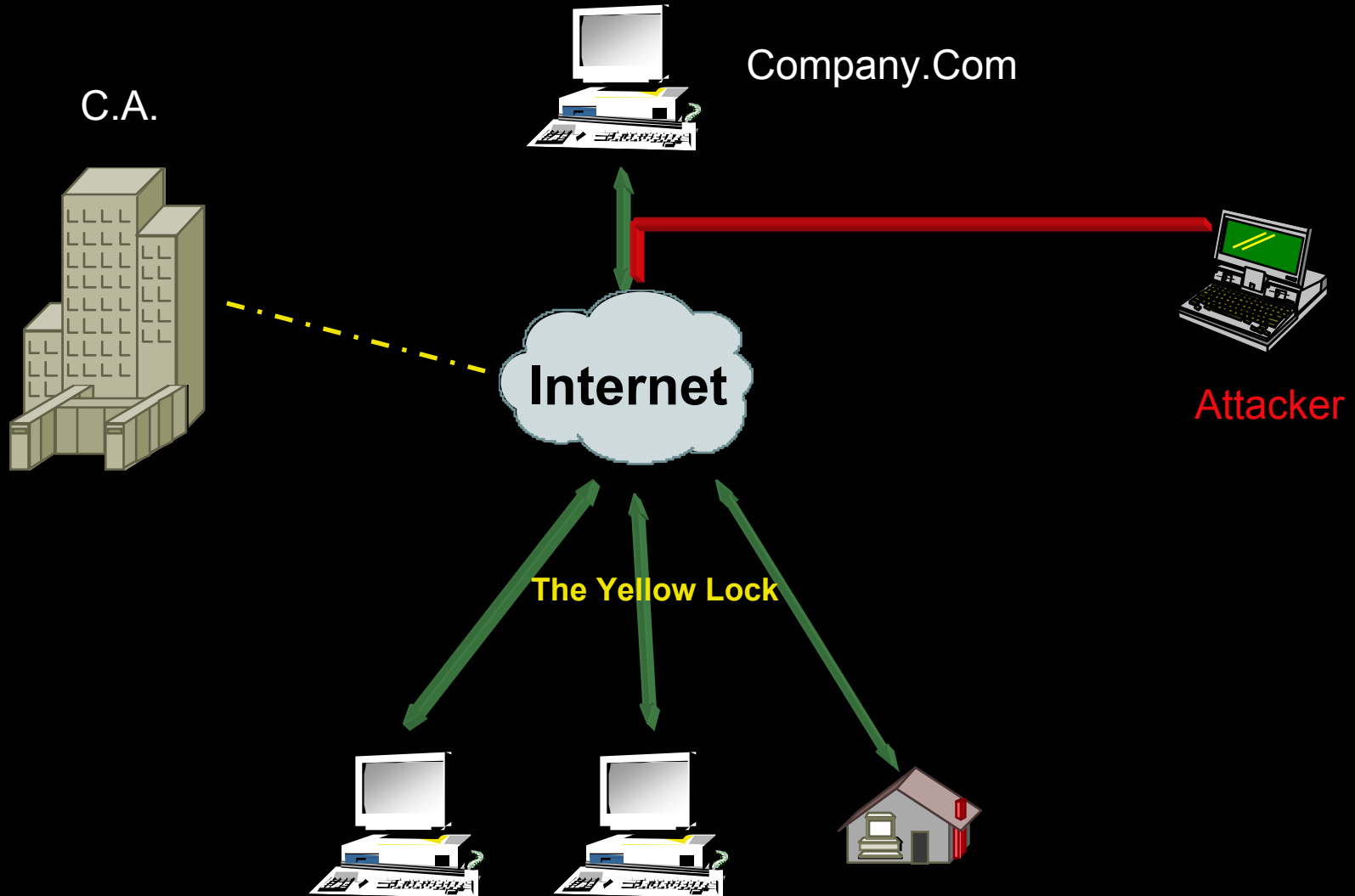
Problems with Today's PKI/SSL

- Authentication for **GENERATION**
 - SocEng, What Notaries Really Do
- Authentication for **CONFIRMATION**
- Why don't certs expire?
- Positioned as Marketing Tools?!
- Not a stand-alone security solution
- Consumers still believe "trust" in established entities

