Computer Network Security

Dr. Mohammad Iqbal

Thanks to P.S.Dhekne BARC

Presentasi

- What is Security all about?
- What is at Risk?
- Why Risks Exist?
- General Threat Perceptions
- Security
  - Data (local, Remote)
  - Communications
- Secure Backup
- Network Perimeter Security
  - General Policy
  - Min. Security Enforcement
- Intrusion Detection System
- Cryptographic Security
- VPN: A Roadmap
- Points for Action
- Emergency Response Team

KEAMANAN INFORMASI

- The information systems are known to be vulnerable to many threats like cyber crime, hacking and terrorism
- Regardless of whether the information has been stolen by the attacker or not, the security breaches and virus attacks result in adverse publicity to the organization.
- Thus issues like protection and security of the information systems have become greater concern.

Beberapa Fakta Serangan Keamanan : (IDC report)

- 85% detected computer security breaches within the last twelve months.
- 64% acknowledged financial losses due to computer breaches.
- 36% reported the intrusions to law enforcement; a significant increase from 2000, when only 25% reported them.

INFORMATION SECURITY

- Information & Network penetration do occur

  - from outsiders & insiders

  in spite of having various security measures such as Anti-virus, Firewalls, Routers

- There are two ways to attack computers

  - Gain physical access to machines & conduct physical attack

  - Attack by use of malicious software; Malware

Lingkup Keamanan

- Confidentiality:
  - Protecting sensitive information from unauthorized disclosure or intelligible interception; Only seen by entities to whom it is addressed
- Integrity:
  - Not modified/destroyed in a unauthorized way; safeguarding the accuracy & completeness of information & software
- Access Control:
  - Access (computation, data, service) follows the prescribed policy
- Authentication:
  - Verifying the identity claimed

Lingkup Keamanan

- Availability:
  - System accessible/usable on demand
- Nonrepudiation:
  - Protection against false denial of comm.
- Audit Trail:
  - Chronological record of system activities to enable reconstruction/examination of environments/activities leading to an operation from inception to final results.
- Privacy:
  - Breach of confidentiality is also invasion of privacy.
  - Collecting a dossier based upon his activities - inferring habits, movements, expenditures → Security Risk

Defenisi Resiko

1. Data, Time and Money
   - Obvious: deletion/modification of data
   - Slowly modifying data so that breach is not discovered right away
   - Using Service providers' software (say a online brokers CD software) – provides flexibility than by standard browsers. However it is a golden opportunity for an attacker with the knowledge of how that software works.

Defenisi Resiko

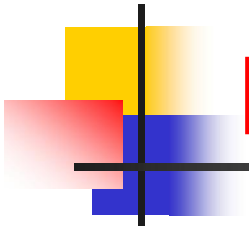
2. Confidentiality
   - Data disclosure is often overlooked risk
   - A breach of confidentiality is much less likely to be discovered than the deletion of data
   - Best Defence: well-designed cryptographic protected system – note that the data must be in the clear at some point (it is here attacker can get in …)

Defenisi Resiko

3. Privacy:
   - One of the things that is risk in today's computerized and networked world.
4. Resource Availability:
   - Denial of Service attacks

Mengapa Ada Resiko?

- Erroneous Program
  - Lack of prudent Software Engineering Practices
  - Complexity of software (millions of lines)
  - Urgently developed Components of The Shelf (COTS)
- The user (Systems should be User proof!)
  - Responsibility lies with the user (ignorance/non co-operation are problems)
  - Security policy should convince the users
- Poor Administration
  - Configuration, backup procedures, constant updates, monitoring, disaster recovery ...



