TLS/SSL 在Web 部署中的安全问题分析

段海新

duanhx@Tsinghua.edu.cn

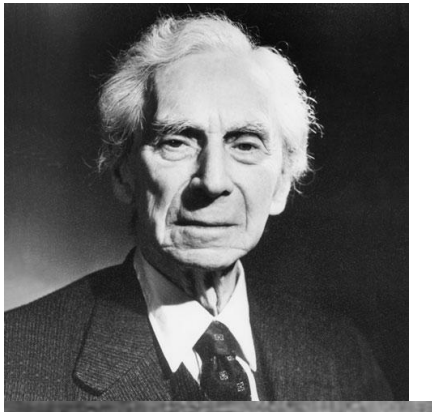
2015年1月20日，哈尔滨

提纲

- 互联网哲学、End-to-End原则及其质疑
- TLS和Web 的目标：认证、保密和完整性
- HTTPS在CDN中的保密性和授权问题
- 同源访问控制和完整性
- 思考与讨论

互联网哲学（Internet Philosophy）

- 哲学是介于神学和科学之间的东西（罗素《西方哲学史》）
- 哲学是幼稚的、失败的科学（胡适《哲学的未来》）
- 日常用语中的哲学：个人或团体基本的信仰、概念或态度（webster字典）
- David Clark: "We reject kings, presidents and voting. We believe in rough consensus and running code”



The Tao of IETF: A Novice's Guide to the Internet Engine
http://www.ietf.org/tao.html

Design Principles of Internet Architecture, By David Clark, 1984

- **End-to-End Arguments In System Design, Trans On Computer Systems, 1984 Vol. 2(4), pp 277-288**
  - The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible.
- **The Design Philosophy of the DARPA Internet Protocols , Sigcomm 1988**
  - **Stateless middle box(survivability), E2E**
  - **Best Effort of IP (Layer separate from TCP)**
- **But, Early trade-offs: ARPANET IMP**

4.1 The future of the end to end arguments

- End to end argument is the most respected Internet design principle.
- End to end argument state that mechanism should not be placed in the network if it can be placed at the end node.

David Clark, Tussle in Cyberspace: Defining Tomorrow's Internet , 2002

Overview of 1999 IAB Network Layer Workshop， RFC2956, By IAB

https://tools.ietf.org/html/rfc2956#section-2.2

2.2 NAT, Application Level Gateways & Firewalls

The previous section indicated that the deployment of NAT (Network Address Translation), Application Level Gateways and firewalls causes loss of network transparency. Each of them is incompatible with certain applications because they interfere with the assumption of end to end transparency. NAT especially complicates setting up servers, peer to peer communications and "always-on" hosts as the endpoint identifiers, i.e. IP addresses, used to set up connections are globally ambiguous and not stable (see [2]).

NAT, application level gateways and firewalls however are being increasingly widely deployed as there are also advantages to each, either real or perceived. Increased deployment causes a further decline of network transparency and this inhibits the deployment of new applications. Many new applications will require specialized Application Level Gateways (ALGs) to be added to NAT devices, before those applications will work correctly when running through a NAT device. However, some applications cannot operate effectively with NAT even with an ALG.

Arguments On End-to-End (from Clark's Slides)

- van Schewick, *Architecture & Innovation: The role of the end-to-end arguments in the original Internet,* PhD, TUB
- Tim Moors, *A critical review of "End-to-end arguments in system design",* 2002 ICC
- Chen and Jackson, editors, *Commentaries on "Active network and end-to-end design", !EEE Network, May/June 1998*
- Kempf and Austein, *The rise of the middle and the future of end-to-end,* RFC 3724
- Reed, *The end of the end-to-end argument,* 2002 www.reed.com
- Blumenthal and Clark, *Rethinking the design of the Internet: the end to end arguments vs. the brave new world*, ACM ToIT, 2001

Criticism of End to End

- Douglas Comer(Prof. Purdue, TCP/IP) :
  - Lessons Learned From The Internet Project, 2005, Lecture in Tsinghua:
  - 端到端的原则也没象当初想象的那么关键，比如NAT, Firewall等都已被广为接受
  - 一个专家委员会设计的东西，通常不会有什么好结果
    - OSI 参考模型
    - IPSEC, DNSSEC, BGPSEC 进展缓慢
    - SSL, SSH却遍地开花

Lixia Zhang, A Retrospective View of NAT, IETF Journal October 2007

张丽霞：对地址转换（NAT）的回顾与反思（翻译：段海新）

netsec.ccert.edu.cn/duanhx/archives/536

为什么IETF错过了把NAT标准化的机会

在NAT开始部署的10年里，IETF内部对是否应该部署NAT有很大争议。NAT使用私有地址，这样就偏离了IP协议的基本模型：为任何主机之间提供端到端的可达性，违背了互联网最初的体系结构。这场争论持续多年，最近在2000年4月，IETF的mailinglist上有则消息称，NAT从结构上就是不合理的，IETF和IESG决不应该提倡使用部署NAT。有这种想法的人不在少数。

今天大多数人认同IETF最初没有标准化NAT是错误的。为什么错过了机会？简单来说是由于当时一切都不明朗。我相信稍微深入一点就能理解不明朗的原因。我认为下面的因素起了很大作用：

http://netsec.ccert.edu.cn/duanhx/archives/536

Principles of Internet Architecture RFC 1958, by IAB, 1996

- In this environment, some architectural principles inevitably change.
- The principle of constant change is perhaps the only principle of the Internet that should survive indefinitely.
- As Lord Kelvin stated in 1895, "Heavier-than-air flying machines are impossible." We would be foolish to imagine that the principles listed below are more than a snapshot of our current understanding.

小结

- 互联网最早的设计，没有什么指导原则
- 只有一组共同认可的需求：互联、共享
- 即便是最高的指导原则 E2E，一开始就折衷
- 没有不变的指导原则（principle）

- 在世界范围内的需求都是相互冲突的，如何设计？

提纲

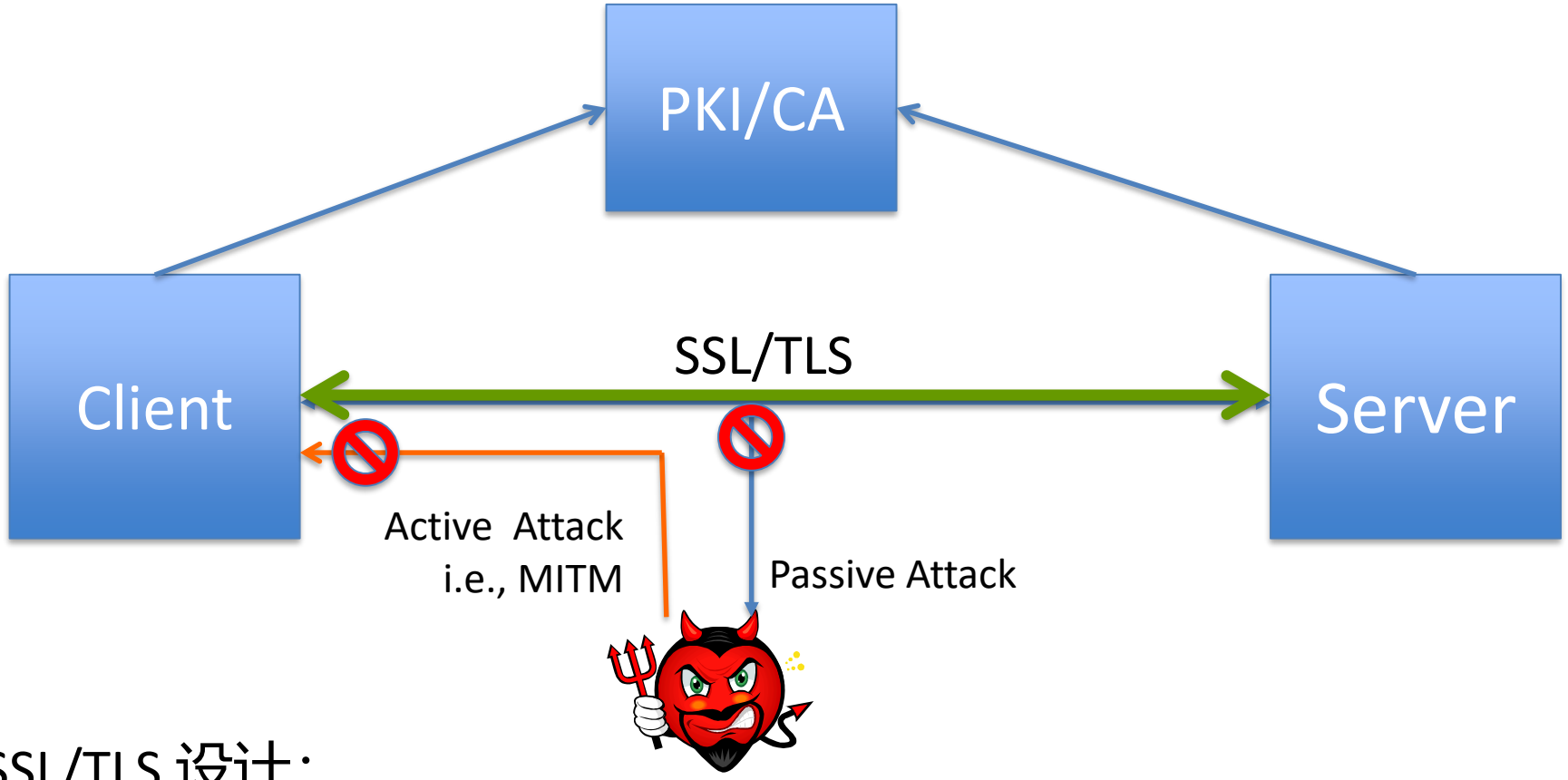
- 互联网哲学、End-to-End原则及其质疑
- TLS和Web 的目标：认证、保密和完整性
- HTTPS在CDN中的保密性和授权问题
- 同源访问控制和完整性
- 思考与讨论

History of TLS/SSL

- SSL 2.0, 1994, by Kipp Hickman, Netscape
  - **1996, Ian Goldberg and David Wagner**, **Randomness and the Netscape Browser,** http://www.cs.berkeley.edu/~daw/papers/ddj-netscape.html
  - Prohibiting Secure Sockets Layer (SSL) Version 2.0, RFC 6176, 2011
- SSL 3.0, 1996 by Netscape(RFC6101)
  - Disabled by POODLE, 2014
- TLS 1.0, RFC2246 1999
- TLS 1.1, RFC 4346, 2006
- TLS 1.2, RFC 5246, 2008

TLS出来这么久了，而且SSL有这么多问题，为什么直到很晚（7-8年）才禁用了SSL？

TLS/SSL 是 E2E 吗?



