Chair for Network Architectures and Services
Department of Informatics
TU München – Prof. Carle

Network Security

Chapter 8

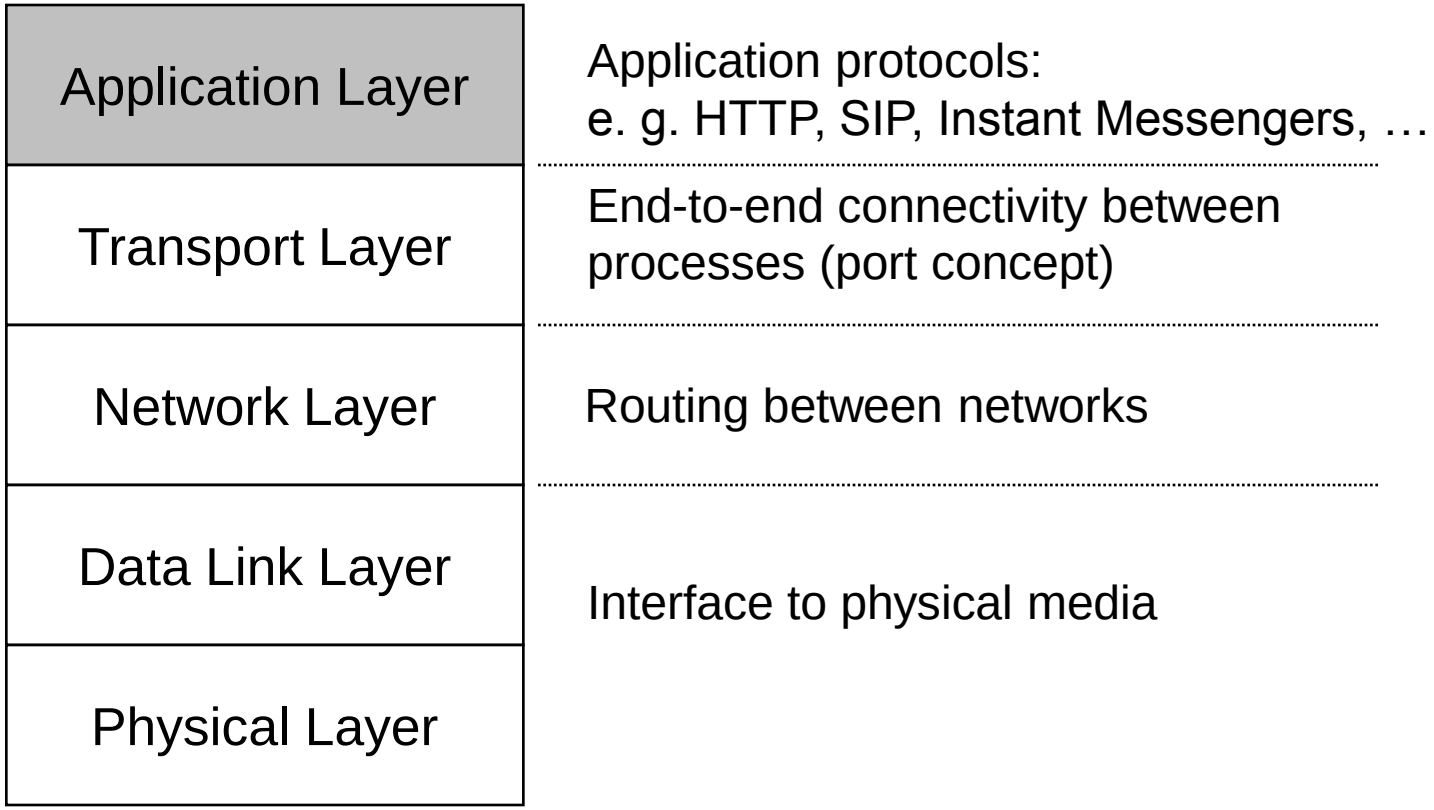
Application Layer Security

with friendly support by
P. Laskov, Ph.D.,
University of Tübingen

Application Layer Security

- WWW Security
- Identity Federation

Recap: Internet Protocol Suite



- TCP/IP stack has no specific representation for OSI layers 5, 6, 7 („session“, „representation“, „application“):
  the Application Layer is responsible for all three

Why Application Layer Security?

- So far, we were concerned with layers below the application layer:
  - Cryptography (mathematics)
  - Link Layer security
  - Crypto protocols: IPSec, SSL, Kerberos…
  - Firewalls
  - Intrusion Detection
- There are attacks where these defenses do not work:
  - Cross-Site Scripting, Buffer Overflows, …
- Possible because
  - These attacks are not detectable on lower layers (→ cf. WWW Security), or
  - The mechanisms do not secure the correct communication end-points (→ cf. Web Service Security, next lecture)
- In general, many applications need to provide their own security mechanisms
  - E. g. authentication, authorization

Part I: Introduction to the WWW

- Part I: Introduction to the WWW and Security Aspects
- Part II: Internet Crime
- Part III: Vulnerabilities and Attacks

Most important Web technologies

Name	Used for	Comment
HTML	Document structure	…
CSS	Document rendering	…
HTTP	Carrier protocol	…
Cookies	Session state keeping	…
URL/URI	Document location	…
JavaScript	Client-side computation and interaction	…
Flash	Client-side code execution	…
…	…	…

Introduction to the World Wide Web

- You all know it – but what is it exactly?
- Conceived in 1989/90 by Tim Berners-Lee at CERN

- Hypermedia-based extension to the Internet on the Application Layer
  - Any information (chunk) or data item can be referenced by a Uniform Resource Identifier (URI)
  - URI syntax (defined in RFCs) :
    `<scheme>://<authority><path>?<query>#<fragment>`
  - Special case: URL (“Locator”)
    `http://www.net.in.tum.de/de/startseite/`
  - Special case: URN (“Name”)
    `urn:oasis:names:specification:docbook:dtd:xml:4.1.2`

- Probably the best-known application of the Internet
- Currently, most vulnerabilities are found in Web applications

HTML and Content Generation

- HTML is the *lingua franca* of the Web
  - Content representation: structured hypertext documents
  - HTML documents – i. e. Web pages – may include:
    - JavaScript: script that is executed in browser
    - Java Applets: Java program, executed by Java VM
    - Flash: multimedia application, executed (played) by Flash player
- Today, much (if not most) content is created dynamically by server-side programs
  - (Fast-)CGI: interface between Web server and such a server-side program
  - Possible: include programs directly as modules in Web server (e.g. Apache)
- Often, dynamic Web pages also interact with the user
  - Examples: searches, input forms → think of online banking
- Examples of server-side technology/languages:
  - PHP, Python, Perl, Ruby, …
  - Java (several technologies), ASP.NET
  - Possible, but rare: C++ based programs

HTTP

- HTTP is the carrier protocol for HTML
  - Conceived to be state-less: server does not keep state information about connection to client
  - Mostly simple `GET`/`POST` semantics (`PUT` is possible)
  - HTML-specific encoding options
- OK for the beginnings – but the Web became the most important medium for all kinds of purposes (e. g. e-commerce, forums, etc.)
  → today: real work flows implemented with HTTP/HTML
  → need to keep state between different pages
  → **sessions**

Sessions Over HTTP

- Sessions: many work-arounds around the state-less property
  - Cookies (later)
  - Session-IDs (passed in HTTP header)
  - Parameters in URL
  - Hidden variables in input forms (HTML-only solution)
- Session information is a valuable target
  - E. g., online banking: credit card or account information
- Session IDs in the URL can also be a weakness
  - Can be guessed or involuntarily compromised (e. g. sending a link) → “session hijacking”
- **`GET`** command may encode parameters in the URL
  - Can be a weakness
  - Some URLs are used to trigger an action, e.g. `http://www.example.org/update.php?insert=user`
  - Attacker can craft certain URLs (→ Cross-Site Request Forgery)

HTTP Authentication

- HTTP Authentication
  - Basic Authentication: not intended for security
    - Server requests username + password
    - Browser answers in plain text → relies on underlying SSL for security
    - No logout! Browser keeps username and password in cache
  - Digest Authentication: protects username + password
    - Server also sends a nonce
    - Browser reply is MD5 hash: md5(username,password,nonce)
    - No mutual authentication – only client authentication
    - More secure and avoids replay attacks, but MD5 is known to have weaknesses
    - SIP uses a similar method
- HTTP authentication often replaced with other methods
  - Requires session management
  - Complex task

Cookies

- Small text files that the server asks the browser store
  - Client authenticates to server, receives cookie with a secret value
  - Uses this value to keep the session alive when transmitting HTTP(s)
- Problematic: which cookies is a site allowed to access?
  - `abc.com` must not access cookies for `xyz.com`
- Cookies come with a security policy implemented in the browser
- Problematic:
  - Cookie scope can be set via `domain` parameter, but need for care
  - Some browsers allow to restrict scope to a host name; others only to a domain
- Example: cookie set at foo.example.com

value of `domain`	Non-IE	Internet Explorer
(omitted)	`foo.example.com`	`*.foo.example.com`
`bar.example.com`	`not set, domain mismatch`	`not set, domain mismatch`
`example.com`	`*.example.com`	`*.example.com`

Cookies: a few more aspects

- Cookies can be exploited to work against privacy
  - User tracking: identify user and store information about browsing habits
  - 3rd party cookies: cookies that are not downloaded from the site you are visiting, but from another one
    - Can be used to track users across sites
  - Cookies can be set without the user knowing (there are reasonably safe standard settings)
  - Security trade-off: many Web pages require cookies to work, disabling them completely may not be an option
- Cookies may also contain confidential session information
  - Attacker may try to get at such information (→ Cross-Site Scripting)