Persepsi Umum Threat

- Network threatened by external running malicious scripts (Malware)
- Adversaries attempting access protected services, break into machines, snoop communications, collect statistics of transactions …
- Insiders and outsiders
- Disasters (natural and man-made)

Mengamankan Penyimpanan Data (Local Storage)

- Physical Security
  - Protect machine
  - Limit network access
  - Most secure (without external access)
  - **Suppose it falls into an adversary**
  - **All the data can be obtained in the clear**
- Cryptographic Secure.
- Protects even if the m/c falls to adversary
- Of course person having access can delete -- Hence, BACKUP
- Data Integrity
- Cryptography: Fragile
  - System issues, user interfaces , Crypto-file servers …

Mengamankan Penyimpanan Data (Remote Storage)

Need (also advantages!):

- Data protected from local disk failure
- Sharing of files
- Centralized administration and backup
- Use of diskless workstations

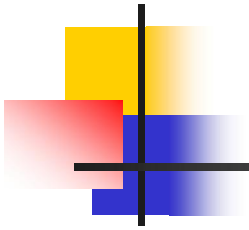
Adding Security:

- passwords, cryptography, access control lists, capabilities
- Physical security (Key servers etc)

Mengamankan Backup

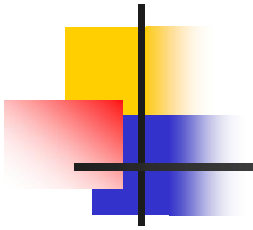
Prevent what you cannot detect and detect what you cannot prevent

- Security of the backup itself
- Backup over a network
  - Cryptographic encryption
  - Key servers
- Incremental Backup
- Deleting Backups



Mengamankan Komunikasi

- Cryptography
  - Encryption/decryption
  - Key management
  - Session key protocols
- Public Key Infrastructures
  - Certification
  - Digital Signatures



Replay Prevention

- Replay attacks are simple yet very effective
  - Records a message say from A to B, and later replays it to impersonate A
  - Attack is effective as attacker need not decrypt
- Needs to be addressed regardless of layer chosen

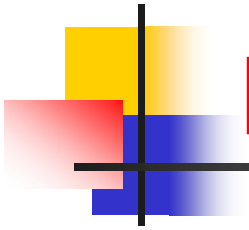
Perimeter Keamanan Network (Proteksi dari Outsider)

General (Policies to be enforced)

- Policies delineating appropriate and inappropriate behaviour
- Security Classification of data and Machines and enforce access controls
- Only required access to be given to insiders
- Enforce Physical security for file servers, secure nodes, key servers, authentication servers, backups etc.
- Audit Procedures (manual and automated)

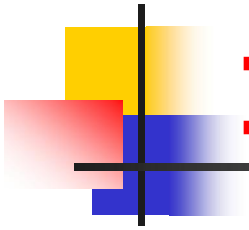
Perimeter Keamanan Network (Min. Security Enforcement)

- External Access:
  - One point access: Internet, Dialups (callbacks), Broadband, DSL, wireless …; violation only with cryptographic encryption
- Minimum Standards for Hardware
- Software Standards:
  - OS, Browsers, Compilers, Tools – prefer open source
- Secure Configuration
  - email, mobile agents/systems, only required ports to be open, restrictions on shell (corresponding to required security levels)
  - Viruses (continuous protection)
- Denial of Service Protection



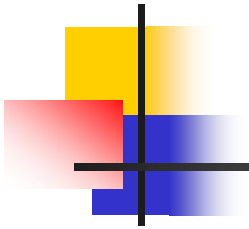
Minimum Security (contd)

- Web Security: embarrassing quite often;
  - Have Exit Control (ensures web modifications through authentication)
  - Check Mirror sites periodically
- Auditing the usage and traffic
- Backup (automatic, mirroring, remote, …) and disaster recovery -- Perhaps use



Intrusion Detection Systems

- Attack detection, with automated response
  - Damage prevention and containment
  - Tracing and isolation of attack origin points
- Mimic hackers attacking networks (including ISPs) continuously highlighting dangerous infrastructure flaws that could cripple the system
  - Leads to required Upgrades in Security
  - Leads to next generation design of devices