SSL/TLS 设计：

（1）服务器的标识与认证

（2） 内容的保密性（Confidentialit

（3） 内容的完整性（Integrity）

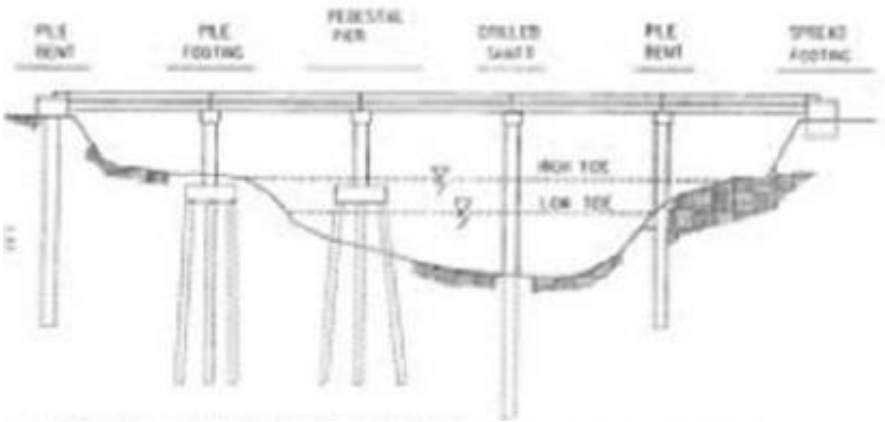
可以防范中间人攻击
（Active attacking）

Web 安全的基石

- 身份认证
  - Server : TLS Certificate, Signed by CA
  - Client: Cookie, Token,…
- 访问控制
  - 同源策略（Same Origin Policy)
- 保密性 : HTTP over TLS
- 完整性: HTTP over TLS

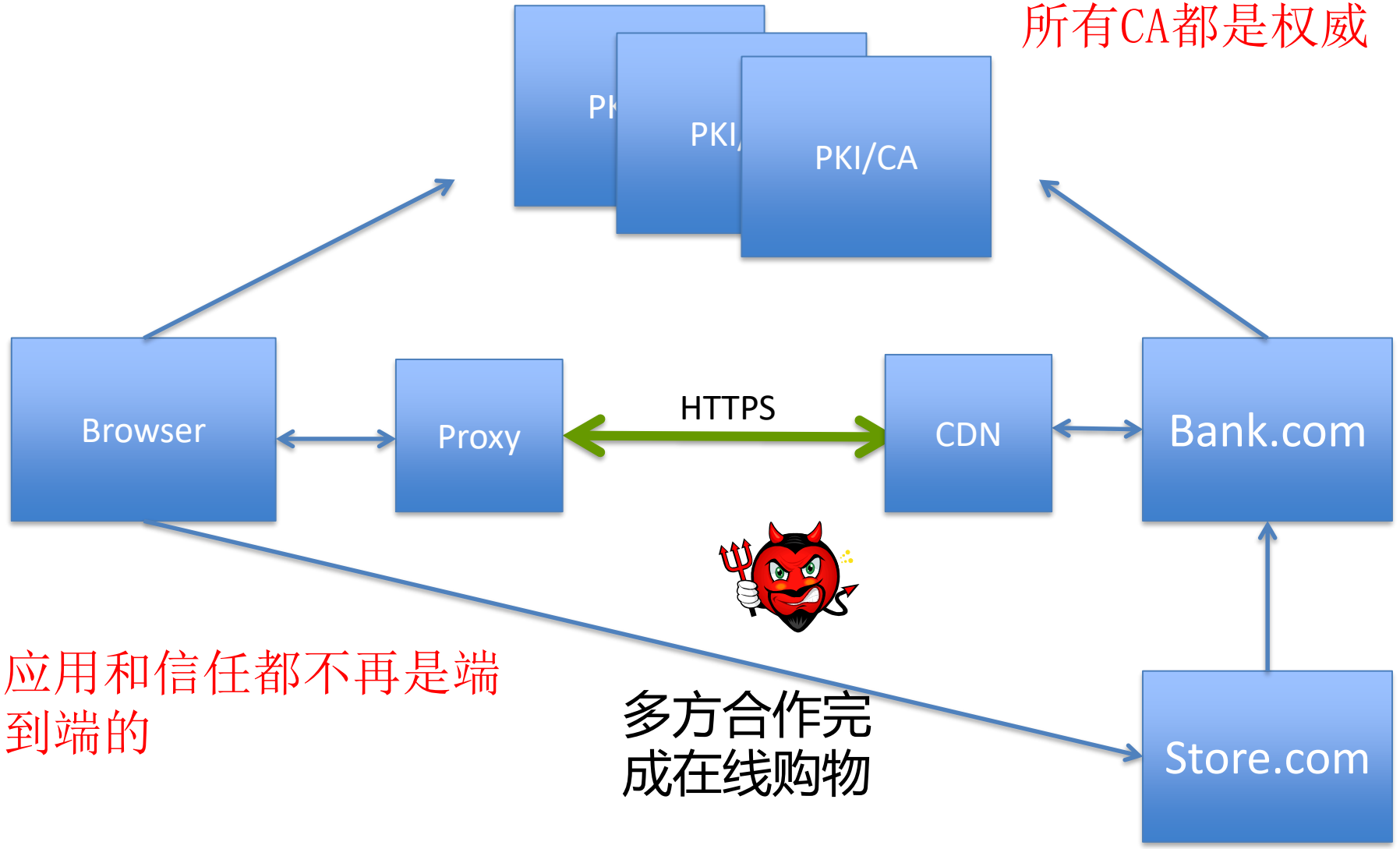
一个不准确的类比：软件开发过程

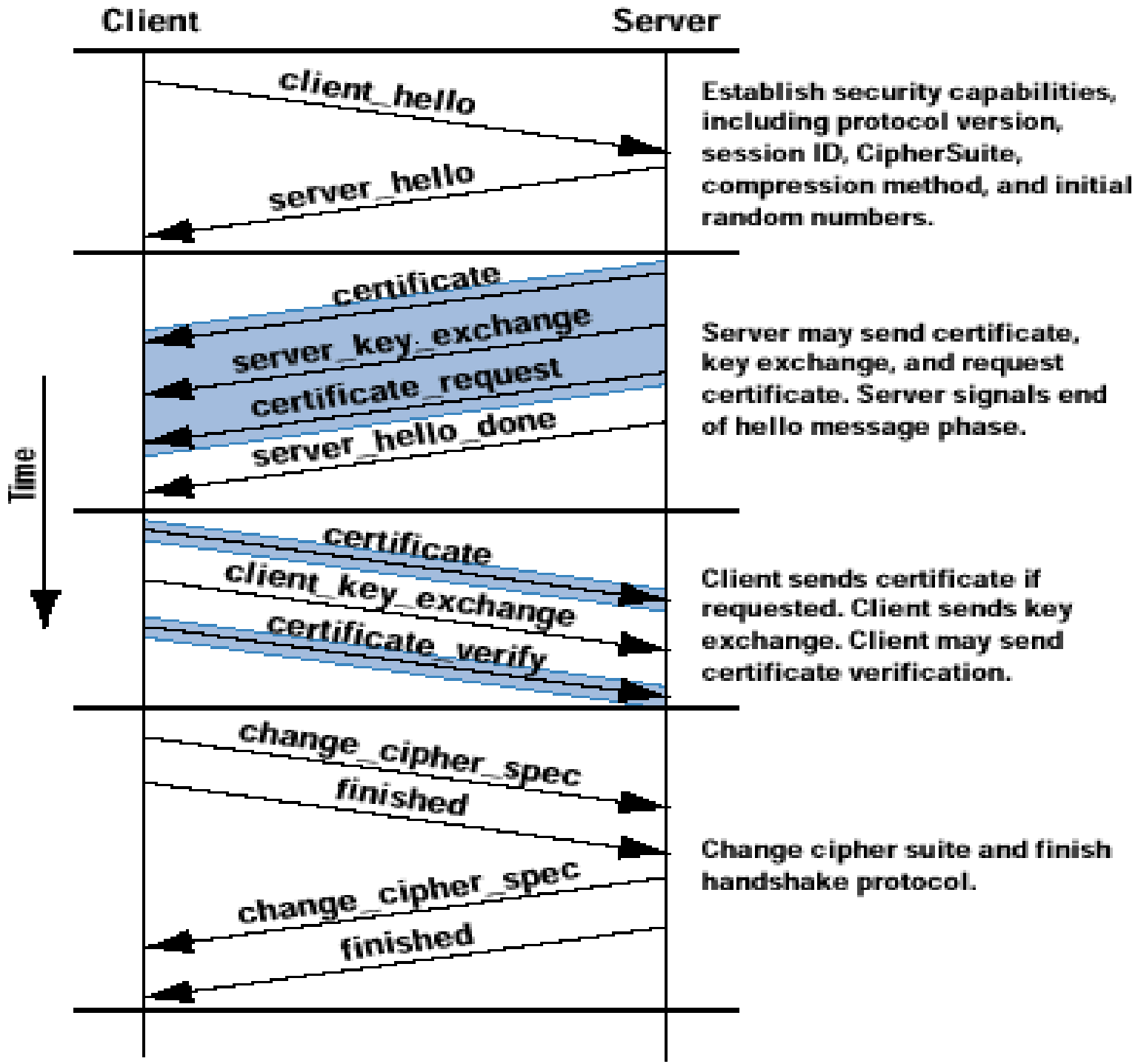
架构师设计



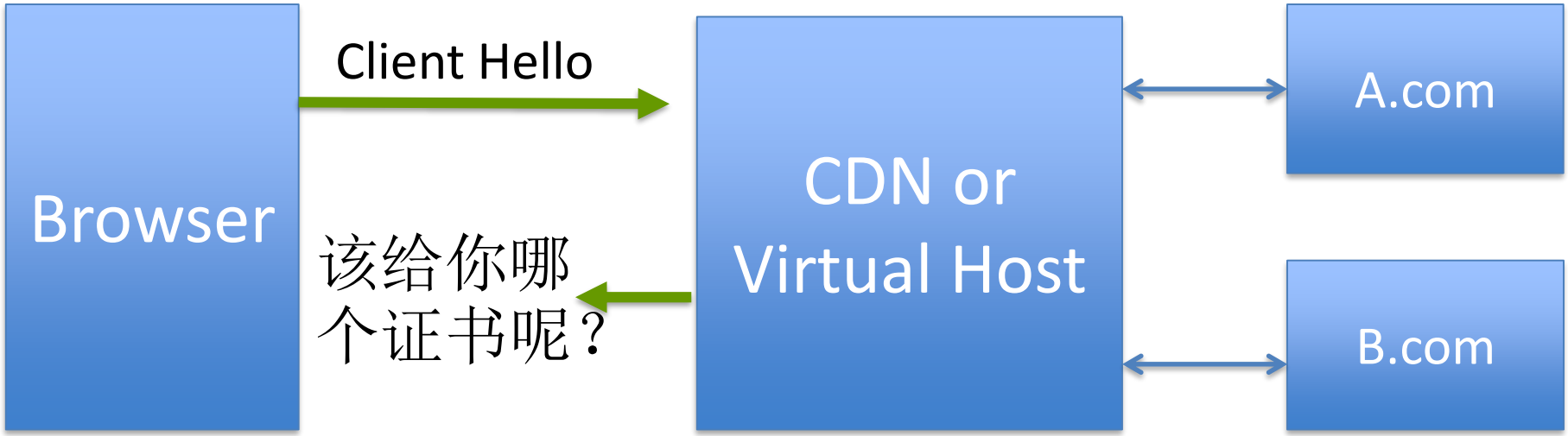
http://bbs.wenxuecity.com/joke/622215.html

Complicated Real World




Client
Server
client_hello
server_hello
Establish security capabilities, including protocol version, session ID, CipherSuite, compression method, and initial random numbers.
certificate
server_key_exchange
certificate_request
server_hello_done
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.
Time
certificate
client_key_exchange
certificate_verify
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.
change_cipher_spec
finished
change_cipher_spec
finished
Change cipher suite and finish handshake protocol.