JavaScript

- Script language that is executed on client-side (not only in browsers!)
  - Originally developed by Netscape; today more or less a standard
  - Object-oriented with C-like syntax, but multi-paradigm
  - Allows dynamic content for the WWW → AJAX etc.
  - Allows a Web site to execute programs in the browser
- The Web is less attractive without JavaScript – but anything that is downloaded and executed by a client may be a security risk

JavaScript

- Security Issues:
  - Allows authors to write malicious code
  - Allows cross-site attacks (we look at these a bit later in this lecture)
- Defenses:
  - Sandboxing of JavaScript execution
    - Difficult to implement
  - Same-origin policy (SOP)

Same-Origin Policy (SOP)

- One of the stronger defences for JavaScript
  - One JavaScript context should not be able to modify the context of another
  - Such access is otherwise possible with the Document Object Model API
- All browsers have a SOP – with OK consistency (IE is a bit different)
- Original idea (Netscape, 1995!):
  - Two JavaScript contexts are allowed access to each other if and only if protocols, host names and ports associated with the documents in question match **exactly**

Originating doc	Accessed doc	Non-IE	Internet Explorer
`http://abc.com/a/`	`http://abc.com/b/`	`Access OK`	`Access OK`
`http://ab.com/`	`http://www.abc.com`	`Host mismatch`	`Host mismatch`
`http://abc.com/`	`https://abc.com/`	`Protocol mismatch`	`Protocol mismatch`
`http://abc.com:81/`	`http://abc.com/`	`Port mismatch`	`Access OK (!)`

Same-Origin Policy (SOP)

- Critique of SOP:
  - Sometimes too restrictive: two co-operating Web sites `abc.com` and `xyz.com` cannot exchange information
  - Sometimes too broad: SOP can be violated
- Trying to make the SOP less restrictive is dangerous:
  - Common way: use JS property `document.domain`
  - Two sites sharing the same top-level-domain can agree to share context
  - Symmetric: both sites must opt-in and define the property
  - Critique: too broad
    - Assume `login.abc.com` wants to share with `payments.abc.com` and set `document.domain` to `abc.com` – suddenly all sub-domains are included, even `mallory.abc.com`
- Better method: use `postMessage()` as defined for HTML 5
  - Based on notion of JavaScript handle – allows to send to another window for which senders holds a handle

Same-Origin Policy

- The SOP only refers to JavaScript interactions
- It does not cover any other interactions and credentials, like:
  - State of SSL connection – good authentication or not
  - IP connectivity – SOP matches via host names
  - Information in cookies (they have their own kind of SOP)
- Example:
  - Assume two windows A and B in a browser, co-operating within SOP
  - A is a site with login, and user is logged in as „Alice“
  - A and B will now remain same-origin even if the user logs out as Alice and logs in again as Bob
  - Here, SOP provides no notion at all of „identity in a session“
- Interesting fact:
  - The XMLHttpRequest mechanism used in AJAX (Web 2.0) has a tweaked SOP
  - `document.domain` does not work
  - And IE supports ports, too

Most important Web technologies

Name	Used for	Comment
HTML	Document structure	Often abused for representation; theoretically XML/SGML-based; requires diligent parsing
CSS	Document rendering	Some parts in the standard can be exploited
HTTP	Carrier protocol	Several versions; stateless
Cookies	Session state keeping	Need to prevent cross-domain interactions
URL/URI	Document location	Inconsistent interpretation of RFCs; requires diligent parsing
JavaScript	Client-side computation and interaction	Requires safe execution environment
Flash	Client-side code execution	Requires safe execution environment
…	…	… there‘s much more …

Part II: Internet Crime

- Part I: Introduction to the WWW and Security Aspects
- Part II: Internet Crime
- Part III: Vulnerabilities and Attacks

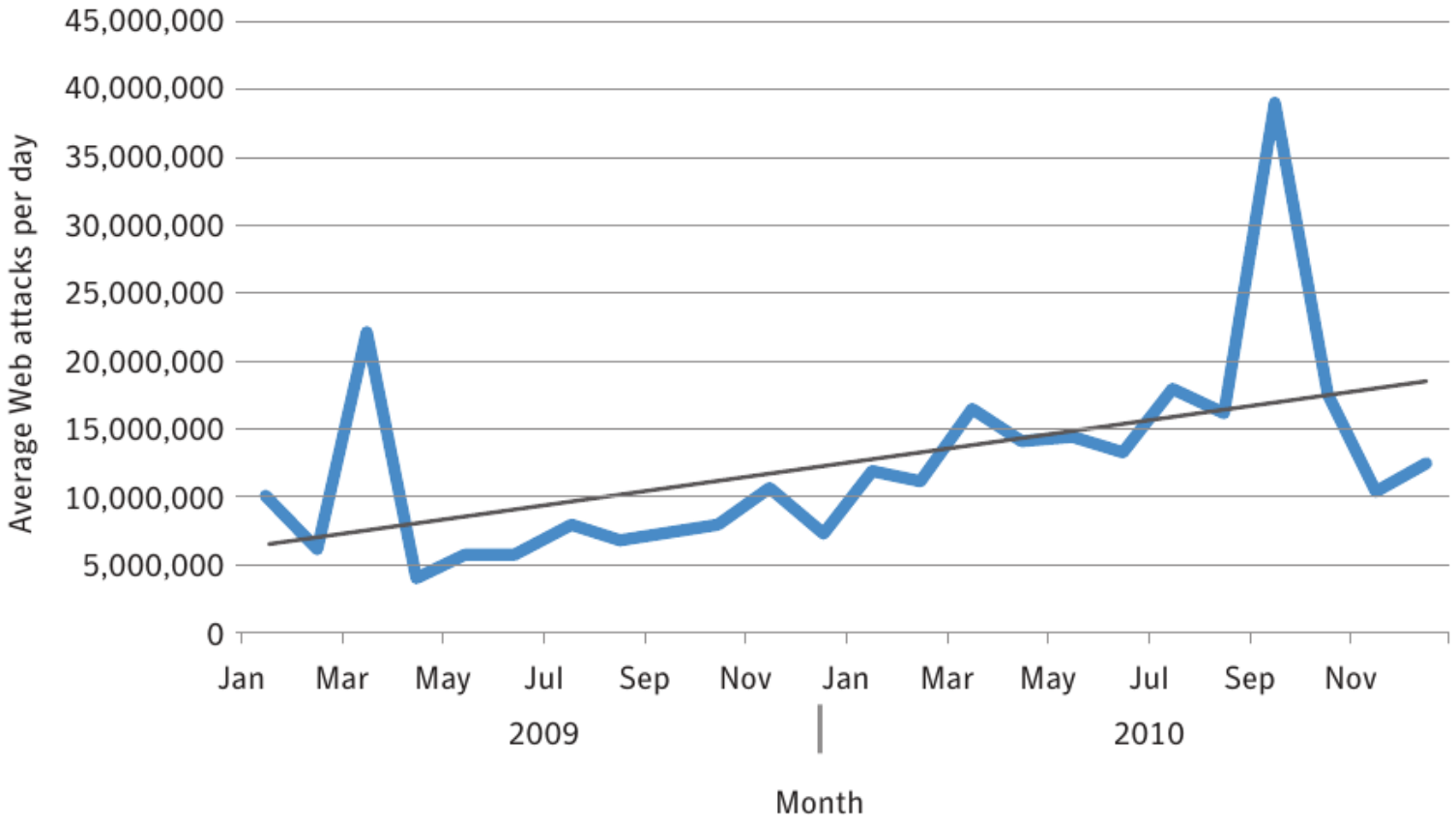
Vulnerabilities: some numbers

- 3,462 vs 2,029 web/non-web application vulnerabilities were discovered by Symantec in 2008
- Average exposure time: 60 days
- 12,885 site-specific XSS vulnerabilities submitted to XSSed in 2008 alone
- Only 3% of site-specific vulnerabilities were fixed by the end of 2008

- The bad guys are not some hackers who “want to know how it works”
- These days, it’s a business!
- “Symantec Underground Economy Report 2008”:

“Moreover, considerable evidence exists that organized crime is involved in many cases …“
[ed.: referring to cooperation between groups]

From the Symantec Report 2011



Average Web-based attacks per day, by month, 2009–2010

Source: Symantec Corporation

From the Symantec Report 2011

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	$0.07–$100
2	2	Bank account credentials	16%	19%	$10–$900
3	3	Email accounts	10%	7%	$1–$18
4	13	Attack tools	7%	2%	$5–$650
5	4	Email addresses	5%	7%	$1/MB–$20/MB
6	7	Credit card dumps	5%	5%	$0.50–$120
7	6	Full identities	5%	5%	$0.50–$20
8	14	Scam hosting	4%	2%	$10–$150
9	5	Shell scripts	4%	6%	$2–$7
10	9	Cash-out services	3%	4%	$200–$500 or 50%–70% of total value

From the Symantec Report 2011

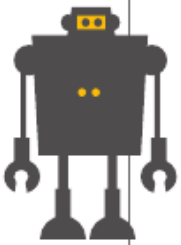
Item	Bulk Prices Observed	Unit Price
Credit card information	10 credit cards for $17	$1.70
	100 credit cards for $100	$1.00
	1000 credit cards for $300	$0.30
	750 credit cards for $50	$0.07
Credit card dumps	101 dumps for $50	$0.50
Full identities	30 full identities for $20	$0.67
	100 full identities for $50	$0.50

From the Symantec Report 2011

1M+

Bots

Rustock, the largest botnet observed in 2010, had well over 1 million bots under its control. Grum and Cutwail followed, each with many hundreds of thousands of bots.