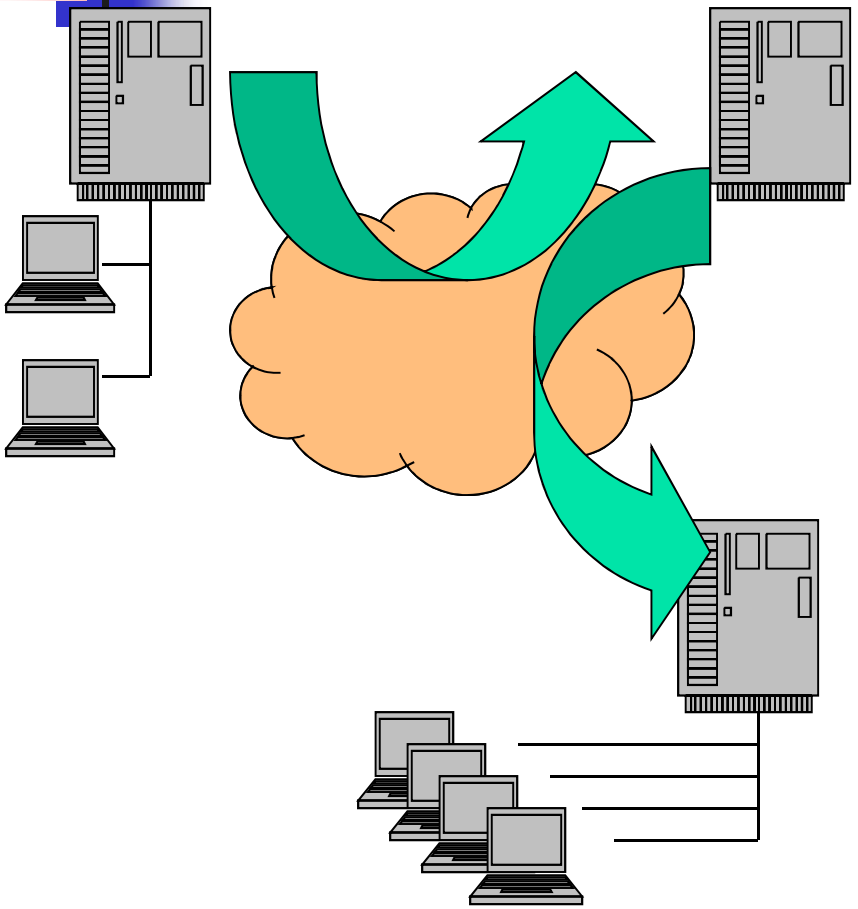
Intrusion Detection System

- Host Intrusion Detection System
  - Security Monitoring System Developed at BARC
- Network Intrusion Detection System
  - Open Source SNORT IDS implemented with rule set customized for our environment.

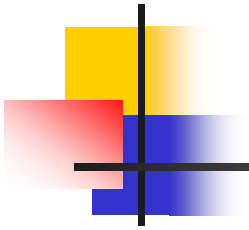
Sertifikasi Keamanan : Key Servers, PKI Infrastructure

- Needed security
  - Via parameters identified in the policy
- Authenticated usage
  - Computing
  - Data
- Backup of Data and its integrity
  - Online
  - offline

Securing Communication



- Trusted sites
- Use of public network
- Secure channels
- Transparent to users



Virtual Private Network:VPN

Secure use of public communication channel with

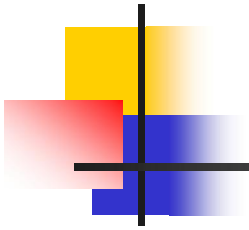
- Off the shelf hardware
- IP tunneling
- Software encryption

Dasar VPN

- Fixed encryption algorithm
- Static keys per pair of sites
- An encrypting PC router per site
  - Off the shelf hardware
  - Custom software
- Secures communication between sites

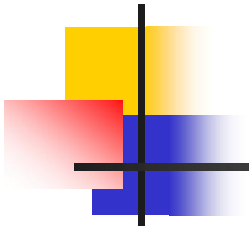
Mengelola VPN

- Introduce key servers
  - Manage dynamic keys on the network
- Customize encryption algorithms
- Involves software upgrades at each site.
- Provide a scalable management model



Tighten Exit Security

- Fake traffic on the links
- Reroute traffic
- Insulate from statistical inferences



Internal Security

- Introduce encryption within a site
- Involves software upgrades to the OS

- Minimize damage from within (may be crypto fileservers)

Points for action

- Policy
  - Access Control and Log
  - Encryption
  - Certification
  - Backup
- Teams
  - Routine Audit and Management Structure
  - Emergency Response Team
  - Dynamic IDS and Crypto-Systems Work

Emergency Response Team

Plan

- Person on firecall and in-charge
- Reaction to security breach.
  - Internal expertise
  - If not alternatives
- Determine chain of command

BIAYA LINGKUNGAN TI TANPA PERLINDUNGAN KEAMANAN

- Loss of data
- Loss of server up time
- Loss of user's productivity
- Loss of money

Average cost per virus encounter **US $ 2454**

How much protection is enough ?

