CS3235
Tenth set of lecture slides

Hugh Anderson

National University of Singapore
School of Computing

November, 2007
More insecurity

Hmmmm....

...Who are you and how did you get in here?

...I’m a locksmith. And, I’m a locksmith. [Leslie Nielsen]
Outline

1. Administration

2. Insecurity (Continued)
   - Design Principles
   - IPSec
   - Formal Methods
   - Formal evaluation

3. Biometrics
Design principles

Paper by Saltzer and Schroeder, summarized below:

- **Economy of mechanism:** Keep design as simple and small as possible. (audit code and protocols)
- **Fail-safe defaults:** Base access decisions on permission rather than exclusion. The default is no access. (MS port security)
- **Complete mediation:** Every access to every object must be checked for authority. (DNS cache poisoning)
- **Open design:** The design should not be secret. (DVDs, Microsoft SAM hashes...)
Design principles

Paper - continued...

- **Separation of privilege**: Two keys are better than one. No single event can compromise the system. (su - password and wheel group)

- **Least privilege**: Every program and every user of the system should operate using the least set of privileges necessary to complete the job. (Military need-to-know)

- **Least common mechanism**: Minimize the amount of mechanism common to more than one user and depended on by all users. (online store and D.O.S.).

- **Psychological acceptability**: Human interface easy to use.
IPSec

IPSec is a set of standards:

- intended to support communication security between networked computers, particularly in the newer IPv6 (IP Next-Generation) network.

- IPSec software is available in Windows2000, Linux, and on routers on the Internet.

- [http://www.faqs.org/rfcs/rfc2401.html](http://www.faqs.org/rfcs/rfc2401.html)

- IPSec may be used in a range of ways.
IPSec VPN

Provides secure connection so machine appears on remote network
IPSec point-to-point

Or secure communication from one PC to another
IPSec network-to-network

Or from one network to another
IPSec headers

The IP headers contain the extra information needed
There are two types of header, one used for **authentication**, and the other used for **encryption**:

1. **AH** - the **Authentication Header** for data integrity, anti-replay and authentication
2. **ESP** - the **Encapsulating Security Payload** header, for confidentiality. ESP can also provide AH services.

Communicating parties agree on a **Security Association** (SA), one SA for each direction, and one SA for each type of communication.
Modes of operation

An end-to-end SA - Transport mode:

- **Original IPv6 hdr**
  - **AH**
  - **Transport segment**
  - **authenticated**

- **Original IPv6 hdr**
  - **ESP**
  - **Transport segment**
  - **ESP**
  - **encrypted**
  - **authenticated**
Modes of operation

An SA between security gateways - Tunnel mode

SAs form a kind of distributed database.
Formal methods

FM encompasses a wide range of techniques...

- Model checking:
  - constructing formal *models*, with
  - appropriate formal *specifications*.

- Example is Promela and Spin.
Promela and spin

In a nutshell...

- The **language** Promela is ’C’ like, with an initialization procedure. It can model asynchronous or synchronous, deterministic or non-deterministic systems.
- Spin is the **checker** for Promela models.
- Assertions to test correctness of model:

```plaintext
assert(some_boolean_condition);
```

- If condition not TRUE then assertion violated.
Temporal claims

What is a temporal claim? Something like:

- *We got here again without making any progress!*

The support for temporal claims takes the form of:

- **Endstate** labels - for determining valid endstates
- **Progress** labels - claim no non-progress cycles
- **Never** claims - impossible temporal assertions
Simple example