$15

per 10,000 Bots

Symantec observed an underground economy advertisement in 2010 promoting 10,000 bots for $15. Bots are typically used for spam or rogueware campaigns, but are increasingly also used for Distributed Denial of Service attacks.

$0.07 to $100

per Credit Card

This was the range of prices seen advertised in the underground economy for each “stolen” credit card number, and, as in the real economy, bulk buying usually gets the buyer a significant discount.

Just FYI: from the Symantec Report 2008

Rank for Sale	Rank Requested	Category	Percentage for Sale	Percentage Requested
1	1	Credit card information	31%	24%
2	3	Financial accounts	20%	18%
3	2	Spam and phishing information	19%	21%
4	4	Withdrawal service	7%	13%
5	5	Identity theft information	7%	10%
6	7	Server accounts	5%	4%
7	6	Compromised computers	4%	4%
8	9	Website accounts	3%	2%
9	8	Malicious applications	2%	2%
10	10	Retail accounts	1%	1%

Table 1. Goods and services available for sale, by category[56]

Source: Symantec Corporation

Just FYI: from the Symantec Report 2008

Rank for Sale	Rank Requested	Goods and Services	Percentage for Sale	Percentage Requested	Range of Prices
1	1	Bank account credentials	18%	14%	$10–$1,000
2	2	Credit cards with CVV2 numbers	16%	13%	$0.50–$12
3	5	Credit cards	13%	8%	$0.10–$25
4	6	Email addresses	6%	7%	$0.30/MB–$40/MB
5	14	Email passwords	6%	2%	$4–$30
6	3	Full identities	5%	9%	$0.90–$25
7	4	Cash-out services	5%	8%	8%–50% of total value
8	12	Proxies	4%	3%	$0.30–$20
9	8	Scams	3%	6%	$2.50–$100/week for hosting; $5–$20 for design
10	7	Mailers	3%	6%	$1–$25

Table 2. Breakdown of goods and services available for sale and requested[64]

Just FYI: from the Symantec Report 2008

Exploit Type	Average Price	Price Range
Site-specific vulnerability (financial site)	$740	$100–$2,999
Remote file include exploit (500 links)	$200	$150–$250
Shopadmin (50 exploitable shops)	$150	$100–$200
Browser exploit	$37	$5–$60
Remote file include exploit (100 links)	$34	$20–$50
Remote file include exploit (200 links)	$70	$50–$80
Remote operating system exploit	$9	$8–$10

Table 8. Exploit prices

Source: Symantec Corporation

Just FYI: from the Symantec Report 2008

Attack Kit Type	Average Price	Price Range
Botnet	$225	$150–$300
Autorooter	$70	$40–$100
SQL injection tools	$63	$15–$150
Shopadmin exploiter	$33	$20–$45
RFI scanner	$26	$5–$100
LFI scanner	$23	$15–$30
XSS scanner	$20	$10–$30

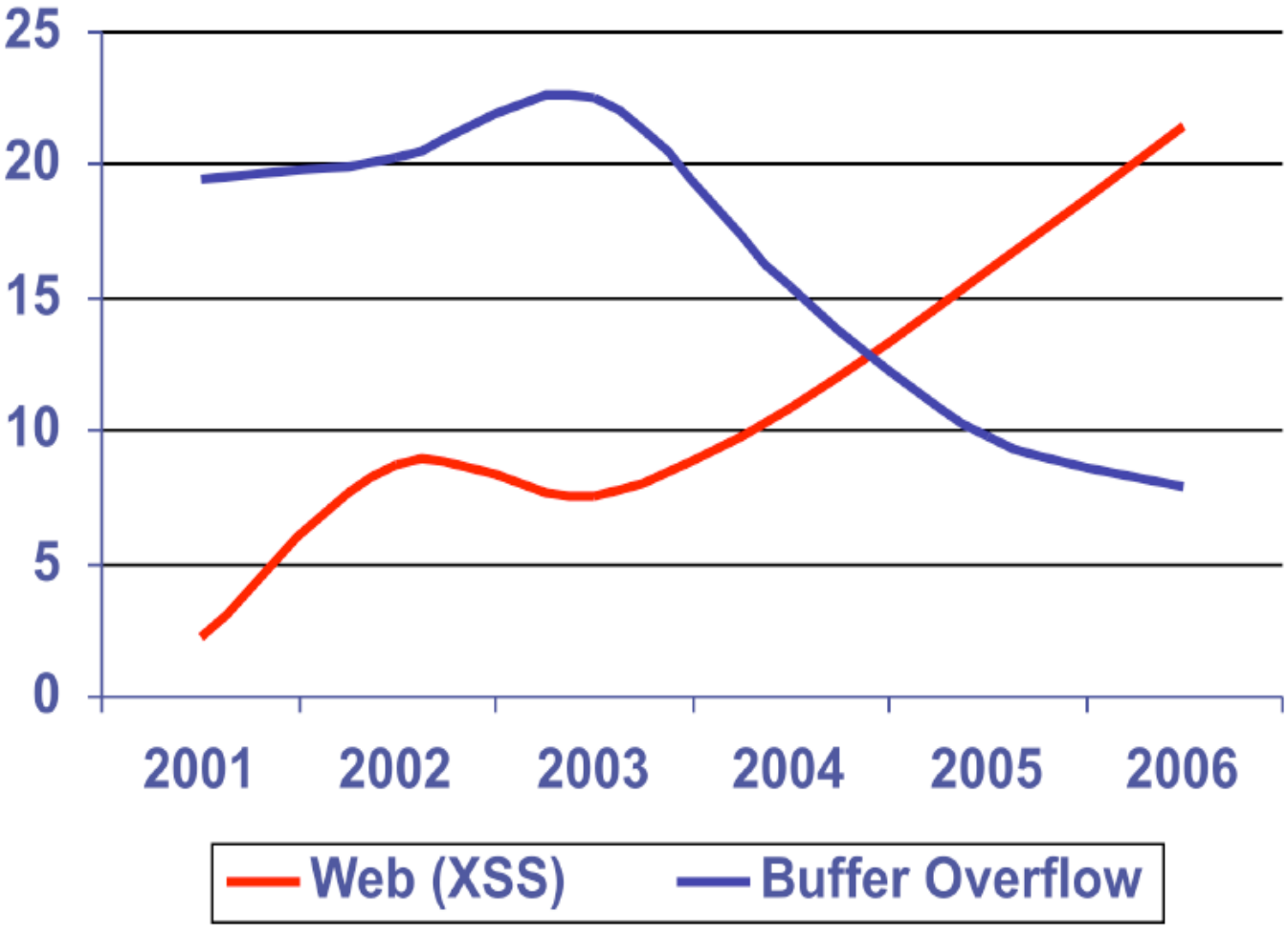
Table 5. Attack kit prices

Source: Symantec Corporation

Part III: Vulnerabilities and Attacks

- Part I: Introduction to the WWW and Security Aspects
- Part II: Internet Crime
- Part III: Vulnerabilities and Attacks

Comparison: two classic vulnerabilities



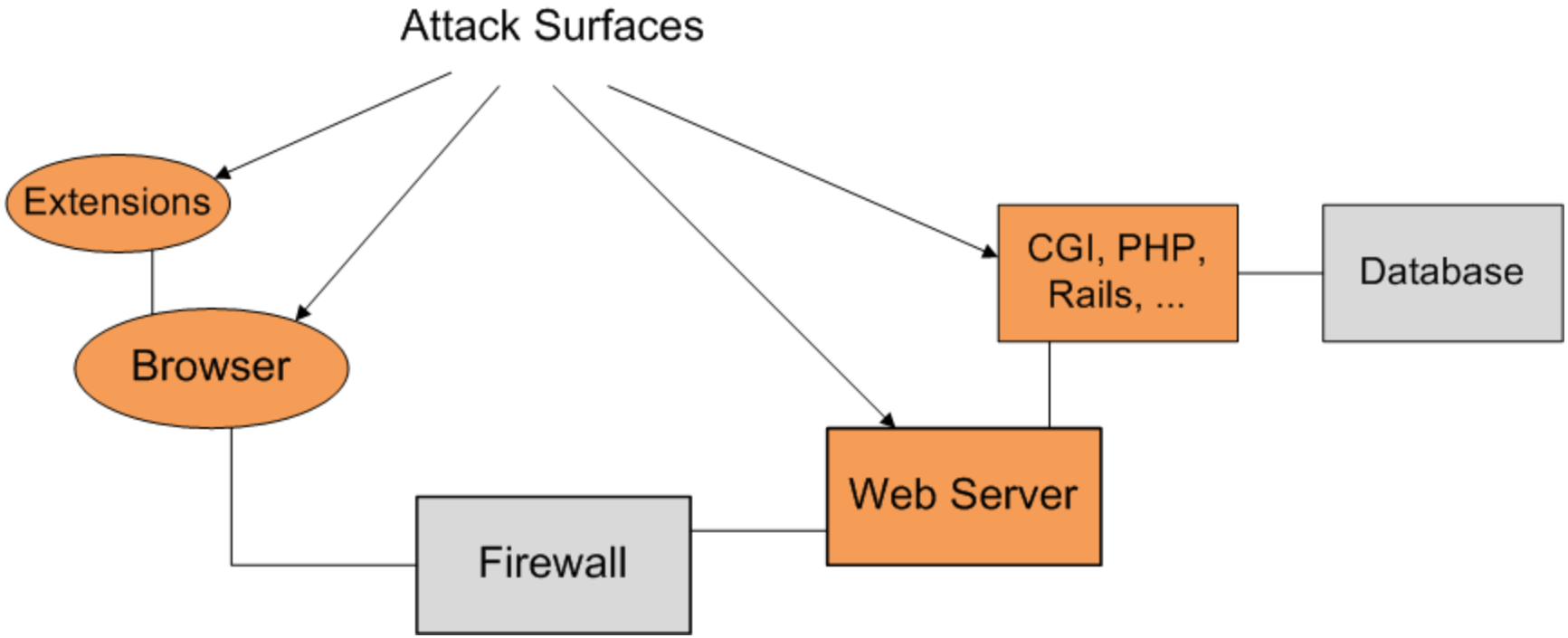
Source: MITRE CVE trends

Classification of Attacks (incomplete)