No one knows!!

Information Security Management System (ISMS)

Organization Security

Personnel Security

Physical & Environmental security

Security Policy

Asset Classification & Control

Access Control

Communications & Operations Management

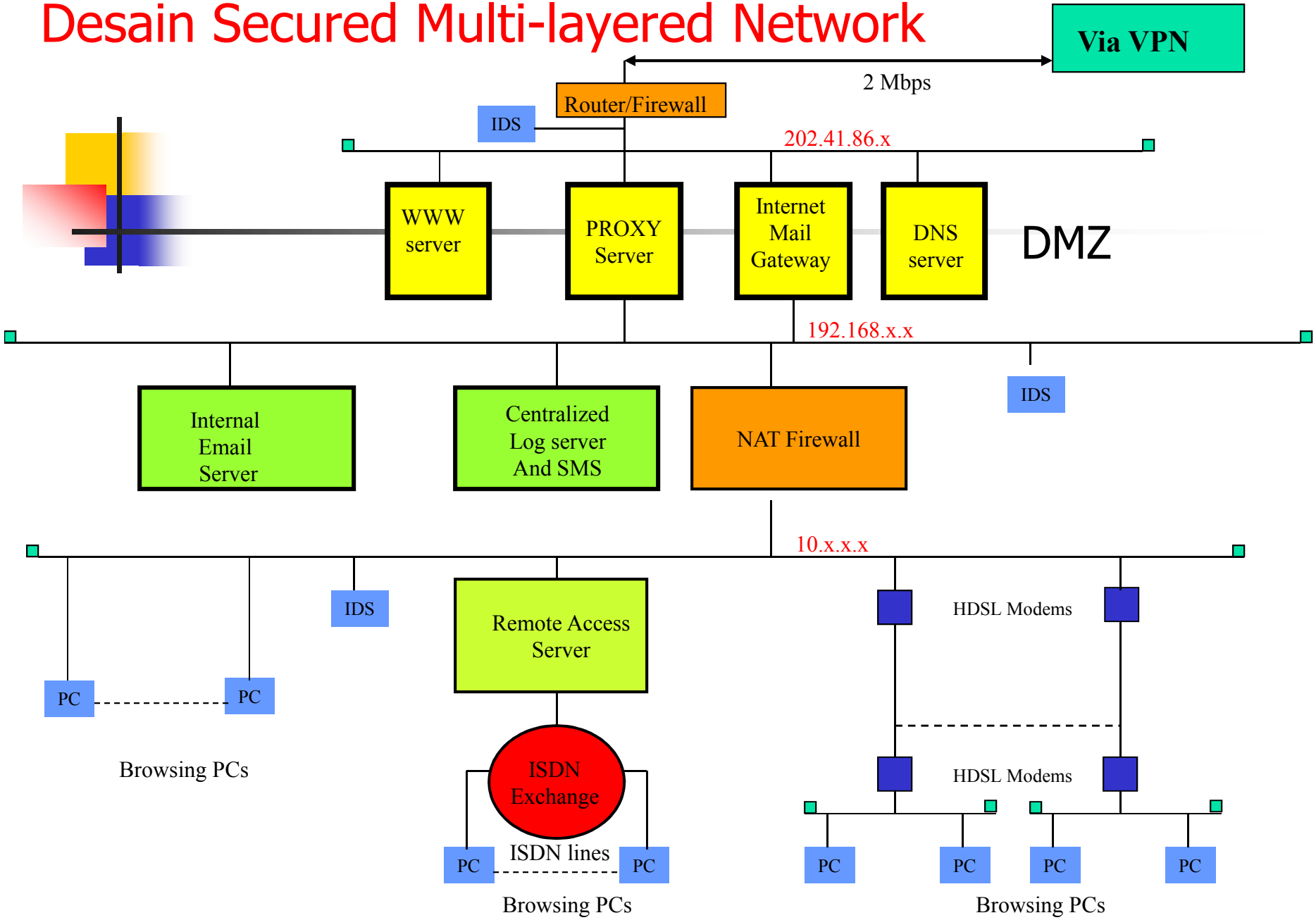
System Development & Maint.