TLS Extension, RFC 3546, 2003



TLS is now used in an increasing variety of operational environments - many of which were not envisioned when the original design criteria for TLS were determined.

提纲

- 互联网哲学、End-to-End原则及其质疑
- TLS和Web 的目标：认证、保密和完整性
- HTTPS在CDN中的保密性和授权问题
- 同源访问控制和完整性
- 思考与讨论

35th IEEE Symposium on Security and Privacy

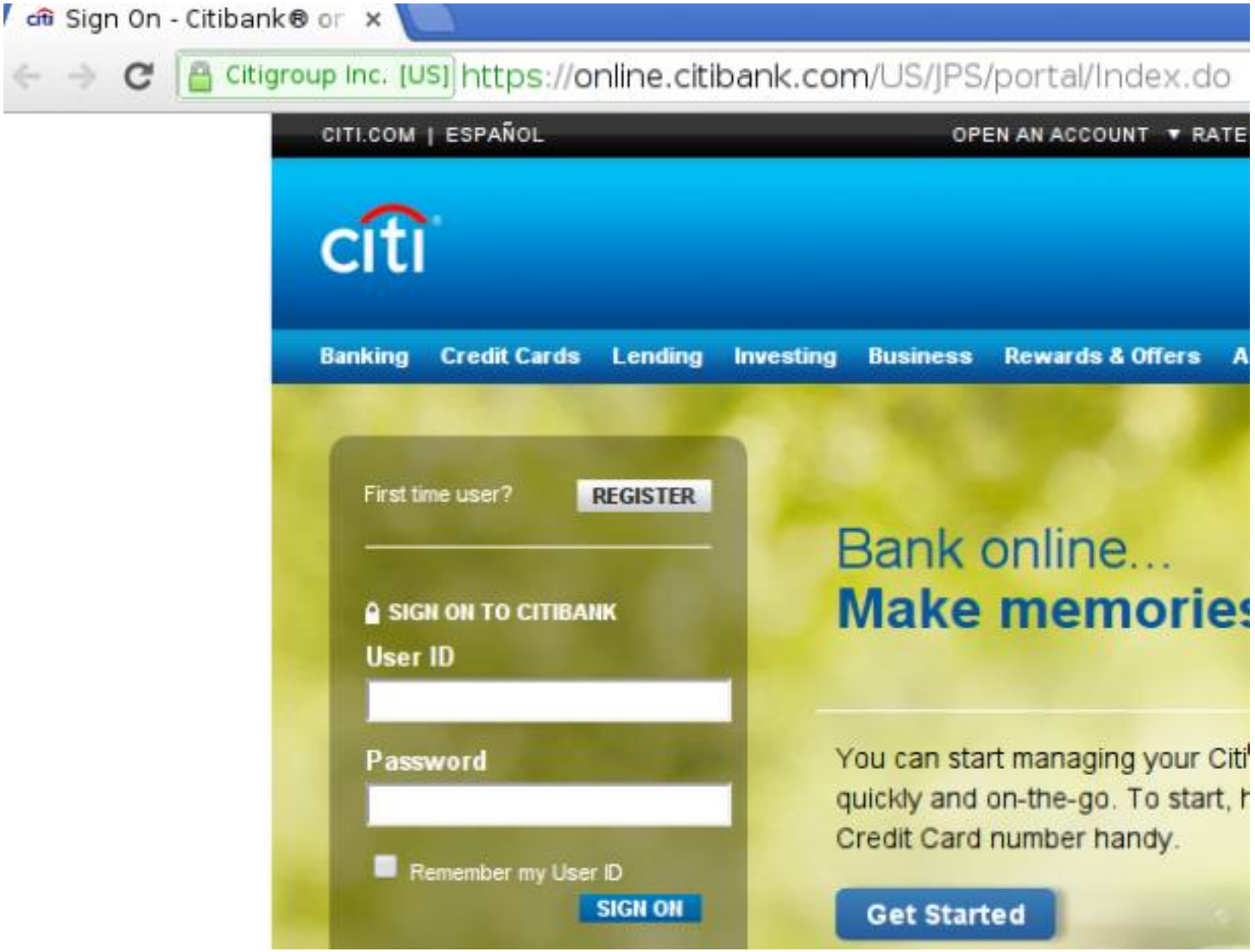
When HTTPS Meets CDN

A Case of Authentication in Delegated Service

Jinjin Liang[1], Jian Jiang[1], Haixin Duan[1],
Kang Li[2], Tao Wan[3], Jianping Wu[1]

[1] Tsinghua University [2] University of Georgia [3] Huawei Canada

Our Sensitive Information Is Transmitted Over the Web

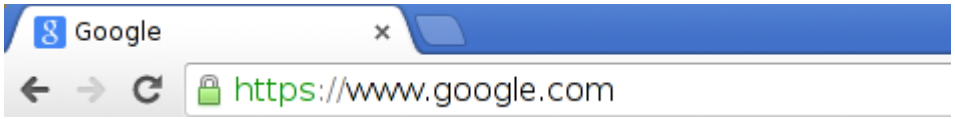


Our Sensitive Information Is Transmitted Over the Web


```
 CNAME    online.citibank.com.edgekey.net.
IN CNAME  e5035.b.akamaiedge.net.
 A        184.28.156.106
```

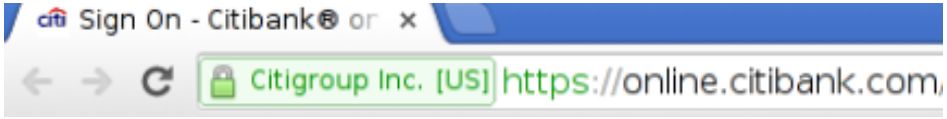
The Website Is Using HTTPS

- HTTP over SSL/TLS
  - Authentication, Encryption
- Server Certificate serves as website identity
  - Domain Validation (DV)
  - Organization Validation (OV)



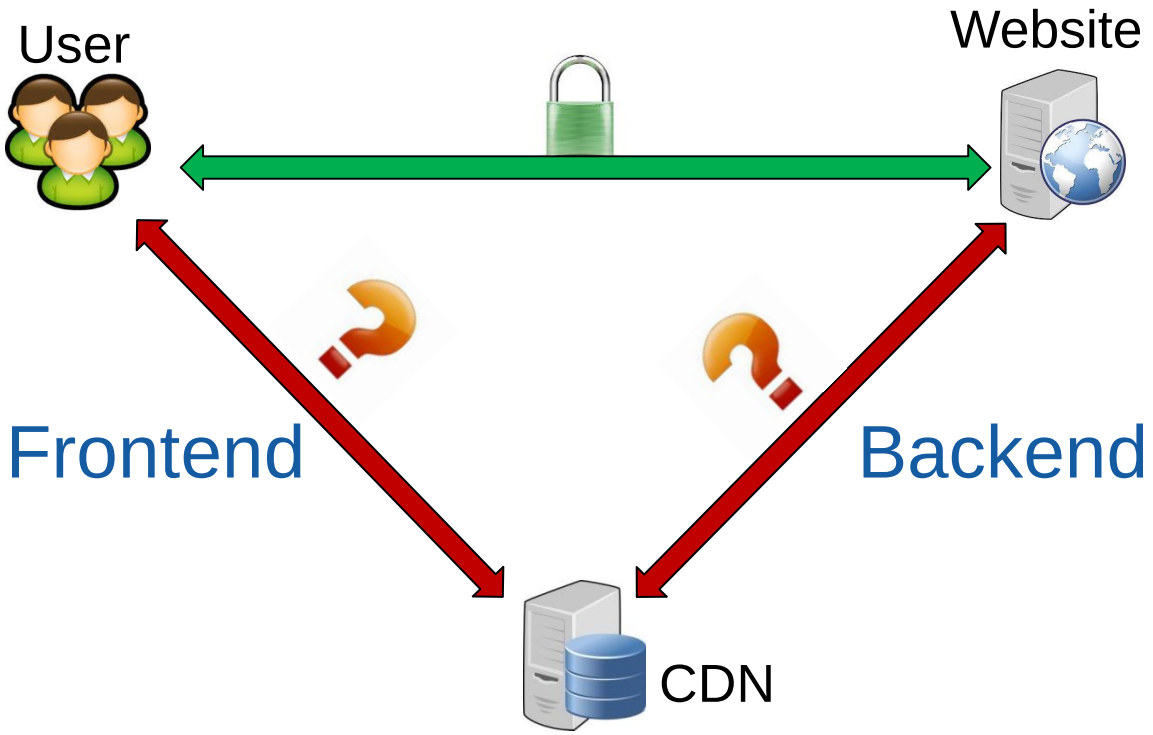
CA是商业公司，
自动签发证书

  - Extended Validation (EV)

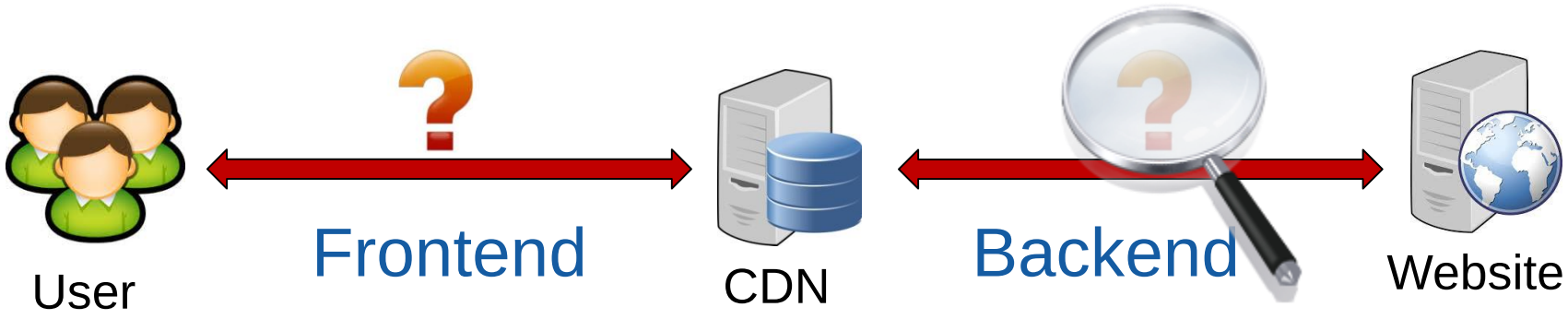


When HTTPS Meets CDN

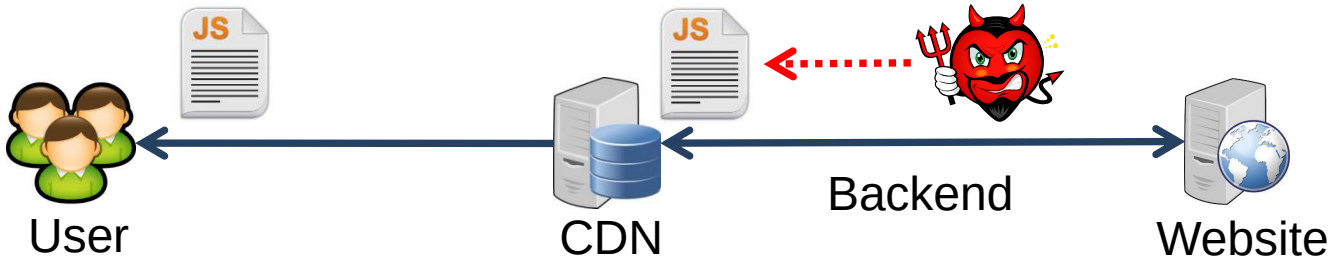
- From 2 parties to 3 parties
- Break into Frontend and Backend