	Client-side	Server-side
Common implementation languages	❑ C++ (e. g. Firefox) ❑ XULRunner ❑ Java	❑ Web Server: C++, Java ❑ Script languages
Common attack types	❑ Drive-by downloads ❑ Buffer overflows	❑ Cross-Site scripting ❑ Code Injection ❑ SQL Injection ❑ (DoS and the like)
Result of attack	❑ Malware installation ❑ Computer manipulation ❑ Loss of private data	❑ Defacement ❑ Loss of private data ❑ Loss of corporate secrets

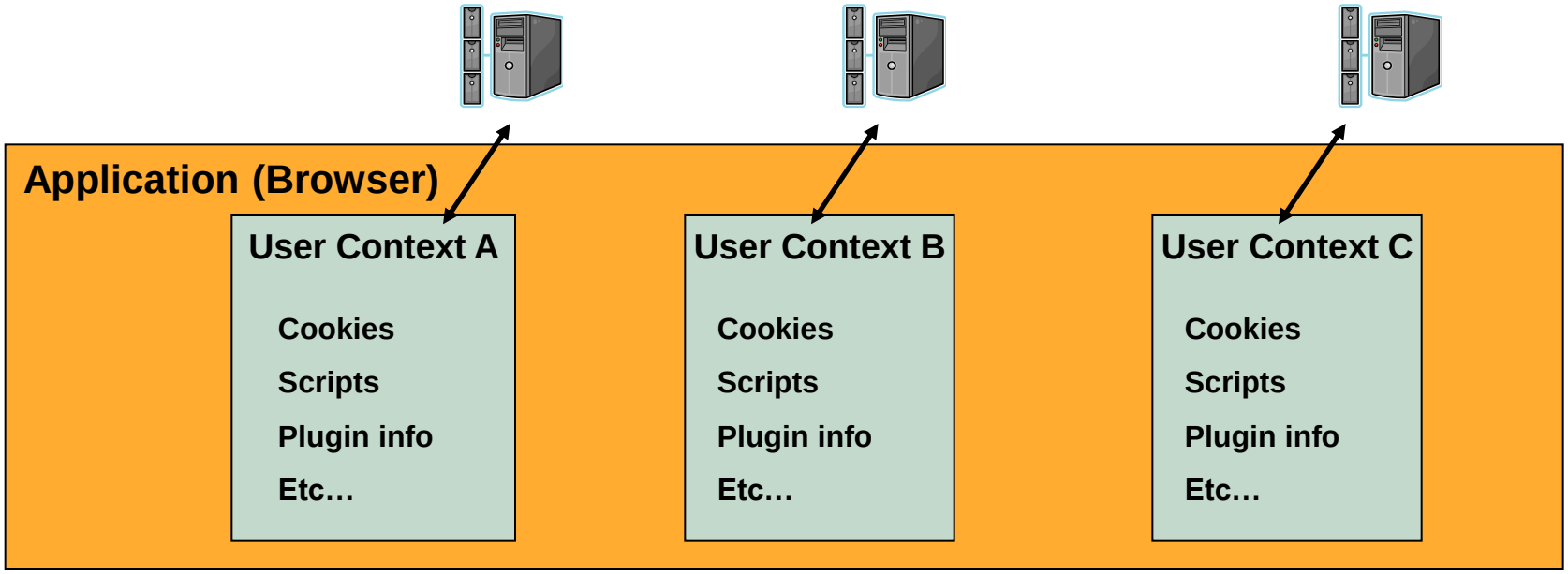
One Step Back: why is the WWW so vulnerable?

- Many important business transactions take place
- Much functionality, much complexity in software
  → many attack vectors, huge attack surface
- Even though we may implement protocols like TCP/IP really well, any (Web) application that interacts with the outside world must be open by definition and reachable even across a firewall



Informal Definition: Contexts

- Context (in general): collection of information that belongs to a particular session or process
  - Useful abstraction that helps us to classify the target of an attack
  - Here: not a formal definition, nor a model of actual implementation
- User Context (in a browser):
  - Collection of all information that “belongs” to a given session
  - Cookies, session state variables, plugin-specific information…
  - JavaScripts: downloaded and executed → obey same-origin policy!
  - Information from session A should not be accessible from Session B
  - Client and server must remain synchronized w.r.t. state information



Attack 1: Session Variables

- **Target of attack:**
  Synchronization of state information between client and server
  (in other words: the session management is attacked)
- **Typical scenario:**
  Exchange between client and server that takes
  several steps to complete
- **Typical approach of attack:**
  Swap state information during one step
- **Cause of vulnerability:**
  Server (or client) relies on information sent by the other party
  instead of storing it itself

- Best explained by example. Here:
  Server: a CA that can issue X.509 certificates
  Client: a Web browser that wants to acquire such a certificate

Attack 1: How the Work-Flow Should Be

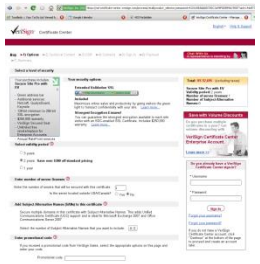
Browser = client

CA = server

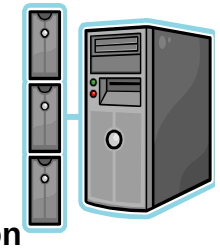
State:

A→CA

xyz.de



A: Request cert for domain `xyz.de`



State:

A→CA

xyz.de

2) Background:
Ownership verification

A owns xyz.de

Offer for xyz.de by CA

CA: Offer cert for domain `xyz.de`

A: Acknowledge request: cert for domain `xyz.de`

(A pays for xyz.de)

CA: Issue cert for domain `xyz.de`

Has cert

Question: where do you keep the session information?

If your answer is "in the cookie": serious mistake.

In fact, the CA must NOT trust information by the browser. We show you why now.

Attack 1:
How to Attack the Synchronization of State Information

In this example, all state information is stored on client-side and retransmitted in each step (e. g. by reading from a cookie). The server does not store state.

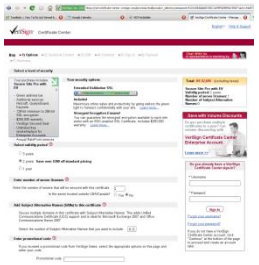
Browser = client

CA = server

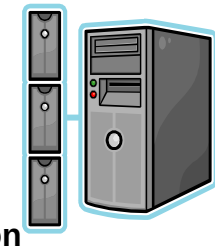
State:

A→CA

xyz.de



A: Request cert for domain `xyz.de`



State:

A→CA

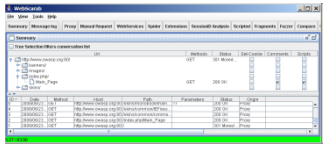
xyz.de

2) Background: Ownership verification

A owns xyz.de

Offer for xyz.de by CA

CA: Offer cert for domain `xyz.de`



Swap variables on the fly

A: Acknowledge request: cert for domain `mozilla.com`

(A pays for xyz.de)

CA: Issue cert for domain `mozilla.com`

Has cert!!!

Why Was the Attack Possible?

- In our example, all state information was kept on client-side in a cookie
- All the attacker did was to swap `mozilla.com` for `xyz.de` in the second HTTP request
- The server issued a cert for the wrong domain because it failed to notice that the *domain name in the first request was not the same as the name in the second request*.
- That was possible because the relevant information was not stored on server-side
- Do you think this is too easy and will not happen “in the real world”?
  - In fact, something like this ***may*** have happened in the beginning of 2009 to a CA that is included in Firefox’s root store.
  - Background info:
    - The attack did not succeed – because there was a second line of defense: all “high-value” domain names are double-checked by *human personnel*.
  - The CA publicly acknowledged there was an intrusion.
    - The CA described an attack pattern that hinted at what we have just seen.
    - The CA contacted the attacker – it was a White Hat

Defense / Mitigation

- Guideline 1: For each entity in the protocol:
  - Everything that is relevant for the correct outcome must be stored *locally*
  - It can be difficult to identify this information if you have complex work-flows…
- Guideline 2: All Input Is Evil
  - Always treat all input as untrusted
  - Never use it without verification

- Nota bene: what if the server uses Javascript/Java to “force” browser to behave correctly? → just use a HTTP proxy → NOT a defense!