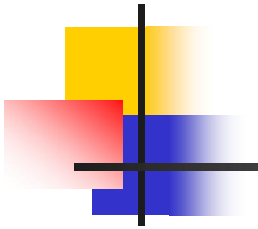
Security Standard Compliance: IS 15150/27001

Pendekatan Keamanan Informasi

- Secure Network Design, Layered approach (Defense in Depth concept), SPF and Application firewalls
- Harden the Operating System
- Use Secure Applications with Secure Configurations
- Centralized logging and Monitoring
- Intrusion Detection System (HIDS,NIDS)
- Encryption
- Local Vulnerability tests, self auditing

Desain Secured Multi-layered Network





SECURITY BUILDING BLOCKS

- Authentication (passwords, biometric devices)
- Encryption - so that unauthorized user cannot make sense of the data even if he intercepts it.
- Access control - a policy by the organization to decide who has access to what.
- Key management - the properties of the encryption/decryption keys.
- Resource isolation- so that damage is contained.
- Network Perimeter Protection – Firewall, NAT

Administrasi & Monitoring Terpusat

- To ensure that IT Security policies within a organization are properly implemented, it is necessary to conduct periodic audits
- Need powerful automated tools for
  - Auditing
  - Intrusion detection
  - Performance measurement

  And to find a variety of threats, vulnerabilities and advance warning for any penetration that might occur

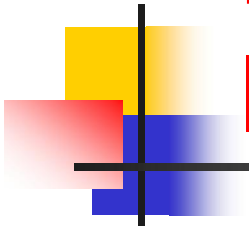
Logging & Sistem Monitoring Terpusat

- All Internet Servers, routers logs are collected on centralized log server
- Logs are parsed for abnormal events on Routers, Internet connected hosts
- All incoming/outgoing mail archived
- Mail logs are parsed for generating Mail usage, abnormal event statistics
- Proxy server logs are parsed for generating proxy server usage statistics

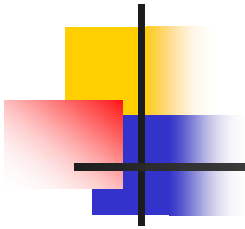
Penggunaan Secure Software

- Centralized Logging and Security Monitoring System
- Web-Pages Integrity check module for Apache Web-Server
- Securing Web Server
- Securing Mail-gateways
- Securing DNS servers
- Use of Public Domain Firewalls, Proxy and NAT servers with value additions

Level Keamanan Programming language/Level Aplikasi

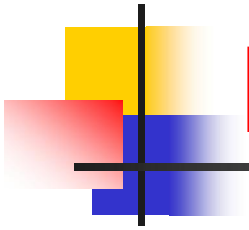


- Previous focus in this class has been on secure *protocols* and *algorithms*
- For real-world security, it is not enough for the *protocol/algorithm* to be secure, but also the *implementation* must be secure



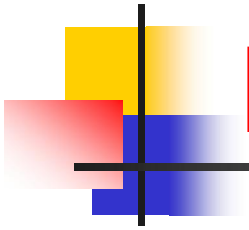
Pentingnya masalah ini

- The amount of time we are devoting to the problem is *not* indicative of its relative importance
- In practice, attacks that exploit implementation flaws are *much* more common than attacks that exploit protocol flaws
  - Damage from such flaws also typically much greater
  - Viruses/worms almost always exploit such flaws
- If you ever program security-sensitive applications, learn about secure programming



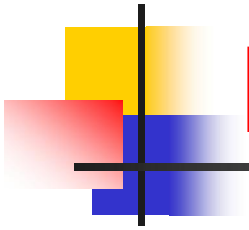
Pentingnya masalah ini

- Most common cause of Internet attacks
  - Over 50% of CERT advisories related to buffer overflow vulnerabilities
- Morris worm (1988)
  - 6,000 machines infected
- CodeRed (2001)
  - 300,000 machines infected in 14 hours
- SQL slammer worm (2003)
  - 75,000 machines infected in 10 minutes(!)