Model of two machines communicating using a simple protocol
Promela example

Promela source code

```
init
{
  chan AtoB = [1] of { mtype, byte };
  chan BtoA = [1] of { mtype, byte };
  chan Ain = [2] of { mtype, byte };
  chan Bin = [2] of { mtype, byte };
  chan Aout = [2] of { mtype, byte };
  chan Bout = [2] of { mtype, byte };
  atomic {
    run application( Ain, Aout );
    run transfer( Aout, Ain, BtoA, AtoB );
    run transfer( Bout, Bin, AtoB, BtoA );
    run application( Bin, Bout )
  };
  AtoB!err(0)
}
```
The transfer protocol for each end

```c
#define MAX 10
mtype = { ack, nak, err, next, accept }
proctype transfer( chan in, out, chin, chout )
{
    byte o,i;
in?next(o);
    do
        :: chin?nak(i) -> out!accept(i); chout!ack(o)
        :: chin?ack(i) -> out!accept(i); in?next(o);
            chout!ack(o)
        :: chin?err(i) -> chout!nak(o)
    od
}
```
A simple simulation of an application

```proctype application( chan in, out )
{
    int i=0, j=0, last_i=0;
    do
    :: in?accept(i) ->
        assert( i==last_i );
        if
            :: (last_i!=MAX) -> last_i = last_i+1
            :: (last_i==MAX)
        fi
    :: out!next(j) ->
        if
            :: (j!=MAX) -> j=j+1
            :: (j==MAX)
        fi
    od
}
```
Spin simulation

Time goes down, each column is a process...
Formal evaluation - TCSEC

TCSEC (The Orange book) - first rating system for security

- **C1** - For **same-level** security access. Not currently used.
- **C2** - **Controlled access protection** - users are individually accountable for their actions.
- **B1** - **Mandatory BLP policies** - for more secure systems handling classified data.
- **B2** - **structured protection** - mandatory access control for all objects in the system. Formal models.
- **B3** - **security domains** - more controls, minimal complexity, provable consistency of model.
- **A1** - **Verified design** - consistency proofs between model and specification.
Formal evaluation - ITSEC

ITSEC derives from...

- Dutch, English, French and German national security evaluation criteria.
- Adaptable.
- Sponsor determines operational requirements, threats and security objectives.
- ITSEC specifies the interactions and documents between the sponsor and the evaluator.
Again there are various levels of evaluation: E0..E6, with E6 giving the highest level of assurance - it requires two independent formal verifications.


- The smart-cards are electronic purses - that is they carry value,
- Forgery must be impossible.
- The certification encompassed the communication with the card, as well as the software within the card, and at the bank.
Data Diode E6, BLP

An example

http://www.tenix.com/Main.asp?ID=908
Biometrics

Biometrics is the use of human physical characteristics to support authentication.

FPC1010 Area Sensor

FEATURES
- Internal A/D
- SPI interface
- 3.3 Volt operation
- Robust surface coating
- >1 000 000 wear cycles
- >15kV ESD protection

APPLICATION EXAMPLES
- Mobile phones, PDAs
- PC peripherals
- Security systems
- Smart cards
Biometrics - eyes

Retinal scans
Minimal hardware biometrics

(See Terence and Roland!)

- **Voices** - Record and process voice leading to either speaker verification or recognition.
- **Faces** - Capture either a static or moving image of a face.
- **Keystrokes** - capture a sequence of keystrokes, recording timing.

Combinations of characteristics may be used, but in general biometric techniques are not reliable on their own. Good second key for separation of privilege.
Sample systems: PGP

Pretty Good Privacy...

- PGP is a public key encryption package to protect E-mail and data files.
- It lets you communicate securely with people you’ve never met, with no secure channels needed for prior exchange of keys.
- PGP can be used to append digital signatures to messages, as well as encrypt the messages, or do both.
Properties...

- It uses various schemes including patented ones like IDEA and RSA.
- The patent on IDEA allows non-commercial distribution, and the RSA patent has expired.
- However there are also commercial versions of PGP.
- PGP can use, for example, 2048 bit primes, and it is considered unlikely that PGP with this level of encryption can be broken.
PGPfone

Encrypted phone conversations (before Skype!)

- Speech compression and *strong cryptography*
- In 2003, it was available in two versions:
  1. An international version available *outside* America, and a prohibited import *into* America.
  2. An *American* version available *inside* America, and a prohibited import *out of* America.

These two versions are also exactly the same! (Restrictions on the import and export of *munitions* - strong cryptography is considered a munition).
PGPfone

Source is available...

[Image of PGPfone interface with details on call status, encryption, and sound output]
When initially setting up a link, Diffie-Hellman key exchange is used to ensure safety in the choice of an encryption key.