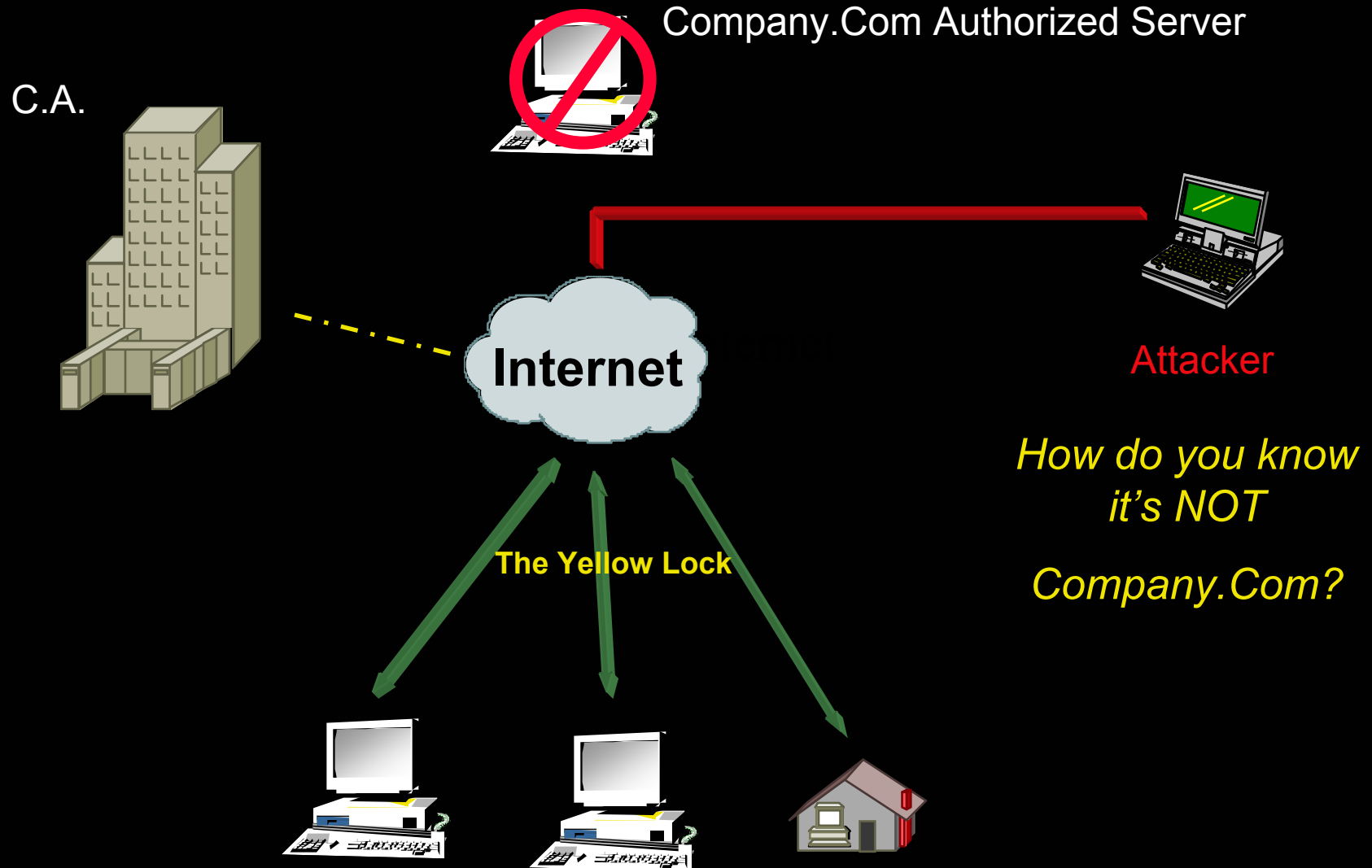
“Trusted” Systems



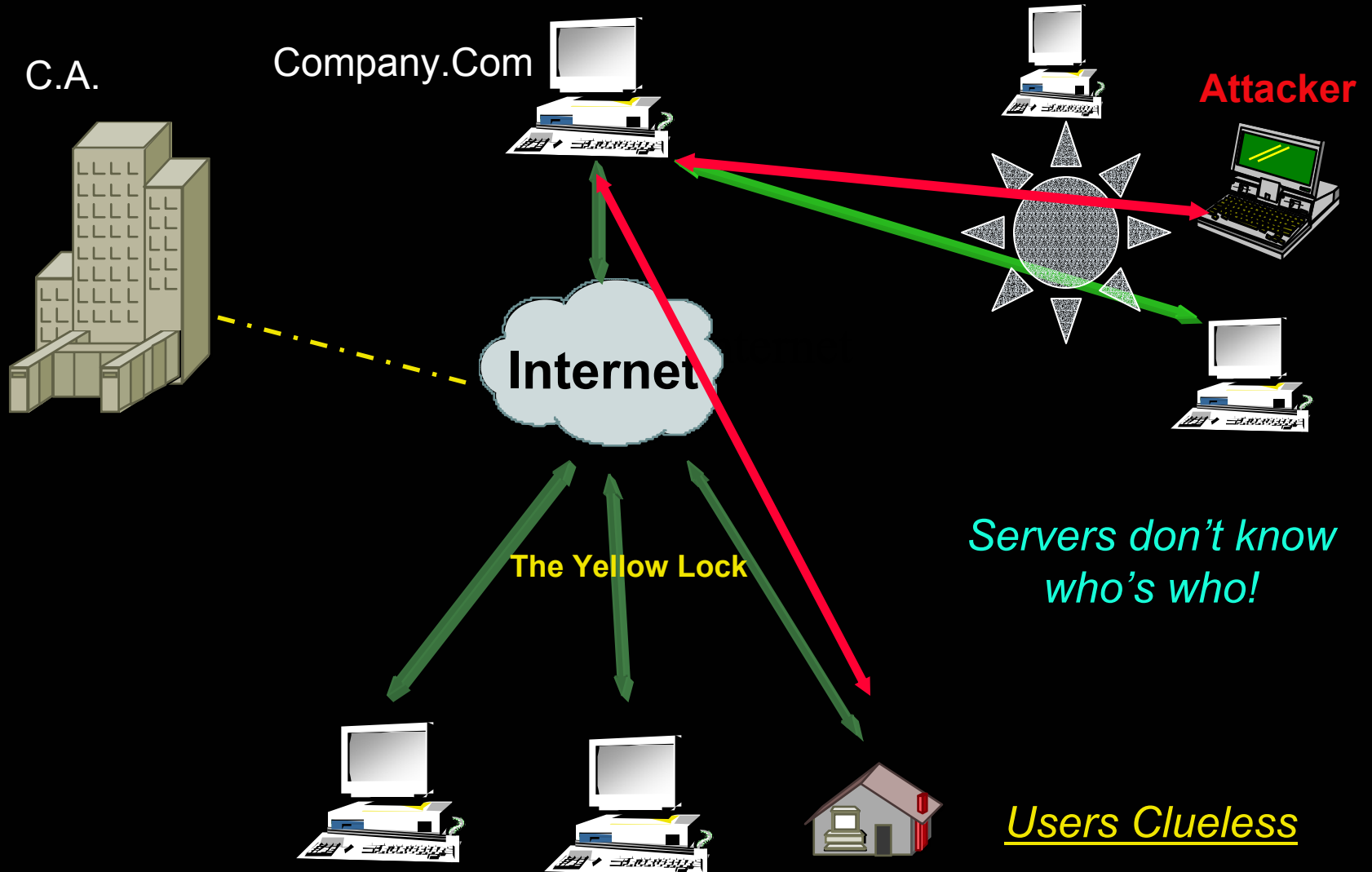
DNS Redirect Attack



DNS Redirect Attack In Effect



Insider Attack



Subscription-Ware

- No positive control over your information
- Complacency
 - Paid in Advance
 - Vendor decides when/how to resolve problems
- Single Point of Failure and Attack
- Single Sign-On using PKI model
 - We already know it's flawed
 - Cookies
 - .NET?

PKI's Needed Improvements

- Reconsider how certificate requests are vetted
- Use point-of-use verification procedures
 - Realtime CRL checks; credit card models
- Force expiration dates on certs and CA
- Host and User-level authentication measures
 - MAC/IP/VLAN/Personnel measures
- Vendor accountability and applications

PKI As Part of Total Security

- Used in more than Webservers
 - How can you trust the site you're visiting?
 - Does the yellow lock *really* mean anything?
- Does not need to be used everywhere
- CA is a single point of failure/attack
- Is a tool, not a stand-alone solution
 - Not ideal for medical uses (old school rules here)
 - Becoming an overused tool for marketing and consulting firms ... economics show slowing corp. PKI retention

Further Reading

Ten Risks of PKI: What You're not Being Told

Carl Ellison and Bruce Schneier

<http://www.counterpane.com/pki-risks-ft.txt>

Thirteen Reasons to Say 'No' to Public Key Cryptography

<http://www.connotech.com/13reas.htm>

Risks of the Microsoft Passport Single Sign-On Protocol

David P. Kormann and Aviel D. Rubin

<http://avirubin.com/passport.html>

A MATTER OF TRUSTING TRUST

Why Current Public-Key Infrastructures are a House of Cards

<http://www.infowarrior.org/articles/2001-01.html>

PKI: A Question of Trust and Value

Inside Risks 132, CACM 44, 6, June 2001

<http://www.csl.sri.com/users/neumann/insiderisks.html#132>

Rx: The **Red Pill**



Do you want *real* security, or the *illusion* of security?

Contact

Richard Forno

rforno@infowarrior.org