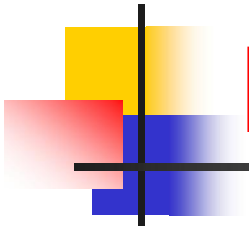
PL attacks

- Many of the most common PL attacks come down to *not properly validating input from (untrusted) users before use*
  - Buffer overflow attacks
  - Format string vulnerabilities
  - Cross-site scripting (XSS) attacks
  - SQL injection attacks
  - etc.
- There are other PL security issues as well, but we will not cover these in this class



PL attacks : Buffer overflows

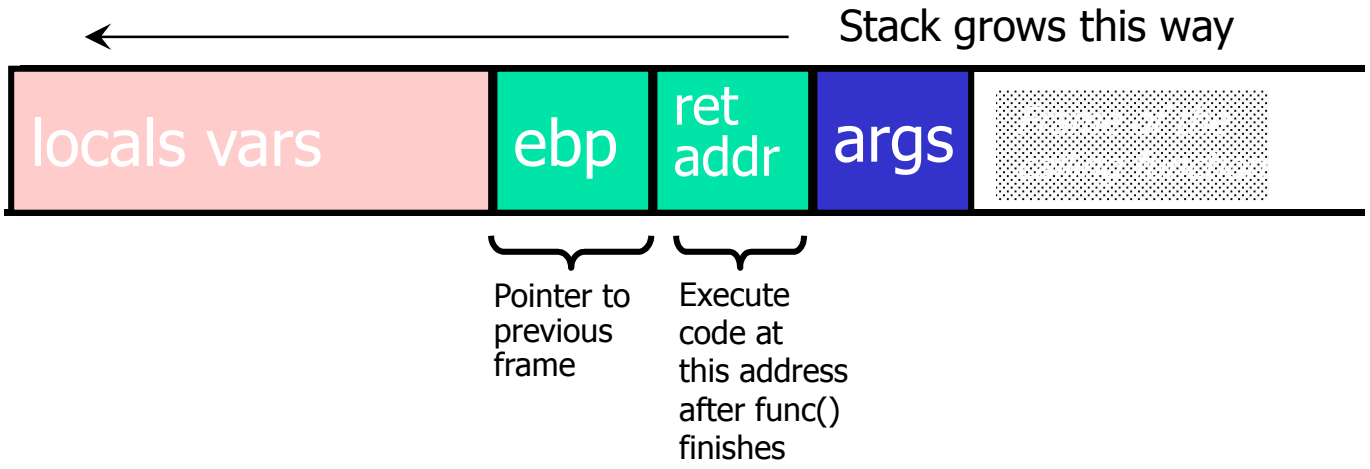
- Fixed-sized buffer that is to be filled with unknown data, usually provided directly by user
- If more data “stuffed” into the buffer than it can hold, that data spills over into adjacent memory
- If this data is executable code, the victim’s machine may be tricked into running it
- Can overflow buffer on the stack or the heap…