- This was just a simple attack because an entity failed to obey these rules.
- In particular, Guideline 1 was violated.
- However, in the following, we show you that attacks are possible even if state is stored correctly and only Guideline 2 is violated.

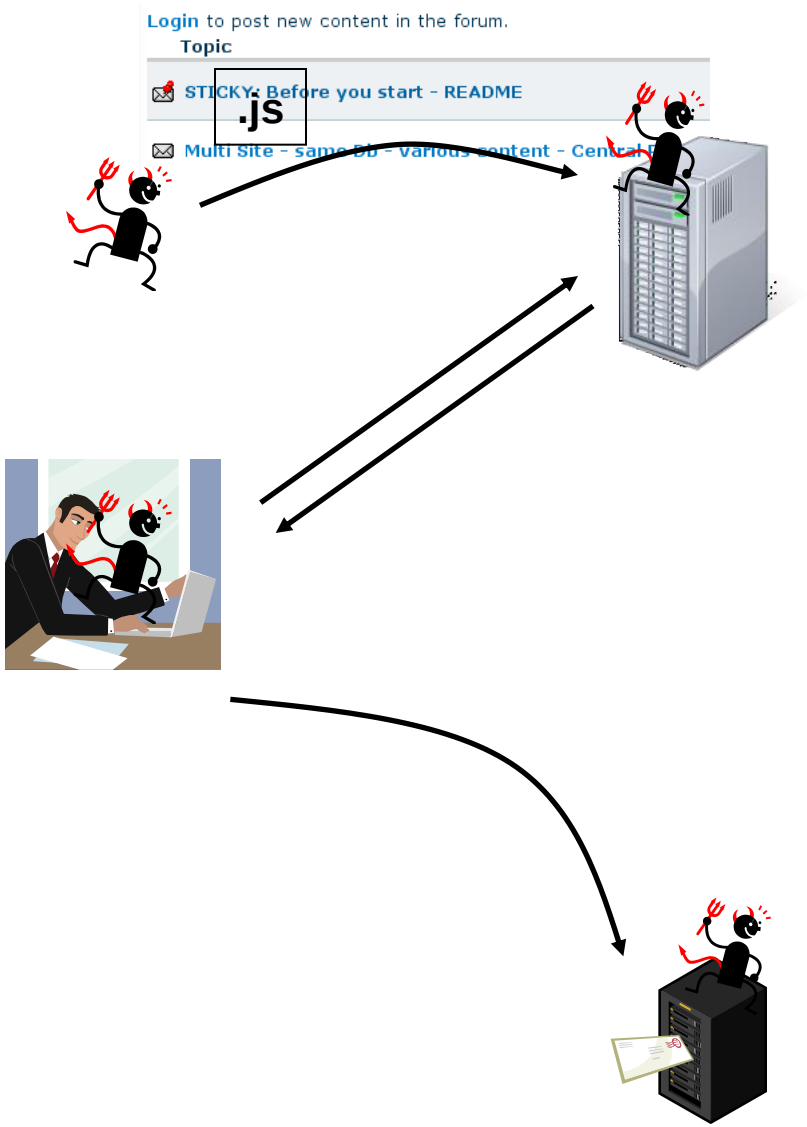
Cross-Site Scripting (XSS)

- **Target of attack:**
  Attempt to access user context from outside the session
  Goal is to obtain confidential information from the user context
- **Typical scenario:**
  User surfing the Web and accessing a Web site
  while having (Java)script enabled
- **Typical approach to attack:**
  Attacker plants a malicious script on a Web page;
  the script is then executed by the user's browser
- **Cause of vulnerability:** two-fold
  1) Attacker is able to plant malicious script on a Web page
  → flaw in Web software needed
  2) User browser executes script from a Web page
  → user's "trust" in Web site is exploited

- XSS is one of the most common attacks today

Cross-Site Scripting: Typical Attack

- Stage 1: Attacker injects malicious script
  - Here: in a Web forum where you can post messages
  - In addition to normal text, the attacker writes: `<script>[malicious function]</script>`
  - The server accepts and stores this input
- Stage 2: Unaware user accesses Web forum
  - Here: reads poisoned message from attacker
  - User receives:
    `<p>Hello, this is a harmless message`
    `<script>[malicious function]</script>`
    `</p>`
  - Everything within `<script>` is executed by browser *in the user's context*
- Possible Consequences:
  - Script reads information from cookies etc. and sends it to attacker's server
  - Script redirects to other site
    → download trojan etc.



Cross-Site Scripting: Why Does it Work?

- Why was the attack possible?
- Reason 1: The Web application did not **sanitize** input it received
  - Remember: all input is evil; and the attacker can *choose* his input
  - If the Web app had just dropped all HTML input, there would be no script uploaded
    → and none executed in the browser
  - Unfortunately, many Web sites allow users to post at least some HTML
    → a nice feature, but dangerous
- Reason 2:
  The user had trusted the Web site and did not assume
  malicious content could be downloaded and executed
  → **abuse of trust**

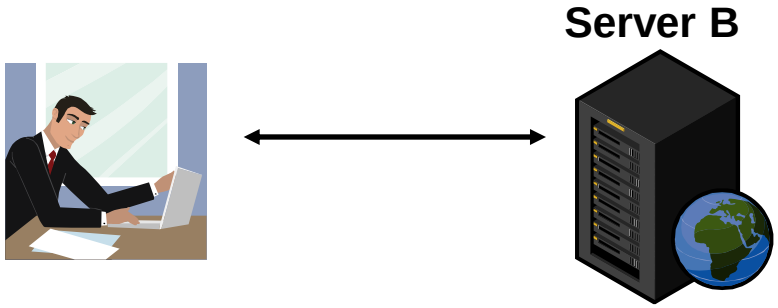
- Nota bene: none of the mechanisms you know so far is a defense!
  - Crypto protocols: encrypting/signing does not help here
  - Firewalls: work on TCP/IP level
  - XSS is a particularly useful example to show why there is a need
    for ***application layer security***

Cross-Site Request Forgery (XSRF)

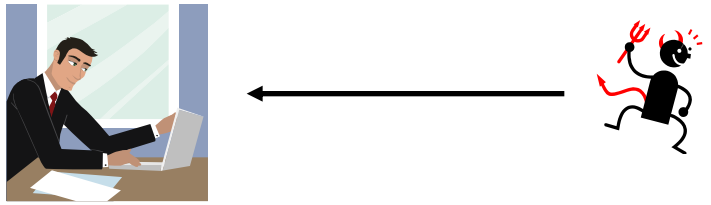
- **Target of attack:**
  User-Server context: session of client A with a server B
- **Typical scenario:**
  Authenticated user on a Web page on B which is OK and trusted; then the user surfs to server M which is malicious
- **Typical approach to attack:**
  - Attacker knows that user is logged in
    → crafts a URL to server B that executes an action
  - Attacker causes victim to call that URL
- **Cause of vulnerability:**
  - Attacker URL is called by user; within his user context
    → **abuse of server's trust** into requests from client
  - Browser **cannot recognise that request to the URL is malicious**
    → it seems to be in the correct context
    → instance of **"Confused Deputy"** problem (browser is deputy): authority of deputy (login to B) is abused

Cross-Site Request Forgery (XSRF)

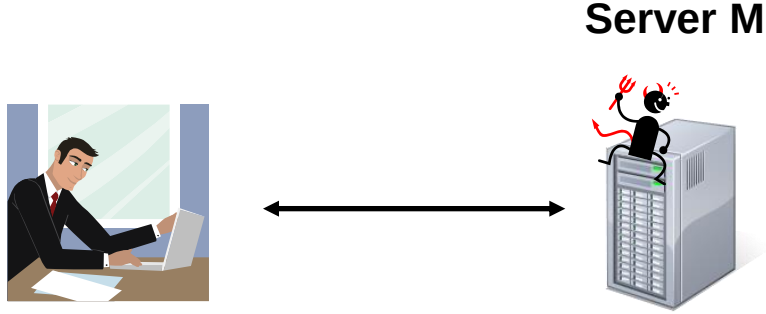
- Stage 1: user logs into Web site
  - Authenticated user
  - Session with server B
  - User keeps this session open



- Stage 2: attacker tricks user to surf to his own site, server M. Methods:
  - Phishing
  - XSS



- Stage 3: user surfs to malicious server M
  - In the HTML he receives, a malicious link is embedded
    harmless text
    ****
    more harmless text



→ undesired action executed

Defence against XSRF

- Particularly good defence against XSRF: Secret Tokens
- I.e. a Web site requires that the client (browser) proves knowledge of a secret value before acting on a URL
- Requires: server needs to transmit this value first, can be done via hidden field in input form etc.