Backend Communication



Backend is Vulnerable



- A Security Incident We (CCERT) handled
  - CERNET; April 15, 2014
  - Victims: a large CDN and a famous website
  - A MITM attack injected a fake JS file into CDN caching server

```
if(typeof(AC)=="undefined"){AC={}}Object.extend(Event,{_domReady:function(){if(arguments.callee.done){return
}arguments.callee.done=true;if(this._timer){clearInterval(this._timer)}AC.isDomReady=true;
if(this._readyCallbacks){this._readyCallbacks.each(function(b){b()})}this._readyCallbacks=null
},onDOMReady:function(c){if(AC.isDomReady){c()}else{if(!this._readyCallbacks){var d=this._domReady.bind(this);
if(document.addEventListener){document.addEventListener("DOMContentLoaded",d,false)
}if(document.all){document.onreadystatechange=function(){if(this.readyState=="complete"){d()
}}}if(/WebKit/i.test(navigator.userAgent)){this._timer=setInterval(function(){if(/loaded|complete/.test(document.readyState)){d()
}},10)}Event.observe(window,"load",d);Event._readyCallbacks=[]}Event._readyCallbacks.push(c)
}});AC.decorateSearchInput=function(z,K){var u=$(z);var D=null;var E=0;var y="";
var A="";if(K){if(K.results){E=K.results}if(K.placeholder){y=K.placeholder}if(K.autosave){A=K.autosave
}if(AC.Detector.isWebKit()){if(AC.Detector.isWin()){u.addClassName("not-round")
}u.setAttribute("type","search");if(!u.getAttribute("results")){u.setAttribute("results",E)
}if(null!=y){u.setAttribute("placeholder",y);u.setAttribute("autosave",A)}}else{u.setAttribute("autocomplete","off");
D=document.createElement("input");u.parentNode.replaceChild(D,u);var G=document.createElement("span");
Element.addClassName(G,"left");var x=document.createElement("span");Element.addClassName(x,"right");
var B=document.createElement("div");Element.addClassName(B,"reset");var J=document.createElement("div");
Element.addClassName(J,"search-wrapper");var C=z.value==y;var F=z.value.length==0;
if(C||F){u.value=y;Element.addClassName(J,"blurred");Element.addClassName(J,"empty")
}J.appendChild(G);J.appendChild(u);J.appendChild(x);J.appendChild(B);var v=function(){var a=Element.hasClassName(J,"blurred");
if(u.value==y&&a){u.value=""}Element.removeClassName(J,"blurred")};Event.observe(u,"focus",v);
var H=function(){if(u.value==""){Element.addClassName(J,"empty");u.value=y}Element.addClassName(J,"blurred")
};Event.observe(u,"blur",H);var I=function(){if(u.value.length>=0){Element.removeClassName(J,"empty")
}};Event.observe(u,"keydown",I);var w=function(){return(function(b){var a=false;
if(b.type=="keydown"){if(b.keyCode!=27){return}else{a=true}}u.blur();u.value="";
Element.addClassName(J,"empty");u.focus()})};Event.observe(B,"mousedown",w());Event.observe(u,"keydown",w());
if(D){D.parentNode.replaceChild(J,D)}}};Element.addMethods({getInnerDimensions:function(l){l=$(l);
var h=Element.getDimensions(l);var j=h.height;var d=Element.getStyle;j-=d(l,"border-top-width")&&d(l,"border-
top-width")!="medium"?parseInt(d(l,"border-top-width"),10):0;
j-=d(l,"border-bottom-width")&&d(l,"border-bottom-width")!="medium"?parseInt(d(l,"border-bottom-width"),10):0;
j-=d(l,"padding-top")?parseInt(d(l,"padding-top"),10):0;j-=d(l,"padding-bottom")?parseInt(d(l,"padding-bottom"),10):0;
var g=h.width;g-=d(l,"border-left-width")&&d(l,"border-left-width")!="medium"?parseInt(d(l,"border-left-width"),10):0;
g-=d(l,"border-right-width")&&d(l,"border-right-width")!="medium"?parseInt(d(l,"border-right-width"),10):0;
g-=d(l,"padding-left")?parseInt(d(l,"padding-left"),10):0;g-=d(l,"padding-right")?parseInt(d(l,"padding-right"),10):0;
return{width:g,height:j}},getOuterDimensions:function(d){d=$(d);var l=d.cloneNode(true);
var p=(d.parentNode)?d.parentNode:document.body;p.appendChild(l);Element.setStyle(l,{position:"absolute",visibility:"hidden"});
var m=Element.getDimensions(l);var o=m.height;var j=Element.getStyle;o+=j(l,"margin-top")?parseInt(j(l,"margin-top"),10):0;
o+=j(l,"margin-bottom")?parseInt(j(l,"margin-bottom"),10):0;var n=m.width;n+=j(l,"margin-left")?parseInt(j(l,"margin-left"),10):0;
n+=j(l,"margin-right")?parseInt(j(l,"margin-right"),10):0;Element.remove(l);return{width:n,height:o}
},translateOffset:function(e){var f,g,h=null;f=e.getStyle("transform");if(!f){f=e.getStyle("webkitTransform")
}if(!f){f=e.getStyle("MozTransform")}if(!f){f=e.getStyle("msTransform")}if(!f){f=e.getStyle("oTransform")
}if(f){g=f.match(/.*(translate|translate3d|translateZ|translateX|translateY)\(([^)]+).*/);
if(g){h=[];switch(g[1]){case"translateX":h[0]=parseInt(g[2]);h[1]=0;break;case"translateY":h[1]=parseInt(g[2]);
h[0]=0;break;case"translateZ":h[2]=parseInt(g[2]);h[0]=0;h[1]=0;break;default:h=g[2].split(/,\s*/);
if(typeof h[0]!=="undefined"){h[0]=parseInt(h[0])}if(typeof h[1]!=="undefined"){h[1]=parseInt(h[1])
}if(typeof h[2]!=="undefined"){h[2]=parseInt(h[2])}break}h.type=g[1];h.x=h[0];h.y=h[1];
h.z=h[2]}else{g=f.match(/.*(matrix)\(([^)]+).*/);if(g!==null){g=f.match(/.*(matrix)\(([^)]+).*/)[2].split(", ");
h=[parseFloat(g[4]),parseFloat(g[5])];h.type="matrix";h.x=h[0];h.y=h[1];h.z=null
}}}return h},removeAllChildNodes:function(b){b=$(b);if(!b){return}while(b.hasChildNodes()){b.removeChild(b.lastChild)
}},setVendorPrefixStyle:function(n,j,l){if(!(Object.isElement(n)&&typeof j==="string"&&(typeof l==="string"||typeof l==="number"))){throw"Incorrect
input arguments for Element.setVendorPrefixStyle."
}l+="";if(j.match(/^webkit/i)){j=j.replace(/^webkit/i,"")}else{if(j.match(/^moz/i)){j=j.replace(/^moz/i,"")
}else{if(j.match(/^ms/i)){j=j.replace(/^ms/i,"")}else{if(j.match(/^o/i)){j=j.replace(/^o/i,"")
}else{if(j.match("-")){var g=j.split("-"),m=g.length;j="";for(var h=0;h<g.length;
h++){j+=g[h].charAt(0).toUpperCase()+g[h].slice(1)}}else{j=j.charAt(0).toUpperCase()+j.slice(1)
}}}}if(l.match("-webkit-")){l=l.replace("-webkit-","-vendor-")}else{if(l.match("-moz-")){l=l.replace("-moz-","-vendor-")
}else{if(l.match("-ms-")){l=l.replace("-ms-","-vendor-")}else{if(l.match("-o-")){l=l.replace("-o-","-vendor-")
}}}}n.style["webkit"+j]=l.replace("-vendor-","-webkit-");n.style["Moz"+j]=l.replace("-vendor-","-moz-");
```

免费下载 (安全认证)

动<>态 网系列软件

自由门7.42专业版 (2013年11月8日) 历史最久，使用人数最多。	下载exe 下载zip
自由门7.42专家版 (2013年11月8日) 用户界面为专业人士最爱。	下载exe 下载zip
自由门7.42限制版 (2013年11月8日) 缺省只能上少数几个网站，进一步增强安全性。	下载exe 下载zip

自由门手机版软件 (使用说明)

自由门安卓版3.1（2013年8月2日）	下载apk 数字签名 数字指纹
自由门Java手机版2.3(2012年9月3日)	下载jad 下载jar
自由门WM手机版1.3 (2012年7月31日)	下载exe 下载zip

动 <>态网其它软件

GProxy火狐工具条2.1版 （2012年7月5日） 火狐浏览器**Firefox**和雷鸟电邮**Thunderbird**的附加软件，让用户在火狐浏览器和雷鸟电邮中方便的切换代理服务器，支持世界通、自由门、无界、花园，支持正体、简体中文和英文界面。	下载zip 下载xpi 数字签名 数字指纹

Today, we came across an incident on "images.apple.com", which is hosted by Akamai:

When we visit the URL "http://images.apple.com/global/scripts/apple_core.js" in CERNET in China,
we will get a fake Javascript file; however, when we visit the same URL using HTTPS, we will get the true file.

The DNS resolution of "images.apple.com" in CERNET is as follows:

```
images.apple.com.       2992    IN      CNAME   images.apple.com.edgesuite.net.
images.apple.com.edgesuite.net. 8473 IN CNAME   images.apple.com.edgesuite.net.globalredir.akadns.net.
images.apple.com.edgesuite.net.globalredir.akadns.net. 2992 IN CNAME a199.cn.w.tl88.net.
a199.cn.w.tl88.net.     20      IN      A       58.205.224.231
a199.cn.w.tl88.net.     20      IN      A       58.205.224.234
```

Several possible reasons may result in this incident, such as MITM attack, the two servers are compromised and etc.
However, from outside, we could not figure out what exactly is happening. So we turn to you for help.
Please let us know if you need more information or if you have any idea about this incident. Thank you.

Besides, Chinanetcenter, a CDN provider in China, seems involved in this case as well. So we are curious about
the cooperation between Akamai and Chinanetcenter and how it works. Could you introduce more details on this for us?

We will really appreciate your help and look forward to your reply.

Thank you.