PL attacks : Stack overview

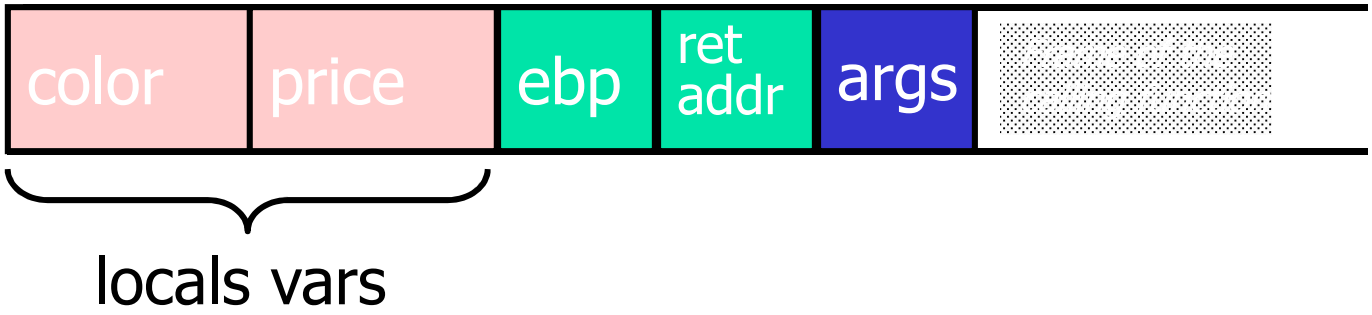
- Each function that is executed is allocated its own *frame* on the stack
- When one function calls another, a new frame is initialized and placed (*pushed*) on the stack
- When a function is finished executing, its frame is taken off (*popped*) the stack

PL attacks : Function frame



“Simple” buffer overflow

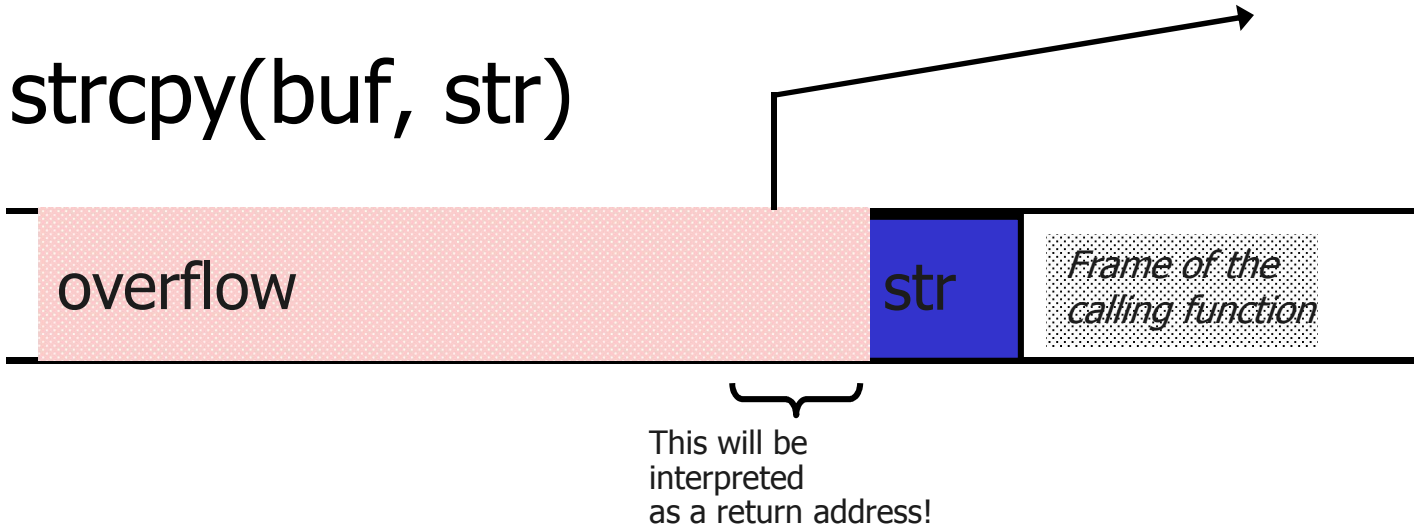
- Overflow one variable into another



- gets(color)
  - What if I type “blue 1” ?
  - (Actually, need to be more clever than this)