- Advantage:
  - Reliable if secret values cannot be guessed
- Disadvantage:
  - State-keeping on server-side necessary

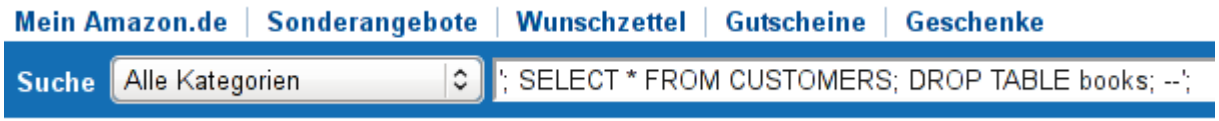
SQL Injection

- **Target of attack:**
  Server context
- **Typical scenario:**
  Web server runs with an SQL database in the background; attacker wants to extract or inject information to/from the database
- **Typical approach to attack:**
  Attacker writes SQL code into an input form, which is then passed to the SQL database; evaluated and output returned
- **Cause of vulnerability:**
  Web server does not sanitize the input and accepts SQL code

- SQL Injection is a real classic attack

SQL Injection

- Attacker injects SQL into search form:



- The author of the Web page may have intended to execute:

```
SELECT author,book FROM books WHERE book = '$title';
```

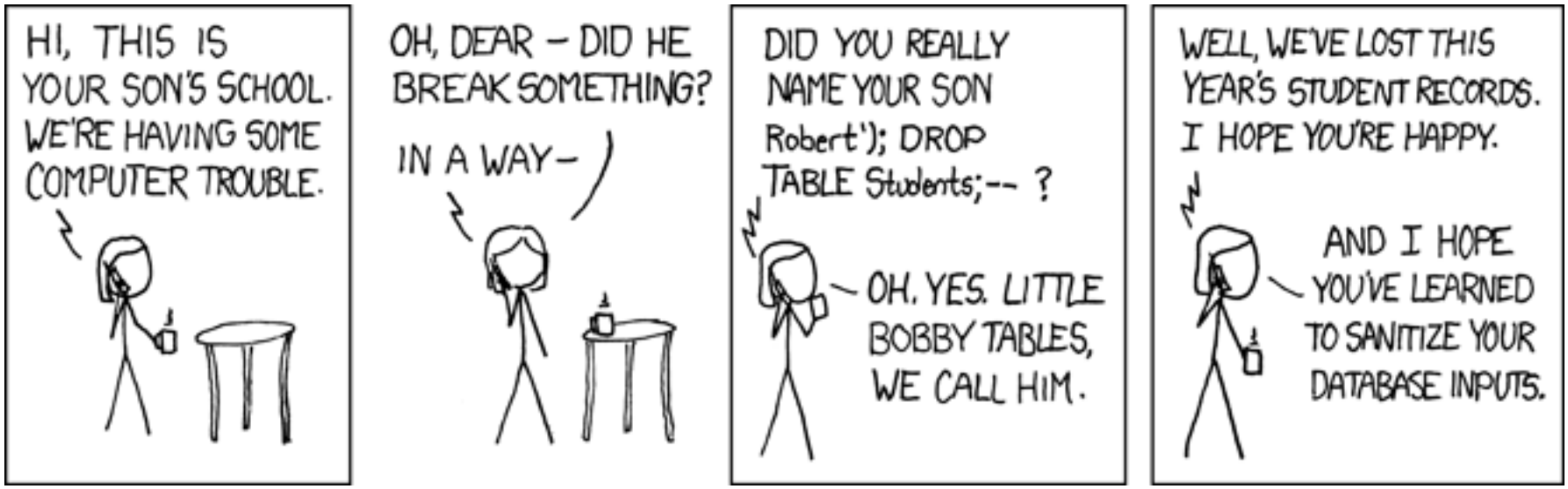
- Through the SQL injection, this has become something like:

```
SELECT author,book FROM books
WHERE book = ''; SELECT * FROM CUSTOMERS; DROP TABLE
books;
```

- You just lost your catalogue and compromised your customers data
- Amazon, of course, is too clever not too sanitize their input – but it is amazing how many other Web sites fail to do so!

- Fortunately, this exact example won't work anymore

Sanitize or Be Sorry



General defences for XSS, XSRF, SQL Injection

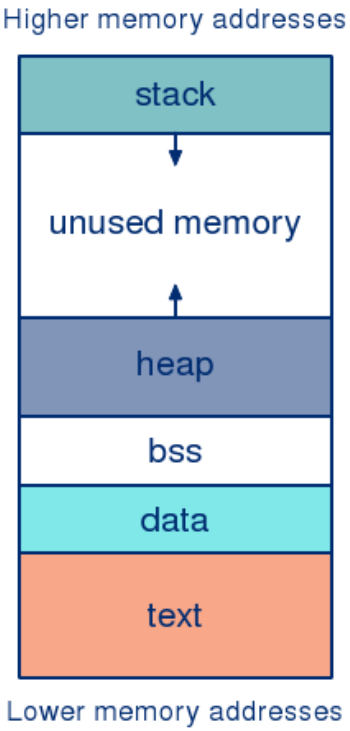
- Some options on **client-side** against XSS/XSRF:
  - JavaScript is often a must for many “good” Web pages
    → turning it off is not an option
    → better sandboxing? → very complex
  - Turning on some security settings can provide some security
    → unfortunately, these are often not activated by default
- Better protection can be achieved on **server-side**:
  - Treat all input as **untrusted**
  - **Sanitize** your input and output: proper **escaping**
    - Escape (certain) HTML tags and JavaScript
    - Exceedingly difficult and complex task!
    - Whitelisting is better than blacklisting – the black list may grow
- Do not write your own escaping routines
  - Modern script languages offer this functionality

Buffer Overflows

- **Target of attack:**
  Running process on a server (process has a context!)
- **Typical scenario:**
  An application that is accessible on the Internet and has a certain built-in flaw
  Vulnerable C(++)-based application on the Internet
- **Typical approach to attack:**
  - Attacker sends byte stream to vulnerable application; either causing it to crash or to execute attacker code in the process context of the application
- **Cause of vulnerability:** two-fold
  - Buffer overflow in application → serious programming mistake (root cause: von Neumann machine)
  - Application does not check its input

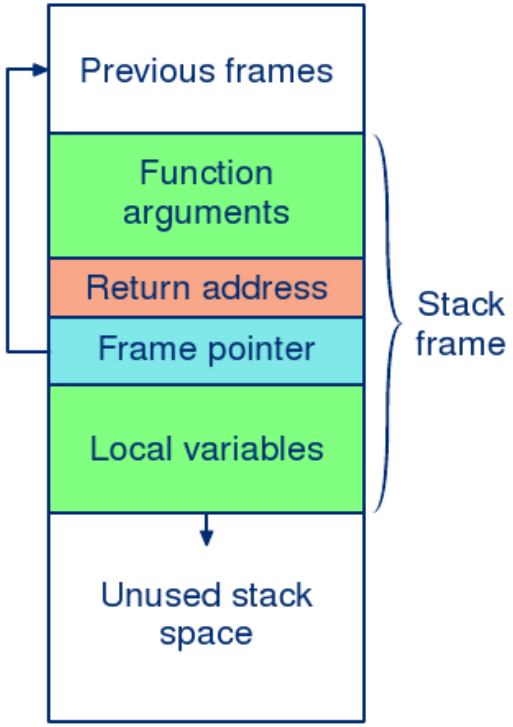
Buffer Overflows

- von Neumann machine:
  program and data share memory
- Applies to all kinds of software
- Memory segments:
  - text – program code
  - data – initialized static data
  - bss – unitialized static data
  - heap – dynamically allocated memory
  - stack – program call stack
- The vulnerability is in the code:
  - Programmer creates buffer on the stack and does not check its size when writing to it
    `char* buffer; readFromInput(buffer);`
- Exploit:
  - Because of the way the stack is handled, you can overwrite the return address



Buffer Overflows

- Stack is composed of frames
  - Pushed on the stack during function invocation, and popped back after returning
- Each frame comprises
  - functions arguments
  - return address
  - frame pointer to start address of previous frame
  - local variables
- Stack grows to bottom; local variables are written towards top
- Without proper boundary checking, a buffer content can overspill into adjacent area
- Attacker:
  - Find out the offset to the return address
  - Write data to the buffer: overwrite return address, add your own code
  - Application continues to run from the new address, executing the new code



Simple Code Example

```
#include <stdio.h>
#include <string.h>
int vulnerable(char* param)
{
   char buffer[100];
   strcpy(buffer, param);
}

int main(int argc, char* argv[] )
{
   vulnerable(argv[1]);
   printf("Everything's fine\n");
}
```

(from [ISec2010])

Buffer Overflows

- Buffer overflows are mostly a problem for applications written in languages with direct control over memory (like C/C++)
- These are becoming less frequent on Web servers, and checks have become better: correspondingly, we observe a switch to other attacks

- Mitigation of this kind of exploit:
  - Data execution protection:
    mark certain areas in memory as non-executable
  - Address space layout randomization: choose stack memory allocation at random (“hardened kernels” do this)
    → Support by operating system helps
  - The latter two are very effective together
  - Canaries: precede the return value with a special value:
    before following the return value, check if is still the same
- Be careful when writing in C/C++, use up-to-date compilers, use the defences the hardware and OS offers

Summary

- **Web applications** have a **natural attack surface**:
  they must accept input from outside
- **Very complex interactions** between protocols, client+server:
  - Difficult to find all weaknesses in advance
  - In part due to the many mechanisms for session management

- **Typical attacks:**
  - Cross-Site Scripting (XSS): violation of user context, abuse of user trust
  - Cross-Site Request Forgery: confused deputy
  - SQL injection
  - Buffer overflows