[redacted]@akamai.com> 1:49 AM (7 hours ago)

to [redacted]

Hello Ji[redacted],
Thanks for pointing this out! Sorry for the long time it took me to respond. Yes, it appears that this was due to a MITM attack on CERNET. One of our proxy servers obtained the fake file in response to the request issued. Using HTTPS we're able to authenticate the origin and this type of attack can't happen.
If you ever encounter something suspicious again, please let us know.

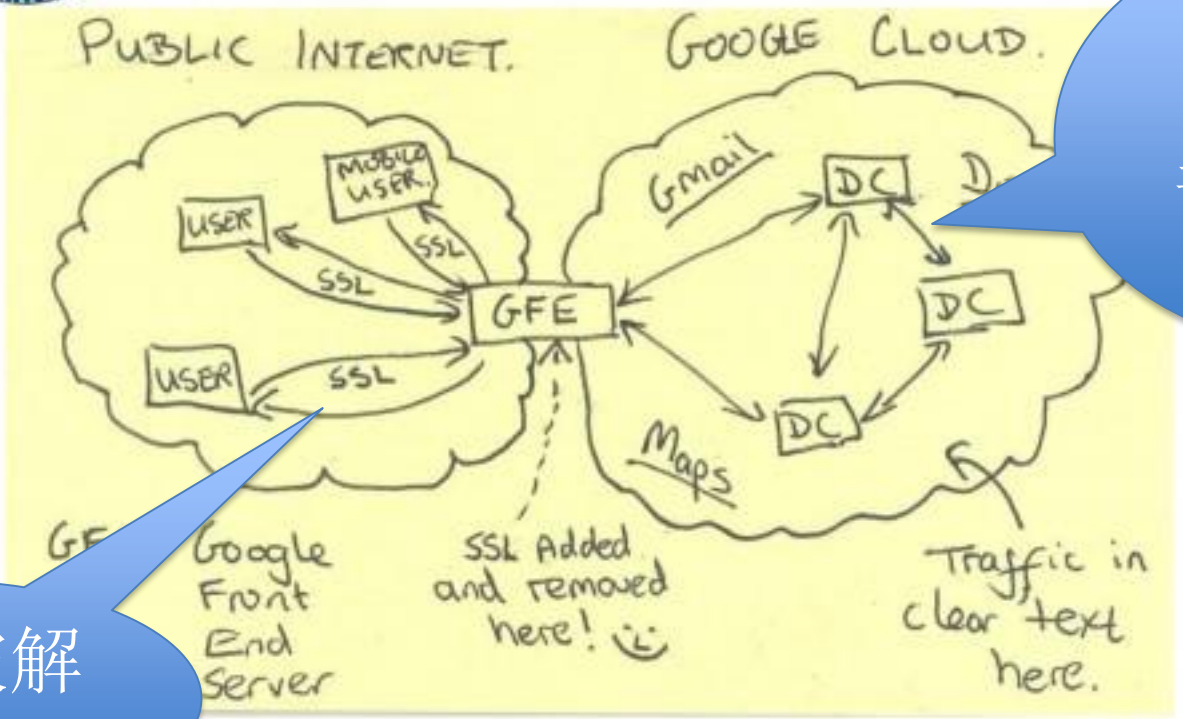
Thanks

...

NSA: Bypass HTTPS

TOP SECRET//SI//NOFORN

Current Efforts - Google



监听google内部未加密通信

不必破解SSL

TOP SECRET//SI//NOFORN

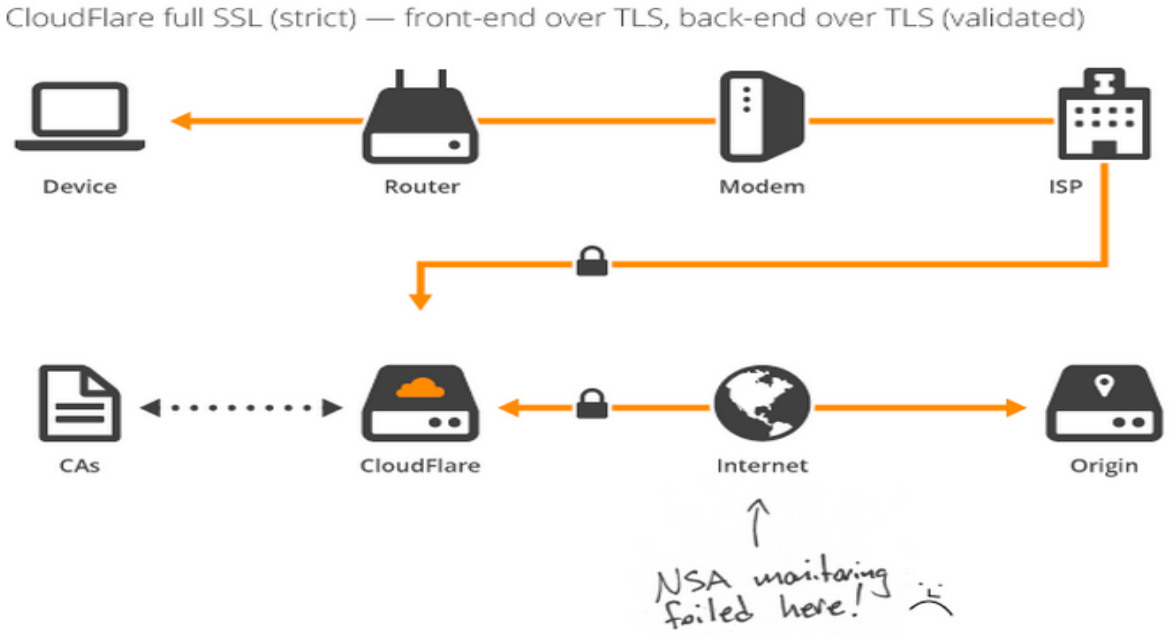
The Current Practice in Backend

- Experiment on 5 CDNs in Nov. 2013

CDN Provider	Result
CDN77	HTTP
CDN.NET	HTTP
CloudFlare	HTTPS, not validate certificate
Incapsula	HTTPS, not validate certificate
CloudFront	HTTPS, not validate common name

来自工业界的反馈

- 论文发布之前通报知名的CDN厂商
- CloudFlare, Akamai,Incapsula, Amazon积极反馈
- CloudFlare 在1个月内推出Strict SSL 服务



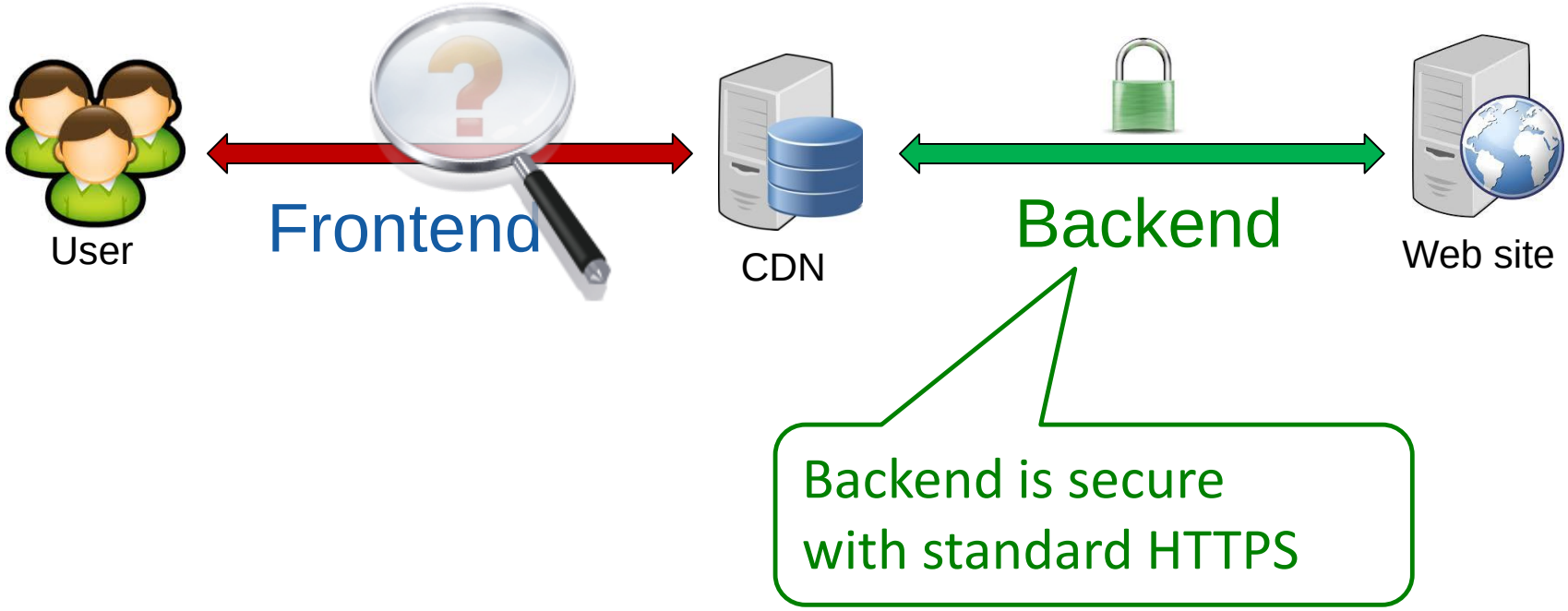
http://blog.cloudflare.com/introducing-strict-ssl-protecting-against-a-man-in-the-middle-attack-on-origin-traffic

Backend Should Use HTTPS and Validate Certificate

- Response from industries
  - CloudFlare (Fixed)
  - CloudFront (Fixed)
  - Incapsula (Fixing)，fighting Heart Bleed

- Customers want to use self-signed certificates?

Frontend Communication



Broken HTTPS Authentication
in DNS Based Request Routing

Root Cause: Browser does not know the delegation from website to CDN!