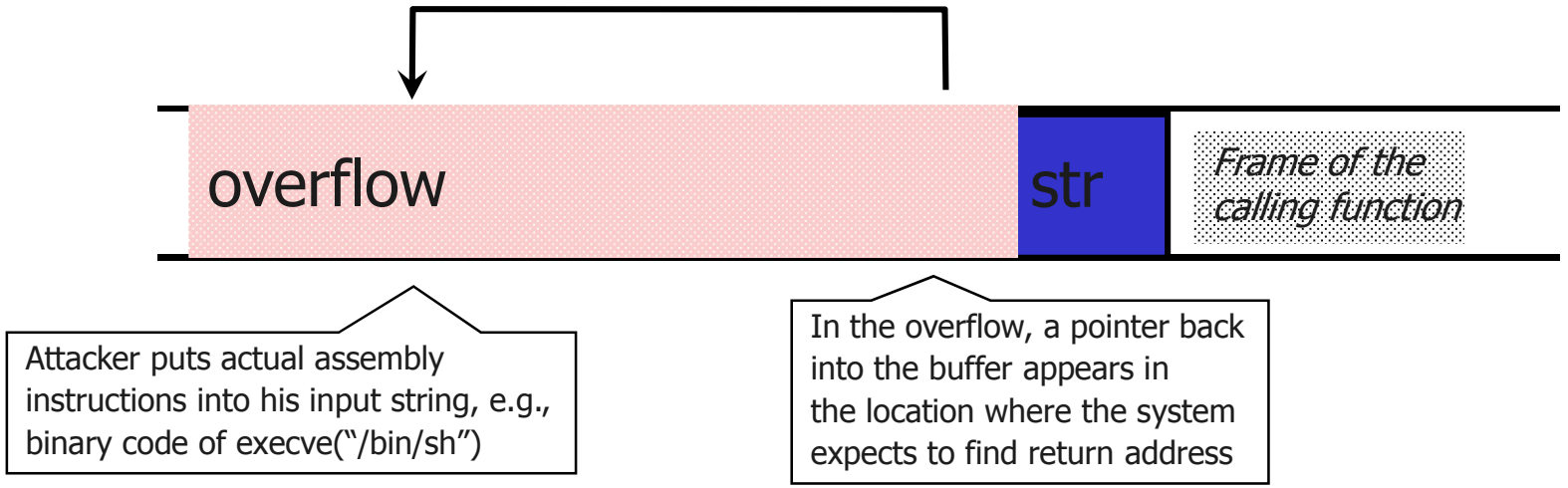
More devious examples…

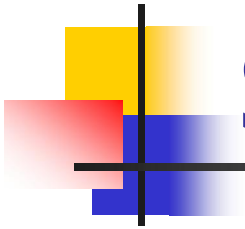
- strcpy(buf, str)



- What if str has more than buf can hold?
- Problem: strcpy does not check that str is shorter than buf

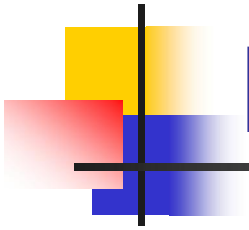
Even more devious…





Severity of attack?

- Theoretically, attacker can cause machine to execute arbitrary code *with the permissions of the program itself*
- Actually carrying out such an attack involves many more details
  - See “Smashing the Stack…”



Preventing this attack

- We have seen that strcpy is unsafe
  - strcpy(buf, str) simply copies memory contents into buf starting from *str until "\0" is encountered, ignoring the size of buf
- Avoid strcpy(), strcat(), gets(), etc.
  - Use strncpy(), strncat(), instead
  - Even these are not perfect… (e.g., no null termination)
  - Always a good idea to do your own validation when obtaining input from untrusted source
  - Still need to be careful when copying multiple inputs into a buffer

Does range checking help?

- strncpy(char *dest, const char *src, size_t n)
  - No more than n characters will be copied from *src to *dest
    - Programmer has to supply the right value of n!
- Bad:

```
… strcpy(record,user);
  strcat(record,":");
  strcat(record,cpw); …
```

- Published "fix" (do you see the problem?):

```
… strncpy(record,user,MAX_STRING_LEN-1);
  strcat(record,":");
  strncat(record,cpw,MAX_STRING_LEN-1); …
```

Off-by-one overflow

- Consider the following code:

```
char buf[512]; int i;
for (i=0; i <= 512; i++)
  buf[i] = input[i];
```

- 1-byte overflow: can't change return address, but can change pointer to previous stack frame
  - On little-endian architecture, make it point into buffer