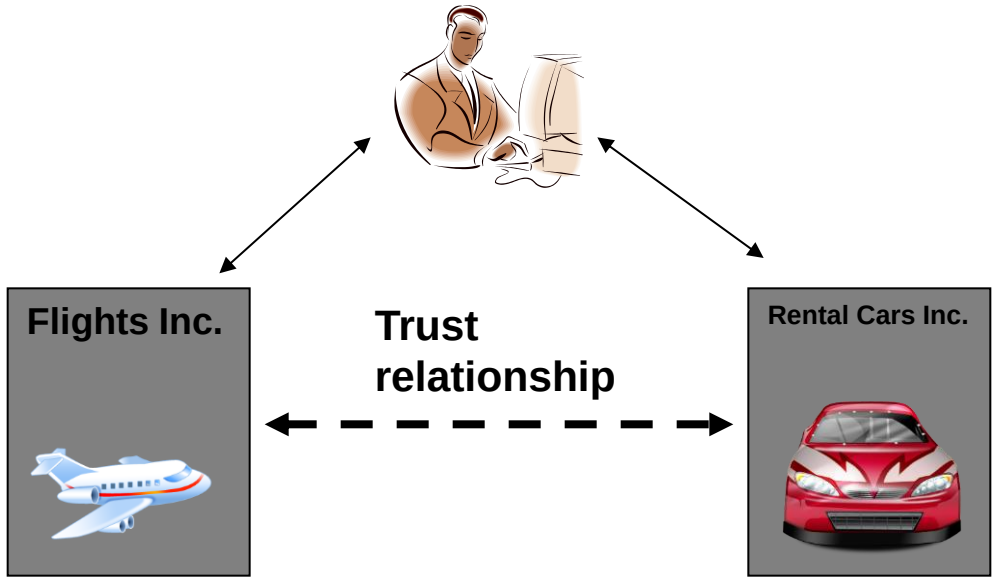
- **Defenses:**
  - Most important defense is to **sanitize** and **validate** input data
  - **All input is evil**
  - Also, be aware of your **{user,server,process} contexts**
  - Conventional defenses like cryptography or firewalls are no protection

Application Layer Security

- 10.1: WWW Security
- 10.2: Identity Federation

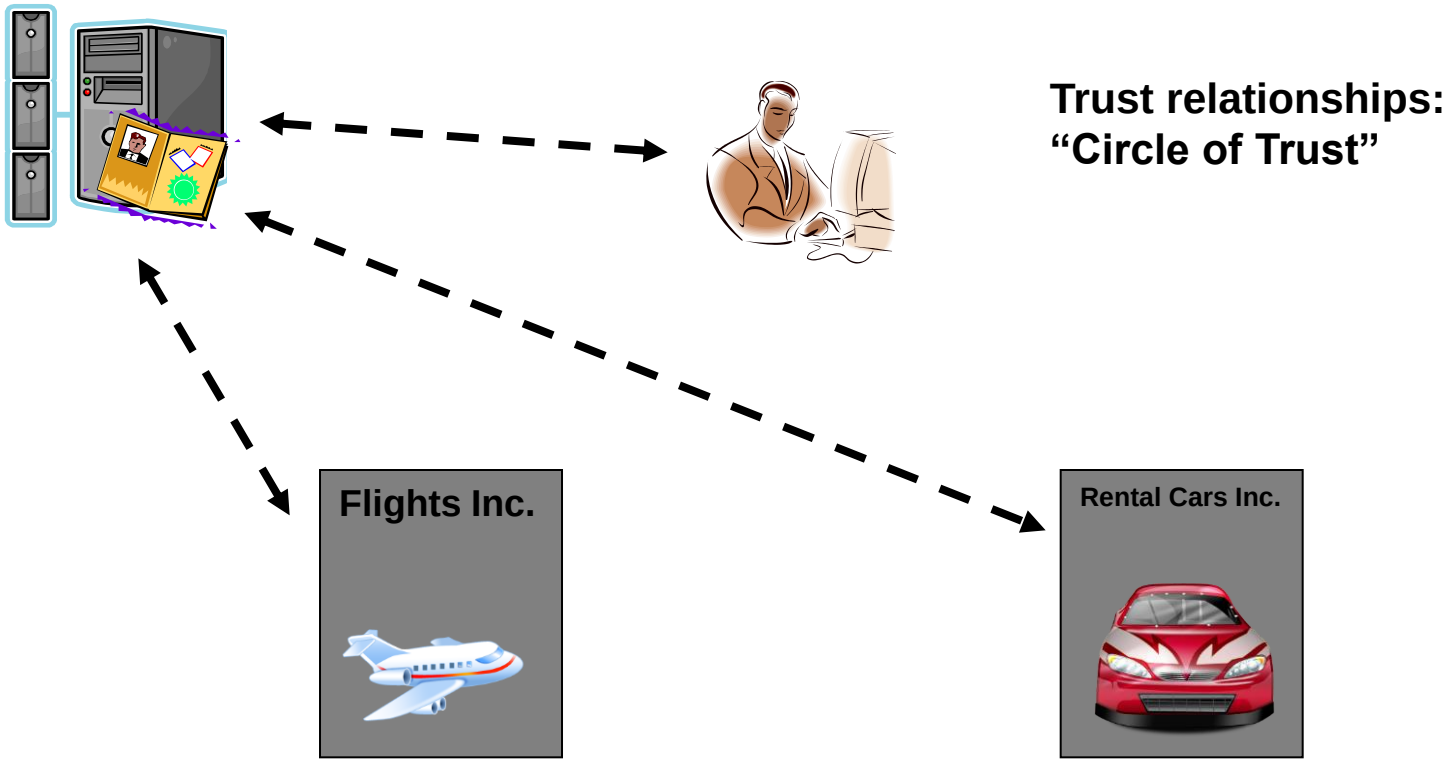
Identity Federation As Shared Authentication

- Entity Bob wishes to do business:
  - Bob wants to reserve a flight from Flights Inc.
  - Bob also wants to rent a car from Rental Cars Inc.
- On booking the flight, Bob consents to federate an identity
  - A pseudonym for use with Rental Cars Inc. is generated
  - Bob is redirected to Rental Cars Inc. with a security token that proves his membership with Flights Inc. (with the pseudonym!)
    Assertion: *"pseudo_bob is a member of domain Flights Inc."*
- Identity Federation: propagation of trust / authentication across organizational boundaries



Identity Provider

- Example may be extended by having a third party acting as the Identity Provider for Bob
- Bob authenticates with credential from Identity Provider



Identity Federation: Concepts

- **Concept is not new: sharing of Identities between organisations**
  - Portability of an identity
  - You know similar concepts, e. g. Kerberos
- **Use-cases**:
  - Allows users (or Web Services) to access services outside their own administrative domain
  - Most common example: Single Sign-On
- **Several standards implement Identity Federation,** also with Web Service technology, esp. SAML:
  - WS Federation (OASIS), part of the Web Services suite
  - ID-FF by Liberty Alliance
  - Shibboleth (Internet2)
  - OpenID: decentralized, more “community-oriented” and simpler standard

Identity Federation: Concepts

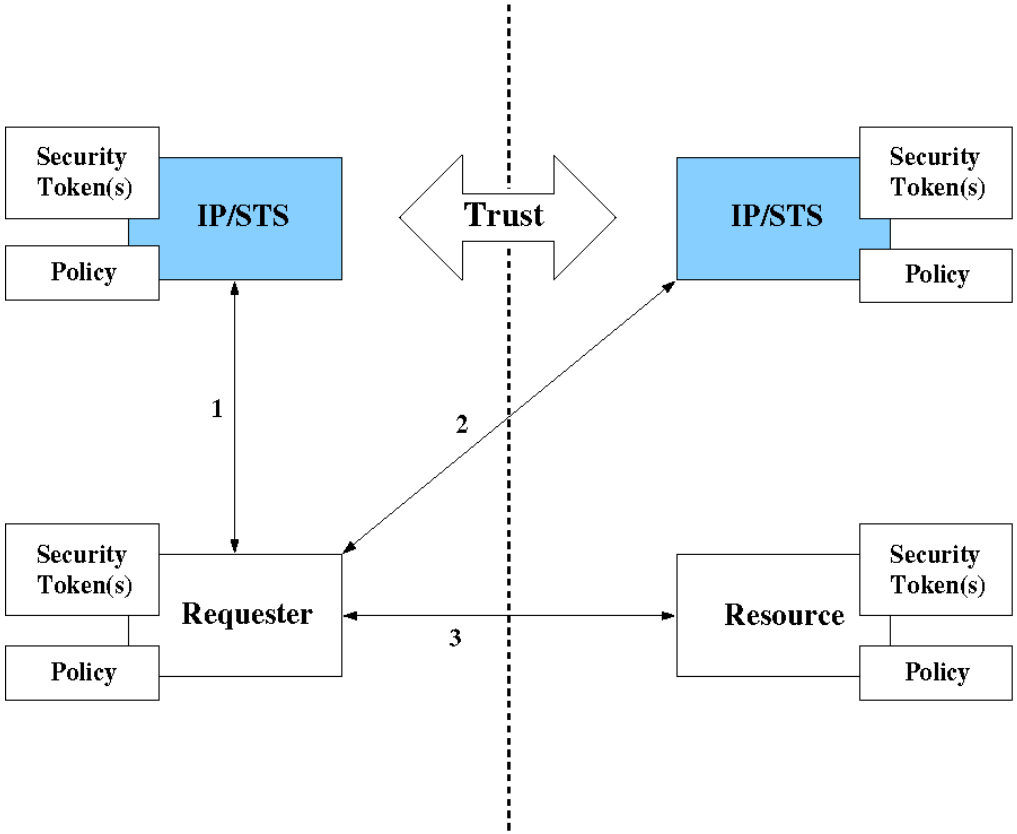
- The **basic schema** is always the same
  - An **entity has an Identity Provider (IdP) vouching for its identity**
  - In order to access a service, the entity **requests a credential from IdP**
    - May be explicitly for the service or generic
  - Entity **presents this credential to the Service Provider**

- Participants in an Identity Federation form a **"Circle of Trust"**
  - Within this circle of trust, an entity may use its federated identity to authenticate, access services etc.
  - Any organisation may act as an Identity Provider (if it is trusted by reyling participants)

- Nota bene: concepts like **Identity Management** that (may) build on Identity Federation **require much more than the pure security concepts** we present here
  - Validity between domains
  - Expiry
  - Secure administration
  - Roles & Access Control
  - Etc.