Survey on CDNs and Websites

- 20 popular CDN providers

Support DNS Routing	Support HTTPS
20	19

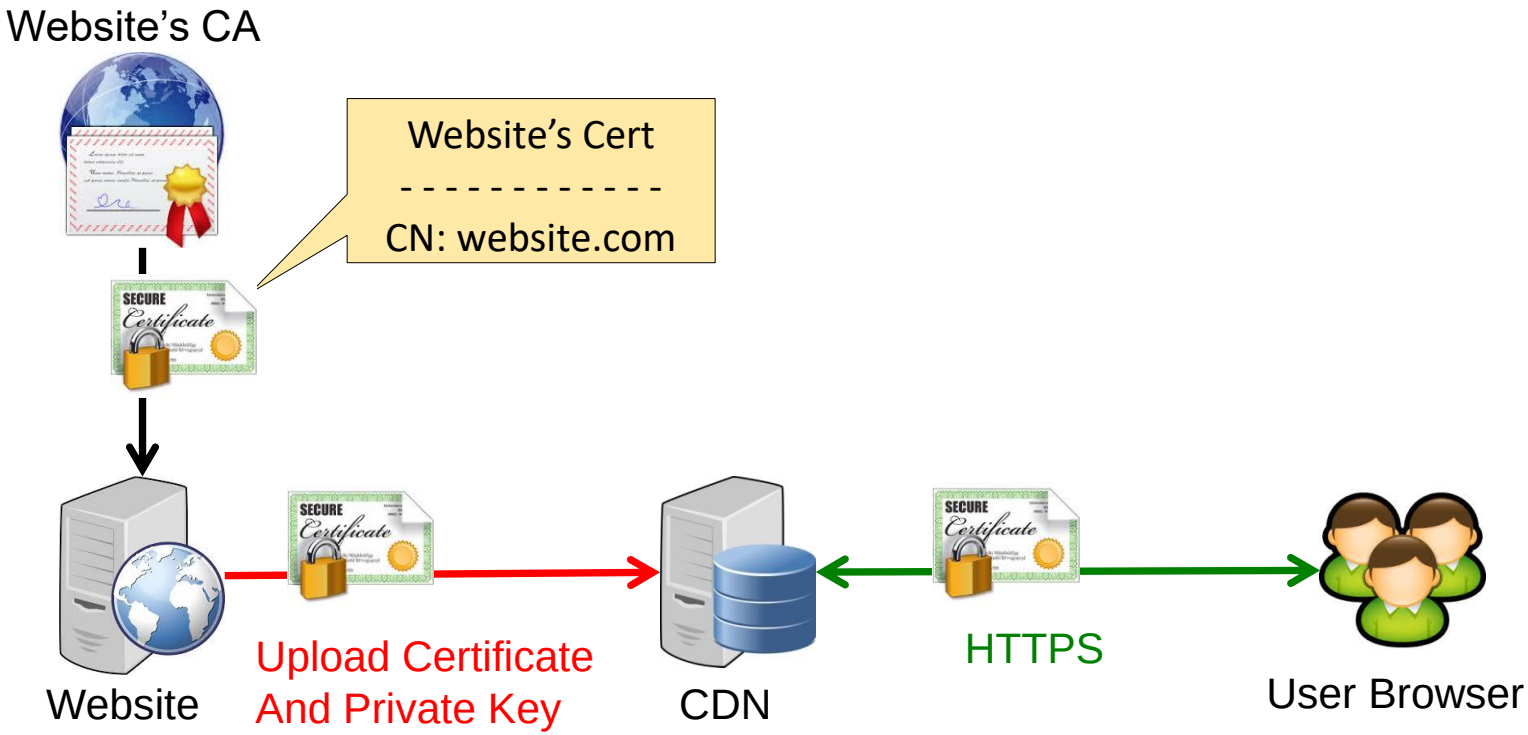
- Alexa Top 1M websites
  - 10,721 use CDN and HTTPS

Invalid Certificate		Valid Certificate	
Status 200	Other	Custom Cert	Shared Cert
15%	54%	20%	11%
69%		31%	

有可能原始网站没有启用HTTPS

它们如何解决无效证书问题的呢？

Custom Certificate (Type I)



- Have to share private key
- Heavy key management overhead
- Inefficient revocation

Custom Certificate (Type II)

This certificate has been verified for the following usages:

SSL Server Certificate

Issued To

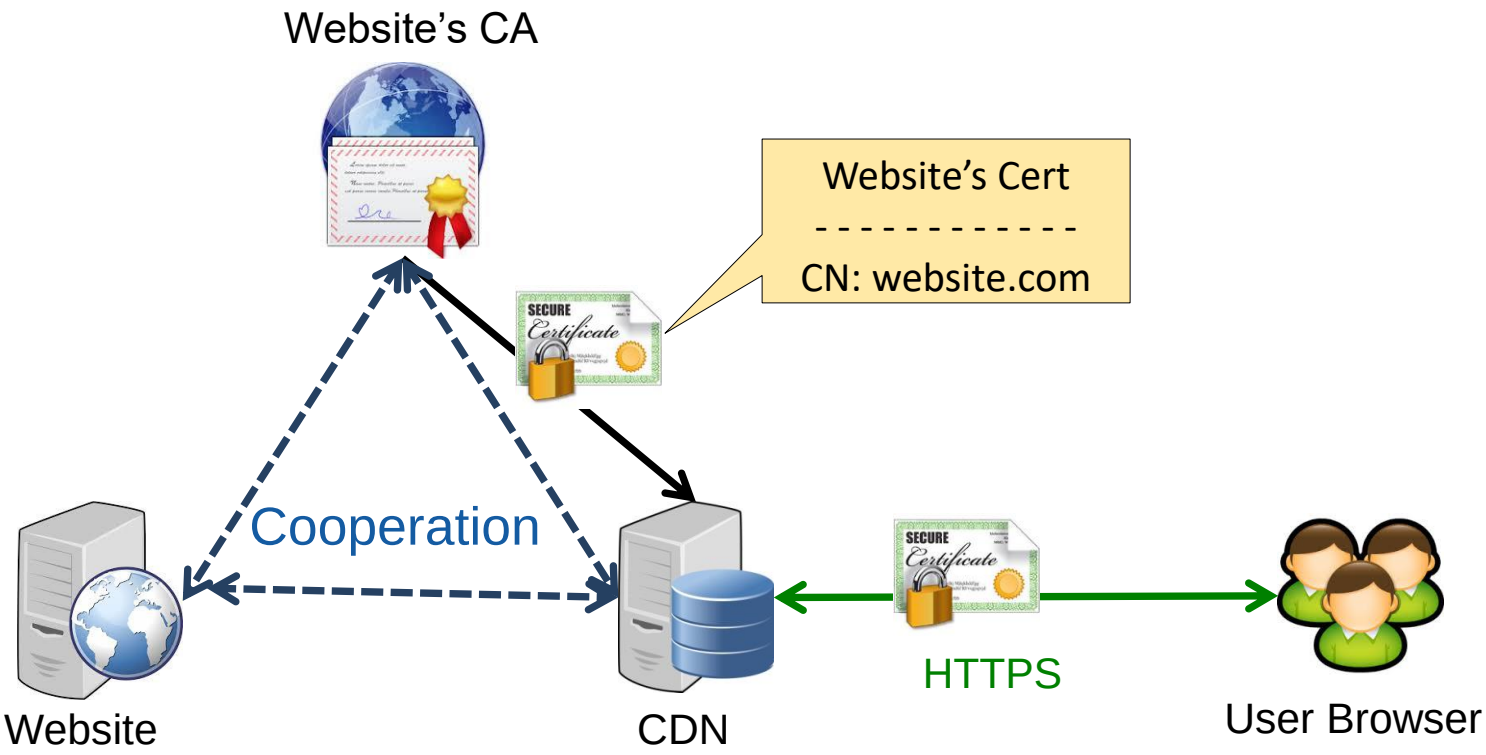
Common Name (CN)	www.apple.com
Organization (O)	Apple Inc.
Organizational Unit (OU)	Internet Services for Akamai
Serial Number	52:C3:FD:89:F2:C5:37:84:50:FE:53:AC:1A:74:79:74

Issued By

Common Name (CN)	Symantec Class 3 EV SSL CA - G3
Organization (O)	Symantec Corporation
Organizational Unit (OU)	Symantec Trust Network

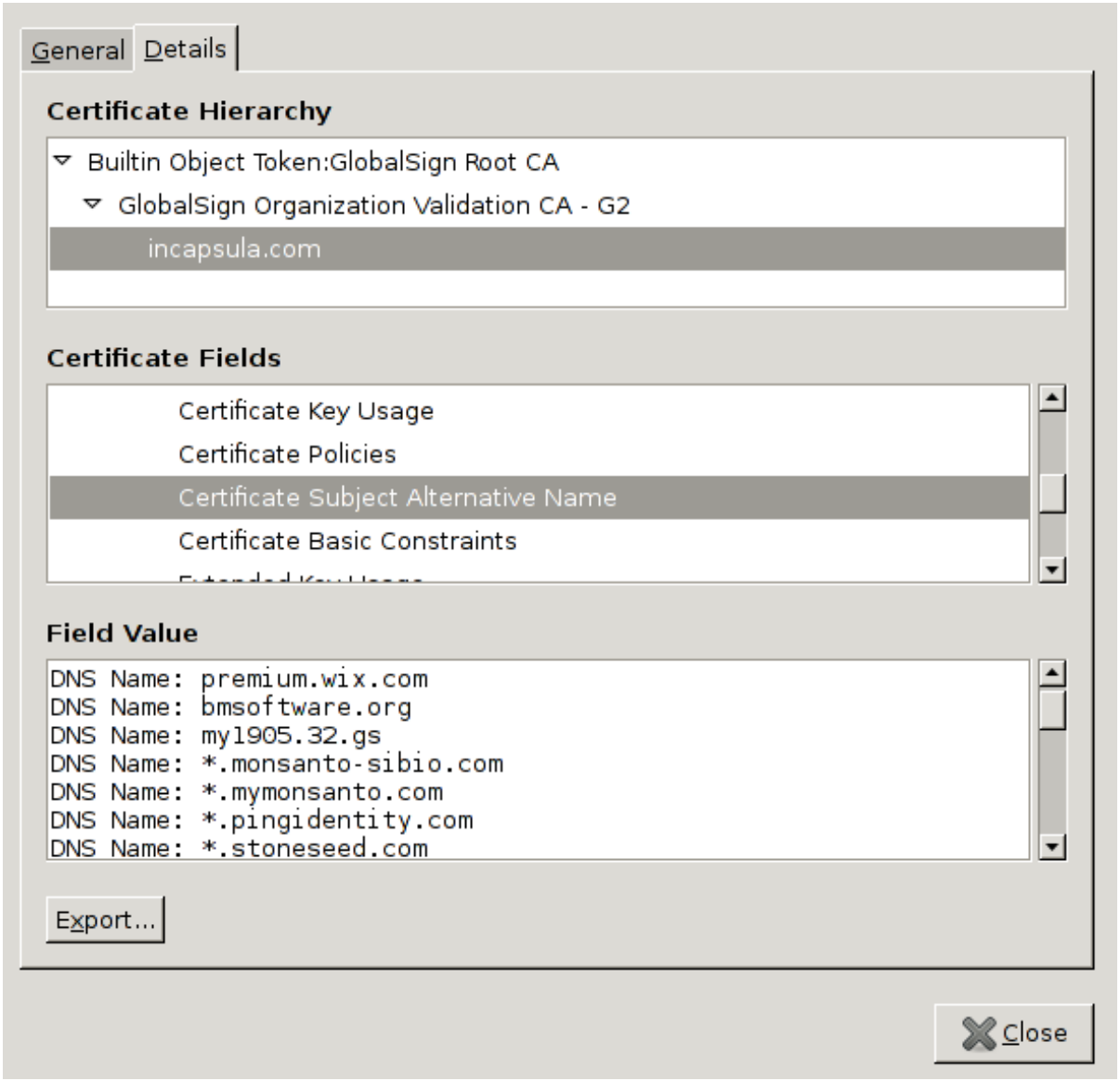
Custom Certificate (Type II)