Identity Federation: Relationships 1

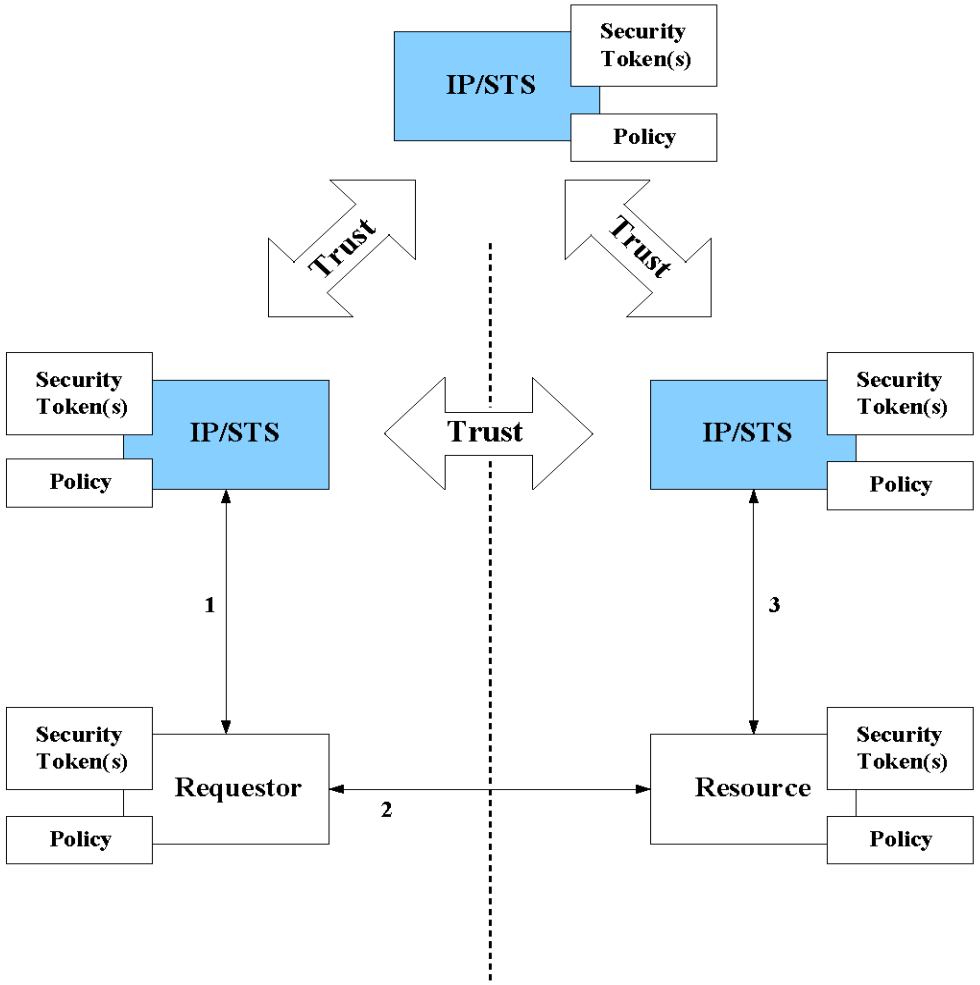
Note:
STS = Security Token Service



- **Simple model: direct trust between organisations**
  - Each organisation has an Identity Provider
  - Requester asks for a credential from his Identity Provider and presents it to the STS of the Service Provider he wishes to access
  - That STS may then grant access to the service
- Each participant may follow his own policies in this process

Identity Federation: Relationships 2

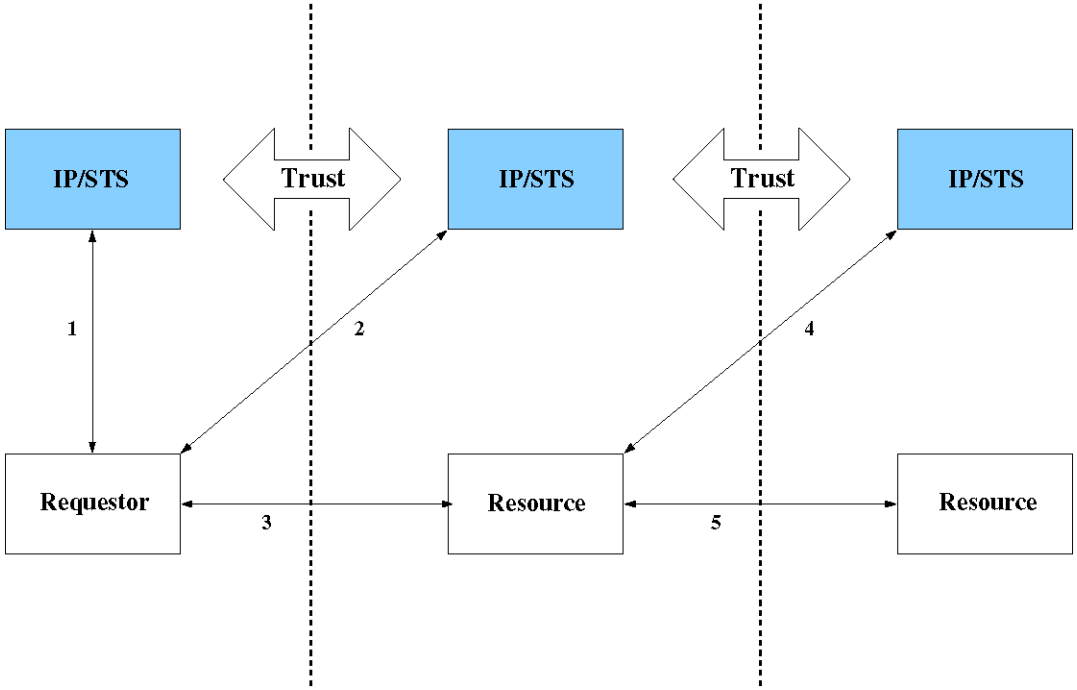
Note:
STS = Security Token Service



- **Extended model: trust between organisations is mediated by a Trusted Third Party**

Identity Federation: Relationships 3

Note:
STS = Security Token Service



- **Extended model with delegation**:
  - In order to fulfill a request, a resource accesses another (third-party) resource first
  - First resource acts “on behalf” of requestor

References WWW Security

[RFC3986] *Uniform Resource Identifier (URI): Generic Syntax*. RFC 3986. http://tools.ietf.org/html/rfc3986

[RFC2965] *HTTP State Management Mechanism*. RFC 2965. http://tools.ietf.org/html/rfc2965

[ECMA262] *ECMAScript Language Specification*. http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-262.pdf

[Sym2009] Symantec. *Symantec Report on the Underground Economy*. Symantec. 2009. http://www.symantec.com

[HoEnFr2008] T. Holz, M. Engelberth, F. Freiling. *Learning More About the Underground Economy: a Case Study of Keyloggers and Dropzones*. Technical Report TR-2008-006. Universität Mannheim. 2008.

[Za2011] M. Zalewski. *The Tangled Web – a guide to securing modern Web applications*. No Starch Press. 2011.

[HoLe2002] M. Howard, D. LeBlanc. *Writing Secure Code*. Microsoft Press. 2002.

[Wil2009] T. Wilhelm. *Professional Penetration Testing*. Syngress Media. 2009.

[ISec2010] International Secure Systems Lab. http://www.iseclab.org. 2010.

[Mo2010] Timothy D. Morgan. *Weaning the Web off of Session Cookies: Making Digest Authentication Viable*. http://www.vsecurity.com/download/papers/WeaningTheWebOffOfSessionCookies.pdf

References Web Service Security

[XMLEnc] W3C. *XML Encryption*. http://www.w3.org/standards/techs/xmlenc.

[XMLDSig] W3C. *XML Signature*. http://www.w3.org/standards/techs/xmlsig

[Gu2004] P. Gutmann. *Why XML Security is Broken.* http://www.cs.auckland.ac.nz/~pgut001/pubs/xmlsec.txt. 2004.

[RoRe2004] J. Rosenberg, D. Remy. *Securing Web Services with WS-Security*. SAMS Publishing. 2004.

[XMPPSig] RFC 3923. *End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP)*.

[iSecAttack] iSEC Partners. Attacking XML Security. http://www.isecpartners.com/files/iSEC_HILL_AttackingXMLSecurity_bh07.pdf

[SAML2010] OASIS. *OASIS Security Services (SAML) TC*. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[OWASP] Open Web Application Security Project. 2010. http://www.owasp.org

[WSI] Web Services Interoperability Organization. *Basic Security Profile Version 1.0*. 2010. http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html

[OpenID] OpenID Foundation Web Site. http://openid.net/

[iSec2010] iSEC Partners. *Attacking XML Security*. http://www.isecpartners.com/files/iSEC_HILL_AttackingXMLSecurity_bh07.pdf