Not covered in the paper

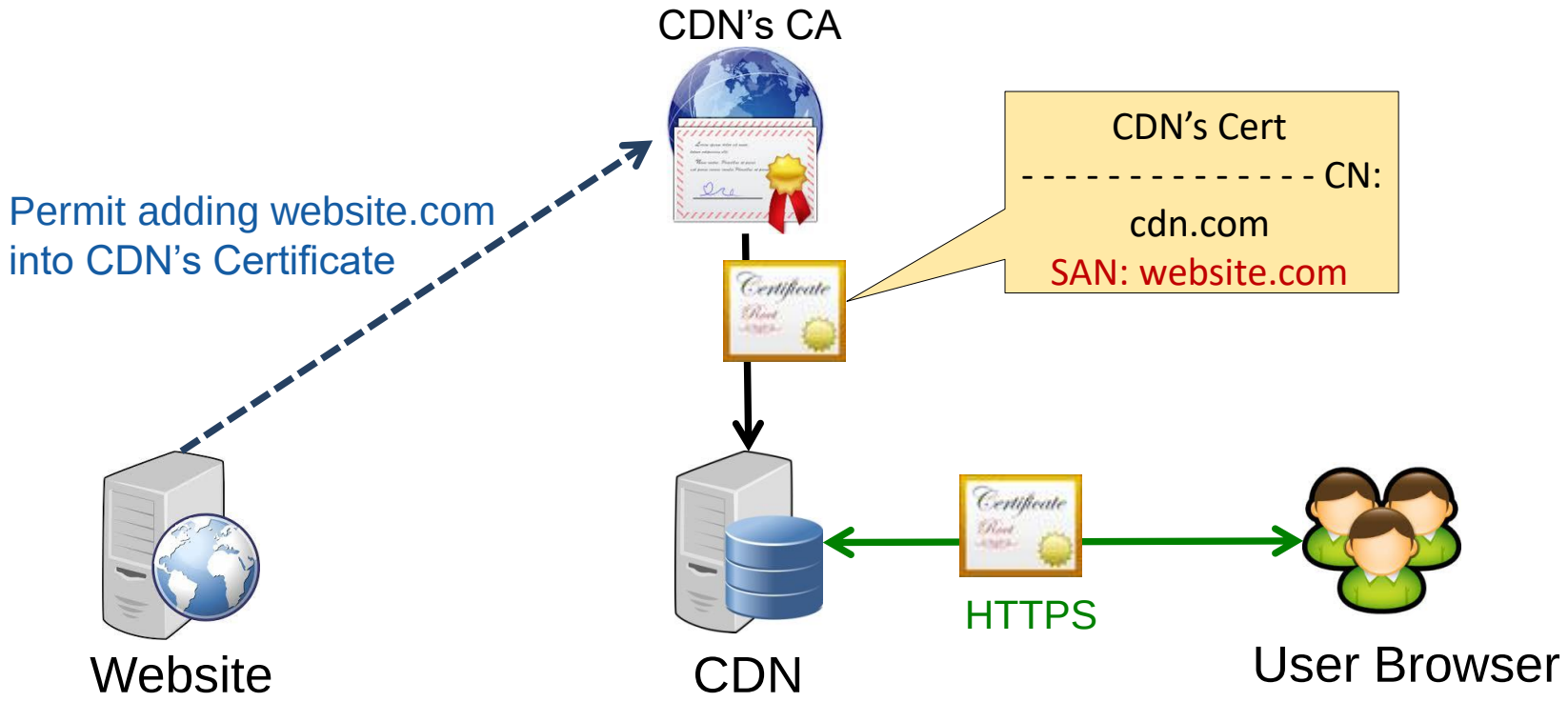


- Heavy key management overhead
- Inefficient issuance and revocation

Shared Certificate



Shared Certificate



- Improper security indicator (e.g. website has EV but CDN has DV/OV)
- Website can not revoke the certificate

Case Study on Shared Certificate

- CDN: Incapsula (CA: GlobalSign)
  - Issuance: Email confirmation from CA
  - Revocation
    - Incapsula removed our website domain name in a new shared certificate
    - But our stale certificate was not revoked by CA
    - Contacted GlobalSign, but no response
- Incapsula said they would work on this problem with their CAs

Revocation Problem of Shared Certificate

- 1198 websites using shared certificate
- Certificate update, CRL and OCSP
- Last for 3 months
- 1865 certificate updates from 5 CDNs, but none was revoked
- Also discovered by Web PKI (NDSS 2014)
  - "this form of operation should be more strongly regulated"

提纲

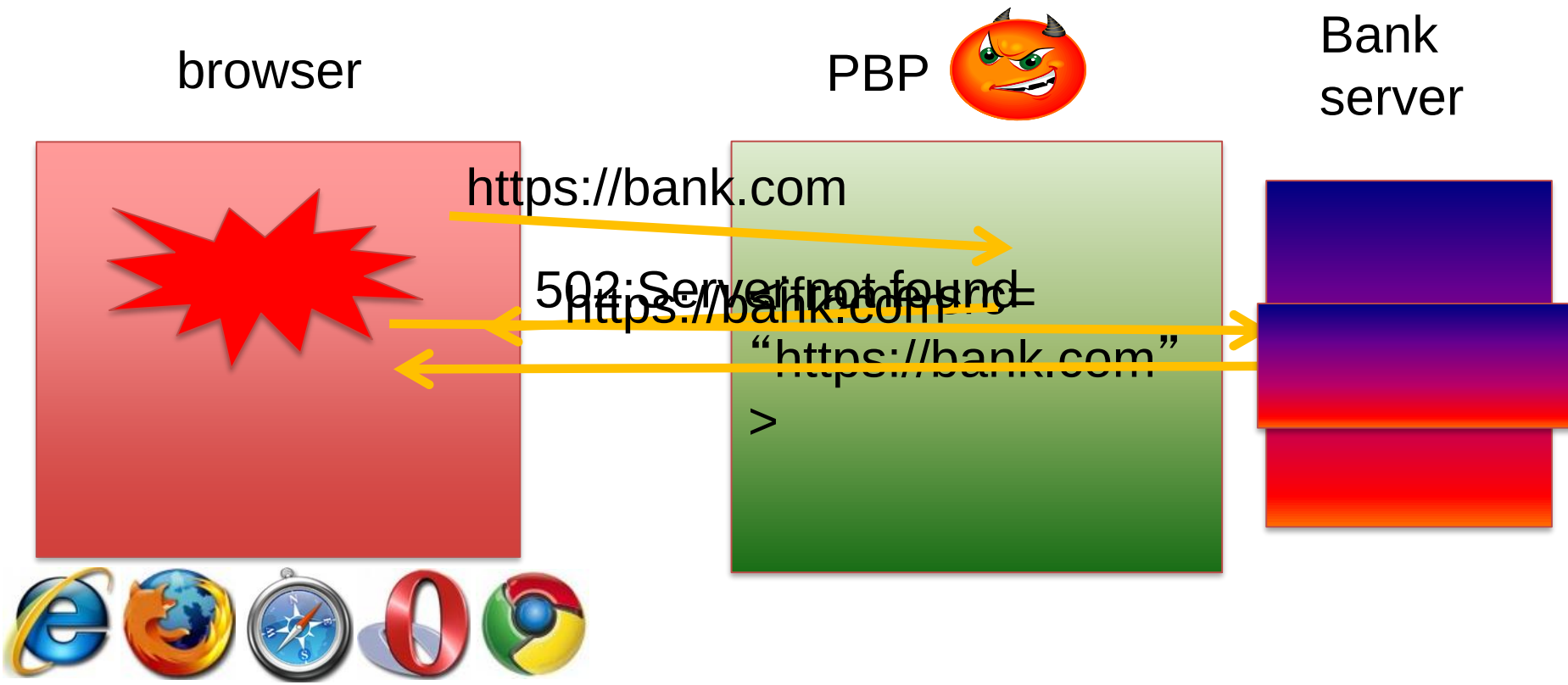
- 互联网哲学、End-to-End原则及其质疑
- TLS和Web 的目标：认证、保密和完整性
- HTTPS在CDN中的保密性和授权问题
- 同源访问控制和完整性
- 思考与讨论

Same Origin Policy

- 一个浏览器同时多个网站
- 不同来源的资源应该相互隔离
- Origin for DOM:
  - Scheme： http or https
  - Hostname
  - Port number(other than IE)
- Origin is different for:
  - XMLHttpRequest, Cookie, Java, …

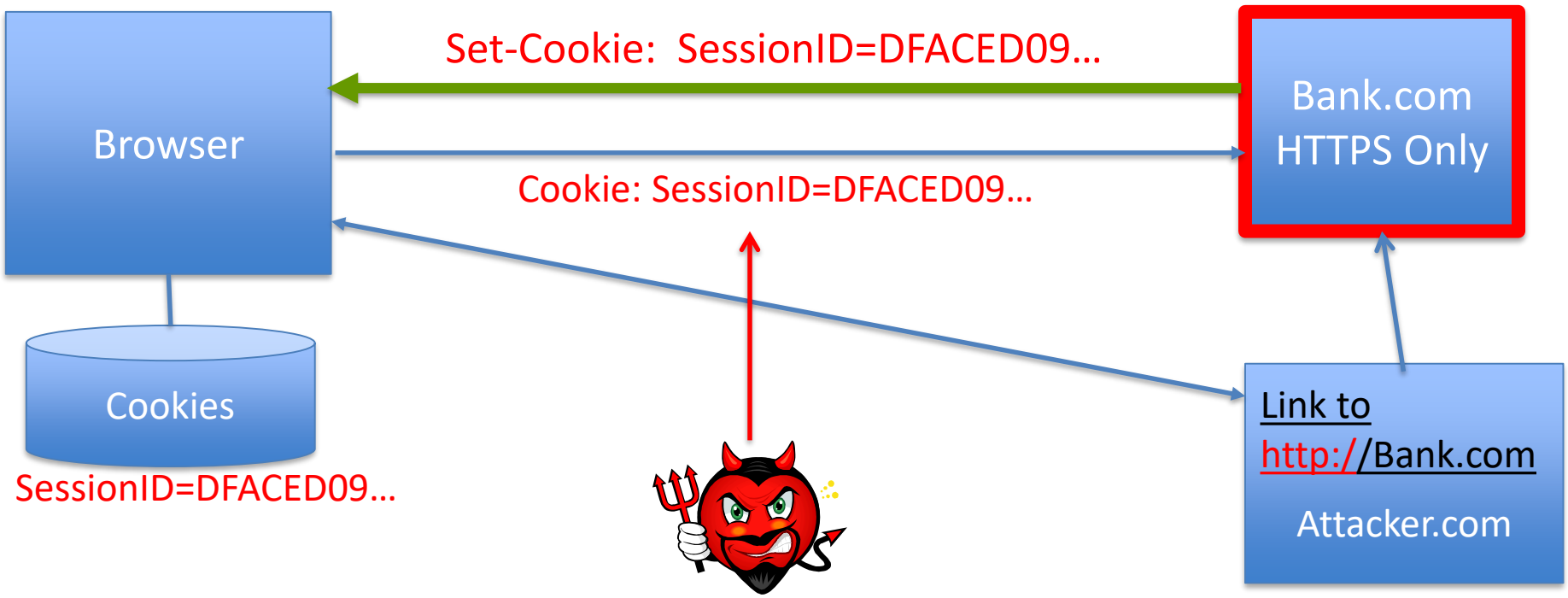
Pretty Bad Proxy(PBP), by 陈硕等, 2009

- Proxy’s error/redirect page: e.g., 502-server-not-found;
- Script in error page runs in https://bank.com.



Confidentiality Attack： Surfjacking

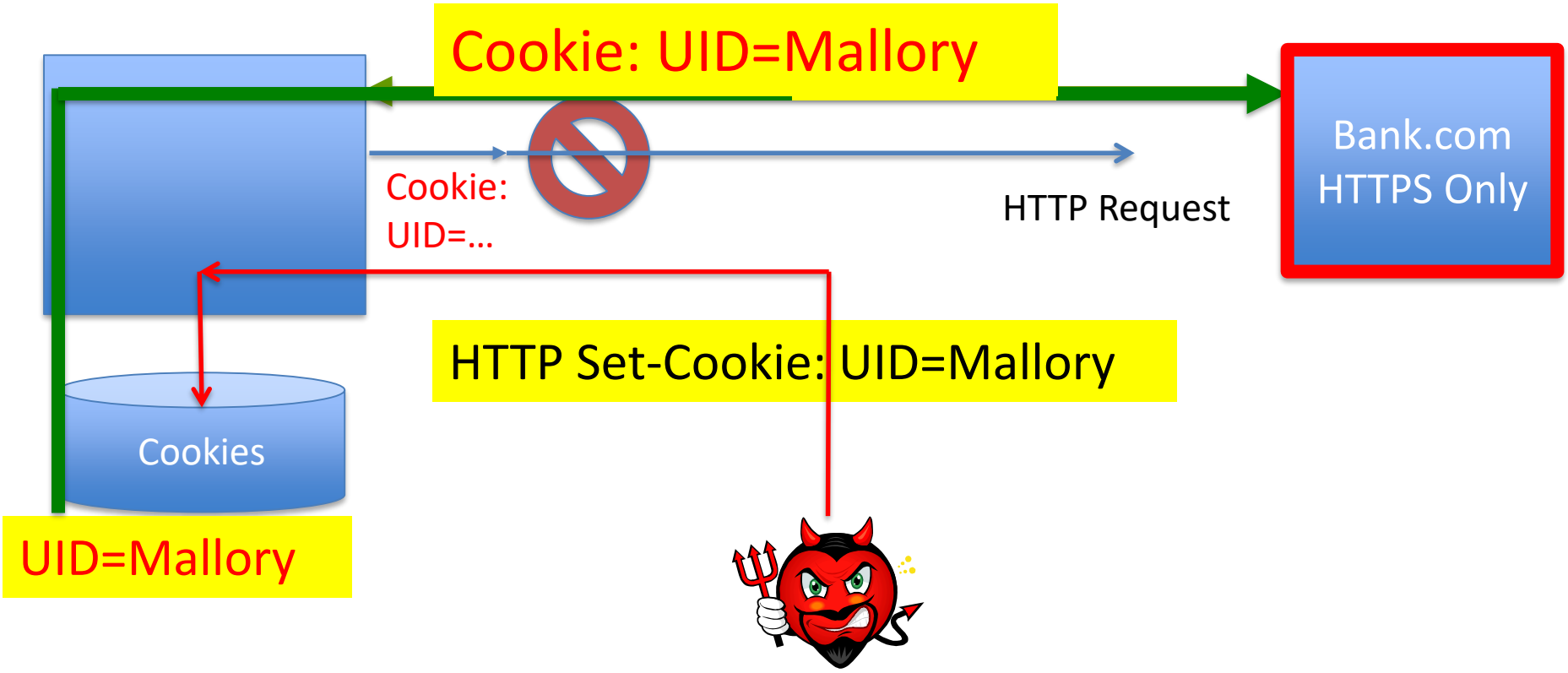
- Mike Perry, DefCon16, 2008



Surf Jacking Gmail demonstration: http://vimeo.com/1507697

Integrity Attack: Cookie Forcing

- Chris Evans, 2008



A Secure Flag doesn't protect Integrity !!!

What we can do by cookie Forcing?

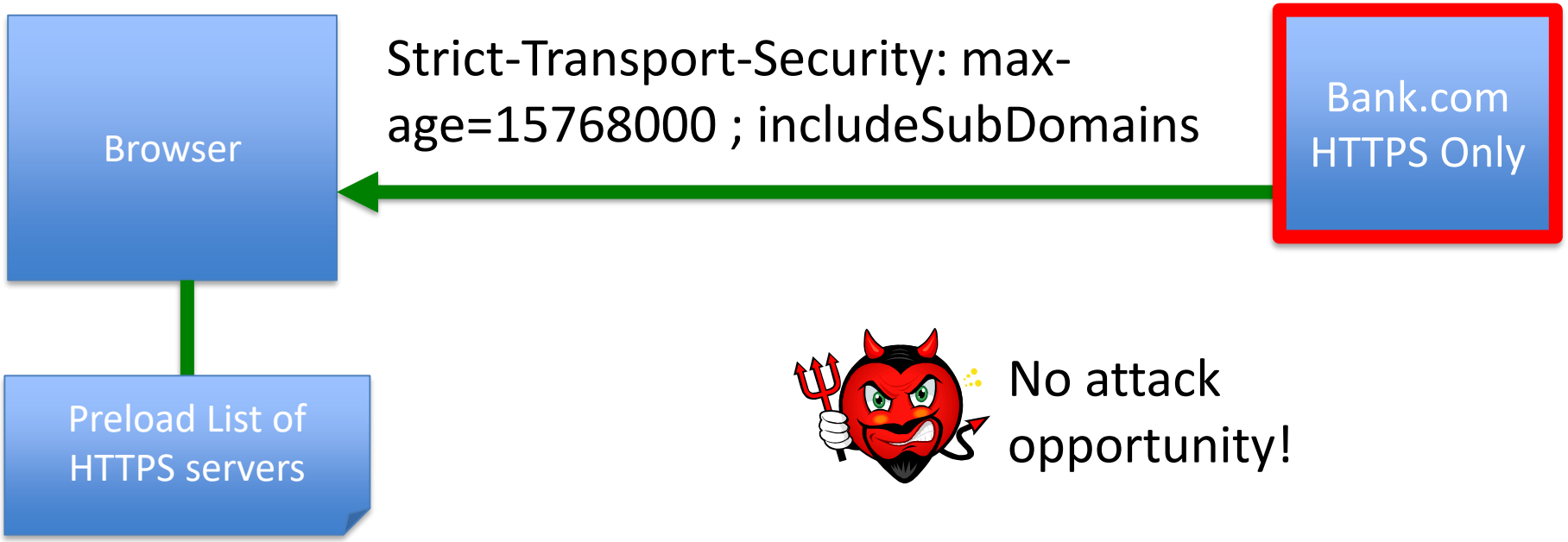
- 郑晓峰，段海新，陈建军，HTTPS 劫持展示 GeekPwn，Oct. 24, 2014

- Google Talk 好友列表的替换
- Unipay 关联银行卡攻击
- 结合网站XSS漏洞实现银行支付的劫持

- 我们没有演示的：Amazon, BoA, Facebook, ….

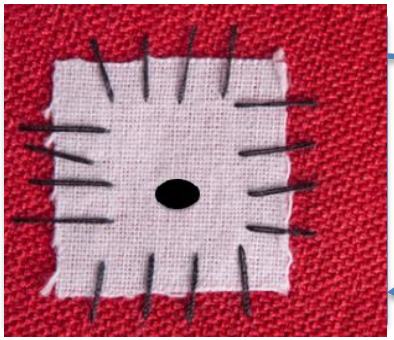
Solution:HSTS(RFC 6797, 2012)

- If a browser knows the server is HTTPS only, then it will never initiate a HTTP request
- Two ways to notify the browser:
  - (1) STS Header; (2) Preload HSTS server list



PBP 407: a hole in the patch!
腾讯TCSR通用漏洞披露10万元奖金

- Bank.com is HSTS enabled, so browser cannot initiate a HTTP request
- But if a browser use HTTP Proxy….



https://bank.com

Proxy

Bank.com
HTTPS Only

407: Authentication Required
Set-Cookie: UID=XSS

提纲

- 互联网哲学、End-to-End原则及其质疑
- TLS和Web 的目标：认证、保密和完整性
- HTTPS在CDN中的保密性和授权问题
- 同源访问控制和完整性问题
- 解决方案与讨论

解决方案？

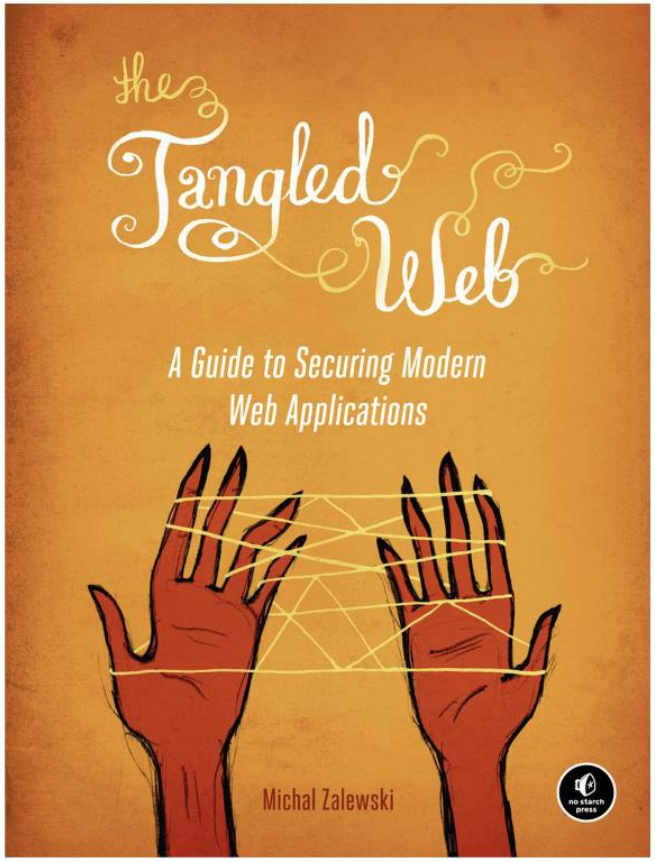
- 与Akamai, Cloud Flare讨论过CDN的解决方案
  - Duan Haixin, DANE Based Solution (IETF Toronto, 2014)
  - CloudFlare, Keyless SSL
- 与Google， Ali等互联网厂商讨论HTTPS和SOP的解决方案
- 不影响现有系统运行的情况下，很难找到完美的解决方案

Why Tangled, Tussle or Mass?

- 现有互联网并非源于一个宏伟的设计蓝图
- 需求、威胁、设计在扭斗中演化(Evolving)
  - 标准是后来定义的，而且定义模糊
  - 例如 SOP: DOM, Cookie, Flash, Storage, WebSocket
- 许多RFC标准只是对业界实践的总结，而非要求
  - HTTP State Management Mechanism(RFC 6265, 2011)
- 应用开发者混乱的理解，折衷的实现：
  - “HTTPOnly”？“Secure”?
- 用户、运维者：改动的风险可能大于被攻击
- TLS/SSL 设计是E2E，但Web正在快速演化

The Tangled Web, The Tangled Mass

- Michal Zalewski (google) The Tangled Web
- Narseo Vallina-Rodriguez, A Tangled Mass: The Android Root Certificate Stores, 2014
- 我们看到了很多问题，且没有完美的答案
- 没有上帝/哲人，没有指南



作为大学教师而非教父，希望是使惑而非解惑

? & #

duanhx@tsinghua.edu.cn